jamk

Cyber Incident Response in Public Cloud

Implications of modern cloud computing characteristics for cyber incident response

Henri Loukasmäki

Master's thesis
April 2023
Master's Degree Programme in Information Technology

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

jamk

Description

Loukasmäki Henri

Cyber incident response in public cloud – Implications of modern cloud computing characteristics for cyber incident response.

Jyväskylä: Jamk University of Applied Sciences, April 2023, 108 pages.

Technology, Information and Communications. Degree Programme in Information and Communications Technology. Master's thesis.

Permission for open access publication: Yes

Language of publication: English

Abstract

Modern cloud computing has fundamentally changed how IT-resources are consumed by organizations and end-users. The cloud is also defined by some of its key characteristics: on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. On the other hand, industry standard frameworks for cyber incident response were mainly developed during the time when cloud computing had not yet emerged, and the same models and frameworks are still utilized when responding to cyber security incidents in the cloud domain.

The main objective was to research and to illuminate some of the complexities related to responding to cyber security incidents in the public cloud domain, and to provide practical guidance and insights on how to prepare, detect, analyze, contain, eradicate, recover, and learn from cloud-based incidents by comparing, contrasting, and evaluating different cloud capabilities and their viability and potential use-cases for various phases of incident response. Secondary objective was to research the typical public cloud operating environment from an incident responders' point of view, and also to assess different types of incident response capabilities, tooling, approaches, and strategies by analyzing two different large cloud providers services and products.

While it was observed that generally the same processes and models can be utilized when responding to incidents in the cloud, and the overall goals for different incident response phases still remain the same, the tools and techniques for efficient incident response need to be able to utilize, exhibit, and take advantage of common cloud-based characteristics. Also, the importance of mitigating threats targeting identities was highlighted, as in the cloud, identity is the de facto security perimeter. Overall, when responding to cyber security incidents in the cloud, incident responders should have a deep understanding of the cloud platform, what kind of services they offer, and what kind of interdependencies they have. Also, it is important to understand what kind of telemetry the platform and the services produce, and what kind of limitations some cloud service models bring with them.

Keywords/tags (subjects)

Incident Response, Cyber Incidents, Cloud Computing, AWS, Azure, Public Cloud

Miscellaneous (Confidential information)

No confidential information in this thesis.

Contents

Figures

Tables

Acronyms

API	Application Programming Interface
AWS	Amazon Web Services
CDN	Content Delivery Network
CIA	Confidentiality, Integrity, and Availability
CIR	Cyber Incident Response
CSA	Cloud Security Alliance
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
EDR	Endpoint Detection and Response
IAM	Identity and Access Management
IOC	Indicator of Compromise
ISO	International Organization of Standardization
IaaS	Infrastructure as a service
LAN	Local Area Network
NIST	National Institute of Standards and Technology
NSG	Network Security Group
OODA	Observe, Orient, Decide, Act
OS	Operating System
PaaS	Platform as a Service
SIEM	Security Information and Event Management
SOC	Security Operations Center
SaaS	Software as a Service
TTP	Techniques, Tactics, and Procedures
UEBA	User Entity and Behavior Analytics
VDI	Virtual Desktop Infrastructure
VPC	Virtual Private Cloud
VPN	Virtual Private Network
WAN	Wide Area Network
XDR	Extended Detection and Response
XaaS	Anything as a Service

1 Introduction

IT-resources, development, and operations are being moved into the cloud by organizations and governments at an accelerated speed, and the new operating environment compared to a traditional on-premises environment requires a shift in thinking when it comes to responding to cyber security incidents in the cloud. The new operating models and characteristics that enable modern cloud computing to bring value to its users and customers inevitably complicate the frameworks and established ways of working that were initially created and developed to be utilized in completely different types of environments. This also is evident when applying industry standard incident response frameworks to modern cloud computing environments and infrastructure as the response actions may vary depending on the cloud vendor, the cloud deployment model, or the cloud service model. This thesis aims to illuminate some of these complexities related to responding to cyber security incidents in the cloud domain and the main objective is to produce practical guidance on how to prepare, detect, analyze, contain, eradicate, recover, and learn from cloud based cyber security incidents by comparing, contrasting, and evaluating different cloud capabilities and their viability and usefulness in cyber incident response. These insights will be valuable to anyone or any entity operating in the cloud domain. The thesis does not have a commissioner and is self-assigned by the researcher.

The thesis aims to research best practices for cyber incident response in public cloud environments, and also, to highlight the typical public cloud operating environment from incident responders' point of view. One of the goals is to produce a qualitative comparative assessment of what kind of cloud native capabilities and services two of the arguably largest public cloud environments, Amazon Web Services and Microsoft Azure offer that could be utilized in and support different phases of industry standard incident response frameworks. These two large cloud vendors were chosen partly due to familiarity to the researcher, but also, because the thesis will aim to compare these two vendors capabilities to determine whether there are any significant differences in the capabilities and services they offer that could be helpful for cyber incident response. It will also try, through comparing different cloud vendors, assess different types of potential incident response capabilities, tooling, approaches, and strategies. The main framework, or model, that the thesis will focus on is described in the National Institute of Standards and Technology's (NIST) special publication 800-61 revision 2 (Cichonski et al., 2012, p. 21).

The thesis starts by first introducing the main research objectives and methodologies used and then introduces main phenomena that the thesis is focusing on, cyber incident response and cloud computing. After this, the thesis evaluates and assesses general cloud specific considerations for each incident response phase and analyzes different cloud service providers products, services, tools, and capabilities to draw conclusions on best practices on incident response in these environments, and what kind of similarities or differences they possess.

2 Research objective and methodology

This thesis aims to illuminate some of the complexities related to responding to cyber security incidents in the cloud domain. The objective of the thesis is to produce practical guidance on how to prepare, detect, analyze, contain, eradicate, recover, and learn from cloud based cyber security incidents. The objective of the research is also to answer the following main research questions: "when comparing approaches for incident response in traditional on-premises environments, what kind of capabilities are required for efficient incident response in the cloud domain?", and "are there any major differences in the approaches, cloud native capabilities, or services between two large cloud service providers environments and services that could act as inputs, or have any other role in the different phases of the industry standard incident response frameworks and processes?". Additionally, one supporting research question that the thesis will try to answer is "What does the typical public cloud operating environment look like from incident responders' point of view?"

2.1 Research methodology

To reach the objectives of the research, and research questions, the thesis aims to define different types of cloud security tooling, best practices, and to analyze how industry standard incident response models should be applied in the context of cloud environments through qualitative comparative analysis method. In comparative analysis, the goal is to generate new theories based on comparing and contrasting different categories and phenomena, and to analyze their differences and similarities to discover new patterns, conceptual similarities, and how they influence each other (Tesch, 1990). The phenomena this thesis is comparing and contrasting are cyber incident response and cloud computing. Utilizing the analysis method practically and unilaterally, another

goal of the thesis is to mirror one of the industry standard incident response models, which is described in NIST SP.800-61 revision 2 (Cichonski et al., 2012, p. 21) against different capabilities, services, and tools applicability to support different phases of the model, and to perform capability comparison of different vendors. The relevant services for each vendor are through qualitative comparative analysis enumerated, tabulated, and mapped into each phase of the incident response model phases where the researcher identifies they could be beneficial. The data in the thesis is collected from public sources such as National Institute of Standards and Technology, Amazon Web Services official documentation, Amazon Web Services management console, Microsoft Azure official documentation, Microsoft Azure portal, literature and previous academic research related to cloud computing, incident response, and cyber security.

2.2 Research ethics

Impartiality and objectivity are important to maintain the ethicality of the thesis considering that one of the goals is to compare two different cloud providers' services, capabilities, and tools against each other. The initial assumptions and expectations on the end-results before the information gathering and analysis and comparing the two providers is that, in all probability, there is not a substantial difference in the capabilities themselves, but there could potentially exist slight nuances on the approaches and implementation. The thesis could still theoretically nudge a potential customer to choose one cloud provider over another based on the results of the qualitative analysis of different capabilities. However, based on the researchers' own experiences, when choosing a cloud provider, there are a myriad of other variables that the cloud customer will primarily consider such as the past, current, or future goals, geolocation, price, local legislation, or even just subjective favoritism of some specific cloud provider. As the overall maturity of both cloud providers that are being compared can be seen as high, having some nuanced advance in some highly specialized scenario hardly seems as something that is viewed as important when deciding a cloud provider. Also, it is important to highlight that the goal of the comparative analysis is not to determine whether any of the products, services, capabilities, methodologies, or models provided by these two cloud providers are objectively or subjectively better, but rather, to produce practical guidance on how to perform incident response in these two environments by gathering insights from these.

2.3 Research reliability

Regarding the reliability of qualitative analysis, which by its nature routinely deals with intangible and potentially inexact information, there are several concepts and methods that were considered when collecting and analyzing the data. These being: Reflexivity i.e., being transparent and aware of the researchers own potential biases that could influence the research, meaning self-conscious critique and evaluation on how the researcher's subjectivity and context influence the research process (Olmos-Vega et al., 2022). Triangulation i.e., the use of multiple data sources whenever possible to enhance the validity of the findings and to develop a comprehensive understanding of the phenomena (Carter et al., 2014). Credibility i.e., that the researcher has the required expertise to conduct the research (Sandström, 2018). In this case, the researcher has extensive working experience as a subject matter expert of both cyber incident response and public cloud, both AWS and Azure. Other aspects to consider are, employing a systematic approach to data analysis, such as using a matrix to organize and compare the collected data of different services and capabilities. Finally, testing of the tools, services, and capabilities themselves for their intended purposes whenever applicable or possible within the context of the research questions and goals, and thorough critical analysis of the collected data.

3 Cyber incident response

This chapter examines general concepts related to cyber incident response. The chapter 5 "Incident response in public cloud" will later discuss how these concepts reflect in the cloud domain. Before defining what incident response means, some key concepts must be introduced. These are occasionally used interchangeably, but when inspecting them closer they all have notable differences. Additionally, cyber and information domains are concepts that are sometimes used interchangeably, but here the cyber domain relates to anything happening with a computer system, network, or data within these, and the information domain relates to data in any form.

3.1 Events and Incidents

The US National Institute of Standards and Technology (NIST) defines an event as an "any observable occurrence in a system or a network" (Cichonski et al., 2012, p. 6). An event is generated for example when a user is sending an email, a firewall or a cloud security group blocking a connection attempt, or a web server receiving a request for a resource it is supposed to serve (Cichonski

et al., 2012, p. 6). A security event can be considered as any observable event that relates to a security function and is generated for example when a user is accessing a document stored on a restricted cloud share, or an attacker conducting a port scan. (Chapple, 2020, p. 379). The International Organization for Standardization (ISO) defines a security event as "an occurrence indicating a possible breach of information security or failure of controls" (SFS ISO/IEC 27035, 2016). Adverse events on the other hand are events that have negative consequences and are generated for example when a malware executes and destroys data or causes a system to crash, unauthorized access to sensitive data, or unauthorized use of elevated privileges. Note that an adverse event can be man-made, or they can be caused by external factors such as natural disasters or power failures (Cichonski et al., 2012, p. 6).

By NIST's definition, "a computer security incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices" (Cichonski et al., 2012, p. 6). The ISO definition on the other hand notes the close relationship with events by stating that an "information security incident is a one or multiple related and identified information security events that can harm an organization's assets or compromise its operations" (SFS ISO/IEC 27035, 2016). The ISO 27035 also states that security incidents can be intentional or unintentional, and be caused by technical, or by non-technical means (SFS ISO/IEC 27035, 2016). In a more practical manner and to expand this a bit further, another definition would be any unlawful, unauthorized, or unacceptable action involving a data network or a computer system (Luttgens et al., 2014, p. 5). This means that a security incident can be considered a negative event (all incidents have events, but not all events are incidents) that adversely affects an organization or its people, systems, data, or the general ability to execute mission critical or business functions (Meyers, 2018, p. 510). What is important to observe here is that an incident can be defined in various ways, but it is implied by all definitions that an incident is something that requires an action to be taken to be recovered from, i.e., as something that requires a response.

To further demonstrate the different relationships between typical objects in a security incident, and how they typically influence each other, the ISO 27035 describes a schematic relationship model between the different objects that is described in the figure 1 below.

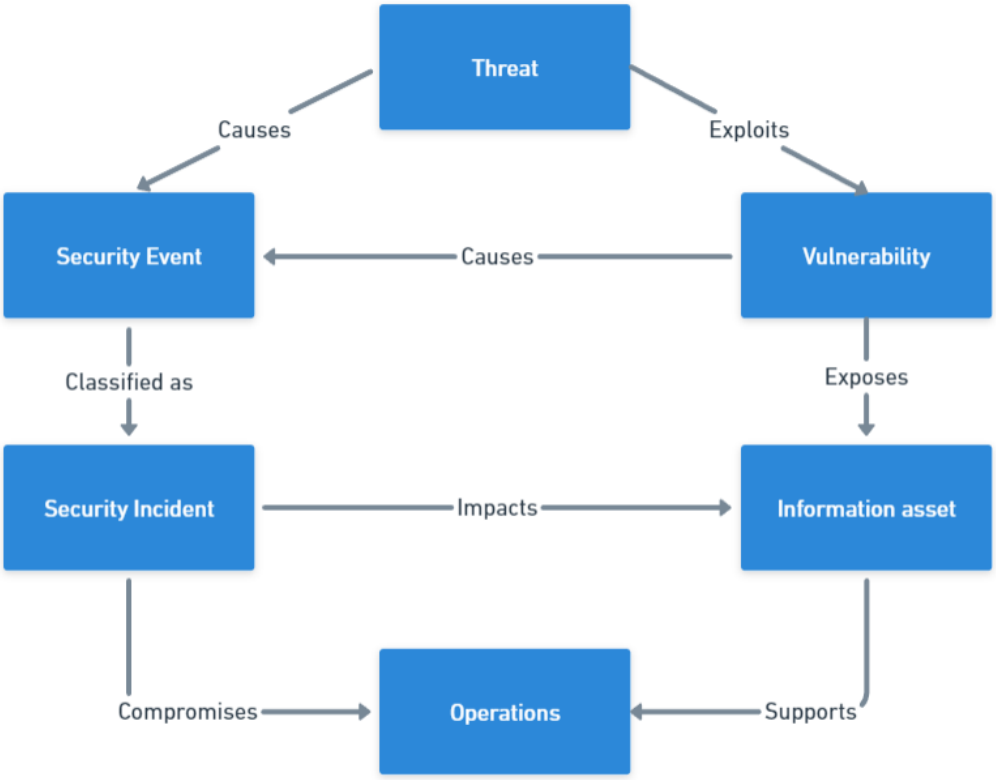

Figure 1. Relationships of objects in a security incident (SFS ISO/IEC 27035, 2016, modified)

Cyber security incidents can all generally be divided into having a detrimental effect, or impact, on one or more aspects of the so-called CIA triad: confidentiality, integrity, or availability, as seen in the figure 2. The CIA triad, or model, is widely considered the foundation of the modern cyber and information security theory and is something that security professionals strive to secure in each security model, program, and technology (Meyers, 2018, p. 20). Important to note is that an accurate categorization is not always feasible, and a security incident can also be formed before there is a categorically defined and an existing threat to operations or information assets, and while the threat is still only hypothetical. Also, an incident can start by affecting one aspect of the CIA triad and then later evolve to affect another or multiple aspects.

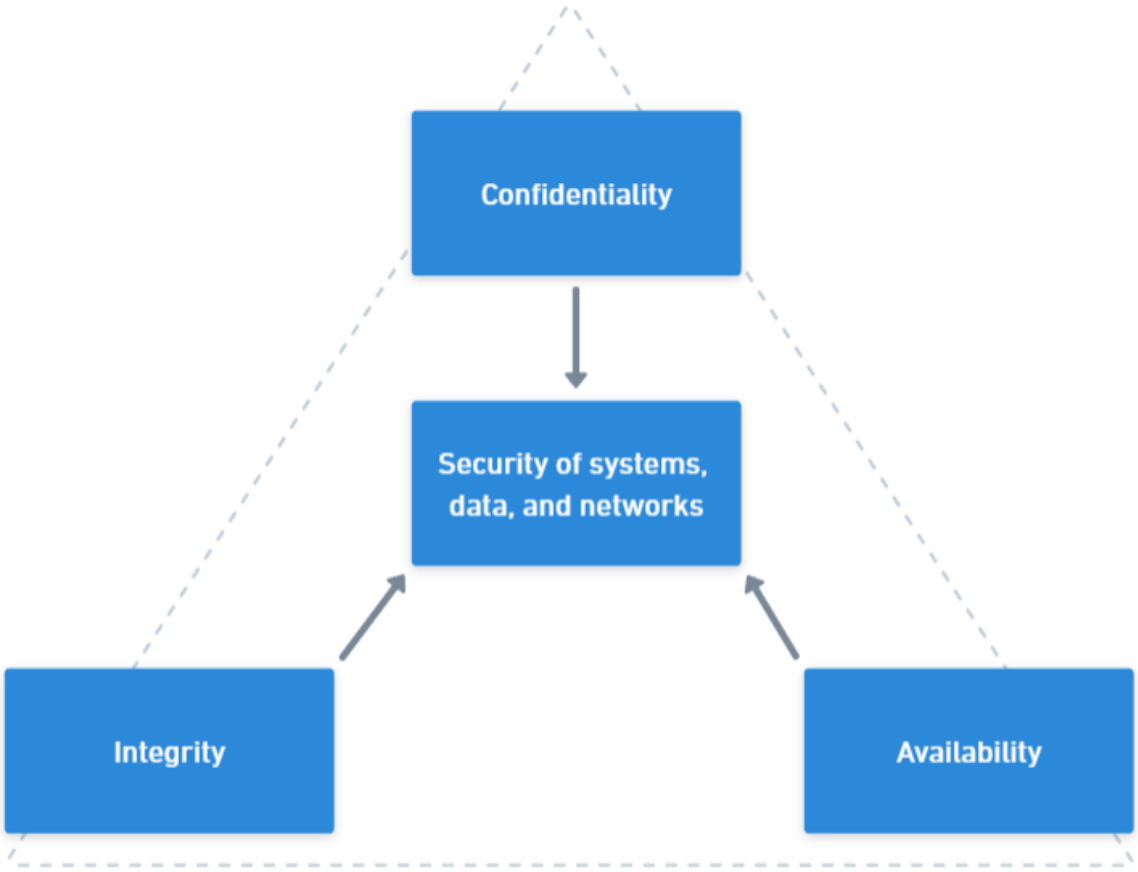

Figure 2. The CIA triad (Meyers, 2018, p. 20, modified)

Confidentiality refers to preventing access, or unauthorized interaction to systems, networks, and data unless the entity is authorized to do so, while simultaneously ensuring that those who have been authorized can (Meyers, 2018, p. 20). Some examples of incidents that affect confidentiality are related to unauthorized access to data or systems such as attempts to retrieve password files, hijack legitimate network connections, misconfigured systems, or information stealing malware infections (SFS ISO/IEC 27035, 2016).

Integrity refers to maintaining data and systems in an unaltered state while being stored, processed, and transmitted unless the alteration is intended (Meyers, 2018, p. 21). Some examples of incidents that affect integrity are uncontrolled or unauthorized changes to sensitive data, systems, or networks (SFS ISO/IEC 27035, 2016).

Availability refers to ensuring that systems and data are available for authorized entities when they require them (Meyers, 2018, p. 21). Some examples of incidents that affect availability are related to denial-of-service attacks (DoS), and Distributed denial-of-service attacks (DDoS). These are a broad category of incidents which threaten the availability of systems, networks, or services by the means of for example resource elimination or resource starvation (SFS ISO/IEC 27035, 2016).

3.2 What is incident response?

When operating in the modern interconnected world, cyber security incidents are happening to even the most security conscious organizations. In some cases, varying levels of cyber security attacks can even pose an existential threat to the continuity of the organization (Svahn & Karppi, 2021), arguably cause a major energy crisis (Kaspersky, 2021), block entire countries from accessing the internet (Davis, 2007), and even cause direct harm to human life and safety (Umawing, 2023). Cyber security incidents have the capability to cause serious qualitative damages, such as reputational damage that translate to losing customer trust and business (Pinsker, 2014), and quantitative damages, such as monetary losses caused by recovering from the incident and dropping stock prices (Greenberg, 2018) and legal or regulatory fines (Hill, 2022). To any organization operating in the cyber domain, it is not a question of *if* an incident will ever happen, but more specifically, *when* an incident will occur, and because negative events or incidents will happen, incident response cannot be simply ignored by organizations and is something that requires careful planning in advance (Meyers, 2018, p. 509).

Incident response can be defined as a structured and coordinated step of actions and approach to get from incident detection to incident resolution, and the primary goal is to efficiently remove a threat from the environment that the response is targeting, while minimizing damages and restoring normal operations as fast as possible (Luttgens et al., 2014, p. 25). The aim of having a consistent response methodology is to support systematic response to incidents so that the correct activities are executed, and the appropriate actions are taken when they are required (Cichonski et al., 2012, p. 6), and the calm and consistent response, utilizing a thought-out and refined process helps organizations avoid poor decision making in crisis-like situations (Chapple, 2020, p. 380). Typical incident response activities include confirming whether an incident has occurred,

provide rapid detection, analysis, and containment, determine the scope and impact of the incident, minimize disruption to operations and the damages to the organization, restore normal operations, and to provide feedback and enhance the security posture of the compromised entity so that future incidents can be avoided (Luttgens et al., 2014, p. 5). The last activity highlights one of the key benefits of utilizing a systematic approach of responding to incidents, that is, the ability to use the information gained during the response to better prepare for handling any potential future incidents, and to apply the gained knowledge to harden the systems and data to better withstand potential future attacks (Cichonski et al., 2012, p. 6).

There are several incident response frameworks that describe different structured approaches for cyber incident response, albeit with similar overall goals. Incident response has “officially” been around since 1988, and therefore many models, methodologies, and frameworks have naturally been developed to help overcome the complexities of responding to cyber security incidents (Knerler, et al., 2022, p. 126). The framework this thesis is predominantly focusing on is the NISTs’ incident response process described in the special publication 800-61 revision 2 "Computer Security Incident Handling Guide". The process itself will be described in detail in the next chapter.

The 800-61r2 publication focuses on three parts. Firstly, it aims to provide guidance on establishing and implementing computer incident response capabilities. For this it includes recommendations such as how to establish said capabilities, how to create an incident response policy, how to plan for incident response, how to develop procedures related to incident response, what are efficient ways to organize an incident response team, and how they should be staffed with people with appropriate skills. Secondly, it provides a comprehensive framework that can be tailored to an organization’s specific needs (the process mentioned earlier and discussed later), and thirdly, it gives recommendations on incident coordination and information sharing such as to plan incident coordination with external parties before incidents occur, to perform information sharing throughout the incident response lifecycle, and to consult with the legal department before initiating any coordination efforts (Cichonski et al., 2012, p. 4).

Other notable and related incident response frameworks that are not primarily focused on are for example the Cloud Security Alliances (CSA) Cloud Incident Response framework (Lim et al,. 2021), SANS Institutes’ Information Security Reading Room Incident Handler’s Handbook (Kral, 2012), and

the observe, orient, decide, and act (OODA) loop, as described in the figure 3 below, and developed by the military strategist and United States Air Force Colonel John Boyd to help soldiers think clearly during the "fog of war" (Knerler, et al., 2022, p. 28). In the OODA loop, observing can be considered as incident detection, orient relates to understanding internal and external landscapes, deciding means choosing the best tactics and actions based on the observations, and acting means executing the chosen actions (AT&T Cybersecurity, 2015).

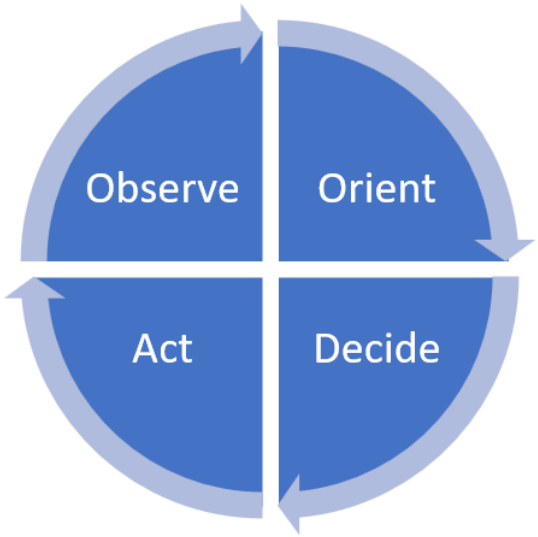

Figure 3. The OODA Loop (Knerler, et al., 2022, p. 28, modified)

3.3 Incident response process in the NIST-SP 800-61r2

The NISTs incident response process has several phases as described in the figure 4. These are "preparation, detection, analysis, containment, eradication, recovery, and post-incident activities" (Cichonski et al., 2012, p. 21). Process wise, the detection and analysis phases, and also the following containment, eradication and recovery phases are usually grouped together even though they all have different distinctive goals. Still, to make the comparative analysis clearer later on, they will all be discussed separately in their own respective chapters. The overall process does not follow a direct linear progression from start to finish, but instead, it includes loops that allow returning to previous phases that reflects the reality of cyber security incidents (Chapple, 2020, p. 380). In the inner loop, detection and analysis phases provide insights that can be beneficial for the containment, eradication, and recovery phases, that in turn provide feedback to enhance the detection

and analysis phases and capabilities (Anson, 2020, p. 24). In the outer loop, the insights gathered from a handled incident improve the preparation phase so that responders can better handle similar incidents in the future (Chapple, 2020, p. 386). In this framework, incident response should be considered as an ongoing cycle rather than a short-term mission, and it is something that should be used regularly and not only during an emergency (Anson, 2020, p. 24).

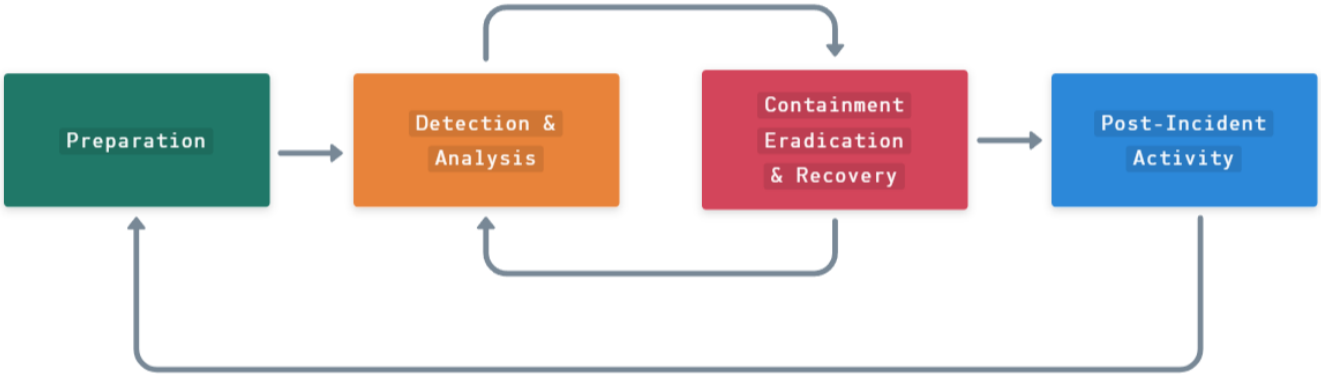

Figure 4. The Incident Response Cycle (NIST-SP 800-61r2, 2012, p. 21, modified)

3.3.1 Preparation

Incident response preparation phase can be considered as one of the most important phases, and the decisions made in this phase can reflect to all of the subsequent phases either negatively or positively (Meyers, 2018, p. 511). A useful analogy to describe the preparation phase comes from the military world, where armies generally train for war during peace time, and harden and fortify their position before an imminent conflict to gain an advantage in the battle (Anson, 2020, p. 21). To describe the phase less dramatically, the preparation phase essentially attempts to prepare the organization's people, processes, and technology to methodologically monitor, investigate, remediate, and recover from incidents (Luttgens et al., 2014, p. 46). What this means is that the preparing organization should have correct equipment, tools, and capabilities in place, responsibilities clear as to who is in charge of what, and that the relevant people are trained what to do before an incident occurs (Meyers, 2018, p. 511). Generally, proper preparation can be considered to enhance the overall cyber resiliency of the organization, or the ability to withstand, anticipate, adapt to, and recover from adverse conditions, attacks, or compromises (Anson, 2020, p. 22).

The NIST incident response process gives recommendations and emphasizes the importance of two separate aspects of preparation: preparing to handle incidents by establishing an incident response capability, and the importance of preventing incidents from happening (Cichonski et al., 2012, p. 22). It also highlights that even though the incident response team or capability typically is not responsible for incident prevention, and that it is important to recognize that preventative controls will eventually fail, it is still fundamental to the success of the incident response program (Cichonski et al., 2012, p. 23). Some general recommendations that NIST gives on how to prepare people, processes, and technology for both handling and preventing incidents are described in the appendix 1, although, and as mentioned before, the document highlights that the recommendations are general and are not to be considered as exhaustive or necessarily applicable to everyone (Cichonski et al., 2012, p. 22).

3.3.2 Detection

Countless of events occur in even in a smaller environment every day (Anson, 2020, p. 30), and one of the hardest parts of incident response for many organization is establish the capability to accurately detect and assess potential incidents, that is, determining if an incident has occurred, and if it has, what kind of incident has happened and what is the impact it potentially poses (Cichonski et al., 2012, p. 26). NIST lists several challenges and separate factors that make accurate incident detection hard. These are related incidents having numerous means, and that the detections may have varying levels of details and fidelity. Also, the volume of potential signals, that is, the various types of signs of incidents are typically high, and extensive knowledge and specialized experience are essential to understand incident related data (Cichonski et al., 2012, p. 26).

According to NIST, “signs of an incident fall into one of the two categories, precursors, and indicators” (Cichonski et al., 2012, p. 26). A precursor is a signal that foreshadows an incident, and if one is observed, an incident may occur in the near future (Cichonski et al., 2012 p. 26). While most attacks do not have any detectable or identifiable precursors, they still can, if observed, present an opportunity for an organization to prevent an incident from happening by adapting their security posture to better mitigate the potential incident by for example enhancing monitoring activities involving the target system (Cichonski et al., 2012 p. 26). Some examples of precursors are for example a public facing server log event that imply scanning events from a vulnerability scanner, or a

public announcement of a release of a proof-of-concept exploit to a known vulnerability that affects an organization's critical asset (Cichonski et al., 2012 p. 27). Unlike precursors, indicators on the other hand are not rare (Cichonski et al., 2012 p. 26). According to NIST "an indicator is a sign that an incident may have occurred, or may be occurring now" (Cichonski et al., 2012 p. 26). Some examples of indicators are numerous failed login-attempts from an unfamiliar remote system, unusual deviations of typical traffic flows, or that an endpoint protection software alerts that it has detected a suspicious executable running on the system (Cichonski et al., 2012 p. 26).

Indicators and precursors can be identified using numerous different sources. Some of the common sources are publicly available information, reports from the people within or outside the organization, various security software alerts, and log-based alerts (Cichonski et al., 2012 p. 28). Publicly available information could be for example public information on a new vulnerability, an exploit, or a security incident and a breach (Cichonski et al., 2012 p. 28). Another source could be organizations' own employees, users, administrators, or security staff that report seeing or hearing something abnormal happening within the organization's information assets (Cichonski et al., 2012 p. 28). Software based alerts are being created by for example various endpoint detection and response, or EDR (Knerler, et al., 2022, p. 198), and security information and event management, or SIEM solutions (Cichonski et al., 2012 p. 27). Note that there are many other software and solutions that can also provide detective and alerting capabilities, but these are just good examples. For detection, EDR solutions generally utilize large libraries of detection rules, leverage a combination of detection techniques, provide a deep linking to cyber threat intelligence, and use observables and indicators seen from one system to inform detection capabilities across other systems (Knerler, et al., 2022, p. 198).

SIEMs on the other hand utilize more log-based analytics capabilities where for example various operating system, network, and application logs are being ingested to a SIEM solution, and where various correlation rules have been developed to alert on certain types of events or patterns of events (Knerler, et al., 2022, p. 243). Generally, SIEMs can collect, aggregate, filter, store, triage, correlate, and display security related data, and on addition to their detection capabilities, they also support both real-time and historical analysis, and therefore they are typically heavily utilized by security operations centers or SOCs (Knerler, et al., 2022, p. 243). Different sources for security

related data can also be divided into either providing contextual information, i.e., what has happened, or they can provide more actionable alerts, or something in between, as described in the figure 5 below (Knerler, et al., 2022, p. 20).

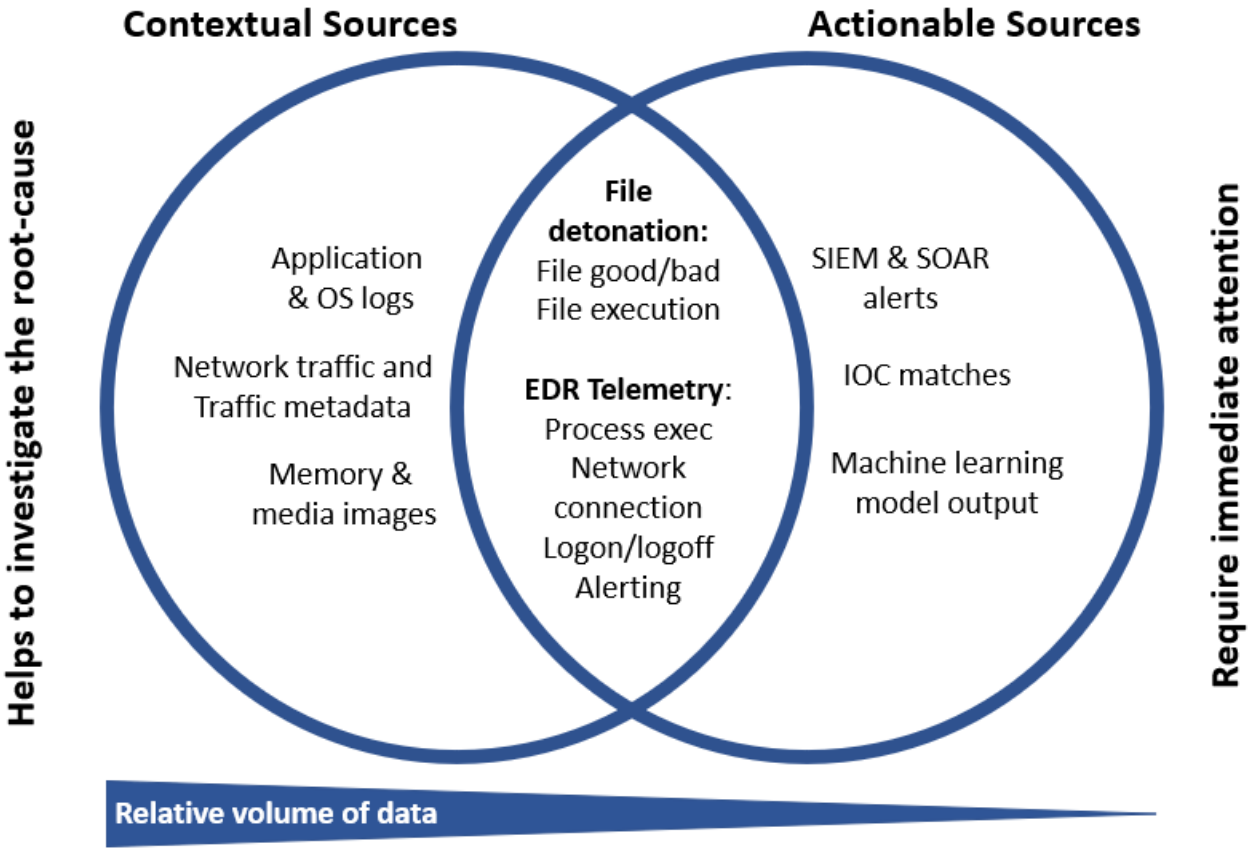

Figure 5. Contextual and actionable sources for security related data (Knerler, et al., 2022, p. 20, modified)

Efficient detection requires a large amount of security related data to be collected, and the balance between having adequate visibility to organizations information assets and collecting too much data, so that the organization becomes overwhelmed, i.e., the relevant signals, indicators, and precursors are lost into the noise, requires careful planning from any organization (Knerler, et al., 2022 p. 179). This balance is described in figure 6 and is different for every organization. The optimal amount and the quality of the data translates directly to the value the data will have for detection and analysis, and therefore the overall success of the incident response effort (Knerler, et al., 2022, p. 180). Appropriate risk assessment on the organizations most critical assets can help identifying the relevant events that have the greatest value from an incident response and the

overall cyber security perspective (Anson, 2020, p. 33), but still, the optimal strategy for data collection largely depends on the organization's maturity, risk appetite, existing capabilities, and the cost they are willing to pay (Knerler, et al., 2022, p. 180).

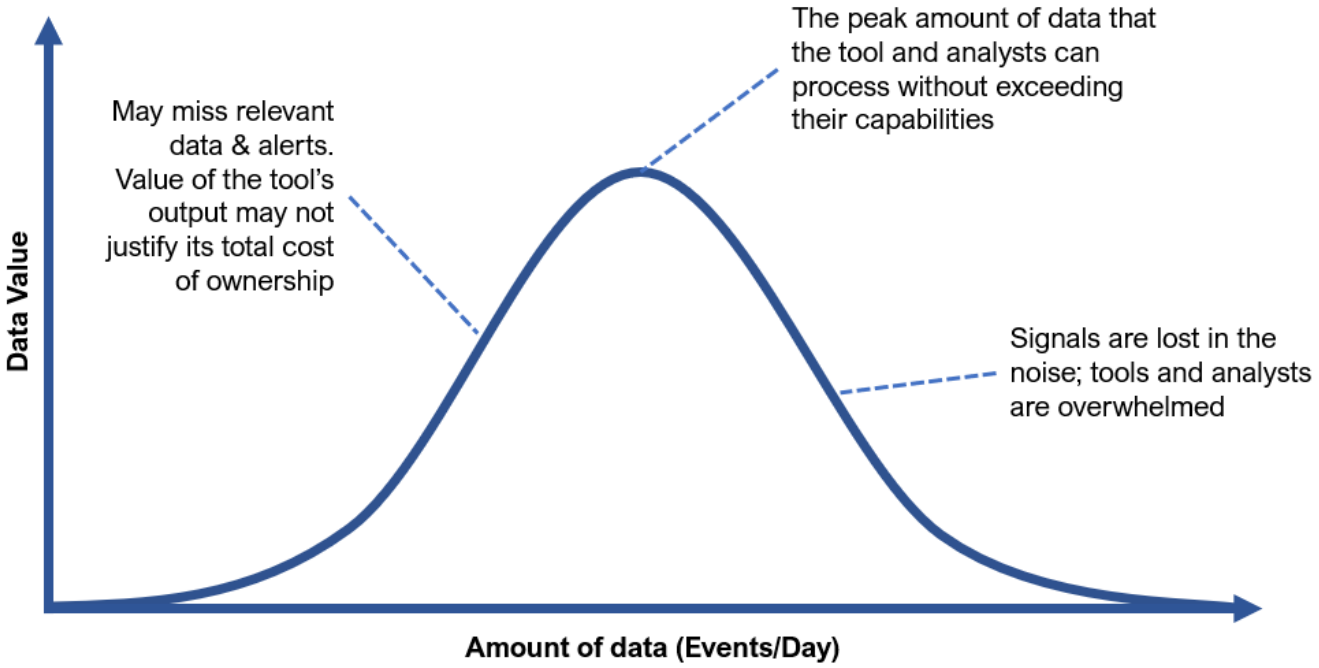

Figure 6. The value of security related data compared to the amount of data (Knerler, et al., 2022, p. 179, modified)

3.3.3 Analysis

Incident analysis is the logical next step after the detection phase. Various signals such as precursors, indicators, and reports coming from different sources should be first triaged, validated, categorized, and evaluated whether they constitute and cyber security incident (Knerler, et al., 2022, p. 132), and if so, the incident analysis should aim to determine and capture what has happened, what is the source of the incident, document the findings, determine the scope, what is the impact, and to prioritize proceeding actions and notify all relevant stakeholders (Cichonski et al., 2012, p. 28). In short, incident analysis aims to determine who, what, where, when, why, and how. As mentioned earlier, these two phases, detection, and analysis are process-wise connected to each other in the NISTs framework and aim to generate insights and guidance to the proceeding containment, eradication, and recovery phases (Cichonski et al., 2012 p. 21).

Most incidents do not start out as incidents, but anomalous or unexplained activity (Knerler, et al., 2022, p. 132), and incident analysis can be a difficult endeavor since the accuracy of precursors, indicators, and other signals is not always guaranteed (Cichonski et al., 2012 p. 28). Also, indicators are not always accurate, and even if they are, there is no guarantee that an incident has occurred, but some events that become indicators can also happen for other reasons than a security incident (Cichonski et al., 2012 p. 28). Also, some incidents can be easy to detect, but some incidents do not necessarily have clear indicators at all (Knerler, et al., 2022, p. 133). Often the people investigating incidents are responsible for analyzing incomplete, contradictory, and ambiguous data to determine the root cause of the incident (Cichonski et al., 2012 p. 28). Still, one part of the analysis process is determining what is the nature of the signal, while understanding why, or the reason a single signal, such as an alert, may not be telling the full story (Knerler, et al., 2022, p. 136). Determining whether an indicator, or an alert, is actually an incident requires a good understanding of both the technical and contextual environments and may also require collaboration with other relevant stakeholders (Cichonski et al., 2012 p. 29).

One of the goals of the analysis phase is to determine whether an incident has happened (Cichonski et al., 2012 p. 29), and when a signal is detected, after the initial analysis incidents generally fall into one of the four categories as described and defined in the table 1 below, based on what was uncovered during the analysis (Knerler, et al., 2022, p. 136). These being a true positive, a false positive, a false negative, and a true negative (Knerler, et al., 2022, p. 136). Sometimes a fifth category is also used, a benign true positive, where intent is to describe situations where a detection worked properly, but the activity is correctly understood as non-malicious (Knerler, et al., 2022, p. 137).

	Bad behavior occurred	Bad behavior did not occur
Alert Fired	**True Positive** Something bad happened, and the system caught it.	**False positive** The system alerts, but the activity was not actually malicious.
Alert did not fire	**False negative** Something bad happened, but the system did not catch it.	**True negative** The activity is benign, and no alert has been generated.

Table 1. Four categories of activity (Knerler, et al., 2022, p. 136, modified)

NIST also gives recommendations for making incident analysis easier. These are techniques and capabilities such as profiling networks and systems, understanding what normal behavior is, having a proper log retention policy, performing event correlation, keeping all host clocks synchronized, maintaining, and using a knowledge base for incident information, filtering unnecessary data from the dataset that is being analyzed, and seeking assistance from others when the incident has insufficient information (Cichonski et al., 2012 p. 29). Also, it is important to ensure that the assumptions on the detection data are made carefully while being aware of investigators' own potential bias, and not only to satisfy a certain hypothesis that fits (Knerler, et al., 2022, p. 133). Other techniques to ensure that the correct conclusions are derived from the detection data are for example, seeking additional data that can augment the analysis if there are any apparent gaps, creating a timeline of events to distinguish potential patterns that shows a sequence of the adversary actions, and comparing good and known to suspicious activity by for example comparing known application or system file hashes to existing ones (Knerler, et al., 2022, p. 133). Also, another technique that can help the incident analysis is utilizing scenario or hypothesis analysis where a hypothesis is formed based on existing data on where an adversary could be resident, what is already breached, and where the adversary could be moving next (Knerler, et al., 2022, p. 134).

Even though thorough analysis of available indicators is important, the analysis should still not rely solely on IOCs as some of them, such as IP addresses or file hashes are trivial for an adversary to change, but instead, the analysis should be striving to recognize adversary techniques, tactics, and procedures, or TTPs, from the incident data (Knerler, et al., 2022, p. 134). This relationship of how hard or trivial for an adversary to change indicators is described in the "pyramid of pain" in the figure 7 (Knerler, et al., 2022, p. 333).

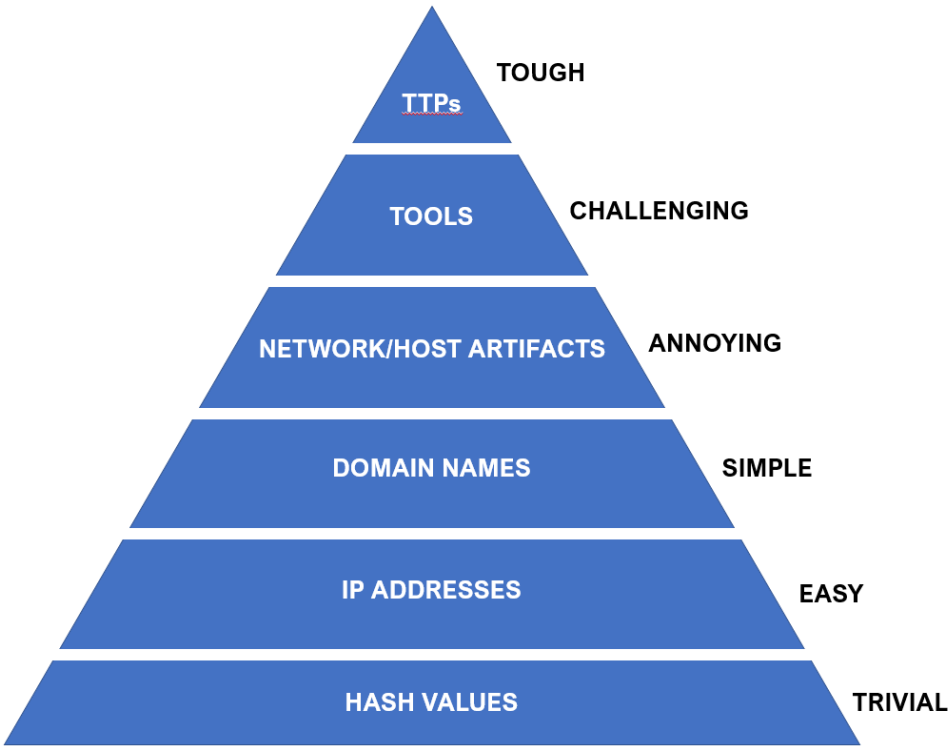

Figure 7. The pyramid of pain (Knerler, et al., 2022, p. 333, modified).

Both incident analysis and detection phases can benefit from utilizing attack lifecycle frameworks such as the Lockheed Martin's Cyber Kill Chain (Zimmerman, 2014, p. 30), or MITREs ATT&CK framework (Knerler, et al., 2022, p. 167). Different attack lifecycle frameworks generally attempt to model and describe attack methodologies and different phases or the anatomy of an attack (Anson, 2020, p. 12). For example, in the Lockheed Martin's Cyber Kill Chain, these phases are "reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on objectives" (Chapple, 2020, p. 51). Not all stages are always present in an attack, nor do they necessarily follow this order, but from an incident detection and analysis point of view, it is beneficial to think about incidents in the context of the different phases of the lifecycle to better understand the context of the discovered activities as they relate to the overall compromise (Luttgens et al., 2014, p. 19). One example of how an attack lifecycle framework could be beneficial for incident analysis is related to the fact that most incidents are detected after the initial entry point, or somewhere after the "right of hack", as described in the figure 8, and therefore, during an incident analysis phase, the framework can be utilized to work backwards and potentially identify previous steps of the attack (Knerler, et al., 2022, p. 134). For detection, a similar example could be that monitoring and detection rules or use cases could be developed and mapped for

each of the attack lifecycle phases to cover and detect different phases of an attack (Toropainen, 2020, p. 23). Overall, by laying out different signals across the different phases of the life cycle, more holistic insights and recommendations can be provided for the proceeding containment, eradication, and recovery phases (Luttgens et al., 2014, p. 19).

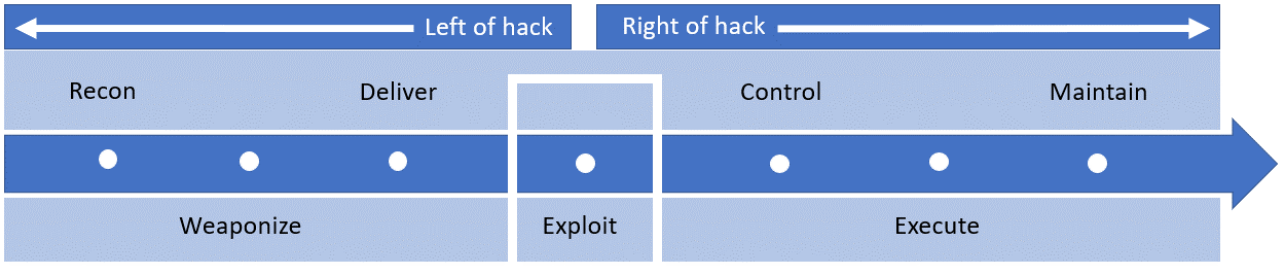

Figure 8. The Cyber Attack Lifecycle (Zimmerman, 2014, p. 30, modified)

3.3.4 Containment

In the NISTs incident response process, after the detection and analysis phase provide insights as to what has happened and where, these insights are then used to guide the next phase which is incident containment, eradication, and recovery (Cichonski et al., 2012 p. 21). This chapter will focus only on containment. As per the process, containment, eradication, and recovery also provide feedback to the detection and analysis phases to improve and guide actions with these phases (Cichonski et al., 2012 p. 21).

Containment refers to preventing an attacker from performing actions that the organization cannot allow to continue (Luttgens et al., 2014, p. 529). Most incidents require containment, and it is important to contain an incident to limit the damages it can cause to the business, and to prevent any additional damages from happening (Cichonski et al., 2012 p. 35). Containment can also provide crucial time for developing an efficient eradication and remediation strategy, and to loop back to the previous analysis phase if for example the full incident scope is still not understood (Cichonski et al., 2012 p. 35). Essential for containment is to know the impact the decision made in this phase can have, and this can made be easier, if the organization has defined what kind of risks related to incidents are acceptable, and if various predefined strategies and procedures are developed before an incident happens (Cichonski et al., 2012 p. 35). Different types of containment

strategies may also be required for different types of incidents (Meyers, 2018. p. 514). For example, if the incident is a network-based attack, such as a denial-of-service attack, containment could mean isolating the network segment that is being attacked by removing it from the network. If on the other hand data is being extracted from the network, containment may require blocking certain types of traffic at the network perimeter (Meyers, 2018, p. 516). In a malware related incident where a malware is observed running on a system, containment could mean isolating, or quarantining, the host for example using an EDR tool and preventing the malware spreading to other systems or an adversary getting a foothold within the environment (Meyers, 2018, p. 516). Quarantining can prevent an incident from spreading to the rest of the environment, and by only removing the device from the network, important evidence and further indicators can be gathered to provide insights back to the analysis phase (Meyers, 2018, p. 516).

NIST recommends that organizations should create different containment strategies for different incident types which can help and facilitate crucial, and potentially time sensitive, decision making (Cichonski et al., 2012 p. 35). Deciding an appropriate containment strategy may depend on for example what are the potential damages the incident can cause, or if any evidence needs to be preserved, or what is the effort i.e., time and resources the containment strategy implementation requires, how effective is the containment strategy, and how permanent is the containment solution (Cichonski et al., 2012 p. 35).

3.3.5 Eradication

Eradication refers to eliminating the threat, or the components of the incident, from the environment, such as disabling breached accounts, changing their passwords, deleting malware, or mitigating and identifying all vulnerabilities that were potentially exploited (Cichonski et al., 2012 p. 37). One of the main goals for eradication is removing, or denying, the attacker's ability to access the environment, such as compromised systems, accounts, and data (Luttgens et al., 2014). In eradication, unlike containment that only tries to remove or limit the attackers access to a specific network segment, application, or data, the goal is to remove all of the attacker's access from the environment (Luttgens et al., 2014, p. 532). Also, it is important for eradication that the incident root-cause is understood from the analysis phase, and that all of the affected assets have been identified (Cichonski et al., 2012 p. 37). A comprehensive eradication largely depends on the level of understanding of the scope of the incident, and as with the previous containment phase, the

insights from the previous analysis phase are crucial to build understanding as to where the malicious artifacts are, how systems or settings were changed, or if any persistent mechanisms were employed, and where all of these should be removed and how (Luttgens et al., 2014, p. 533). One important expectation for comprehensive eradication is that, if an attacker has gained an extensive foothold to the environment, they will try to regain access to if the incident is only contained (Luttgens et al., 2014, p. 533).

3.3.6 Recovery

After the incident root cause has been understood, contained, and eradicated, systems, networks, and data should be restored to their original states so that they can resume their normal operations. Also, the recovery phase should aim to confirm that the affected assets are functioning normally and improve security controls to prevent similar future incidents (Cichonski et al., 2012 p. 37). The types of actions required for recovery depends on the type of the incident and may include tasks as restoring a system from a clean backup, rebuilding systems, installing patches, hardening the system, changing user passwords, and adjusting the firewall or the network perimeter (Cichonski et al., 2012 p. 37). For example, in a malware related system compromise, it may not be sufficient to just remove or to clean the system from the malware as it may be difficult to ensure that the malware has been completely eradicated from the system, but instead, rebuilding the compromised system from a known good state may be more sufficient and deliver more reliable results (Luttgens et al., 2014, p. 540). Also, during the recovery phase, it is essential to monitor the affected systems and networks for additional attacks or other abnormal behavior, and to validate that the compromised systems and the organizations other are not being attacked in a similar way, or being reinfected with malware (Cichonski et al., 2012 p. 37). NIST also recommends that recovery should utilize a phased approach, and that the remediation steps are properly prioritized. Larger incident with a large scope and scale may take a long time to recover from, and the initial and early stages of remediation should aim to improve and increase the security posture of critical targets to prevent future incidents, and the later stages should focus on continuous improvements and long-term changes to the overall security posture of the organization (Cichonski et al., 2012 p. 37).

3.3.7 Post incident activities

Post-incident activities phase is the last phase of the NISTs incident response process. The phase has two main goals: learning from the handled incident and improving existing capabilities to handle similar incidents in the future (Cichonski et al., 2012 p. 38). Reflection, and holding a "lessons learned" meeting with all the relevant stakeholders to collect observations regarding suboptimal security practices can help to improve said practices, and also the incident handling process itself (Knerler, et al., 2022, p. 142). In the lessons learned meeting, NIST recommends that all the relevant stakeholders reflect on what exactly happened, what was done to intervene, and how well the response actions worked (Cichonski et al., 2012 p. 38). They also provide a list of questions that should guide the reflection in the meeting such as: what happened, when was the incident first detected, by whom, what information was needed sooner, were the procedures followed, how adequate they were, did any actions inhibit the recovery, what should be done different next time, how was information shared with others, what should be done to prevent similar incidents in the future, what kind of precursors and indicators should be monitored to detect similar incidents, and are there any additional tools or resources required to detect, analyze, or mitigate future incidents (Cichonski et al., 2012 p. 38). The answers to these questions can be then translated back into for example adjusted plans, fixing inaccurate policies or procedures, training materials, incident playbooks, or any other future investments to support previous incident response phases that the incident post post-mortem found deficiencies in (Cichonski et al., 2012).

4 Cloud computing

This chapter discusses basic concepts and characteristics regarding modern cloud computing. These foundational cloud computing concepts are critical to define before their impact on modern incident response frameworks can be discussed in the chapter 5 that discusses incident response in the public cloud domain.

4.1 Cloud concepts and characteristics

Cloud computing has changed the modern enterprise information technology operations and architecture, and in a fundamental way changed how organizations and end users consume IT-resources. Compared to the 2000's, or even to the early 2010's, the IT-requirements for custom-

ers, organizations, and employees have changed radically: to stay competitive, digital transformation and accelerated innovation require organizations to be more agile, scale elastically, and optimize IT-spending (Savill, 2020, p. 1). Customers on the other hand want to be able to engage digital experiences across all of their devices using their existing digital identities wherever practical, and employees wish to be able to work from anywhere, or from any platform or device (Savill, 2020, p. 1).

Cloud computing can be described as outsourcing data center operations, IT-infrastructure, or applications to a provider which offers computing resources, called a cloud service provider. The NIST special publication 800-145 defines cloud computing as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction" (Mell & Grance, 2011). Cloud computing enables for the provision of exactly the right type and size of computing resources as is required, and the ability to access them almost instantly i.e., it follows the utilities model where a provider sells computing resources in an as-needed or as-consumed model (Montgomery & Olson, 2018, p. 3). NIST defines the cloud model to have five distinct characteristics: "On-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service" (Mell & Grance, 2011). On-demand self-service refers to a model that allows customers the ability to provision, and to scale their compute resources in real time, and as needed, without human or provider intervention (Malisow, 2020, p. 3). Organizations may still include internal approval workflows for certain conditions (Savill, 2020, p. 5). Broad network access means that the provider's services are consistently accessible over the network, regardless of the user's location or the source system (Malisow, 2020, p. 3). Resource pooling refers to the characteristic where all the providers resources are provided in a multitenant model, where the resource isolation is provided with software (Savill, 2020, p. 5), meaning that the underlying hardware, software, and networking assets are shared by multiple customers (Malisow, 2020, p. 3). Rapid elasticity is the ability to rapidly grow and shrink, or to scale or to descale, or to acquire and dispose IT-resources based on the service demand, and to meet the operational requirements without having excess capacity (Malisow, 2020, p. 3). Finally, measured service refers to the utilities model described earlier, meaning that the consumer is only charged based on what they use, while the usage is measured by the provider (Malisow, 2020, p. 3).

There are several advantages that organizations benefit from cloud computing compared to traditional on-premises infrastructures and deployments that can be used as justifications for the business case for cloud deployments. These advantages aim to both optimize IT-infrastructure and operational spending, but also to solve for example engineering or geographical issues. For example, Amazon Web Services highlights several advantages organizations benefit from their services such as trading fixed expenses for variable expenses, meaning trading capital expenditures to operating expenses (AWS, 2023bd). This means that the customers do not have to invest in expensive infrastructure before they have a clear objective on how to use it, but instead, they can only use and pay for what they consume. This also means that there is no need to guess or estimate the capacity that will eventually be needed in the infrastructure, but only the capacity required can be accessed, and scaled up or down as required (AWS, 2023bd). According to AWS, their customers also benefit for massive economies of scale, or the notion that since AWS operates in such a gigantic scale, they can operate more cost efficiently compared to if the customers would try to engage in similar operations in a more minor scale, which eventually translates into lower pay-as-you-go pricing for the customers (AWS, 2023bd). The scale in which they operate also enables global operations, meaning infrastructure, latency, and the overall end-user experience can be optimized geographically at minimal cost and effort (AWS, 2023bd). Other qualitative advantages can be for example increased speed and agility, or the cloud characteristic where new resources can be deployed in just minutes, which dramatically increases the development and operational efficiency, adaptability, consistency, and ease of use (AWS, 2023bd). From a quantitative point of view, in addition to the aforementioned lowered infrastructure cost, there are advantages such as lowered support and licensing cost, guaranteed uptime, high availability, redundancy, faster recovery times from outages, and lowered release frequency for development (AWS, 2023bd).

4.2 Cloud service models

Core cloud services are generally offered in different models, often characterized with the term “as a service” (Montgomery & Olson, 2018, p. 7). The primary service types, or the core service offerings are regularly defined as Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (Iaas) (Montgomery & Olson, 2018, p. 7). Additionally, often different cloud service providers also provide more detailed or definitive terms in marketing or sales offerings, such as anything as a service (XaaS), but all of these can generally be fitted into either SaaS,

PaaS, or IaaS (Montgomery & Olson, 2018, p. 7). The figure 9 describes the responsibilities between the cloud provider and customer for each different cloud service model, or the so called ”shared responsibility model”.

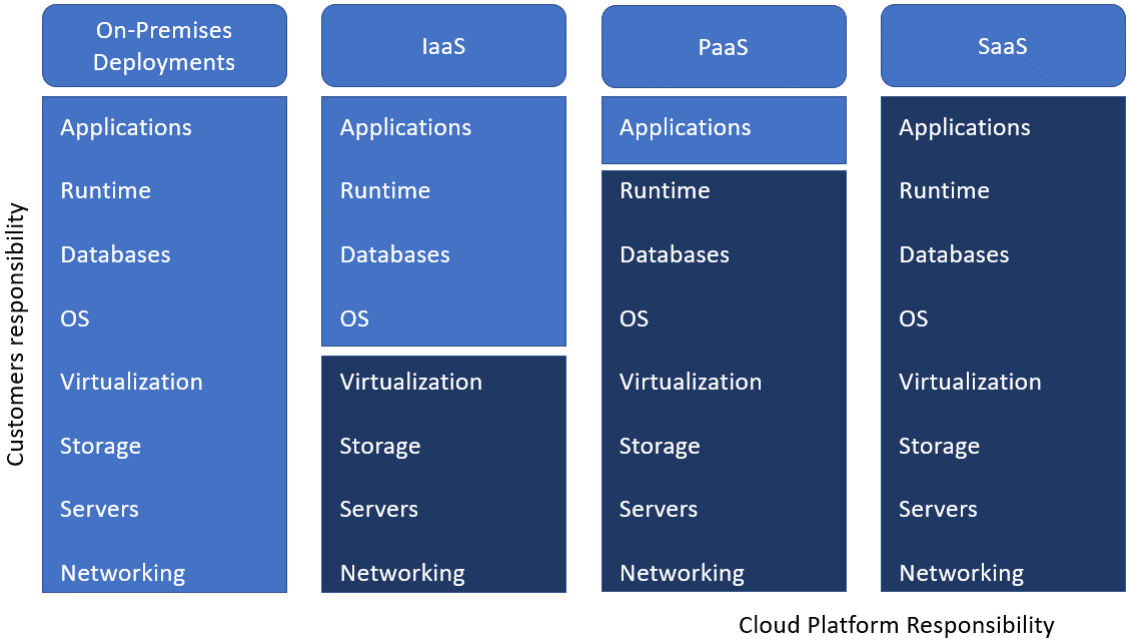

Figure 9. Cloud service models (Piper & Clinton, 2019, p.6, modified)

The NIST special publication 800-145 defines the Software as a Service “as the cloud provider developed and maintained applications running on a cloud infrastructure, that are accessible from various client devices and interfaces” (Mell & Grance, 2011), and also as a model where “the consumer does not manage or control the underlying cloud infrastructure, with possible exceptions of limited application configuration settings” (Mell & Grance, 2011). In the SaaS model, the cloud provider is responsible for updating, administering, and patching the software, and the cloud customer is only concerned with processing and uploading data within the service, or application (Malisow, 2020, p. 11). All the application logic, networking, storage, and computing resources are offered as a service in the Saas model (Montgomery & Olson, 2018, p. 8). Several business, and hosted applications are examples of the SaaS model, and they provide such as e-mail, enterprise resource planning, human resources, and software development applications that are available through different interfaces, usually through a web-browser (Montgomery & Olson, 2018, p. 8).

Platform as a Service is an intermediary service model that provides resources where custom software and applications can be run (Savill, 2020, p. 11). The cloud provider usually provides the platform, such as a selection of hardware and operating system abstractions that the provider maintains and administers, and the customer can focus on building and running applications on top of (Malisow, 2020, p. 11). The NIST special publication 800-145 defines PaaS as "a service model where the customer does not manage or control the underlying cloud infrastructure, such as networks, servers, operating systems, or storage, but has control over the deployed applications and environment configurations" (Mell & Grance, 2011). The model can be seen as especially beneficial for software development, as software can be tested in an isolated environment, and testing can be performed across a wide range of platforms and operating systems (Malisow, 2020, p. 11). The PaaS model offerings typically include services such as container services, different types of "serverless" offerings, cloud database engines, and "big data" warehousing and data mining (Savill, 2020, p. 11).

Infrastructure as a Service is described by the NIST special publication 800-145 as a model where the cloud customer can "provision processing, storage, network, or other fundamental computing resources" (Mell & Grance, 2011), and where the can "run arbitrary software, systems, and applications while not having responsibility or control of the underlying infrastructure, but still maintaining control over the deployed operating systems, storage, applications, and to a limited extent, the networking components" (Mell & Grance, 2011). The main goal when deploying and purchasing IaaS model offerings is to purchase a standard computing platform, and to build solutions on top of that, which allowed, and still allows organizations to replace their own data center equipment with cloud equivalent infrastructure (Montgomery & Olson, 2018, p. 9). IaaS can be considered as the most elemental cloud service models that enables the cloud customer to install software and operating systems on a hardware owned, administered, and connected by the cloud service provider (Malisow, 2020, p. 11), and IaaS products generally try to simulate features and characteristics similar to when the customer would manage their own physical resources (Piper & Clinton, 2019, p. 5). What this also means is that the liability and responsibility of the consequences of any detrimental configurations are owned by the customer (Piper & Clinton, 2019, p. 5). Another practical way to describe IaaS is as virtual computing in the cloud where the provider has a virtual environment where the customer purchases virtual machine instances and manages the operating system, patching, data, and applications (Savill, 2020, p. 11).

The so-called “shared responsibility model”, as described already in the figure 9, also relates to the security responsibilities in the cloud, and depending on the service model, the level of responsibility over the security controls vary between the cloud customer and provider (Microsoft, 2023ab). When operating in the cloud, at the bare minimum all physical security is the responsibility of the cloud provider, and depending on the model, additional responsibilities are shift over to the provider while the customer in most models is still responsible for the devices used to access the cloud, network connectivity, identities, and data (Microsoft, 2023ab). To illustrate this with IaaS, PaaS, and SaaS models, in the IaaS model, the cloud providers sole responsibility is to provide physical security of the facility and the systems, and the customer is responsible for all other security aspects, such as securing operating systems, applications, network connectivity, and identities (Malisow, 2020, p. 133). In the PaaS model, the customer is utilizing and installing, and therefore responsible for securing, software solutions on top of operating systems and hardware secured and provided by the cloud vendor (Malisow, 2020, p. 133). In the SaaS model, the customer is only responsible for securing who has the authorization and access to view and manipulate data within the SaaS solutions and the provider is responsible for securing everything else (Malisow, 2020, p. 134).

4.3 Cloud deployment models

Cloud deployment models can be considered as models that describe the type, nature, ownership, and purpose of the cloud environment (Montgomery & Olson, 2018, p. 11). According to NIST, there are generally four types of cloud deployment models: “public cloud, private cloud, community cloud, and hybrid cloud” (Mell & Grance, 2011).

The NIST special publication 800-145 defines public cloud as a model “where the cloud infrastructure is provisioned for open use by the general public” (Mell & Grance, 2011). In the public cloud deployment model, the cloud resources such as hardware and software are owned and operated by the cloud service provider and sold and leased to anyone who wishes to use them, i.e., they are by nature multi-tenant environments (Malisow, 2020, p. 12). The multi-tenancy also means that potentially the same hardware can be hosting several different customers virtual deployments without the customers having visibility or knowledge of each other’s existence, and the isolation being provided by the software layer (Malisow, 2020, p. 12).

Private cloud is defined by the NIST special publication 800-145 as a model where the cloud infrastructure is “provisioned exclusively to a single organization having multiple consumers such as different business units, and it may be owned and operated by the same organization or a third party, and it may exist on or off premises” (Mell & Grance, 2011). That means that in the private cloud model, the resources are dedicated to a single entity and no other entity shares the underlying resources, i.e., it is not a multitenant environment (Malisow, 2020, p. 12). Important to note is that since private cloud deployments come in many shapes and form, e.g., the private cloud could be owned and operated directly by the organization through hypervisor and virtualization solutions, or it could be just reserved or carved out sections from a specific cloud service providers physical and logical data center resources through contractual agreements (Malisow, 2020, p. 12), to categorize something as “private cloud”, it must embody or exemplify common cloud computing characteristics already discussed before (Savill, 2020, p. 5). These being characteristics such as measured service, on-demand self-service, rapid elasticity, resource pooling, broad network access (Mell & Grance, 2011).

Community cloud deployment model is defined by the NIST special publication 800-145 as a model “where the cloud infrastructure is provisioned for exclusive use for a specific community of consumers from organizations that have shared concerns” (Mell & Grance, 2011). They are designed to be shared by organizations with similar business needs, regulatory compliance, security, or policy requirements (Montgomery & Olson, 2018, p. 12); different parts may be owned and controlled by different individuals or organizations, but they all share similar goals and perform joint functions and tasks (Malisow, 2020, p. 12).

Finally, the hybrid cloud deployment model is a combination of different cloud deployment models and contains elements of two or more other models discussed earlier (Mell & Grance, 2011). An organization could for example operate private cloud resources due to legacy reasons, but also utilize public cloud resources as well in their overall infrastructure (Malisow, 2020, p. 13). In a hybrid cloud deployment, all of the utilized models provide their unique entities to the infrastructure, and the cloud consumer can benefit from the different advantages brought by different deployment models, but the resources are still bound together through technologies that enable data and application portability (Mell & Grance, 2011).

4.4 Common cloud components

Modern cloud computing can be considered to offer similar capabilities and components as data center centric, or on-premises capabilities and offerings, with the primary differentiator being the heavy utilization of the common cloud characteristics mentioned earlier (Montgomery & Olson, 2018, p. 13). Common cloud computing components, or the common building blocks that enable to build and consume IT-resources in modern cloud computing deployments and infrastructure are components such as: cloud compute, data processing, virtualization resources, data storage, networking, and database capabilities (Montgomery & Olson, 2018, p. 13). They also commonly provide automation, security, digital identity, and cloud management, and application integration related capabilities (Montgomery & Olson, 2018, p. 14).

Cloud compute resources are services that imitate traditional physical servers in the cloud, and they offer various configuration possibilities that facilitate characteristics, such as autoscaling, load balancing, or different types of “serverless” architectures (Piper & Clinton, 2019, p. 7). Compute resources facilitate central processing of applications and data in the cloud (Montgomery & Olson, 2018, p. 13). Virtualization, and by extension containerization, is one of the main enablers of modern cloud compute environments, and also one of the main technologies that enable cloud services to be offered as a financially viable business model as the cloud provider can offer services to a large number of customers using the same hardware resources (Malisow, 2020, p. 16). Virtualization is essentially the ability to create software representations of physical IT-resources such as RAM, CPU, storage, and networking (Montgomery & Olson, 2018, p. 14), and what they enable is more efficient use of the physical resources by creating the ability to divide one resources to multiple virtual machines or containerized applications through the use of a hypervisor (Savill, 2020, p. 4). The virtual resources are also completely abstracted from the physical hardware, as described in the figure 10, which means that for example each virtual machine can have its own operating system installed on virtualized hardware, meaning the same underlying hardware can support multiple operating systems, each isolated and individual (Savill, 2020, p. 4). Since the hardware is being emulated using software, it can also be programmatically created and disposed of, enabling one of the key cloud characteristics, dynamic elasticity (Montgomery & Olson, 2018, p. 14).

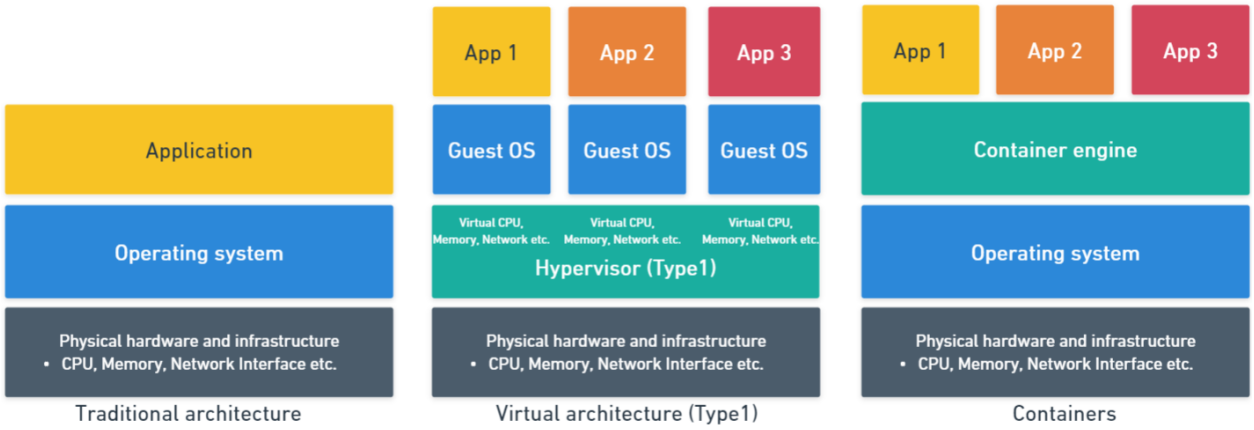

Figure 10. Traditional architecture and virtualization – Adapted from Savill, 2020, p269

Storage capabilities facilitate data storage in the cloud in various forms, such as objects, meaning various types of unstructured data, or block storage, meaning arbitrary organized storage volumes, or file-based data storage systems (Malisow, 2020, p. 78). To further elaborate on the different types, object storage can be utilized to store large amounts of unstructured data, such as videos, images, or documents, and typically the objects are stored in a key-value interface to store and retrieve data in a highly available and durable fashion (Piper & Clinton, 2019, p. 139). Block storage typically stores structured data in blocks and is typically used for data that has high performance requirements, such as databases and virtual machines (Piper & Clinton, 2019, p. 124). File storage, as the name suggests, emulates traditional file server and system characteristics, typically using network file system (NFS), or server message block (SMB) protocols, and is typically utilized as a shared storage for user or application data (Piper & Clinton, 2019, p. 146). Cloud storage can be utilized for example through large storage arrays, or through large storage area networks, and can be optimized for accessibility, high availability, and durability, or then for long term storage and archival (Montgomery & Olson, 2018, p. 19). Usually, the cost models vary depending on the optimization model (Montgomery & Olson, 2018, p. 14).

Networking capabilities ensure application connectivity and remote connections of various cloud resources, and is essentially transporting data to, from, and between different cloud resources (Piper & Clinton, 2019, p. 176). Cloud networking services typically offer different types of capabilities such as connectivity, network protection, network delivery, and network monitoring capabilities (Savill, 2020, p. 171). Cloud networking services enable the use of logically isolated virtual networks that connect cloud resources in a private, secure, and scalable way (Piper & Clinton, 2019,

p. 176). They also offer various ways to handle traffic distribution and load balancing capabilities, and also capabilities for secure, encrypted connections and virtual private networks (VPN) (Piper & Clinton, 2019, p. 179). Also, most cloud providers resources utilize their internal, sometimes global, wide area networks (WAN), that connect all of their data centers across all regions with high capacity and utilizing highly available connections, meaning when data is being moved between these data centers, the data is not being send over public internet, but rather it stays within the cloud providers WAN (Savill, 2020, p. 25). These large networks also enable large content delivery networks (CDN), that can cache and deliver content in different geographical regions, which improves performance and reduces latency for the end users (Piper & Clinton, 2019, p. 183).

Database capabilities enable applications to store, organize, and retrieve data efficiently, and follow traditional database models; they come in both relational and nonrelational database models (Piper & Clinton, 2019, p. 96). In the cloud, the cloud consumers can either build their own database infrastructure utilizing the IaaS model, that is, installing and configuring their own virtualized database servers, or then alternatively, they can utilize cloud-based database services that are offered in various different cloud service models, meaning they can be for example fully cloud provider managed PaaS, or SaaS offerings with varying levels of configuration options available to the cloud consumer (Piper & Clinton, 2019, p. 158). On top of database resources, some cloud providers also offer tools for big data and analytics for extremely large datasets, that can be utilized for example in machine learning capabilities (Montgomery & Olson, 2018, p. 13). Cloud management services on the other hand typically offer cloud monitoring, auditing, and configuration capabilities (Piper & Clinton, 2019, p. 10). These offerings can for example monitor the overall cloud infrastructure, performance, resource utilization, compliance, or account usage (Piper & Clinton, 2019, p. 10). They can also help cloud consumers to build automation, or for example standardization by defining a desirable configuration state for any specific cloud resource, or be utilized in troubleshooting (Piper & Clinton, 2019, p. 10).

Security and identity related cloud services offer tools to keep cloud deployments secure, and typically offer services managing authentication and authorization in the cloud, data at rest, in use, and in transit encryption capabilities, and threat detection and security monitoring capabilities (Piper & Clinton, 2019, p. 10). These services help cloud consumers to ensure the security and compliance of their cloud resources Identity and access management (IAM) has become especially

critical with the rise of modern cloud computing where digital identity, instead of the network, has fundamentally become the modern primary security perimeter for most organizations (Savill, 2020, p. 95). Therefore, most cloud providers offer dependable and comprehensive solutions for user authentication, authorization, and auditing, and also for policy management, federation, and identity repositories and directory services (Malisow, 2020, p. 159).

5 Incident response in public cloud

This chapter focuses on how the common cloud concepts, characteristics, models, and components described in chapter 4 reflect, have impact, and should be taken into consideration in the incident response model and process described in chapter 3. While generally the same processes and mechanisms can still be utilized when responding to security incidents in the cloud, and the overall goals of each of the phase of the incident response process still remain the same (AWS, 2023e, p. 6), the tools and techniques may vary, and having cloud platform specific knowledge is still required for both incident response (Malisow, 2020, p. 144), and for establishing understanding of the threat landscape in the cloud (AWS, 2023e, p. 17). The bright-line definitions of the traditional IT-perimeter, where all of the IT-assets belong to the organization, do not apply with cloud computing. Within the cloud domain, the difficulty defining where the essential risks are, and how far do they extend, ultimately arise from the customers data residing on an environment owned by someone else, operating on hardware infrastructure that is largely outside of the customers control, and often running on software that the customer has a limited or non-existing knowledge of (Malisow, 2020, p. 31). To overcome these challenges, responding to incidents in the cloud requires a shift in thinking compared to traditional on-premises environments (Knerler, et al., 2022, p. 143), and overcoming these challenges is important for any organization operating in the cloud domain because a comprehensive incident response strategy is an essential part of any organizations risk management efforts (Lim et al,. 2021, p. 7).

5.1 Cloud considerations for incident response preparation

For the preparation phase of the incident response process, the overall goals and objectives remain the same in the cloud, that is, to prepare the organization’s people, process, and technology assets to both handle and prevent incidents (Lim et al,. 2021, p. 13). Some of the most notable differences in the preparation approaches arise from the presence of the “shared responsibility

model" that was already described in the chapter 4.2., that dictates what falls under the responsibility of the cloud customer to secure, i.e., what part of the cloud environment the customer needs to prepare to handle and prevent incident for (Lim et al,. 2021, p. 14). A practical example of the shared responsibility model is described below in figure 11. Since in some of the models the cloud provider has this responsibility, the customers should understand and align their incident response plans and procedures with the provider through service level agreements and contracts (Lim et al,. 2021, p. 14). This in mind, in the preparation phase, the cloud customer should conduct a thorough analysis of the existing environment, cloud architecture, and responsibility model to better understand the line where the customer is responsible to respond to incidents, and where in turn the cloud provider should respond (Lim et al,. 2021, p. 14). This can include actions such as identifying the inventory of the cloud services and components in use, and understanding how they integrate and interact with each other, determining concrete roles, obligations, and responsibilities for different stakeholders in the overall cloud architecture, include the cloud provider's contacts in the incident reporting structure where applicable, and have a list of the providers incident assistance teams readily available (Lim et al,. 2021, p. 14). Also, the data privacy and local regulatory compliance requirements may vary as the customers data may be stored in various locations (Lim et al,. 2021, p. 14).

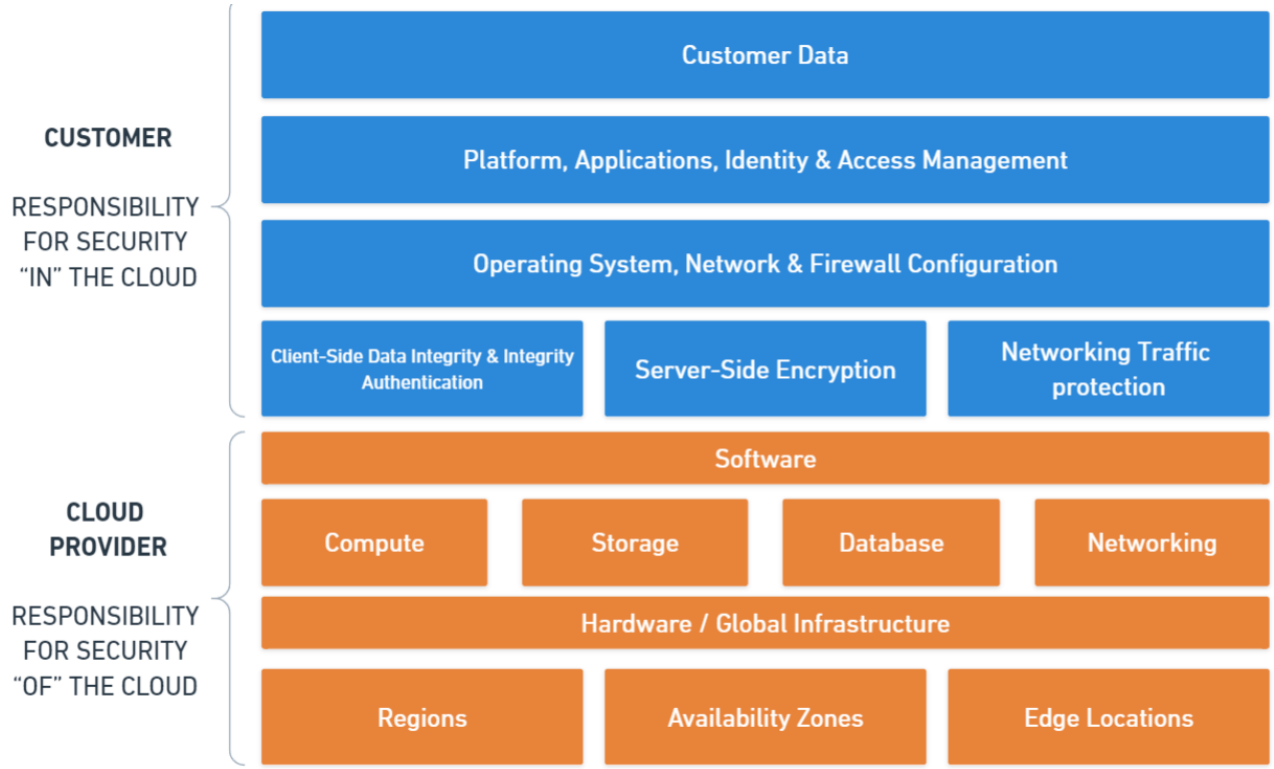

Figure 11. Practical responsibilities in the shared responsibility model (AWS, 2023gj, modified)

The cloud customers technical preparation on the other hand should aim for defining adequate preventing measures, as well as, aim to proactively monitor for indicators of malicious activities and operational deficiencies (Lim et al,. 2021, p. 15), as with particularly internet facing resources in the cloud, it can be easier to make mistakes and getting compromised can happen faster and easier when compared to on-premises environments (Knerler, et al., 2022, p. 226). Especially important in the preparation phase is to establish an understanding of what kind of events and logs are available from especially cloud management, SaaS, and PaaS related services, what does the logging schema look like, how long is the retention period provided by the cloud provider for these events, and to understand what kind of limitations this poses for incident related detection, data gathering, and storage (Lim et al,. 2021, p. 23). Other general actions that can help to prepare for handling incidents in the cloud domain are actions such as reviewing the technical architecture to determine whether any gaps exist, having redundancy in place for critical operations and storage, and to perform regular assessments of vulnerabilities, risk, and threat detection capabilities (Lim et al,. 2021, p. 15).

5.2 Cloud considerations for incident detection and analysis

Detection and analysis phases also have specific considerations when operating in the cloud. Typically, there are three separate domains within the cloud customer's responsibility that incidents can occur. These are the service domain, where the incidents are generally associated with the customers configurations, data, or resource and IAM permissions, the application domain, where the incidents occur in the application code, or in the software deployed on top of the cloud services or infrastructure, and the infrastructure domain, where the incidents happen within the virtualized network, operating system, or container infrastructure (AWS, 2023e, p. 7). These roughly translate to SaaS, PaaS, and IaaS domains, although the service level can be understood to encompass more than just SaaS such as the cloud platform, account, IAM, resource metadata, and billing (AWS, 2023e, p. 5). To efficiently detect and analyze incidents in each of these, the collection of data related to signals, or potential precursors and indicators, should cover the cloud management plane, cloud services specific events, and the deployed virtualized assets (Lim et al,. 2021, p. 19).

Establishing adequate visibility and performing incident analysis requires data and logs. This is also true in the cloud, but especially in the SaaS and PaaS domains, the data collection, detection, and analysis mechanisms typically require different approaches compared to IaaS and on-premises environments (Knerler, et al., 2022, p. 144). For example, in SaaS and PaaS domain related incidents, the incident investigation is unlikely to involve traditional forensics, endpoint protection, or network traffic analysis tools, and the response is mainly going to happen utilizing the clouds control, service, and identity planes where the cloud service and user-based analytics can help determining whether an incident has happened (Knerler, et al., 2022, p. 144). Therefore, collecting telemetry from these planes is essential to efficiently monitor and detect cloud specific indicators and precursors (Knerler, et al., 2022, p. 227). One example of such telemetry is for example Azure Active Directory's risk-based detections, or risky sign-in events as described in the figure 12 below. Other PaaS and SaaS aspects that are essential to monitor, but are not unique to the cloud, rather they are more important when compared to on-premises environments, are scenarios such as monitoring various identity providers and integrations, secrets management and storage, internet facing storage, structured data storage, containers and containers as a service, web infrastructure as a service, and continuous integration and continuous development platforms (Knerler, et al., 2022, p. 228).

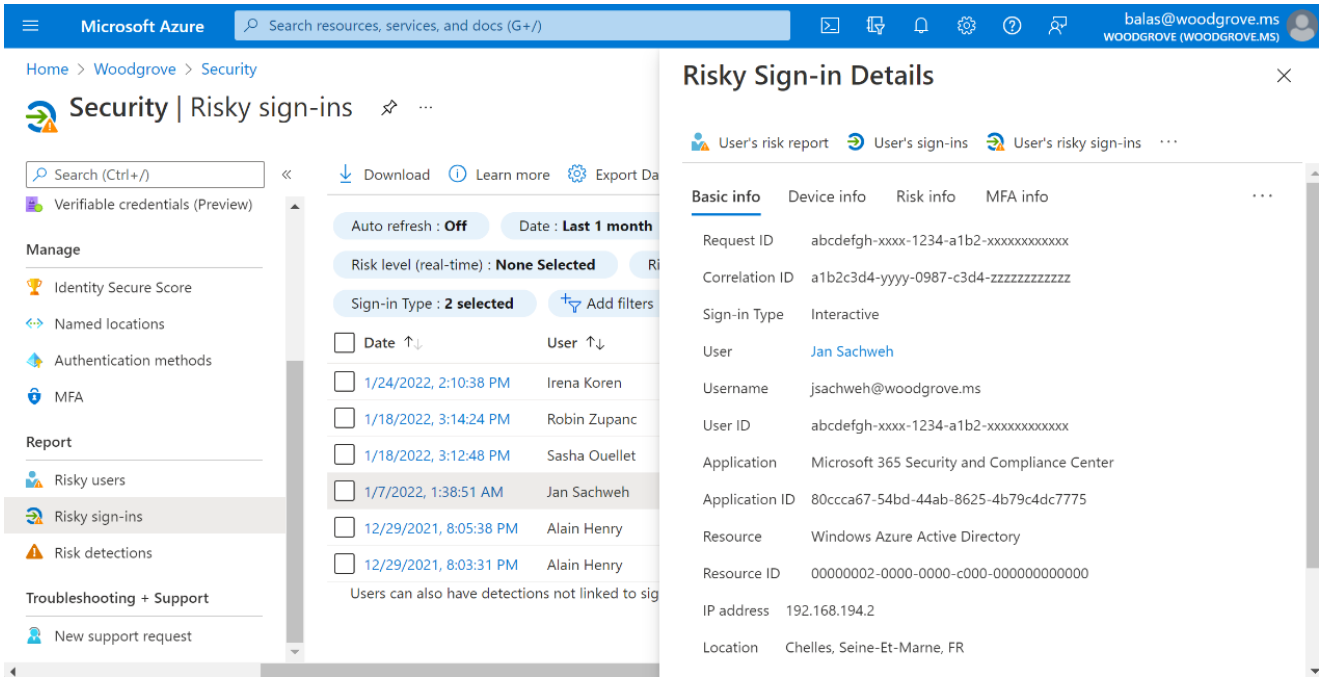

Figure 12. Azure Active Directory risk based detections (Microsoft, 2023bi)

IaaS domain-based incidents on the other hand resemble the most incidents in traditional on-premises environments, and similar approaches from on-premises incident detection and analysis will likely work for IaaS (Knerler, et al., 2022, p. 226). With this domain, the cloud customer has the largest responsibility as per with the shared responsibility model, that also translates to the largest visibility to the security related signals that can be detected and analyzed not only from the cloud management level, but also from the host operating system and network levels (AWS, 2023e, p. 7). Regarding the network level, the clouds distributed asset topology does make network monitoring less effective, and also performing incident analysis at this level may not scale across the disparate cloud resources shifting the focus towards monitoring cloud services and virtualized endpoints (Knerler, et al., 2022, p. 227). Virtualization, as already discussed in chapter 4, is one of the main enablers of modern cloud computing (Malisow, 2020, p. 16), and its characteristics generate specific considerations for incident response. On the other hand, these characteristics can streamline the response actions such as analysis, containment, and recovery as virtual resources can be easily paused, decommissioned, cloned, and recovered utilizing cloud providers security tooling and even native automation (Knerler, et al., 2022, p. 144). On the other hand, the dynamic and ephemeral nature of these resources arising from the cloud elasticity can complicate some response actions such as incident identification and analysis (Knerler, et al., 2022, p. 226). Cloud elasticity, as described below in the figure 13, and also already defined in the chapter 4.1, is one of

the key cloud characteristics and emerges from the automatic scaling of resources based on the load the cloud resources are experiencing.

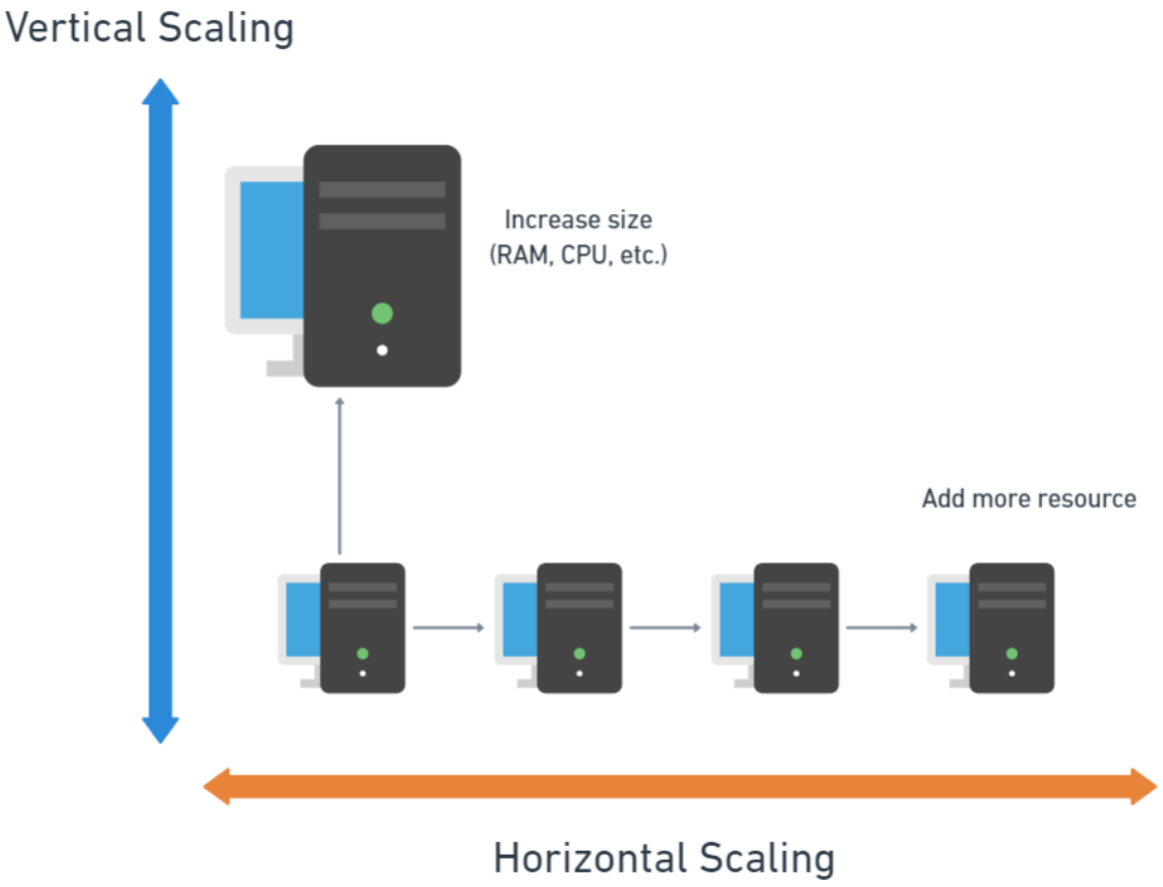

Figure 13. Resource scaling that enables cloud elasticity – Adapted from Piper & Clinton, 2019, p199

5.3 Cloud considerations for incident containment, eradication, and recovery

The containment, eradication, and recovery phases also have specific considerations arising from similar cloud characteristics as with the previous phases, and similarly, the actions may vary depending on whether the incident affects IaaS, PaaS, or SaaS domains. Generally, in the cloud for each of these incident response phases, it is central that the cloud specific architecture, tooling, and platform specific knowledge are understood, and that the cloud characteristics regarding elasticity, automation, and the ease of redeployment are utilized (AWS, 2023e, p. 7). For containment phase, this means utilizing cloud specific tools for isolation such as virtual private networks, secu-

rity groups that control ingress and egress network traffic (AWS, 2023e, p. 6), or the cloud's identity plane to isolate, restrict, or revoke permissions for specific users or service principals (Knerler, et al., 2022, p. 144). In short, the containment actions in the cloud can either focus the incident source, technique and access, or destination containment (AWSe, 2023, p. 29). Also, it is noteworthy to understand that the cloud provider may take actions in response to security incidents that the provider observes that could impact the customers operations, such as suspending accounts or shutting down virtual instances (AWS, 2023e, p. 9).

Eradication on the other hand is similarly to the analysis phase potentially burdened by the dynamic and complex nature of the cloud environment where identifying the root cause of the incident can be challenging due to the ephemeral nature of some cloud resources especially in the IaaS domain (Knerler, et al., 2022, p. 229). For PaaS and SaaS domains, eradication and recovery can be as simple as deactivating accounts or passwords and restoring data from backups (AWS, 2023e, p. 49). Still, once the root cause is sufficiently identified and understood, in the cloud, it is relatively easy to automate the incident remediation and the remediation validation actions compared to the on-premises environments (AWSe, 2023, p. 27). Generally, both eradication and remediation plans in the cloud should utilize and consider the distributed, easily re-deployable, scalable, and elastic nature of the cloud resources (AWSe, 2023, p. 2). Lastly, in the recovery phase, especially when considering the IaaS domain, it is important to understand the impact of the automation capabilities, and cloud storage and backup systems, such as the ability to restore and rebuild virtual machines from snapshots, replicating data and services to new environments (AWS, 2023e, p. 34), or building automated response and alerting flows with for example Microsoft Sentinel and Azure logic apps as described in the figure 14 below.

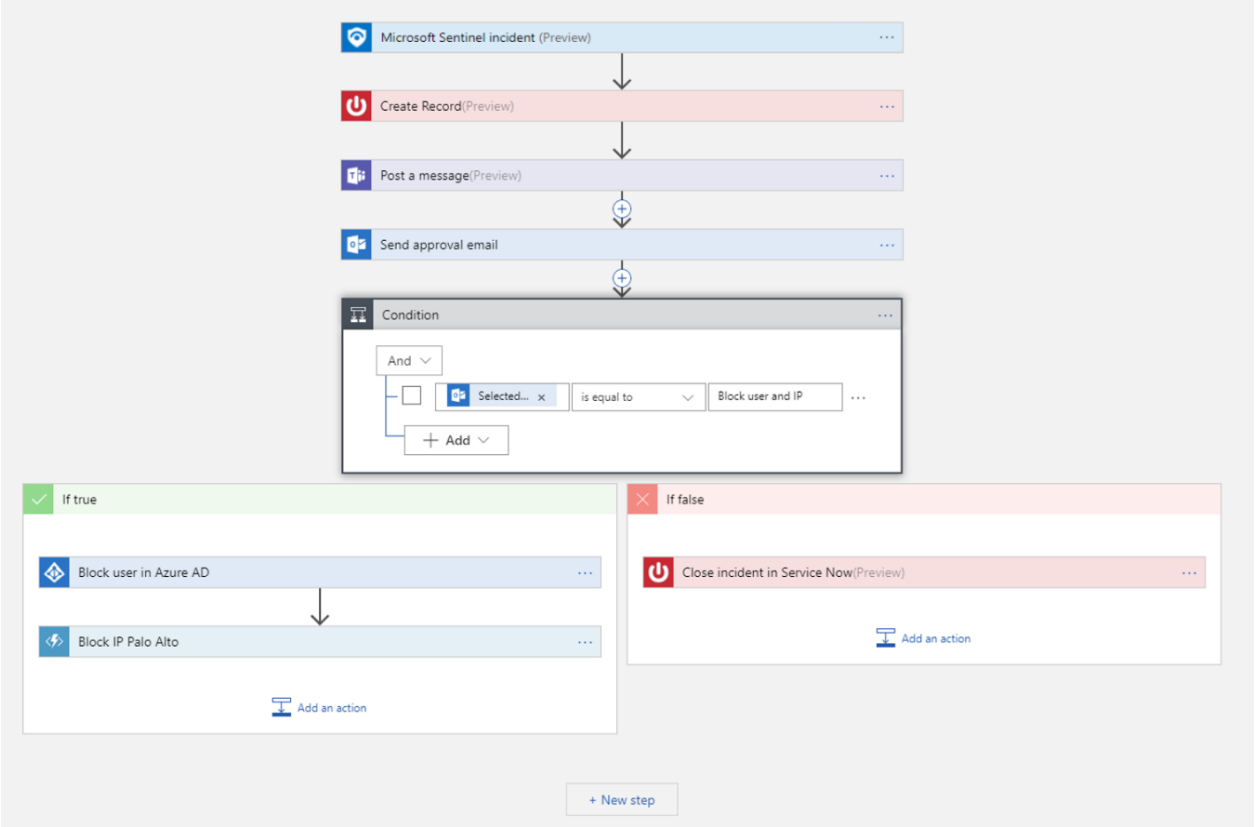

Figure 14. Graphical interface to build automation steps with Azure Logic Apps (Microsoft, 2023bj)

5.4 Cloud considerations for post incident activities

Lastly, the post-incident activities phase, that process-wise focuses on improving the other phases by providing feedback to the preparation phase, is largely platform agnostic since it has a large focus on human reflection (Cichonski et al., 2012 p. 38). Still, some cloud considerations exist that are not specifically unique to the cloud, but nevertheless, they still provide nuanced suggestions to the preparation phase in the cloud domain on how to handle and prevent incidents. In the cloud, for example realistic incident response simulations that provide a structured opportunity to practice the organization incident response plans are relatively easy to run compared to on-premises environments (AWS, 2023e, p. 24). It is however debatable whether simulations actually fall the preparation phase, but nevertheless, simulations can still provide the cloud customer insights to improve both technical and process related deficiencies related to incident response (AWS, 2023e, p. 24). Another interesting consideration for learning from the cloud-based incidents arises from the cloud management and identity plane, where some providers utilize machine learning and automation to identify baselines for what a cloud identity is normally used for, and to determine

how large is the risk that the identity has been compromised (Microsoft, 2023h). This type of utilization of user entity and behavior analytics, or UEBA, is not unique to the cloud, but still, the practices are well adopted by some cloud providers, as they provide an automated way to learn from suspicious and malicious behavior, with the goal to prevent and learn from incidents happening to cloud identities, that can be in many ways considered to be the new security perimeter for organizations (Savill, 2020, p. 95).

6 Capability analysis

This chapter introduces the two cloud providers that the qualitative comparative analysis is focusing on, Microsoft Azure and Amazon Web Services. The chapter also discusses and highlights the requirements that the various cloud products, services, tools, and capabilities have to exhibit to be categorized as having an impact to the different incident response phases.

6.1 Public cloud providers – Microsoft Azure and AWS

The two cloud service providers that the qualitative comparative analysis will focus on are Microsoft's Azure cloud platform, and Amazon Web Services, which is also a subsidiary of Amazon (Gartner, 2022). These cloud providers offer a large and comparable collection of cloud products and services from all the different cloud service models, IaaS, PaaS, and SaaS and from all the different common cloud component categories discussed in chapter 4. They also have a comparable geographical and global reach and operate large data centers around the world (Gartner, 2022).

Generally speaking, AWS is focused on providing a broad selection of cloud services and functionalities and has a diverse customer base with varying sizes, industries, locations, and that are utilizing a broad set of technologies (Gartner, 2022). Compared to Azure, AWS is also more focused on providing services exclusively in the cloud and does not concentrate on providing sales offerings that can be considered to be outside the periphery of what is reasonably considered to be cloud, such as operating system, software, or database licensing (Gartner, 2022). AWS has also typically been an influential forerunner in the overall cloud market where AWS developed technologies and cloud methodologies and models are often copied and reproduced by competing cloud providers (Gartner, 2022).

Azure on the other hand is more suited for Microsoft centric organizations and has an investment focus hybrid and multi-cloud, and its clients tend to be midsize and large enterprises (Gartner, 2022). Azure is only one of the solutions that Microsoft offers in the public cloud space that all can be considered as part of the same Microsoft "ecosystem" that rely on, integrate, and enhance each other's functionalities, and as well with other products within the Microsoft's larger ecosystem, such as their operating systems, security products, and software solutions (Microsoft, 2023m). For example, other Microsoft's cloud product families such as the Microsoft 365, that includes SaaS and SaaS-like capabilities, can integrate, and use Azure specific products for authentication and authorization (Rising, 2020, p.4), but it is not categorically an "Azure offering". These types of overall ecosystem-wide impacts will be considered to ensure that the two platforms are meaningfully compared. This means that some of these products, such as some of the products related to the overall Microsoft's security stack, that are only loosely related to Azure, but are still part of the overall Microsoft's public cloud offerings, can still be included in the analysis if they can be utilized or enhance any of the incident response phases in the Microsoft Azure environment.

6.2 Requirements for products, services, tools, and capabilities

For the preparation phase the goal was to identify cloud capabilities that could be beneficial in the main goals of the preparation phase: to help prevent incidents happening, and also, to prepare the cloud customer to handle incidents. These characteristics relate to being able to develop cyber resiliency that was discussed in the chapter 3.3.1., meaning capabilities that could help the cloud customer to adapt capabilities that could anticipate, recover, withstand, and recover from adverse conditions (Anson, 2020, p. 22). Practically, this means capabilities that could, for example, help with assessing the environment's security posture, implement different types of security controls, manage compliance, and execute various management tasks in the environment. The different requirements and their key characteristics for each incident response phase are described in the table 2 below.

Prepare	Detect	Analyze	Contain	Eradicate	Recover	Post Incident
Requirements: • Help to build controls to both prevent incidents, but also, to help handle incidents • Hardening • Enhance Cyber Resiliency	Requirements: • Help to establish visibility to incident related signals and alerting	Requirements: • Help with the analysis of the incident • Help to determine what has happened and what is the root-cause of the incident	Requirements: • Help with revoking access • Limit, isolate, contain, quarantine the incident	Requirements: • Help with eliminating and removing the root-cause of the incident • Deny attackers access to the environment	Requirements: • Help with restoration • Confirmation of restoration • Improve the environment to better handle similar incidents	Requirements: • Learn from incidents

Table 2. Requirements for potential capabilities in different incident response phases

For the detection phase, the requirements are related to establishing visibility to the cloud environment such as capabilities, services, products, and tools that could help with establishing visibility to the appropriate cloud telemetry, that is, to the various signals such as indicators and precursors for SaaS, PaaS, IaaS, and cloud management plane related incidents. Practically these are services that could provide alerts and other notifications from different technical and non-technical domains and could provide both actionable and contextual sources for security related data and information. Also, the quality and accuracy of the data and information is an important requirement.

For the analysis phase, the requirements for cloud capabilities are that first and foremost, they should be able to help the cloud customer to determine what has happened, and to able to help with incident triage, analysis, and root-cause analysis of incidents, and also the analysis of indicators and precursors of SaaS, PaaS, IaaS, and the cloud management plane related incidents. Practically, this means that the cloud capabilities should ideally be helpful with investigating anomalies, deviations of baselines, data filtering, and event correlation so that the cloud customer could utilize the capabilities to validate, categorize, and evaluate whether an incident has happened, what is the root cause, to which attack lifecycle phase do the signals relate to, what should be done, and what can happen still. So essentially, to be able to answer the questions: What should be contained and how? How can the incident root-cause be eradicated? What is the best way to recover from the incident and restore normal operations?

For the containment phase, the requirements for cloud capabilities are related to the ability to prevent an attacker from performing actions that the cloud customer cannot allow to continue, and to the ability to limit the damages that incident is causing, and to prevent any additional damages from happening. Practically this means being able to utilize cloud capabilities to limit, isolate, contain, revoke, and quarantine the root cause of the cloud-based incident affecting SaaS, PaaS, IaaS, and the cloud management planes.

For the eradication phase, the requirements are related to the ability to eliminate the threat, or the component of the incident from the environment after the root-cause of the incident related to cloud components, services, products, or identities is understood. Practically this means removing or denying the attackers ability to access the environment utilizing cloud-based capabilities and the cloud characteristics such as easily re-deployable, scalable, and elastic infrastructure and environment.

For the recovery phase, the requirements are related to the ability to be able to restore systems, networks, identities, and data to normal operations, and to be able to confirm that they are functioning normally. Also, they should ideally have some capability to improve security controls to prevent similar incidents in the future. Practically this means the ability to be able to utilize cloud characteristics related to the cloud management plane, elasticity, storage, backups, replication, automation, and ease of redeployment for recovery of incidents affecting SaaS, PaaS, IaaS, and the cloud management planes.

For the post-incident phase, the requirements were related to capabilities that the cloud customer could utilize to provide feedback to the preparation phase in order to improve all the incident response phases. This phase emphasizes human reflection and is in many ways platform agnostic, but still, the assessment tried to find ways how the cloud capabilities displaying cloud characteristics could be utilized to learn from cloud bases incidents affecting SaaS, PaaS, IaaS, and the cloud management planes.

Based on these requirements, data and insights were gathered regarding Microsoft Azure and AWS cloud products, services, tools, and capabilities from the cloud providers own documentation, related literature, previous academic research, and also the researchers' own experiences

and knowledge related to these platforms, and were utilized to analyze the data and to identify various cloud capabilities that these two providers offer, and to determine their applicability and practical use-cases to different phases of the NIST's incident response process. The data and insights were collected to appendices 2 and 3 and contain a list of various Microsoft and AWS cloud capabilities and their definitions and features for each of these cloud providers products, services, tools, and capabilities that were identified that could be beneficial in various incident response phases. These appendices also note the initial assumptions on what phase of the incident response process they could be beneficial, or provide input in. The appendix 4 on the other hand then maps them to a specific phase of the incident response process, describes the use-case and how the service, product, or capability could be beneficial in that specific incident response phase based on the data collected earlier regarding the definitions and features, and also utilizing the researchers' own experiences and practical knowledge. These both, meaning the product and service definitions and their applicability and use-cases for each incident response phase were utilized to determine conclusions for the research questions and goals. Also, important to highlight is that 3rd party tools, albeit genuinely useful for incident response for both of these environments, were out-of-scope of the research and capability analysis.

7 Conclusions

The main goals of this thesis were to illuminate complexities related to responding to cyber security incidents in the cloud, and to provide practical guidance on how to prepare, detect, analyze, contain, eradicate, recover, and learn from cloud based cyber security incidents. Two of the research questions were related more generally to incident response in the public cloud domain, and the goal was to highlight and analyze differences in approaches, capabilities, and practical steps from an incident responders' point of view, and differences to incident response in traditional on-premises environments. One research question had a goal of comparing and analyzing different cloud vendors capabilities to assess and highlight different types of incident response capabilities, tooling, approaches, and strategies.

Public cloud environments are complex environments comprising of numerous moving parts and domains and when responding to incidents in the cloud, the incident responders should have a deep understanding of the cloud platform itself, but also what kind of different services they offer, how they can be configured, and what kind of interdependencies they have between them. This

can mean understanding the specific cloud platform, services, access controls, virtualization, containers, storage, network components, and what kind of audit trails and logs these different types of components produce. Generally speaking, the importance of monitoring applications, APIs, and user activities is highlighted in the cloud domain, rather than focusing only on endpoint telemetry or network infrastructure. Also, establishing visibility to the correct telemetry in the cloud plays a crucial role as does understanding the limitations of the visibility to said telemetry with some service models. Especially, the importance of mitigating threats targeting the identity plane is emphasized when comparing the cloud domain to traditional on-premises environments. This comes with no surprise, and as has already been mentioned several times in this thesis, identity is the security perimeter in cloud environments. This means that implementing robust IAM security policies and applying different types of operational and technical preventative and detective control types are essential for mitigating and minimizing risk, and crucial to be able to efficiently perform incident response phases in the cloud.

Varying levels of shared responsibilities of the cloud components also create potential additional complexities for cloud customers to understand regarding for example communication or collaboration with the cloud provider. So does the distributed nature of the cloud environments. Depending on different regulatory or industry requirements, limitations on the data location or sharing may arise that can have implications for data protection, governance, or compliance. These can complicate both incident response planning and actions.

Overall, the threat landscape in the public cloud domain is evolving and moving rapidly, and understanding cloud specific threats, potential vulnerabilities, and common security related misconfigurations are crucial when responding to incidents in the cloud domain. Also, some services may not natively provide adequate tools to protect against the latest threats, and the idiosyncratic nature of incidents can make it hard to both prevent and prepare to handle incidents in the cloud. When responding to incidents arising from these threats, the tools and services that exhibit, utilize, and take advantage of the cloud characteristics are ideal for different incident response phases in the cloud, that is, the response actions are preferably done utilizing the cloud. Also, understanding the implications of these characteristics is crucial for the success of incident response phases. This is apparent when looking at for example virtualization that enables a highly dynamic environment, but simultaneously, ephemeral, and short living resources can make determining

the root-cause of the incident harder. Also, traditional tools to analyze host-based incidents do not necessary scale well with virtualized large-scale and distributed cloud deployments. Another example would be automation capabilities in the cloud that can streamline response actions, such as backup and recovery, if the cloud customers utilize and configure these automatically scalable cloud solutions properly.

In the comparative analysis the goal was to identify various Amazon Web Services and Microsoft Azure services and products, and their potential use cases for various incident response phases. With some services the identification was clearer than others, such as with products and services that had a clear role in providing security to the cloud and the cloud workloads. In most cases, especially when it came to security related tooling, the researcher had a good view of how a specific tool could be utilized, and what kind of potential use cases there might be. Some observations were made based on the service or product descriptions, and some from the incident response related best practices documentation provided by the cloud provider (if there was any). When a service was identified from one provider, it was relatively easy to determine whether a similar capability existed with the other. This shows practically that knowledge of one cloud provider's environment is easily carried over to another because the practices and models are fairly similar. Implementations and capabilities on the other hand vary.

Microsoft is a large player in the overall security software market and also operates as specifically a security product vendor. In the researcher's opinion, based on the collected data, their security related products and product suites, such as Microsoft Sentinel or different Microsoft Defender suites and products have a clearer branding when compared to AWS security tools, have a broader set of use-cases, and extend well beyond just the security context of cloud environments. These suites also seemed to be the most versatile out of all of the assessed tools, and use-cases were observed for all different incident response phases. Microsoft also seems to have a stronger SaaS presence and offerings, and clearly plays to their strengths so that their customers can benefit from their extended ecosystem. Their tools are also potentially more mature to help customers to handle identity related incidents, although the AWS tools are also perfectly capable at this.

AWS on other hand seems to have a stronger presence and are potentially more mature in the IaaS and PaaS domains and have a clearer documentation on how their tools in these domains

could be utilized to benefit from the cloud characteristics when it comes to incident response. The identification of non-security related services for various incident response phases was also relatively easier, since AWS has a good and up-to-date documentation on specifically how to prepare and perform incident response in their environment. Also, although their security related products are capable of providing incident responders with adequate tooling to handle incidents in AWS, they seem acknowledge better that not everyone can or want to do everything with their tools and have potentially developed and documented more ways integrate services and products with third party security related tooling, even to Microsoft products. However, third party tools were out-of-scope of this thesis, as was analyzing the impact of combining different cloud providers tools i.e., utilizing multi-cloud deployments.

For some services and capabilities, the identification of use-cases for incident response phases was easier than for others. Especially the requirements for the preparation and the post-incident phases did leave a lot for interpretation, and there was a thin-line to which phase a use-case should be counted to belong. When considering the preparation phase requirements, and especially the requirement “prevent incidents from happening”, one could argue that this could be applied to any service or product as there are always ways to harden the environment by adhering to best practices, benchmarks, or frameworks, or by applying any type of preventative controls. However, the NIST framework also highlights that incident prevention, even though important, is not generally the main focus of the preparation phase as it rarely falls under the responsibility of people responding to incidents. Still, some preventative use-cases were observed and listed, but the goal was to identify cloud services that were more useful in providing holistic approaches and capabilities for hardening, security best practices, and enhancing the overall cyber resiliency of the environment.

Regarding detection and analysis, both platforms provide similar capabilities but based on the observed use-cases, the Microsoft security product suites seem to be more versatile that can make the response actions more streamlined and efficient to execute when compared to AWS security products and tools. The same seems to be true for the containment, eradication, and recovery phases, although in the recovery phase, more use-cases were observed for AWS services. For the post-incident phase some potential use cases were observed, but as mentioned, the phase focuses on reflection and learning, so similarly to the preparation phase, a lot is left to interpretation and

the validity of these use-cases is debatable. The table 3 below lists the number of services and products that were identified to be beneficial to each phase of the incident response cycle.

IR-Phase	Microsoft	AWS
Preparation	30	24
Detection	32	18
Analysis	27	27
Containment	16	15
Eradication	14	14
Recovery	19	24
Post-Incident	7	2

Table 3. The number of identified services for each incident response phase

Overall, based on the collected data, both vendors provide mature tools to prevent, handle, detect, analyze, contain, eradicate, and recover from incidents that are affecting their cloud services and the cloud management plane. They both have similar offerings when it comes to common cloud components, but slightly different tools and purposes for their cloud-based security specific products and services. Not necessarily all potential cloud services or products, or their potential use-cases for incident response were identified, but in the researchers view, at least the most usual and typical services and their use-cases were listed for both cloud environments. Some edge cases may require other tools to be utilized. Also, during the research, a large amount of data regarding various services and their use-cases were gathered that can provide practical guidance on how to utilize these cloud services for incident response. This was also one of the main goals of this thesis. The researcher also did not have unlimited time to test all of the cloud products in real-life incident response scenarios, and capturing all potential use-cases for various services and phases would require either data or firsthand experience on handling incidents on all different

cloud components, which is not a realistic scenario nor a research topic. As stated before, incidents are by nature idiosyncratic and threat actors are constantly trying to find new and innovative ways to exploit cloud services. This is even more true as the cloud becomes more and more widespread and prevalent. Still, the collected data and insights can help with establishing better understanding of different ways to utilize different cloud products, and the cloud considerations for each phase can help guide response actions in the cloud.

Finally, regarding the reliability and validity of the research analysis, several methods were considered during the research such as reflexivity, or the constant evaluation of researchers' subjectivity when analyzing different phenomena, frameworks, models, and cloud vendors and their products. Reflexivity was considered several times during the research, and the research tried not to specifically highlight any of the products or services provided by the cloud vendors just for the sake of promotion, but rather to research and analyze the phenomena that led to their creation and utilization. There were also ethical reasons for the research not to promote any particular vendor or service, and the goal was not to evaluate any subjective or objective superiority, but rather try to analyze what kind of approaches these vendors have taken to help their customers to secure their cloud environments to produce practical insights of different types of incident response capabilities, approaches, and strategies. The researcher also tried being as impartial as possible, and to utilize various different data sources especially for AWS products and services as the researcher has more practical experience working with incidents in and with Microsoft cloud products. When evaluating a cloud service that the researcher did not have hands-on incident response experience with, nor any potential way to test the hypothesis on a potential use-case for incident response, the goal was to utilize triangulation and utilize multiple data sources to verify that the assumptions that were made based on the providers own descriptions were accurate and reflected reality.

References

AT&T Cybersecurity. AlienVault – Insider's guide to incident response. (2015). Retrieved from https://cybersecurity.att.com/resource-center/ebook/insider-guide-to-incident-response/incident-response-tools

AWS. (2023a). AWS CloudFormation Documentation. Retrieved April 11, 2023, from https://docs.aws.amazon.com/cloudformation/index.html

AWS. (2023b). AWS Config Documentation. Retrieved April 11, 2023, from https://docs.aws.amazon.com/config/index.html

AWS. (2023c). AWS Firewall Manager. Retrieved April 11, 2023, from https://docs.aws.amazon.com/waf/latest/developerguide/fms-chapter.html

AWS. (2023d). AWS Global Infrastructure. Retrieved February 25, 2023, from https://aws.amazon.com/about-aws/global-infrastructure/

AWS. (2023e). AWS Security Incident Response Guide. Retrieved from https://docs.aws.amazon.com/pdfs/whitepapers/latest/aws-security-incident-response-guide/aws-security-incident-response-guide.pdf

AWS. (2023f). AWS Trusted Advisor. Retrieved April 12, 2023, from https://docs.aws.amazon.com/awssupport/latest/user/trusted-advisor.html

AWS. (2023g). AWS WAF. Retrieved April 12, 2023, from https://docs.aws.amazon.com/waf/latest/developerguide/waf-chapter.html

AWS. (2023h). Alert sources. Retrieved April 12, 2023, from https://docs.aws.amazon.com/whitepapers/latest/aws-security-incident-response-guide/alert-sources.html

AWS. (2023i). Amazon Athena. Retrieved April 11, 2023, from https://aws.amazon.com/athena/

AWS. (2023j). Amazon Detective Documentation. Retrieved April 11, 2023, from https://docs.aws.amazon.com/detective/?icmpid=docs_homepage_security

AWS. (2023k). Amazon EBS snapshots. Retrieved April 11, 2023, from https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSSnapshots.html

AWS. (2023l). Amazon Elastic Block Store (Amazon EBS). Retrieved April 11, 2023, from https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AmazonEBS.html

AWS. (2023m). Amazon Inspector Documentation. Retrieved April 11, 2023, from https://docs.aws.amazon.com/inspector/index.html

AWS. (2023n). Amazon OpenSearch Service introduces security analytics. Retrieved April 12, 2023, from https://aws.amazon.com/about-aws/whats-new/2023/03/amazon-opensearch-service-security-analytics/

AWS. (2023o). Amazon RDS and Aurora Documentation. Retrieved April 11, 2023, from https://docs.aws.amazon.com/rds/index.html

AWS. (2023p). Automate incident response and forensics. Retrieved April 11, 2023, from https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/automate-incident-response-and-forensics.html

AWS. (2023q). Automation. Retrieved April 12, 2023, from https://docs.aws.amazon.com/whitepapers/latest/aws-security-incident-response-guide/automation-1.html

AWS. (2023r). Backup and recovery using AWS Backup. Retrieved April 11, 2023, from https://docs.aws.amazon.com/prescriptive-guidance/latest/backup-recovery/aws-backup.html

AWS. (2023s). Benefits of AWS Security Hub. Retrieved April 11, 2023, from https://docs.aws.amazon.com/securityhub/latest/userguide/securityhub-benefits.html

AWS. (2023t). Custom. Retrieved April 12, 2023, from https://docs.aws.amazon.com/whitepapers/latest/aws-security-incident-response-guide/custom.html

AWS. (2023u). Destination containment. Retrieved April 12, 2023, from https://docs.aws.amazon.com/whitepapers/latest/aws-security-incident-response-guide/destination-containment.html

AWS. (2023v). Detection as part of security control engineering. Retrieved April 11, 2023, from https://docs.aws.amazon.com/whitepapers/latest/aws-security-incident-response-guide/detection-as-security-control-engineering.html

AWS. (2023w). How AWS Shield works. Retrieved April 12, 2023, from https://docs.aws.amazon.com/waf/latest/developerguide/ddos-overview.html

AWS. (2023x). How AWS WAF works. Retrieved April 12, 2023, from https://docs.aws.amazon.com/waf/latest/developerguide/how-aws-waf-works.html

AWS. (2023y). Logging and events. Retrieved April 11, 2023, from https://docs.aws.amazon.com/whitepapers/latest/aws-security-incident-response-guide/logging-and-events.html

AWS. (2023z). Six advantages of cloud computing. Retrieved February 25, from https://docs.aws.amazon.com/whitepapers/latest/aws-overview/six-advantages-of-cloud-computing.html

AWS. (2023aa). Understand AWS response teams and support. Retrieved April 12, 2023, from https://docs.aws.amazon.com/whitepapers/latest/aws-security-incident-response-guide/understand-aws-response-teams-and-support.html

AWS. (2023ab). Visibility and alerting. Retrieved April 11, 2023, from https://docs.aws.amazon.com/whitepapers/latest/aws-security-incident-response-guide/visibility-and-alerting.html

AWS. (2023ac). What Is AWS CloudTrail? Retrieved April 11, 2023, from https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-user-guide.html

AWS. (2023ad). What Is AWS Config? Retrieved April 11, 2023, from https://docs.aws.amazon.com/config/latest/developerguide/WhatIsConfig.html

AWS. (2023ae). What Is Amazon EventBridge? Retrieved April 11, 2023, from https://docs.aws.amazon.com/eventbridge/latest/userguide/eb-what-is.html

AWS. (2023af). What Is Amazon S3 Glacier? Retrieved April 11, 2023, from https://docs.aws.amazon.com/amazonglacier/latest/dev/introduction.html

AWS. (2023ag). What Is Amazon SageMaker? Retrieved April 12, 2023, from https://docs.aws.amazon.com/sagemaker/latest/dg/whatis.html

AWS. (2023ah). What Is Service Catalog. Retrieved April 11, 2023, from https://docs.aws.amazon.com/servicecatalog/latest/adminguide/introduction.html

AWS. (2023ai). What is AWS Billing? Retrieved April 11, 2023, from https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/billing-what-is.html

AWS. (2023aj). What is AWS Elastic Beanstalk? Retrieved April 11, 2023, from https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/Welcome.html

AWS. (2023ak). What is AWS Lambda? Retrieved April 11, 2023, from https://docs.aws.amazon.com/lambda/latest/dg/welcome.html

AWS. (2023al). What is AWS Organizations? Retrieved April 11, 2023, from https://docs.aws.amazon.com/organizations/latest/userguide/orgs_introduction.html

AWS. (2023am). What is AWS Security Hub? Retrieved April 11, 2023, from https://docs.aws.amazon.com/securityhub/latest/userguide/what-is-securityhub.html

AWS. (2023an). What is AWS Step Functions? Retrieved April 12, 2023, from https://docs.aws.amazon.com/step-functions/latest/dg/welcome.html

AWS. (2023ao). What is AWS Systems Manager? Retrieved April 12, 2023, from https://docs.aws.amazon.com/systems-manager/latest/userguide/what-is-systems-manager.html

AWS. (2023ap). What is AWS Well-Architected Tool? Retrieved April 12, 2023, from https://docs.aws.amazon.com/wellarchitected/latest/userguide/intro.html

AWS. (2023aq). What is Amazon CloudWatch? Retrieved April 11, 2023, from https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/WhatIsCloudWatch.html

AWS. (2023ar). What is Amazon Detective? Retrieved April 11, 2023, from https://docs.aws.amazon.com/detective/latest/adminguide/what-is-detective.html

AWS. (2023as). What is Amazon EMR? Retrieved April 12, 2023, from https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-what-is-emr.html

AWS. (2023at). What is Amazon GuardDuty? Retrieved April 11, 2023, from https://docs.aws.amazon.com/guardduty/latest/ug/what-is-guardduty.html

AWS. (2023au). What is Amazon Inspector? Retrieved April 11, 2023, from https://docs.aws.amazon.com/inspector/latest/user/what-is-inspector.html

AWS. (2023av). What is Amazon Macie? Retrieved April 11, 2023, from https://docs.aws.amazon.com/macie/latest/user/what-is-macie.html

AWS. (2023aw). What is Amazon OpenSearch Service? Retrieved April 12, 2023, from https://docs.aws.amazon.com/opensearch-service/latest/developerguide/what-is.html

AWS. (2023ax). What is Amazon QuickSight? Retrieved April 12, 2023, from https://docs.aws.amazon.com/quicksight/latest/user/welcome.html

AWS. (2023ay). What is Amazon S3? Retrieved April 11, 2023, from https://docs.aws.amazon.com/AmazonS3/latest/userguide/Welcome.html

AWS. (2023az). What is Amazon SNS? Retrieved April 11, 2023, from https://docs.aws.amazon.com/sns/latest/dg/welcome.html

AWS. (2023ba). What is Amazon VPC? Retrieved April 12, 2023, from https://docs.aws.amazon.com/vpc/latest/userguide/what-is-amazon-vpc.html

AWS. (2023bb). What is Elastic Disaster Recovery? Retrieved April 11, 2023, from https://docs.aws.amazon.com/drs/latest/userguide/what-is-drs.html

AWS. (2023bc). What is IAM? Retrieved April 11, 2023, from https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html

AWS. (2023bd). AWS Cloud Essentials. Retrieved March 4, from https://aws.amazon.com/getting-started/cloud-essentials

AWS. (2023be). What is AWS X-Ray? Retrieved April 14, 2023, from https://docs.aws.amazon.com/xray/latest/devguide/aws-xray.html

AWS. (2023bf). Amazon GuardDuty Features. Retrieved April 15, 2023, from https://aws.amazon.com/guardduty/features

AWS. (2023bg). What is Amazon Route 53? Retrieved April 15, 2023, from https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/Welcome.html

AWS. (2023bh). AWS OpsWorks. Retrieved April 16, 2023, from https://aws.amazon.com/opsworks/

AWS. (2023bi). What is Amazon EC2? Retrieved April 16, 2023, from https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/concepts.html

AWS. (2023bj). Shared Responsibility Model. Retrieved April 18, 2023, from https://aws.amazon.com/compliance/shared-responsibility-model/

Anson, S. (2020). Applied incident response. John Wiley & Sons.

Binnie, C. & McCune, R. (2021). Cloud native security. John Wiley & Sons.

Carter, N., Bryant-Lukosius, D., DiCenso, A., Blythe, J., & Neville, A. (2014). The use of triangulation in qualitative research. Oncology Nursing Forum, 5. Retrieved from https://doi.org./10.1188/14.ONF.545-547

Chapple, M. (2020). CompTIA CYSA+ Study Guide CS0-002. John Wiley & Sons.

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology (NIST SP 800-61r2). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-61r2

Copeland, M. & Jabobs, M. (2021). Cyber security on Azure: an it professional's guide to Microsoft Azure security. Apress.

Copeland, M. (2017). Cyber Security on Azure. Apress. https://doi.org/10.1007/978-1-4842-2740-4

Davis, J. (2007, August 21). Hackers Take Down the Most Wired Country in Europe. Wired. https://www.wired.com/2007/08/ff-estonia/

Gartnes. Magic Quadrant for Cloud Infrastructure and Platform Services. (2022). Retrieved from https://www.gartner.com/doc/reprints?id=1-2AOZQAQL&ct=220728&st=sb&refid=d655fed1-d452-405a-8dc6-682ee5154f83

Greenberg, A. (2018, August 22). The Untold Story of NotPetya, the Most Devastating Cyberat-tack in History. Wired. https://www.wired.com/story/notpetya-cyberattack-ukraine-rus-sia-code-crashed-the-world/

Hill, M. (2022, September 12). The 12 biggest data breach fines, penalties, and settlements so far. CSO. https://www.csoonline.com/article/3410278/the-biggest-data-breach-fines-penalties-and-settlements-so-far.html

Johansen, G. (2017). Digital forensics and incident response. Packt Publishing.

Kaspersky ICS CERT. (2021, May 21). DarkChronicles: the consequences of the Colonial Pipeline at-tack. Retrieved from https://ics-cert.kaspersky.com/publications/re-ports/2021/05/21/darkchronicles-the-consequences-of-the-colonial-pipeline-attack/

Knerler, K., Parker, I., & Zimmerman, C. (2022). 11 Strategies of a World-Class Cybersecurity Oper-ations Center. The MITRE corporation.

Kral, P. (2012). Incident Handler's Handbook. Sans Institute.

Lim, S.T., Siow, A., Leong, R., Roza, M., & Vandendriessche, S. (2021). Cloud Incident Response framework. Cloud Security Alliance CSA.

Luttgens, J., Pepe, M., & Mandia, K. (2014). Incident response & computer forensics. McGraw-Hill Education.

Malisow, B. (2020). (ISC)2® CCSP® Certified Cloud Security Professional: Official Study Guide. John Wiley & Sons.

Mell, P. & Grance, T. (2011). The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology (NIST SP 800-145). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-145

Meyers, M. (2018). Mike Meyers' CompTIA Security+ certification guide 2nd edition. McGraw-Hill Education.

Microsoft. (2023a). About Site Recovery. Retrieved April 11, 2023, from https://learn.microsoft.com/en-us/azure/site-recovery/site-recovery-overview

Microsoft. (2023b). Achieve high availability with Azure Cosmos DB. Retrieved April 11, 2023, from https://learn.microsoft.com/en-us/azure/cosmos-db/high-availability

Microsoft. (2023c). App governance add-on to Defender for Cloud Apps in Microsoft 365 Defender. Retrieved April 11, 2023, from https://learn.microsoft.com/en-us/defender-cloud-apps/app-governance-manage-app-governance

Microsoft. (2023d). Azure global infrastructure. Retrieved from https://azure.microsoft.com/en-us/explore/global-infrastructure/

Microsoft. (2023e). Azure support. Retrieved April 11, 2023, from https://azure.microsoft.com/en-us/support

Microsoft. (2023f). Compare security features in Microsoft 365 plans for small and medium-sized businesses. Retrieved April 11, 2023, from https://learn.microsoft.com/en-us/microsoft-365/security/defender-business/compare-mdb-m365-plans?view=o365-worldwide

Microsoft. (2023g). Compare support plans. Retrieved April 12, 2023, from https://azure.microsoft.com/en-us/support/plans/

Microsoft. (2023h). Configure and enable risk policies. Retrieved from https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-risk-policies

Microsoft. (2023i). Introduction to Azure Advisor. Retrieved April 11, 2023, from https://learn.microsoft.com/en-us/azure/advisor/advisor-overview

Microsoft. (2023j). Introduction to Azure Functions. Retrieved April 11, 2023, from https://learn.microsoft.com/en-us/azure/azure-functions/functions-overview

Microsoft. (2023k). Learn about data loss prevention Retrieved April 11, 2023, from https://learn.microsoft.com/en-us/microsoft-365/compliance/dlp-learn-about-dlp?view=o365-worldwide

Microsoft. (2023l). Log Analytics workspace overview. Retrieved April 11, 2023, from https://learn.microsoft.com/en-us/azure/azure-monitor/logs/log-analytics-workspace-overview

Microsoft. (2023m). Microsoft Cloud. Retrieved from https://www.microsoft.com/en-us/microsoft-cloud

Microsoft. (2023n). Microsoft Defender for Cloud Apps overview. Retrieved April 11, 2023, from https://learn.microsoft.com/en-us/defender-cloud-apps/what-is-defender-for-cloud-apps

Microsoft. (2023o). Microsoft Defender for Endpoint. Retrieved April 11, 2023, from https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-endpoint?view=o365-worldwide(2023).

Microsoft. (2023p). Microsoft Defender for Office 365 security product overview. Retrieved April 11, 2023, from https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/microsoft-defender-for-office-365-product-overview?view=o365-worldwide

Microsoft. (2023q). Network security groups. Retrieved April 11, 2023, from https://learn.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview

Microsoft. (2023r). Overview of Defender for App Service to protect your Azure App Service web apps and APIs. Retrieved April 11, 2023, from https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-app-service-introduction

Microsoft. (2023s). Overview of Log Analytics in Azure Monitor. Retrieved April 11, 2023, from https://learn.microsoft.com/en-us/azure/azure-monitor/logs/log-analytics-overview

Microsoft. (2023t). Overview of Microsoft Defender for Azure SQL. Retrieved April 11, 2023, from https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-sql-introduction

Microsoft. (2023u). Overview of Microsoft Defender for Containers. Retrieved April 11, 2023, from https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-containers-introduction

Microsoft. (2023v). Overview of Microsoft Defender for DNS. Retrieved April 11, 2023, from https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-dns-introduction

Microsoft. (2023w). Overview of Microsoft Defender for Key Vault. Retrieved April 11, 2023, from https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-key-vault-introduction

Microsoft. (2023x). Overview of Microsoft Defender for Resource Manager. Retrieved April 11, 2023, from https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-resource-manager-introduction

Microsoft. (2023y). Overview of Microsoft Defender for Storage. Retrieved April 11, 2023, from https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-storage-introduction

Microsoft. (2023z). Overview of Microsoft Defender for open-source relational databases. Retrieved April 11, 2023, from https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-databases-introduction

Microsoft. (2023aa). Plan your Defender for Servers deployment. Retrieved April 11, 2023, from https://learn.microsoft.com/en-us/azure/defender-for-cloud/plan-defender-for-servers

Microsoft. (2023ab). Risk Assessment Guide for Microsoft Cloud. Retrieved from https://learn.microsoft.com/en-us/compliance/assurance/assurance-risk-assessment-guide

Microsoft. (2023ac). Update Management overview Retrieved April 11, 2023, from https://learn.microsoft.com/en-us/azure/automation/update-management/overview

Microsoft. (2023ad). Virtual machines in Azure. Retrieved April 11, 2023, from https://learn.microsoft.com/en-us/azure/virtual-machines/overview

Microsoft. (2023ae). Welcome to Azure Cosmos DB. Retrieved April 11, 2023, from https://learn.microsoft.com/en-us/azure/cosmos-db/introduction

Microsoft. (2023af). What are Azure management groups? Retrieved April 11, 2023, from https://learn.microsoft.com/en-us/azure/governance/management-groups/overview

Microsoft. (2023ag). What is Azure Active Directory? Retrieved April 11, 2023, from https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-whatis

Microsoft. (2023ah). What is Azure Automation? Retrieved April 11, 2023, from https://learn.microsoft.com/en-us/azure/automation/overview

Microsoft. (2023ai). What is Azure Blob storage? Retrieved April 11, 2023, from https://learn.microsoft.com/en-us/azure/storage/blobs/storage-blobs-overview

Microsoft. (2023aj). What is Azure DDoS Protection? Retrieved April 11, 2023, from https://learn.microsoft.com/en-us/azure/ddos-protection/ddos-protection-overview

Microsoft. (2023ak). What is Azure DevOps? Retrieved April 11, 2023, from https://learn.microsoft.com/en-us/azure/devops/user-guide/what-is-azure-devops?view=azure-devops

Microsoft. (2023al). What is Azure Firewall Manager? Retrieved April 11, 2023, from https://learn.microsoft.com/en-us/azure/firewall-manager/overview

Microsoft. (2023am). What is Azure Information Protection? Retrieved April 11, 2023, from https://learn.microsoft.com/en-us/azure/information-protection/what-is-information-protection

Microsoft. (2023an). What is Azure Logic Apps? Retrieved April 11, 2023, from https://learn.microsoft.com/en-us/azure/logic-apps/logic-apps-overview

Microsoft. (2023ao). What is Azure Network Watcher? Retrieved April 11, 2023, from https://learn.microsoft.com/en-us/azure/network-watcher/network-watcher-monitoring-overview

Microsoft. (2023ap). What is Azure Policy? Retrieved April 11, 2023, from https://learn.microsoft.com/en-us/azure/governance/policy/overview

Microsoft. (2023aq). What is Azure Resource Manager? Retrieved April 11, 2023, from https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/overview

Microsoft. (2023ar). What is Azure Virtual Network? Retrieved April 11, 2023, from https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview

Microsoft. (2023as). What is Azure Web Application Firewall on Azure Application Gateway? Retrieved April 11, 2023, from https://learn.microsoft.com/en-us/azure/web-application-firewall/ag/ag-overview

Microsoft. (2023at). What is Identity Protection? Retrieved April 11, 2023, from https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection

Microsoft. (2023au). What is Microsoft 365 Defender? Retrieved April 11, 2023, from https://learn.microsoft.com/en-us/microsoft-365/security/defender/microsoft-365-defender?view=o365-worldwide

Microsoft. (2023av). What is Microsoft Defender Threat Intelligence (Defender TI)? Retrieved April 11, 2023, from https://learn.microsoft.com/en-us/defender/threat-intelligence/what-is-microsoft-defender-threat-intelligence-defender-ti

Microsoft. (2023aw). What is Microsoft Defender Vulnerability Management. Retrieved April 11, 2023, from https://learn.microsoft.com/en-us/microsoft-365/security/defender-vulnerability-management/defender-vulnerability-management?view=o365-worldwide

Microsoft. (2023ax). What is Microsoft Defender for Cloud? Retrieved April 11, 2023, from https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-cloud-introduction

Microsoft. (2023ay). What is Microsoft Defender for Identity? Retrieved April 11, 2023, from https://learn.microsoft.com/en-us/defender-for-identity/what-is(2023).

Microsoft. (2023az). What is Microsoft Sentinel? Retrieved April 11, 2023, from https://learn.microsoft.com/en-us/azure/sentinel/overview

Microsoft. (2023ba). What is Traffic Manager? Retrieved April 11, 2023, from https://learn.microsoft.com/en-us/azure/traffic-manager/traffic-manager-overview

Microsoft. (2023bb). What is the Azure Backup service? Retrieved April 11, 2023, from https://learn.microsoft.com/en-us/azure/backup/backup-overview

Microsoft, (2023bc). Azure Monitor overview. Retrieved April 11, 2023, from https://learn.microsoft.com/en-us/azure/azure-monitor/overview

Microsoft, (2023bd). Resource Health overview. Retrieved April 11, 2023, from https://learn.microsoft.com/en-us/azure/service-health/resource-health-overview

Microsoft, (2023be). Microsoft Azure Well-Architected Framework. Retrieved April 11, 2023, from https://learn.microsoft.com/en-us/azure/architecture/framework

Microsoft. (2023bf). What is Microsoft Cost Management and Billing? Retrieved April 11, 2023, from https://learn.microsoft.com/en-us/azure/cost-management-billing/cost-management-billing-overview

Microsoft. (2023bg). How does Azure work? Retrieved from https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/get-started/what-is-azure

Microsoft. (2023bh). Introduction to Azure security. Retrieved April 17, 2023, from https://learn.microsoft.com/en-us/azure/security/fundamentals/overview

Microsoft. (2023bi). How To: Investigate risk. Retrieved April 18, 2023, from https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-investigate-risk

Microsoft. (2023bj). Tutorial: Use playbooks with automation rules in Microsoft Sentinel. Retrieved April 18, 2023, from https://learn.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook?tabs=LAC%2Cincidents

Montgomery, T. & Olson, S. (2018). CompTIA Cloud+ study guide 2nd edition. John Wiley & Sons.

Mukhejee, A. (2021). AWS All-in-one Security Guide. BPB Publication.

Olmos-Vega, F., Stalmeijer, R., Varpio, L., & Kahlke, R. (2022). A practical guide to reflexivity in qualitative research. Medical teacher, 149. Retrieved from https://doi.org/10.1080/0142159X.2022.2057287

Pinsker, B. (2014, January 14). Consumers vent frustration and anger at Target data breach. Reuters. https://www.reuters.com/article/us-target-consumers-idUSBREA0D01Z20140114

Piper, B. & Clinton, D. (2019). AWS Certified Cloud Practitioner: Study Guide CLF-C01 Exam. John Wiley & Sons.

Piper, B. & Clinton, D. (2019). AWS Certified Solutions Architect: Study guide Associate SAA-C01 Exam 2nd edition. John Wiley & Sons.

Rising, P. (2020). Microsoft 365 Security Administration: MS-500 Exam guide. Packt Publishing.

Roberts, S., & Brown, R. (2017). Intelligence-driven incident response: outwitting the adversary. O'Reilly.

SFS ISO/IEC 27035. (2016). Information technology – Security techniques – Information security incident management – Part1: Principles of incident management. SFS Online.

SFS ISO/IEC 27035. (2016). Information technology – Security techniques – Information security incident management – Part2: Guidelines to plan and prepare for incident response. SFS Online.

Salfati, E. & Pease, M. (2022). Digital forensics and Incident response framework for Operational Technology. NIST Interagency/Internal Report (NISTIR) – 8428. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8428

Sandtström, A.M. (2018, April 19). 8 ways to determine the credibility of research reports [Blog post]. Retrieved from https://www.eaie.org/blog/8-ways-determine-credibility-research-reports.html

Savill. J. (2020). Microsoft Azure Infrastructure Services for Architects: Designing Cloud Solutions. John Wiley & Sons.

Svahn, N. & Karppi, T. (2021, February 11). Tietomurron kohteeksi joutunut psykoterapiakeskus Vastaamo on haettu konkurssiin. YLE. https://yle.fi/a/3-11784072

Tesch, R. (1990). Qualitative research: analysis types and software tools. Falmer.

Toropainen, P. (2020). Utilizing Cyber Security Kill Chain model to improve SIEM capabilities. [Master's thesis, Jyväskylän ammattikorkeakoulu]. https://urn.fi/URN:NBN:fi:amk-2020060316624

Turton, W. & Mehrotra, K. (2021, June 4). Hackers Breached Colonial Pipeline Using Compromised Password. Bloomgberg. https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password?leadSource=uverify%20wall

Umawing, J. (2023, February 7). Florida hospital takes entire IT systems offline after 'ransomware attack'. Malwarebytes. https://www.malwarebytes.com/blog/news/2023/02/florida-hospital-takes-entire-it-systems-offline-after-ransomware-attack

Zimmerman, C. (2014). Ten Strategies of a World-Class Cybersecurity Operations Center. The MITRE corporation.

Appendices

Appendix 1. Recommendations for incident preparation – Adapted from NIST-SP 800-61r2, 2012

	General recommendations for preparing to handle incidents:	General recommendations for preventing incidents:
People:	- Training for incident response; tabletops, wargaming, attack simulations. - Training and education to identify and report potential cyber security incidents. - Establishing a clear incident response team with designated roles and responsibilities including relevant stakeholders and leadership.	- Security awareness training - Training to understand security policies and procedures. - Gathering and dissemination of insights from previous incidents to relevant stakeholders. - Training IT-staff to maintain infrastructure in accordance with organizations security standards.
Process:	- Develop an incident response policy, plan, and procedures for different types of incidents. - Regularly review and update the incident response plan; continual evaluation of the incident response process and capabilities. - Establish communication protocols; reporting, escalation, contact information, on-call information. - Establish a war room capability for central communication. - Establish incident reporting and issue tracking mechanisms. - Ensure that proper asset documentations are in place and up to date.	- Robust risk management process, risk assessments, and mitigation strategies. - Implementing clear security policies and procedures. - Implement security standards to ensure that security controls are aligned with best practices.
Technology:	- Implement relevant technical and detective security controls that ensure adequate telemetry and visibility to the target environment and infrastructure. - Having baselines of known good states of various parts of the infrastructure and systems.	- Implement relevant technical and preventative controls such as access controls, multi-factor authentication, firewalls, and network segmentation. - Regularly update and patch software and systems - Monitor and assess for potential vulnerabilities and conduct regular penetration testing. - System and network hardening - Upkeeping general IT hygiene

Appendix 2. Microsoft Cloud - All identified products and services

This appendix contains a table containing the cloud providers own definitions, descriptions, and features of identified cloud services, products, and capabilities. In this phase, the goal was to identify services and products that could be utilized in various incident response process phases from available documentation, literature, and previous academic research, and based on the service or product definitions and the researchers' own experiences, note the initial assumptions on what phases a specific service or product could be beneficial in. Incident response phase abbreviation mapping is also described below. The appendix 4 examines, evaluates, and enumerates specific use cases for each service or product that the researcher was able to identify for each phase. Also, it is important to note that the names and features of the products are subject to change.

Pr = Preparation**,** D = Detection**,** A = Analysis**,** C = Containment**,** E = Eradication**,** R = Recovery**,** Pi = Post incident

e.g. PrDA = Could potentially be helpful in incident response preparation, detection, and analysis phases.

Identified service, product, or capability - Microsoft	IR phase
Microsoft 365 Defender – **Product suite**. Includes multiple products. Many of these products also have varying licensing models offering different levels of features (Microsoft, 2023au). - "Microsoft 365 Defender is a unified pre- and post-breach enterprise defense suite that coordinates detection, prevention, investigation, and response across endpoints, identities, email, and applications to provide integrated protection against sophisticated attacks" (Microsoft, 2023au).	PrDA-CERPi

Microsoft Defender for Endpoint - **Part of the Microsoft 365 Defender product suite** - Microsoft Defender for Endpoint - “an enterprise endpoint security platform designed to help enterprise networks prevent, detect, investigate, and respond to advanced threats“ (Microsoft, 2023o). Features include: - “Endpoint behavioral sensors - Cloud security analytics - Threat intelligence - Vulnerability Management - Attack surface reduction - “Next-generation protection” – Emerging threats - Endpoint detection and response - Automated investigation and remediation - Microsoft Secure Score for Devices - Microsoft Threat Experts - Integration with Microsoft solutions“ (Microsoft, 2023o).	PrDACEPi
Microsoft Defender for Office 365 - **Part of the Microsoft 365 Defender product suite** - “Safeguards against malicious threats posed by email messages, links (URLs), and collaboration tools“ (Microsoft, 2023p). Features include: - “Configuration, protection, and detection capabilities - Automation, investigation, remediation, and education capabilities“ (Microsoft, 2023p).	PrDAEPi
Microsoft Defender for Identity - **Part of the Microsoft 365 Defender product suite** “A cloud-based security solution that leverages on-premises Active Directory signals to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions“ (Microsoft, 2023ay). Features include: - “Monitor users, entity behavior, and activities with learning-based analytics. - Protect user identities and credentials stored in Active Directory - Identify and investigate suspicious user activities and advanced attacks throughout the kill chain. - Provide clear incident information on a simple timeline for fast triage“(Microsoft, 2023ay)	DA
Microsoft Defender for Cloud Apps - **Part of the Microsoft 365 Defender product suite** “A Cloud Access Security Broker (CASB) that supports various deployment modes including log collection, API connectors, and reverse proxy. It provides rich visibility, control over data travel, and sophisticated analytics to identify and combat cyberthreats across all your Microsoft and third-party cloud services“ (Microsoft, 2023n). Features include: - “Cloud Discovery - Information Protection - Threat Detection - Conditional Access App Control - Cloud Platform Security - Application insights - Application governance	PrDAR

- Application compliance or anomalous behavior detection - Application remediation capabilities“ (Microsoft, 2023c).	
Microsoft 365 Defender for Businesses - **Part of the Microsoft 365 Defender product suite** - “Standalone version of Defender for Endpoint“ (Microsoft, 2023f)	PrDACE
Microsoft Defender Vulnerability Management - **Part of the Microsoft 365 Defender product suite** - “Delivers asset visibility, intelligent assessments, and built-in remediation tools for Windows, macOS, Linux, Android, iOS, and network devices“ (Microsoft, 2023aw). Features include - “Continuous asset discovery and monitoring - Risk-based intelligent prioritization - Remediation and tracking“(Microsoft, 2023aw).	PrDAR
Microsoft Purview - **Integrates with the Microsoft 365 Defender product suite** - “Implement data loss prevention by defining and applying DLP policies (Microsoft, 2023k). Features include: “Identify, monitor, and automatically protect sensitive items across various Microsoft SaaS products, software, and operating systems. - Microsoft Purview Information Protection helps you discover, classify, protect, and govern sensitive information wherever it lives or travels“ (Microsoft, 2023k).	PrDA
Azure Active Directory Identity Protection - **Integrates with the Microsoft 365 Defender product suite** - “Coordinates alerts with Azure Active Directory Identity Protection“ (Microsoft, 2023at) Features include - “Automation of the detection and remediation of identity-based risks - Investigation of risks using data in the portal - Exporting risk detection data to other tools“(Microsoft, 2023h).	PrDA
Microsoft Defender for Cloud - **Product suite. Includes multiple products.** - “Microsoft Defender for Cloud is a cloud-native application protection platform (CNAPP) with a set of security measures and practices designed to protect cloud-based applications from various cyber threats and vulnerabilities“ (Microsoft, 2023ax). Features include: - “A development security operations (DevSecOps) solution that unifies security management at the code level across multicloud and multiple-pipeline environments - A cloud security posture management (CSPM) solution that surfaces actions that you can take to prevent breaches - A cloud workload protection platform (CWPP) with specific protections for servers, containers, storage, databases, and other workloads“ (Microsoft, 2023ax).	PrDA

Microsoft Defender for Servers - **Part of the Defender for Cloud product suite.** - “Integrates with Defender for Endpoint“ (Microsoft, 2023aa). - “Microsoft Defender for Servers extends protection to your Windows and Linux machines that run in Azure, Amazon Web Services (AWS), Google Cloud Platform (GCP), and on-premises. Defender for Servers integrates with Microsoft Defender for Endpoint to provide endpoint detection and response (EDR) and other threat protection features“ (Microsoft, 2023aa).	PrDACER
Microsoft Defender for Storage - **Part of the Defender for Cloud product suite** - “Microsoft Defender for Storage is an Azure-native layer of security intelligence that detects potential threats to your storage accounts and helps prevent the three major impacts on your data and workload: malicious file uploads, sensitive data exfiltration, and data corruption“ (Microsoft, 2023ay). Features include: - “Activity Monitoring - Sensitive data threat detection - Malware Scanning“ (Microsoft, 2023ay).	PrDA
Microsoft Defender for SQL - **Part of the Defender for Cloud product suite** - “Microsoft Defender for Azure SQL helps you discover and mitigate potential database vulnerabilities and alerts you to anomalous activities that may be an indication of a threat to your databases“ (Microsoft, 2023t). Features include: - “Vulnerability assessment: Scan databases to discover, track, and remediate vulnerabilities. - Threat protection: Receive detailed security alerts and recommended actions based on SQL Advanced Threat Protection to provide to mitigate threats. “ (Microsoft, 2023t).	PrDA
Microsoft Defender for Containers - **Part of the Defender for Cloud product suite** “Microsoft Defender for Containers is the cloud-native solution to improve, monitor, and maintain the security of your clusters, containers, and their applications” (Microsoft, 2023u). Features include: - “Environment hardening - Vulnerability assessment - Run-time threat protection for nodes and clusters” (Microsoft, 2023u).	PrDA
Microsoft Defender for App Service - **Part of the Defender for Cloud product suite** - “Microsoft Defender for App Service uses the scale of the cloud to identify attacks targeting applications running over App Service” (Microsoft, 2023r). Features include: - “Assesses the resources covered by your App Service plan and generates security recommendations based on its findings - Detects a multitude of threats to your App Service resources such as VMs, management interface, requests and responses, sandboxes, app service internal logs” (Microsoft, 2023r).	PrDA

Microsoft Defender for Key Vault - **Part of the Defender for Cloud product suite** - "A cloud service that safeguards encryption keys and secrets like certificates, connection strings, and passwords" (Microsoft, 2023w). - "Microsoft Defender for Key Vault detects unusual and potentially harmful attempts to access or exploit Key Vault accounts. The alerts include the details of the suspicious activity and recommendations on how to investigate and remediate threats" (Microsoft, 2023w)	DA
Microsoft Defender for DNS - **Part of the Defender for Cloud product suite** - "Microsoft Defender for DNS provides an additional layer of protection for resources that use Azure DNS's Azure-provided name resolution capability. It monitors the queries from resources and detects suspicious activities without the need for any additional agents on your resources" (2023v). Features include: - "Detects suspicious and anomalous activities related to DNS traffic originating from Azure resources" (2023v).	D
Microsoft Defender for Resource Manager - **Part of the Defender for Cloud product suite** - "Microsoft Defender for Resource Manager automatically monitors the resource management operations in your organization, whether they're performed through the Azure portal, Azure REST APIs, Azure CLI, or other Azure programmatic clients. Defender for Cloud runs advanced security analytics to detect threats and alerts you about suspicious activity" (Microsoft, 2023x). Features include: "Protection against suspicious resource management operations, use of exploitation toolkits, lateral movement" (Microsoft, 2023x).	D
Microsoft Defender for open-source relational databases - Part of the Defender for Cloud product suite - "Detects anomalous activities indicating unusual and potentially harmful attempts to access or exploit databases" (Microsoft, 2023z).	D
Azure Active Directory - "A cloud-based identity and access management service" (Microsoft, 2023ag). Features include: - "Application management - Manage your cloud and on-premises apps using Application Proxy, single sign-on, the My Apps portal, and Software as a Service (SaaS) apps. - Authentication - Manage Azure Active Directory self-service password reset, Multi-Factor Authentication, custom banned password list, and smart lockout. - Azure Active Directory for developers - Build apps that sign in all Microsoft identities, get tokens to call Microsoft Graph, other Microsoft APIs, or custom APIs. - Business-to-Business (B2B) - Manage your guest users and external partners, while maintaining control over your own corporate data. - Business-to-Customer (B2C) - Customize and control how users sign up, sign in, and manage their profiles when using your apps. - Conditional Access - Manage access to your cloud apps. - Device Management - Manage how your cloud or on-premises devices access your corporate data. - Domain services - Join Azure virtual machines to a domain without using domain controllers.	PrDA-CERPi

- Enterprise users - Manage license assignments, access to apps, and set up delegates using groups and administrator roles. - Hybrid identity - Use Azure Active Directory Connect and Connect Health to provide a single user identity for authentication and authorization to all resources, regardless of location (cloud or on-premises). - Identity governance - Manage your organization's identity through employee, business partner, vendor, service, and app access controls. You can also perform access reviews. - Identity protection - Detect potential vulnerabilities affecting your organization's identities, configure policies to respond to suspicious actions, and then take appropriate action to resolve them. - Managed identities for Azure resources - Provide your Azure services with an automatically managed identity in Azure AD that can authenticate any Azure AD-supported authentication service, including Key Vault. - Privileged identity management (PIM) - Manage, control, and monitor access within your organization. This feature includes access to resources in Azure AD and Azure, and other Microsoft Online Services, like Microsoft 365 or Intune. - Reports and monitoring - Gain insights into the security and usage patterns in your environment. - Workload identities - Give an identity to your software workload (such as an application, service, script, or container) to authenticate and access other services and resources. ” (Microsoft, 2023ag).	
Azure Advisor - “Advisor is a personalized cloud consultant that helps you follow best practices to optimize your Azure deployments. It analyzes your resource configuration and usage telemetry and then recommends solutions that can help you improve the cost effectiveness, performance, Reliability (formerly called High availability), and security of your Azure resources“ (Microsoft, 2023i).	Pr
Azure Automation - “Azure Automation delivers a cloud-based automation, operating system updates, and configuration service that supports consistent management across your Azure and non-Azure environments. It includes process automation, configuration management, update management, shared capabilities, and heterogeneous features“ (Microsoft, 2023ah). - “Deploy and manage - Deliver repeatable and consistent infrastructure as code. - Response - Create event-based automation to diagnose and resolve issues. - Orchestrate - Orchestrate and integrate your automation with other Azure or third party services and products “(Microsoft, 2023ah).	CER

Azure Backup - “The Azure Backup service provides simple, secure, and cost-effective solutions to back up your data and recover it from the Microsoft Azure cloud“ (Microsoft, 2023bb). “Supports backups from: - On-premises - Azure VMs - Azure Managed Disks - Azure Files shares - SQL Server in Azure VMs - SAP HANA databases in Azure VMs - Azure Database for PostgreSQL servers - Azure Blobs“ (Microsoft, 2023bb).	PrER
Azure Blob storage - “An object storage solution for the cloud. Blob Storage is optimized for storing massive amounts of unstructured data“ (2023ai).	R
Azure Cosmos DB - “Azure Cosmos DB is a fully managed NoSQL and relational database for modern app development. - High availability and disaster recovery capabilities“ (Microsoft, 2023b).	R
Azure DDoS protection - “Azure DDoS Protection monitors actual traffic utilization and constantly compares it against the thresholds defined in the DDoS Policy. When the traffic threshold is exceeded, DDoS mitigation is initiated automatically. When traffic returns below the thresholds, the mitigation is stopped“ (Microsoft, 2023aj).	PrDAC
Azure DevOps - “Azure DevOps provides tools and processes for collaboration such as Azure Boards and Azure Repos“ (Microsoft, 2023ak).	Pi
Azure Firewall - “Azure Firewall is a cloud-native and intelligent network firewall security service that provides the best of breed threat protection for your cloud workloads running in Azure. It's a fully stateful, firewall as a service with built-in high availability and unrestricted cloud scalability. It provides both east-west and north-south traffic inspection“ (Microsoft, 2023al).	PrDAC
Azure Firewall Manager - “Azure Firewall Manager is a security management service that provides central security policy and route management for cloud-based security perimeters. You can use Azure Firewall Manager to centrally manage Azure Firewalls across multiple subscriptions. Firewall Manager uses firewall policy to apply a common set of network/application rules and configuration to the firewalls in your tenant“ (Microsoft, 2023al).	PrC

Azure Functions - “Azure Functions is a cloud service available on-demand that provides all the continually updated infrastructure and resources needed to run your applications. Functions provides serverless compute for Azure. You can use Functions to build web APIs, respond to database changes, process IoT streams, manage message queues, and more“ (Microsoft, 2023j).	DCER
Azure Log Analytics - In Azure Monitor - “A tool in the Azure portal that's used to edit and run log queries against data in the Azure Monitor Logs store. You might write a simple query that returns a set of records and then use features of Log Analytics to sort, filter, and analyze them. Or you might write a more advanced query to perform statistical analysis and visualize the results in a chart to identify a particular trend. “ (Microsoft, 2023s).	DA
Log Analytics Workspaces - “A Log Analytics workspace is a unique environment for log data from Azure Monitor and other Azure services, such as Microsoft Sentinel and Microsoft Defender for Cloud. Each workspace has its own data repository and configuration but might combine data from multiple services“ (Microsoft, 2023l).	DA
Azure Logic Apps - “Azure Logic Apps is a cloud platform where you can create and run automated workflows with little to no code. By using the visual designer and selecting from prebuilt operations, you can quickly build a workflow that integrates and manages your apps, data, services, and systems“ (Microsoft, 2023an).	PrDCER
Azure Management Groups - “If your organization has many Azure subscriptions, you may need a way to efficiently manage access, policies, and compliance for those subscriptions. Management groups provide a governance scope above subscriptions. You organize subscriptions into management groups; the governance conditions you apply cascade by inheritance to all associated subscriptions“ (Microsoft, 2023af).	Pr
Azure Monitor - “Azure Monitor is a comprehensive monitoring solution for collecting, analyzing, and responding to telemetry from your cloud and on-premises environments. Azure Monitor collects and aggregates the data from every layer and component of your system into a common data platform. It correlates data across multiple Azure subscriptions and tenants, in addition to hosting data for other services. Because this data is stored together, it can be correlated and analyzed using a common set of tools. The data can then be used for analysis and visualizations to help you understand how your applications are performing and respond automatically to system events“ (Microsoft, 2023bc).	DA

Azure Network Security Groups - Part of Azure Virtual Network - "You can use an Azure network security group to filter network traffic between Azure resources in an Azure virtual network. A network security group contains security rules that allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure resources. For each rule, you can specify source and destination, port, and protocol" (Microsoft, 2023q).	C
Azure Network Watcher - "Azure Network Watcher provides tools to monitor, diagnose, view metrics, and enable or disable logs for resources in an Azure virtual network. Network Watcher is designed to monitor and repair the network health of IaaS (Infrastructure-as-a-Service) products including virtual machines (VMs), virtual networks (VNets), application gateways, load balancers, etc". (Microsoft, 2023ao).	DA
Azure Policy - "Azure Policy helps to enforce organizational standards and to assess compliance at-scale. Through its compliance dashboard, it provides an aggregated view to evaluate the overall state of the environment, with the ability to drill down to the per-resource, per-policy granularity. It also helps to bring your resources to compliance through bulk remediation for existing resources and automatic remediation for new resources "(Microsoft, 2023ap).	PrDAER
Azure Resource Health - "Azure Resource Health helps you diagnose and get support for service problems that affect your Azure resources. It reports on the current and past health of your resources "(Microsoft, 2023bd).	DA
Azure Resource Manager - "Azure Resource Manager is the deployment and management service for Azure. It provides a management layer that enables you to create, update, and delete resources in your Azure account. You use management features, like access control, locks, and tags, to secure and organize your resources after deployment" (Microsoft, 2023aq).	PrCER

Microsoft Sentinel - "A scalable, cloud-native solution that provides: - Security information and event management (SIEM) - Security orchestration, automation, and response (SOAR)" (Microsoft, 2023az). "Microsoft Sentinel delivers intelligent security analytics and threat intelligence across the enterprise. A single solution for attack detection, threat visibility, proactive hunting, and threat response" (Microsoft, 2023az). "Features include: - Collect data at cloud scale across all users, devices, applications, and infrastructure, both on-premises and in multiple clouds. - Detect previously undetected threats, and minimize false positives using Microsoft's analytics and threat intelligence. - Investigate threats with artificial intelligence, and hunt for suspicious activities at scale. - Respond to incidents rapidly with built-in orchestration and automation of common tasks. " (Microsoft, 2023az).	PrAD-CERPi
Azure Site Recovery - "Contributes to business continuity and disaster recovery (BCDR) strategy, by orchestrating and automating replication of Azure VMs between regions, on-premises virtual machines and physical servers to Azure, and on-premises machines to a secondary datacenter" (Microsoft, 2023a).	PrR
Azure Traffic Manager - "Azure Traffic Manager is a DNS-based traffic load balancer. This service allows you to distribute traffic to your public facing applications across the global Azure regions. Traffic Manager also provides your public endpoints with high availability and quick responsiveness" (Microsoft, 2023ba). - "Traffic manager also provides health monitoring for every endpoint. The endpoint can be any Internet-facing service hosted inside or outside of Azure. Traffic Manager provides a range of traffic-routing methods and endpoint monitoring options to suit different application needs and automatic failover models" (Microsoft, 2023ba).	DR
Azure Update Management - Part of Azure Automation - "Manage operating system updates for your Windows and Linux virtual machines in Azure, physical or VMs in on-premises environments, and in other cloud environments. You can quickly assess the status of available updates and manage the process of installing required updates for your machines reporting to Update Management" (Microsoft, 2023ac).	PrE
Azure Virtual Machines - "Azure virtual machines are one of several types of on-demand, scalable computing resources that Azure offers. An Azure virtual machine gives you the flexibility of virtualization without having to buy and maintain the physical hardware that runs it. However, you still need to maintain the virtual machine by performing tasks, such as configuring, patching, and installing the software that runs on it" (Microsoft, 2023ad).	A

Azure Virtual Network / Vnet - ”VNet enables many types of Azure resources, such as Azure Virtual Machines (VM), to securely communicate with each other, the internet, and on-premises networks. VNet is similar to a traditional network that you'd operate in your own data center but brings with it additional benefits of Azure's infrastructure such as scale, availability, and isolation” (Microsoft, 2023ar).	PrCR
Azure Web application firewall - ”Provides centralized protection of your web applications from common exploits and vulnerabilities and is based on the Core Rule Set (CRS) from the Open Web Application Security Project. Azure WAF is a cloud-native service that protects web apps from common web-hacking techniques such as SQL injection and security vulnerabilities such as cross-site scripting. Deploy the service in minutes to get complete visibility into your environment and block malicious attacks” (2023as).	PrDAC
Azure Well-Architected Framework - “The Azure Well-Architected Framework is a set of guiding tenets that you can use to improve the quality of a workload. The framework consists of five pillars of architectural excellence: - Reliability - Security - Cost optimization - Operational excellence - Performance efficiency” (Microsoft, 2023be).	Pr
Azure support - “Azure provides various support plans“ (Microsoft, 2023g).	ER
Microsoft Defender Threat Intelligence - “Microsoft Defender Threat Intelligence (Defender TI) is a platform that streamlines triage, incident response, threat hunting, vulnerability management, and cyber threat intelligence analyst workflows when conducting threat infrastructure analysis and gathering threat intelligence“ (Microsoft, 2023av).	A
Azure Cost Management - “Microsoft Cost Management is a suite of tools that help organizations monitor, allocate, and optimize the cost of their Microsoft Cloud workloads“ (Microsoft, 2023bf).	D

Appendix 3. AWS - All identified products and services

This appendix contains a table containing the cloud providers own definitions, descriptions, and features of identified cloud services, products, and capabilities. In this phase, the goal was to identify services and products that could be utilized in various incident response process phases from available documentation, literature, and previous academic research, and based on the service or product definitions and the researchers' own experiences, note the initial assumptions on what phases a specific service or product could be beneficial in. Incident response phase abbreviation mapping is also described below. The appendix 4 examines, evaluates, and enumerates specific use cases for each service or product that the researcher was able to identify for each phase. Also, it is important to note that the names and features of the products are subject to change.

Pr = Preparation, D = Detection, A = Analysis, C = Containment, E = Eradication, R = Recovery, Pi = Post incident

e.g. PrDA = Could potentially be helpful in incident response preparation, detection, and analysis phases.

Identified service, product or capability - AWS	IR phase
AWS Athena - "Amazon Athena is a serverless, interactive analytics service built on open-source frameworks, supporting open-table and file formats. Athena provides a simplified, flexible way to analyze petabytes of data where it lives. Analyze data or build applications from an Amazon Simple Storage Service (S3) data lake and 25-plus data sources, including on-premises data sources or other cloud systems using SQL or Python" (AWS, 2023i). "In AWS, the main services you can use to query logs are CloudWatch Logs Insights for data stored in CloudWatch log groups, and Amazon Athena and Amazon OpenSearch Service for data stored in Amazon S3 (AWS, 2023e, p. 18).	PrDA
AWS Backup - "AWS Backup is a fully managed backup service centralizing and automating the backup of data across AWS services. AWS Backup provides an orchestration layer that integrates Amazon CloudWatch, AWS CloudTrail, AWS Identity and Access Management (IAM), AWS Organizations, and other services. This centralized, AWS Cloud native solution provides global backup capabilities that can help you achieve your disaster recovery and compliance	PrER

requirements. Using AWS Backup, you can centrally configure backup policies and monitor backup activity for AWS resources“ (AWS, 2023r).	
AWS Billing - “The AWS Billing console contains features to pay your AWS bills and report your AWS cost and usage (AWS, 2023ai). It is also possible to manage your account settings using the AWS Management Console and Billing console“ (AWS, 2023ai).	DR
AWS CloudFormation - “AWS CloudFormation enables you to create and provision AWS infrastructure deployments predictably and repeatedly. It helps you leverage AWS products such as Amazon EC2, Amazon Elastic Block Store, Amazon SNS, Elastic Load Balancing, and Auto Scaling to build highly reliable, highly scalable, cost-effective applications in the cloud without worrying about creating and configuring the underlying AWS infrastructure. AWS CloudFormation enables you to use a template file to create and delete a collection of resources together as a single unit (a stack)“ (AWS, 2023a).	PrACER
AWS CloudTrail - “AWS CloudTrail service enabling governance, compliance, operational auditing, and risk auditing of AWS accounts. With CloudTrail, you can log, continuously monitor, and retain account activity related to actions across AWS services. CloudTrail provides event history of your AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services. This event history simplifies security analysis, resource change tracking, and troubleshooting. “ (AWS, 2023ac).	DA
AWS Cloudwatch - “Amazon CloudWatch monitors your Amazon Web Services (AWS) resources and the applications you run on AWS in real time. You can use CloudWatch to collect and track metrics, which are variables you can measure for your resources and applications. You can create alarms that watch metrics and send notifications or automatically make changes to the resources you are monitoring when a threshold is breached. With CloudWatch, you gain system-wide visibility into resource utilization, application performance, and operational health. “ (AWS, 2023aq)	DA
AWS Config - “AWS Config provides a detailed view of the resources associated with your AWS account, including how they are configured, how they are related to one another, and how the configurations and their relationships have changed over time“ (AWS, 2023ad).	PrDACER

AWS Detective - “Amazon Detective helps you analyze, investigate, and quickly identify the root cause of security findings or suspicious activities. Detective automatically collects log data from your AWS resources. It then uses machine learning, statistical analysis, and graph theory to generate visualizations that help you to conduct faster and more efficient security investigations. The Detective prebuilt data aggregations, summaries, and context help you to quickly analyze and determine the nature and extent of possible security issues“ (AWS, 2023j). - “With Detective, you can access up to a year of historical event data. This data is available through a set of visualizations that show changes in the type and volume of activity over a selected time window. Detective links these changes to GuardDuty findings“ (AWS, 2023ar).	A
AWS Detective - “Amazon Elastic Compute Cloud (Amazon EC2) provides scalable computing capacity in the Amazon Web Services (AWS) Cloud. Using Amazon EC2 eliminates your need to invest in hardware up front, so you can develop and deploy applications faster. You can use Amazon EC2 to launch as many or as few virtual servers as you need, configure security and networking, and manage storage. Amazon EC2 enables you to scale up or down to handle changes in requirements or spikes in popularity, reducing your need to forecast traffic“ (AWS, 2023bi).	PrAR
AWS Elastic Beanstalk - “With Elastic Beanstalk, you can quickly deploy and manage applications in the AWS Cloud without having to learn about the infrastructure that runs those applications. Elastic Beanstalk reduces management complexity without restricting choice or control. You simply upload your application, and Elastic Beanstalk automatically handles the details of capacity provisioning, load balancing, scaling, and application health monitoring” (AWS, 2023aj).	R

AWS Elastic Block Store (EBS) - “Amazon Elastic Block Store (Amazon EBS) provides block level storage volumes for use with EC2 instances. EBS volumes behave like raw, unformatted block devices. You can mount these volumes as devices on your instances. EBS volumes that are attached to an instance are exposed as storage volumes that persist independently from the life of the instance. You can create a file system on top of these volumes, or use them in any way you would use a block device (such as a hard drive). You can dynamically change the configuration of a volume attached to an instance (AWS, 2023l). - You can back up the data on your Amazon EBS volumes to Amazon S3 by taking point-in-time snapshots. Snapshots are incremental backups, which means that only the blocks on the device that have changed after your most recent snapshot are saved. This minimizes the time required to create the snapshot and saves on storage costs by not duplicating data. Each snapshot contains all of the information that is needed to restore your data (from the moment when the snapshot was taken) to a new EBS volume (AWS, 2023l).	PrAER
AWS Elastic Disaster Recovery - “AWS Elastic Disaster Recovery (AWS DRS) minimizes downtime and data loss with fast, reliable recovery of on-premises and cloud-based applications using affordable storage, minimal compute, and point-in-time recovery“ (AWS, 2023bb). - “You can perform non-disruptive tests to confirm that implementation is complete. During normal operation, maintain readiness by monitoring replication and periodically performing non-disruptive recovery and failback drills“ (AWS, 2023bb). - “If you need to recover applications, you can launch recovery instances on AWS within minutes, using the most up-to-date server state or a previous point in time“ (AWS, 2023bb).	RPi
AWS EventBridge (CloudWatch Events) - “EventBridge is a serverless service that uses events to connect application components together, making it easier for you to build scalable event-driven applications. Use it to route events from sources such as home-grown applications, AWS services, and third-party software to consumer applications across your organization. EventBridge provides a simple and consistent way to ingest, filter, transform, and deliver events so you can build new applications quickly“ (AWS, 2023ae).	CER
AWS Firewall Manager - “AWS Firewall Manager simplifies your administration and maintenance tasks across multiple accounts and resources for a variety of protections, including AWS WAF, AWS Shield Advanced, Amazon VPC security groups, AWS Network Firewall, and Amazon Route 53 Resolver DNS Firewall. With Firewall Manager, you set up your protections just once and the service automatically applies them across your accounts and resources, even as you add new accounts and resources“ (AWS, 2023c).	PrDAC

AWS Glacier (S3 Glacier) - “A secure and durable service for low-cost data archiving and long-term backup“ (AWS, 2023af).	R
AWS GuardDuty - “Amazon GuardDuty is a security monitoring service that analyzes and processes Foundational data sources, such as AWS CloudTrail management events, AWS CloudTrail event logs, VPC flow logs, and DNS logs. It also processes Features such as Kubernetes audit logs, RDS login activity, S3 logs, EBS volumes, and Runtime monitoring“ (AWS, 2023at). - “It uses threat intelligence feeds, such as lists of malicious IP addresses and domains, and machine learning to identify unexpected, potentially unauthorized, and malicious activity within your AWS environment. This can include issues like escalation of privileges, use of exposed credentials, or communication with malicious IP addresses, domains, presence of malware on your Amazon EC2 instances and container workloads, or discovery of unusual patterns of login events on your database“ (AWS, 2023at).	PrDACR
AWS IAM - “AWS Identity and Access Management (IAM) is a web service that helps you securely control access to AWS resources. With IAM, you can centrally manage permissions that control which AWS resources users can access. You use IAM to control who is authenticated (signed in) and authorized (has permissions) to use resources“ (AWS, 2023bc).	PrDACER
AWS Inspector - “Amazon Inspector is a security vulnerability assessment service that helps improve the security and compliance of your AWS resources“ (AWS, 2023m). - “Amazon Inspector is a vulnerability management service that continuously scans your AWS workloads for software vulnerabilities and unintended network exposure. Amazon Inspector automatically discovers and scans running Amazon EC2 instances, container images in Amazon Elastic Container Registry (Amazon ECR), and AWS Lambda functions for known software vulnerabilities and unintended network exposure“ (AWS, 2023au).	PrDA

AWS Lambda - “AWS Lambda is a compute service that lets you run code without provisioning or managing servers. Lambda runs your code on a high-availability compute infrastructure and performs all of the administration of the compute resources, including server and operating system maintenance, capacity provisioning and automatic scaling, and logging. With Lambda, you can run code for virtually any type of application or backend service“ (AWS, 2023ak). - “You organize your code into Lambda functions. Lambda runs your function only when needed and scales automatically, from a few requests per day to thousands per second“ (AWS, 2023ak).	DACER
AWS Macie - “Amazon Macie is a data security service that discovers sensitive data by using machine learning and pattern matching, provides visibility into data security risks, and enables automated protection against those risks“ (AWS, 2023av). -“Amazon Macie is an AI-powered security service that helps prevent data loss by automatically discovering, classifying, and protecting sensitive data stored in AWS. Macie uses machine learning (ML) to recognize sensitive data such as personally identifiable information (PII) or intellectual property, assign a business value, and provide visibility into where this data is stored and how it is being used in your organization. Amazon Macie continuously monitors data access activity for anomalies, and delivers alerts when it detects a risk of unauthorized access or inadvertent data leaks“ (AWS, 2023av).	PrDA
AWS Organizations - “AWS Organizations is an account management service that enables you to consolidate multiple AWS accounts into an organization that you create and centrally manage. AWS Organizations includes account management and consolidated billing capabilities that enable you to better meet the budgetary, security, and compliance needs of your business. As an administrator of an organization, you can create accounts in your organization and invite existing accounts to join the organization“ (AWS, 2023al).	Pr
AWS RDS - “Amazon Relational Database Service (Amazon RDS) is a web service that makes it easier to set up, operate, and scale a relational database in the cloud. It provides cost-efficient, resizeable capacity for an industry-standard relational database and manages common database administration tasks. Amazon Aurora is a fully managed relational database engine that's built for the cloud and compatible with MySQL and PostgreSQL. Amazon Aurora is part of Amazon RDS“ (AWS, 2023o).	R

AWS S3 - “Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance. Customers of all sizes and industries can use Amazon S3 to store and protect any amount of data for a range of use cases, such as data lakes, websites, mobile applications, backup and restore, archive, enterprise applications, IoT devices, and big data analytics“ (AWS, 2023ay). - “Amazon S3 is an object storage service that stores data as objects within buckets. An object is a file and any metadata that describes the file. A bucket is a container for objects“ (AWS, 2023ay).	AR
AWS SNS - “Amazon Simple Notification Service (Amazon SNS) is a managed service that provides message delivery from publishers to subscribers (also known as producers and consumers). Publishers communicate asynchronously with subscribers by sending messages to a topic, which is a logical access point and communication channel. Clients can subscribe to the SNS topic and receive published messages using a supported endpoint type, such as Amazon Kinesis Data Firehose, Amazon SQS, AWS Lambda, HTTP, email, mobile push notifications, and mobile text messages (SMS) “ (AWS, 2023az).	DCR
AWS Security Hub - “AWS Security Hub provides you with a comprehensive view of your security state in AWS and helps you check your environment against security industry standards and best practices.Security Hub collects security data from across AWS accounts, services, and supported third-party partner products and helps you analyze your security trends and identify the highest priority security issues“ (AWS, 2023am). “Features include: - Reduced effort to collect and prioritize findings, automatic security checks against best practices and standards, consolidated view of findings across accounts and providers, ability to automate remediation of findings“ (AWS, 2023s).	PrDACER
AWS Service Catalog - “Service Catalog enables organizations to create and manage catalogs of IT services that are approved for AWS. These IT services can include everything from virtual machine images, servers, software, databases, and more to complete multi-tier application architectures. Service Catalog allows organizations to centrally manage commonly deployed IT services, and helps organizations achieve consistent governance and meet compliance requirements. End users can quickly deploy only the approved IT services they need, following the constraints set by your organization“ (AWS, 2023ah).	PrR

AWS Shield - “AWS Shield Standard and AWS Shield Advanced provide protections against Distributed Denial of Service (DDoS) attacks for AWS resources at the network and transport layers (layer 3 and 4) and the application layer (layer 7). A DDoS attack is an attack in which multiple compromised systems try to flood a target with traffic. A DDoS attack can prevent legitimate end users from accessing the target services and can cause the target to crash due to overwhelming traffic volume“ (AWS, 2023w). - “AWS Shield provides protection against a wide range of known DDoS attack vectors and zero-day attack vectors. Shield detection and mitigation is designed to provide coverage against threats even if they are not explicitly known to the service at the time of detection“ (AWS, 2023w).	PrDACER
AWS Step Functions - “AWS Step Functions is a serverless orchestration service that lets you integrate with AWS Lambda functions and other AWS services to build business-critical applications. Through Step Functions' graphical console, you see your application’s workflow as a series of event-driven steps“ (AWS, 2023an). - “AWS Step Functions makes it simple to coordinate the components of distributed applications and microservices using visual workflows. Step Functions provides a graphical console for you to arrange and visualize the components of your application as a series of steps. This makes it simple to build and run multistep applications. Step Functions automatically starts and tracks each step, and retries when there are errors, so your application runs in order and as expected“ (AWS, 2023an).	DACER
AWS Support - “AWS Support offers a range of plans that provide access to tools and expertise that support the success and operational health of your AWS solutions. If you need technical support and more resources to help plan, deploy, and optimize your AWS environment, you can select a support plan that best aligns with your AWS use case“ (AWS, 2023aa).	DER
AWS Systems manager - “AWS Systems Manager gives you visibility and control of your infrastructure on AWS. Systems Manager provides a unified user interface so you can view operational data from multiple AWS services and enables you to automate operational tasks across your AWS resources“ (AWS, 2023ao). “Capabiltieis include: - Application management, change management, node management, operations management, quick setup, shared resources“ (AWS, 2023ao)	PrCER
AWS Trusted Advisor - “Trusted Advisor inspects your AWS environment, and then makes recommendations when opportunities exist to save money, improve system availability and performance, or help close security gaps“ (AWS, 2023f).	Pr

AWS Route 53 - “Amazon Route 53 is a highly available and scalable Domain Name System (DNS) web service. You can use Route 53 to perform three main functions in any combination: domain registration, DNS routing, and health checking. “ (AWS, 2023bg).	PrDACR
AWS VPC - “Amazon Virtual Private Cloud (Amazon VPC) enables you to launch AWS resources into a virtual network that you've defined. This virtual network closely resembles a traditional network that you'd operate in your own data center, with the benefits of using the scalable infrastructure of AWS“ (AWS, 2023ba). “Features include: - Virtual private clouds (VPC) - a virtual network that closely resembles a traditional network - Subnets - IP addressing - Routing - Gateways and endpoints - Peering connections - Traffic Mirroring - Transit gateways - VPC Flow Logs - VPN connections“(AWS, 2023ba)	PrDACR
AWS WAF - “AWS WAF is a web application firewall that lets you monitor the HTTP(S) requests that are forwarded to your protected web application resources. AWS WAF lets you control access to your content“ (AWS, 2023g). “You can protect the following resource types: -Amazon CloudFront distribution -Amazon API Gateway REST API -Application Load Balancer -AWS AppSync GraphQL API -Amazon Cognito user pool -AWS App Runner service“(AWS, 2023g).	PrDACER
AWS Well-Architected Tool - “AWS Well-Architected Tool (AWS WA Tool) is a service in the cloud that provides a consistent process for measuring your architecture using AWS best practices. AWS WA Tool helps you throughout the product lifecycle by: Assisting with documenting the decisions that you make, Providing recommendations for improving your workload based on best practices, Guiding you in making your workloads more reliable, secure, efficient, and cost-effective“ (AWS, 2023ap).	Pr

AWS OpenSearch Service - “Amazon OpenSearch Service is a managed service that makes it easy to deploy, operate, and scale OpenSearch clusters in the AWS Cloud. Amazon OpenSearch Service supports OpenSearch and legacy Elasticsearch OSS (up to 7.10, the final open source version of the software). When you create a cluster, you have the option of which search engine to use“ (AWS, 2023aw).	A
AWS OpsWorks - “AWS OpsWorks is a configuration management service that provides managed instances of Chef and Puppet. Chef and Puppet are automation platforms that allow you to use code to automate the configurations of your servers. OpsWorks lets you use Chef and Puppet to automate how servers are configured, deployed, and managed across your Amazon EC2 instances or on-premises compute environments. “ (AWS, 2023bh).	PrR
AWS QuickSight - “Amazon QuickSight is a cloud-scale business intelligence (BI) service that you can use to deliver easy-to-understand insights to the people who you work with, wherever they are. Amazon QuickSight connects to your data in the cloud and combines data from many different sources. In a single data dashboard, QuickSight can include AWS data, third-party data, big data, spreadsheet data, SaaS data, B2B data, and more“ (AWS, 2023ax). “Quicksight basic workflow: - Connect data: AWS products, On-prem, Files, SaaS - Get ready to analyze: Prepare data, create a data set, share with analysts - Analyze: Examine, visualize, share data - Make decisions: Produce insights from the analysis“(AWS, 2023ax).	A
AWS Machine Learning (AWS SageMaker) - “Amazon SageMaker is a fully managed machine learning service. With SageMaker, data scientists and developers can quickly and easily build and train machine learning models, and then directly deploy them into a production-ready hosted environment. It provides an integrated Jupyter authoring notebook instance for easy access to your data sources for exploration and analysis, so you don't have to manage servers. It also provides common machine learning algorithms that are optimized to run efficiently against extremely large data in a distributed environment“ (AWS, 2023ag)	A
AWS EMR - “Amazon EMR (previously called Amazon Elastic MapReduce) is a managed cluster platform that simplifies running big data frameworks, such as Apache Hadoop and Apache Spark, on AWS to process and analyze vast amounts of data. Using these frameworks and related open-source projects, you can process data for analytics purposes and business intelligence workloads. Amazon EMR also lets you transform and move large amounts of data into and out of other AWS data stores and databases, such as Amazon Simple Storage Service (Amazon S3) and Amazon DynamoDB“ (AWS, 2023as).	A

AWS X-Ray - “AWS X-Ray is a service that collects data about requests that your application serves, and provides tools that you can use to view, filter, and gain insights into that data to identify issues and opportunities for optimization. For any traced request to your application, you can see detailed information not only about the request and response, but also about calls that your application makes to downstream AWS resources, microservices, databases, and web APIs” (2023be).	A

Appendix 4. Use cases for incident response

This appendix contains potential use cases for various services, products, and capabilities in different incident response phases. The services, products, and capabilities were initially identified in the appendix 2 and 3. The use cases are based both on official documentation provided by the cloud providers, but also, based on the researchers' own experiences. Note that the list of use-cases is not necessarily exhaustive, nor is the list of products, services, tools, or capabilities, but the aim was to identify at least the most important ones to be able to provide practical guidance for incident response. The data collected here was also utilized in the comparative analysis to assess different vendors' capabilities to gain insights into different types of ways to approach incident response.

	Preparation use Cases - Microsoft Azure (Larger Microsoft cloud ecosystem impact considered) The requirements were related to incident prevention, preparing to handle incidents, hardening the environment, and enhancing cyber resiliency.	**Preparation use cases - Amazon Web Services** The requirements were related to incident prevention, preparing to handle incidents, hardening the environment, and enhancing cyber resiliency.

	Microsoft 365 Defender - Product suite:
	• **Microsoft Defender for Endpoint**
	  • Capabilities extend to Azure through Defender for Servers (Microsoft, 2023aa).
	  • Enterprise security platform with a large set of capabilities that could be utilized with all preparation requirements utilizing for example (Microsoft, 2023o):
	  • Threat intelligence
	  • Vulnerability management
	  • Attack surface reduction
	  • Security score and posture
	  • Threat expert insights
	  • Preventing and detecting capabilities in EDR
	• **Microsoft Defender for Office 365**
	  • Preparation and prevention of email, URL, and collaboration tool-based threats against Azure identities (Microsoft, 2023p).
	  • Threat protection and real-time threat reporting capabilities (Microsoft, 2023p)
	• **Microsoft Defender for Identity**
	  • Provides insights regarding identity configurations and best practices, and reduces attack surface (Microsoft, 2023ay)
	• **Microsoft Defender for Cloud Apps**
		AWS Athena
		• Visualize security posture related data in S3 with the help of Athena queries (AWS, 2023i).
		AWS Backup
		• Configure backup policies and prepare for disaster recovery scenarios with AWS Backup (AWS, 2023r).
		AWS CloudFormation
		• Deploy and provision infrastructure and resources in a consistent, predictable, and repeatable way (AWS, 2023a).
		AWS CloudTrail
		• Aggregate AWS cloud events to AWS CloudTrail to help with incident investigations (AWS, 2023e, p. 18).
		AWS CloudWatch
		• Establish visibility to AWS resources and related telemetry and signals (AWS, 2023e, p. 43).
		AWS Config
		• Manage, enforce, and monitor configurations, changes to resources, and compliance (AWS, 2023e, p. 43).
		AWS EC2
		• Utilize EC2 autoscaling groups to elastically scale virtual resources if they become unavailable due to an incident (AWS, 2023bi).

- Helps with incident preparation and prevention related to Azure identities and application data (Microsoft, 2023n).
- Cloud platform security, cloud application compliance assessments, information protection, conditional access policies to apps (Microsoft, 2023n).

- **Microsoft 365 Defender for Businesses**
  - Similar capabilities as Defender for Endpoint (Microsoft, 2023f).
- **Microsoft Defender Vulnerability Management**
  - Helps with preparation and prevention with Continuous asset discovery and vulnerability monitoring, and risk-based prioritization (Microsoft, 2023aw).
- **Microsoft Purview - integrates with the Defender suite**
  - Protect, discover, classify, label, and govern data and sensitive information in Azure with DLP policies (Microsoft, 2023k).
- **Azure Active Directory Identity Protection - integrates with the Defender suite**
  - Prevent, prepare, and harden cloud identities with identity protection policies (Microsoft, 2023h).

Microsoft Defender for Cloud - Product suite:

- Cloud posture and vulnerability management (Microsoft, 2023ax).
- Security visibility, policy management, and control over Azure and a broad ecosystem of resources (Microsoft, 2023bh).
- **Microsoft Defender for Servers**
  - Utilize capabilities and features of Defender for Endpoint for Azure based virtual servers (Microsoft, 2023aa).
- **Microsoft Defender for Storage**
  - By enabling, can protect sensitive data in the cloud (Microsoft, 2023ay).
- **Microsoft Defender for SQL**
  - Vulnerability assessment and threat protection; receive various alerts and recommendations to harden the database environments (Microsoft, 2023t).
- **Microsoft Defender for Containers**
  - Environment hardening, vulnerability assessment (Microsoft, 2023u).
- **Microsoft Defender for Key Vault**
  - Store secrets safely and encrypted at Azure Key vault (Microsoft, 2023w).
- **Microsoft Defender for App Service**
  - Security recommendations, resource assessments (Microsoft, 2023r).

Azure Active Directory

AWS Elastic Block Store (EBS)

- Take snapshots of your data and store them in S3 to help incident recovery (AWS, 2023l)

AWS Elastic Disaster Recovery

- Enable to make the environment more resilient (AWS, 2023bb).

AWS Firewall Manager

- Utilize to establish preventative and detective configurations for various AWS network and web traffic protection tools across multiple accounts and regions (AWS, 2023c).

AWS GuardDuty

- Provides recommendations to improve security posture and to help identify potential risks in the environment (AWS, 2023at).

AWS IAM

- Create policies and roles that limit access to critical resources (AWS, 2023bc).

AWS Inspector

- Assess vulnerabilities to identify misconfigurations and improve security posture and/or compliance of AWS resources (AWS, 2023m).

AWS Macie

- Utilize to identify, classify, sensitive data and assess the risk associated with the data and enforce policies related to data access (AWS, 2023av).

AWS Organizations

- Helps with centrally managing policies, security, and compliance for multiple AWS accounts (AWS, 2023al).

AWS OpsWorks

- Deploy and provision infrastructure and resources in a consistent, predictable, and repeatable way (AWS, 2023bh).

AWS S3

- Some examples could be for example storing backups of critical data, incident response process documentation, or incident response tools or toolkits that can be utilized in response.

AWS Security Hub

- Compare the environment against standards and best practices to prioritize risk, security, or compliance related actions (AWS, 2023am).

AWS Service Catalog

- Define standard configurations to ensure consistency of the environment (AWS, 2023ah).

AWS Shield

- Harden public web applications running on AWS against DDoS attacks (AWS, 2023w).

AWS Systems manager

	• Manage the identity and access management related to Azure environment (Microsoft, 2023ag). • Among other, helps with setting preventative policies, manage authentication, identity governance, provides recommendations and reports regarding the health of the identity plane, privileged identity management, identity protection and conditional access, etc. (Microsoft, 2023ag). **Azure Advisor** • Helps with optimization, recommends configurations to improve security in Azure (Microsoft, 2023i). **Azure Backup** • Backup important data and resources before an incident occurs (Microsoft, 2023bb). **Azure DDoS protection** • Enable DDoS protection policies to protect public facing Azure resources (Microsoft, 2023aj). **Azure Firewall** • Configure firewall policies to block, allow, or monitor ingress, egress, and p2p network traffic within Azure and between Azure resources (Microsoft, 2023al). **Azure Firewall Manager** • Centrally manage Azure Firewalls and Firewall policies across multiple subscriptions (Microsoft, 2023al). **Azure Management Groups** • Manage policies, compliance, or access for many Azure subscriptions (Microsoft, 2023af). **Azure Policy** • Assess compliance, enforce standards, or evaluate the state of the environment (Microsoft, 2023ap). **Azure Resource Manager** • Manage and tag Azure resources (Microsoft, 2023aq). • Group resources together; update, delete, deploy resources in the group in a coordinated way (Microsoft, 2023bh). • Utilize templates to deploy resources or environments in a standardized way (Microsoft, 2023bh). **Microsoft Sentinel** • A cloud native SIEM and SOAR solution. Helps with all preparation requirements with for example attack detection, threat visibility, threat response, and threat hunting capabilities (Microsoft, 2023bh). **Azure Site Recovery** • Enable to enhance business continuity and disaster recovery (Microsoft, 2023a). **Azure Update Management** • Can help with managing infrastructure at scale and prepare it to both prevent and handle incidents (AWS, 2023ao). **AWS Trusted Advisor** • Inspects AWS environment and gives recommendations for opportunities to enhance among other things, security (AWS, 2023f). **AWS Route 53** • Ensure that all DNS configurations are accurate and up to date (AWS, 2023bg). **AWS VPC** • Apply network security best practices to help with both incident prevention and incident handling (AWS, 2023e, p. 18). **AWS WAF** • Utilize to create rules to mitigate and block malicious traffic from reaching AWS based applications (AWS, 2023e, p. 29). **AWS Well-Architected Tool** • Review and improve the environment to better align with security best practices (AWS, 2023aw).

	• Apply patches and updates to keep the environment compliant and hardened (Microsoft, 2023ac). **Azure Virtual Network / VNET** • Apply configurations and rules to control the ingress, egress, or p2p network traffic within Azure (Microsoft, 2023ar). **Azure Web application firewall** • Enable and configure Azure WAF to protect public facing Azure resources (Microsoft, 2023as). **Azure Well-Architected Framework** • Utilize the framework to improve the quality and resiliency of Azure environment (Microsoft, 2023be).	
	Detection use Cases - Microsoft Azure **(Larger Microsoft cloud ecosystem impact considered)** The requirements were related to establishing visibility to the incident related signals and alerting	**Detection use cases - Amazon Web Services** The requirements were related to establishing visibility to the incident related signals and alerting

	Microsoft 365 Defender - Product suite:
	• **Microsoft Defender for Endpoint**
	  • Capabilities extend to Azure through Defender for Servers (Microsoft, 2023aa).
	  • Helps to establish visibility to threats against endpoint/server resources with for example endpoint behavioral sensors, threat intelligence, and EDR capabilities (Microsoft, 2023o).
	• **Microsoft Defender for Office 365**
	  • Protect Azure identities with email-based threat alerting (Microsoft, 2023p)
	• **Microsoft Defender for Identity**
	  • Alerts on suspicious activities and potential attacks against Azure identities (Microsoft, 2023ay
	• **Microsoft Defender for Cloud Apps**
	  • Helps with threat detection related to Azure identities and application data (Microsoft, 2023n).
	• **Microsoft 365 Defender for Businesses**
	  • Similar capabilities as Defender for Endpoint (Microsoft, 2023f).
	• **Microsoft Defender Vulnerability Management**
	  • Alerts from vulnerabilities (Microsoft, 2023aw).
	• **Microsoft Purview - integrates with the Defender suite**
	  • Detect data misuse and exfiltration with DLP policies (Microsoft, 2023k).
	• **Azure Active Directory Identity Protection - integrates with the Defender suite**
		AWS Athena
		• Detect anomalies from logs stored in S3 (AWS, 2023e, p. 18).
		AWS Billing
		• Anomalies with billing and cost may indicate that resources are misused (AWS, 2023ai).
		AWS CloudTrail
		• Enable to help with establishing visibility and detective controls to the AWS Cloud services and accounts (AWS, 2023e, p. 25).
		AWS CloudWatch
		• Establish visibility to AWS resources and related telemetry and signals and monitor for specific events or patterns and alert on them (AWS, 2023e, p. 43).
		AWS Config
		• Detect changes to configurations and compliance (AWS, 2023e, p. 43).
		AWS Firewall Manager
		• Centrally monitor for alerts from various network and web protection tools from different accounts and regions (AWS, 2023c).
		AWS GuardDuty
		• Produces alerts and security related insights from various foundational AWS services such as CloudTrail, S3, EC2, VPC, and DNS. (AWS, 2023e, p. 44).
		AWS IAM
		• Monitor account activity logs and create alerts for suspicious activities (AWS, 2023bc).
		AWS Inspector

	• Detect threats affecting cloud identities with risk-based analytics (Microsoft, 2023h).
	Microsoft Defender for Cloud - Product suite:
	• **Microsoft Defender for Servers**
	  • Utilizes capabilities and features of Defender for Endpoint (Microsoft, 2023aa).
	• **Microsoft Defender for Storage**
	  • Activity monitoring, and malware scanning of files in the cloud storage (Microsoft, 2023ay).
	• **Microsoft Defender for SQL**
	  • Alerts on anomalous activities related to database resources (Microsoft, 2023t).
	• **Microsoft Defender for Containers**
	  • Alerts from run-time protection of clusters and cluster nodes (Microsoft, 2023u).
	• **Microsoft Defender for App Service**
	  • Detect threats related to App Service resources (Microsoft, 2023r).
	• **Microsoft Defender for Key Vault**
	  • Detect unusual activities related to secrets stored in the Azure Key vault (Microsoft, 2023w).
	• **Microsoft Defender for DNS**
	  • Detects suspicious and anomalous activities related to DNS traffic originating from Azure resources (Microsoft, 2023v).
	• **Microsoft Defender for Resource Manager**
	  • Detect suspicious resource management operations (Microsoft, 2023x).
	• **Microsoft Defender for open-source relational databases**
	  • Detect anomalous activities related to unauthorized access or exploit of database resources (Microsoft, 2023z).
	Azure Active Directory
	• Detect anomalous and risky activities related to identities and other cloud resources in Azure (Microsoft, 2023ag).
	Azure Blob storage
	• Azure Storage analytics enables visibility to metrics and telemetry related to storage accounts (2023ai).
	Azure DDoS protection
	• Detects DDoS attacks against public facing Azure resources (Microsoft, 2023aj).
	Azure Firewall
	• Detect anomalous ingress, egress, and p2p network traffic within Azure and between Azure resources (Microsoft, 2023al)
	Azure Functions
		• Identify and detect misconfigurations and vulnerabilities related to AWS resources (AWS, 2023m).
		AWS Lambda
		• Utilize to trigger automated alerts on events generated by other AWS services (AWS, 2023e, p. 45).
		AWS Macie
		• Monitors and alerts for suspicious activities related to sensitive data (AWS, 2023e, p. 45).
		AWS Security Hub
		• Generates security findings based on automated compliance checks or other AWS security tooling such as GuardDuty (AWS, 2023e, p. 44).
		AWS Shield
		• Automatically detects and mitigates DDoS attacks against web applications running on AWS (AWS, 2023w).
		AWS SNS
		• Trigger various types of notifications with for example HTTP, email, or SMS for different types of events happening with various event sources such as GuardDuty, Inspector, CloudTrail, and many more services (AWS, 2023e, p. 24).
		AWS Step Functions
		• Utilize to trigger automated alerts on events generated by other AWS services (AWS, 2023e, p. 45).
		AWS Support
		• AWS support might contact customers when AWS identifies abusive or malicious activities (AWS, 2023e, p. 24).
		AWS Route 53
		• Identify unusual or unexpected traffic patterns such as unusual DNS queries (AWS, 2023e, p. 44).
		AWS VPC
		• Helps with establishing visibility to the ingress, egress, and p2p traffic between AWS resources (AWS, 2023ba)
		AWS WAF
		• Establish visibility into web traffic and integrate with for example CloudWatch to send alerts when an anomaly is detected (AWS, 2023g).

	• Utilize Azure Functions automation to alert on various signals and events (Microsoft, 2023j). **Azure Log Analytics - in Azure monitor** • Detect anomalous activities from dashboards built on top of data from Azure monitor (Microsoft, 2023s). **Log Analytics Workspaces** • Detect anomalous activities from dashboards built on top of data from various Azure services (Microsoft, 2023l). **Azure Logic Apps** • Utilize Azure Logic Apps automation to alert on various signals and events (Microsoft, 2023an). **Azure Monitor** • Establish visibility to the Azure resources, build dashboards and visualize (Microsoft, 2023bc). • Detect and investigate anomalies (Microsoft, 2023bh). **Azure Network Watcher** • Establish visibility with monitoring, viewing metrics, and enabling logging for VNET resources (Microsoft, 2023ao). **Azure Policy** • Detect anomalies related to overall the state of the environment (Microsoft, 2023ap) **Azure Resource Health** • Detect anomalies related to the health of Azure resources (Microsoft, 2023bd). **Microsoft Sentinel** • Helps with establishing visibility by collecting data from Azure resources, detecting threats, analytics rules, out-of-the box analytics, automation, orchestration and other SIEM and SOAR capabilities (Microsoft, 2023az). **Azure Traffic Manager** • Detect anomalous activities based on health monitoring (Microsoft, 2023ba). **Azure Web application firewall** • Detect anomalous web application requests and traffic (Microsoft, 2023as). **Azure Cost Management** • Spikes in cost may indicate that resources are misused (Microsoft, 2023bf).	
	Analysis use Cases - Microsoft Azure **(Larger Microsoft cloud ecosystem impact considered)** The requirements were related to helping with the analysis of the incident, meaning helping with determining what has happened and what is the root-cause of the incident.	**Analysis use cases - Amazon Web Services** The requirements were related to helping with the analysis of the incident, meaning helping with determining what has happened and what is the root-cause of the incident.
	Microsoft 365 Defender - Product suite: • **Microsoft Defender for Endpoint**	**AWS Athena**

	• Capabilities extend to Azure through Defender for Servers (Microsoft, 2023aa). • Helps in incident investigations with for example cloud security analytics, automated investigations, endpoint timeline visibility, advanced hunting, and other EDR capabilities (Microsoft, 2023o). • **Microsoft Defender for Office 365** • Investigate email-based threats to protect Azure identities (Microsoft, 2023p) • **Microsoft Defender for Identity** • Helps with investigations and identifying suspicious activities and attack paths across the cyber kill chain (Microsoft, 2023ay) • **Microsoft Defender for Cloud Apps** • Helps with incident analysis with ability to drill into cloud application and identity plane logs and events (Microsoft, 2023n). • **Microsoft 365 Defender for Businesses** • Similar capabilities as Defender for Endpoint (Microsoft, 2023f). • **Microsoft Defender Vulnerability Management** • Vulnerability analysis (Microsoft, 2023aw). • **Microsoft Purview - integrates with the Defender suite** • Investigate data misuse and exfiltration with DLP policies (Microsoft, 2023k). • **Azure Active Directory Identity Protection - integrates with the Defender suite** • Investigate threats affecting cloud identities with risk-based analytics (Microsoft, 2023h). **Microsoft Defender for Cloud - Product suite:** • **Microsoft Defender for Servers** • Utilizes capabilities and features of Defender for Endpoint (Microsoft, 2023aa). • **Microsoft Defender for Storage** • Investigating threat analytics arising from activity monitoring and malware scanning of files in the cloud storage (Microsoft, 2023ay). • **Microsoft Defender for SQL** • Investigate anomalous activities related to database resources (Microsoft, 2023t). • **Microsoft Defender for Containers** • Investigating alerts from run-time protection of clusters and cluster nodes (Microsoft, 2023u). • **Microsoft Defender for App Service**	• Analyze anomalies from logs stored in S3 (AWS, 2023e, p. 18). **AWS CloudFormation** • Utilize in automated deployment of response resources such as for forensics collection, and orchestration (AWS, 2023e, p. 48). **AWS CloudTrail** • Utilize CloudTrail logs for analysis for incident related to AWS services and accounts (AWS, 2023e, p. 27). **AWS CloudWatch** • Utilize for analysis for incidents related to AWS resources (AWS, 2023e, p. 43). **AWS Config** • Identify impacted assets and how the incident has changed configuration from historical data (AWS, 2023e, p. 43). **AWS Detective** • Investigate incidents, identify patterns, and visualize data (AWS, 2023e, p. 45). **AWS EC2** • Utilize snapshots of virtual resources to analyze incident artifacts (AWS, 2023bi). **AWS Elastic Beanstalk** • Utilize to deploy tools and scripts to investigate incidents (AWS, 2023aj). **AWS Elastic Block Store (EBS)** • Analyze incident artifacts in snapshots taken with EBS (AWS, 2023e, p. 28). **AWS Firewall Manager** • Utilize dashboards to gain insights for events generated by various network and web protection tools (AWS, 2023c). **AWS GuardDuty** • Provides detailed information on security events it observes that are valuable for incident analysis and to identify the incident root-cause (AWS, 2023e, p. 44). **AWS IAM** • Use to analyze account permissions, permissions modifications, or potential gaps or excess permissions that may be the root-cause of the incident (AWS, 2023bc). **AWS Inspector** • Analyze misconfigurations and vulnerabilities related to AWS resources (AWS, 2023m). **AWS Lambda** • Utilize to perform real-time analysis on events generated by other AWS services or to enrich event data with additional data (AWS, 2023e, p. 45). **AWS Macie**

- Analyze threats related to App Service resources (Microsoft, 2023r).
- **Microsoft Defender for Key Vault**
  - Analyze unusual activities related to secrets stored in the Azure Key vault (Microsoft, 2023w).

Azure Active Directory
- Investigate anomalous and risky activities related to identities and other cloud resources in Azure (Microsoft, 2023ag).

Azure DDoS protection
- Analyze traffic related to DDoS attacks against public facing Azure resources (Microsoft, 2023aj).

Azure Firewall
- Analyze anomalous ingress, egress, and p2p network traffic within Azure and between Azure resources (Microsoft, 2023al)

Azure Log Analytics - in Azure monitor
- Analyze anomalous activities from data from Azure monitor (Microsoft, 2023s).

Log Analytics Workspaces
- Analyze anomalous activities from dashboards build on top of data from various Azure services (Microsoft, 2023l).

Azure Monitor
- Analyze, correlate, visualize to understand root-causes and how Azure resources are operating (Microsoft, 2023bc).

Azure Network Watcher
- Analyze events and trends of VNET resources (Microsoft, 2023ao).

Azure Policy
- Analyze anomalies related to overall the state of the environment (Microsoft, 2023ap)

Azure Resource Health
- Analyze anomalies related to the health of Azure resources (Microsoft, 2023bd).

Microsoft Sentinel
- Help with investigations with log analytics, event correlation, automation, orchestration and with other SIEM and SOAR capabilities (Microsoft, 2023az).

Azure Virtual Machines
- Utilize snapshots of virtual resources to analyze indicators and incident artifacts (Microsoft, 2023ad).

Azure Web application firewall
- Analyze anomalous web application requests and traffic (Microsoft, 2023as).

Microsoft Defender Threat Intelligence
- Utilize threat intelligence in incident analysis
- Helps to determine what kind of data was breached in the incident (AWS, 2023e, p. 45).

AWS S3
- Store incident data that needs to be analyzed in S3 (AWS, 2023e, p. 27).

AWS Security Hub
- Aggregates and normalizes security findings and summarizes them visually on dashboards with actionable graphs and tables that can be beneficial in incident analysis (AWS, 2023e, p. 44).

AWS Shield
- Provides detailed metrics and event logs of DDoS attacks that can be analyzed (AWS, 2023w).

AWS Step Functions
- Utilize to perform real-time analysis on events generated by other AWS services or to enrich event data with additional data (AWS, 2023e, p. 45).

AWS Systems manager
- Can view application and resource operational data that can be used for troubleshooting, but also for incident analysis (AWS, 2023e, p. 46).

AWS Route 53
- Can help with providing additional context around incident and related network and DNS traffic (AWS, 2023e, p. 44).

AWS VPC
- Utilize to analyze for example VPC flow logs (AWS, 2023e, p. 18).

AWS WAF
- Analyze WAF logs to identify the root-cause and the nature of the attack (AWS, 2023g)

AWS OpenSearch Service
- Utilize to analyze incident related data and signals stored in S3 (AWS, 2023e, p. 18).

AWS QuickSight
- Visualize incident related data with Quick Sight (AWS, 2023ax).

Amazon Machine Learning (AWS SageMaker)
- Can potentially help with incident data analysis by for example training machine learning models to detect and analyze anomalies (AWS, 2023ag)

Amazon EMR
- Can potentially help with incident data analysis as it can store and process large amounts of data that could be analyzed (AWS, 2023as).

Amazon X-Ray
- Collects telemetry regarding applications running on AWS resources. Utilize to gain better

		understanding of the applications and the potential root-cause of the incident (2023be).
	Containment use Cases - Microsoft Azure (Larger Microsoft cloud ecosystem impact considered) The requirements were related to revoking access, limiting, isolating, containing, and quarantining the incident.	**Containment use cases - Amazon Web Services** The requirements were related to revoking access, limiting, isolating, containing, and quarantining the incident.

	Microsoft 365 Defender - Product suite:
	• **Microsoft Defender for Endpoint**
	  • Capabilities extend to Azure through Defender for Servers (Microsoft, 2023aa).
	  • Helps with for example host isolation, file quarantine, and other EDR capabilities (Microsoft, 2023o).
	• **Microsoft Defender for Office 365**
	  • Quarantine email-based threats to protect Azure identities (Microsoft, 2023)
	• **Microsoft 365 Defender for Businesses**
	  • Similar capabilities as Defender for Endpoint (Microsoft, 2023f).
	Microsoft Defender for Cloud - Product suite:
	• **Microsoft Defender for Servers**
	  • Utilizes capabilities and features of Defender for Endpoint (Microsoft, 2023aa).
	Azure Active Directory
	• Limit, delete, revoke access for cloud resources and identities (Microsoft, 2023ag).
	Azure Automation
	• Utilize to automate containment response (Microsoft, 2023ah).
	Azure DDoS protection
	• Block traffic related to DDoS attacks against public facing Azure resources (Microsoft, 2023aj).
	Azure Firewall
	• Contain and limit ingress, egress, and p2p network traffic within Azure and between Azure resources with firewall policies, rules, and configurations (Microsoft, 2023al)
	Azure Firewall Manager
	• Centrally manage Azure Firewalls and Firewall policies across multiple subscriptions (Microsoft, 2023al).
	Azure Functions
	• Utilize Azure Functions to automate containment actions (Microsoft, 2023j).
	Azure Logic Apps
	• Utilize Azure Logic Apps to automate containment actions (Microsoft, 2023an).
	Azure Network Security Groups - VNET
	• Configure rules to control network ingress, egress, and Azure p2p traffic (Microsoft, 2023q).
		AWS CloudFormation
		• Deploy new resources or entirely new environments to isolate the incident to another environment (AWS, 2023e, p. 7).
		AWS Config
		• Apply and roll back changes to the environment to contain the incident (AWS, 2023e, p. 43)
		AWS EventBridge (CloudWatch Events)
		• Trigger automated containment measures (AWS, 2023e, p. 43)
		AWS Firewall Manager
		• Apply new rules to block malicious traffic (AWS, 2023c).
		AWS GuardDuty
		• Utilize and integrate with APIs, CLI tools, or CloudWatch events to trigger automated containment actions with for example AWS Lambda or Step Functions (AWS, 2023bf).
		AWS IAM
		• Limit or revoke access to compromised accounts or restrict access to resources (AWS, 2023bc).
		AWS Lambda
		• Utilize to automate containment actions (AWS, 2023e, p. 45).
		AWS SNS
		• Trigger automated containment actions with for example Lambda or Steps Functions (AWS, 2023e, p. 24).
		AWS Security Hub
		• Can integrate with other tools to automate response actions when findings are observed such as containment actions with automation tools (AWS, 2023s).
		AWS Shield
		• Automatically mitigates DDoS attacks (AWS, 2023w).
		AWS Step Functions
		• Utilize to automate containment actions (AWS, 2023e, p. 45).
		AWS Systems manager

	Azure Resource Manager • Create, update, and delete Azure resources (Microsoft, 2023aq). **Microsoft Sentinel** • Automate and orchestrate containment actions (Microsoft, 2023az). **Azure Virtual Network / VNET** • Isolate network segments to contain the incident (Microsoft, 2023ar). **Azure Web application firewall** • Block anomalous web application requests and traffic (Microsoft, 2023as).	• Automate operational tasks across AWS resources such as containment actions (AWS, 2023e, p. 46). **AWS Route 53** • Block traffic from suspicious or unauthorized sources (AWS, 2023e, p. 44). **AWS VPC** • Isolate compromised resources at the network level (AWS, 2023ba) **AWS WAF** • Utilize WAF rules to block malicious traffic (AWS, 2023g)
	Eradication use Cases - Microsoft Azure **(Larger Microsoft cloud ecosystem impact considered)** The requirements were related to eliminating and removing the root-cause of the incident and denying attackers access to the environment.	**Eradication use cases - Amazon Web Services** The requirements were related to eliminating and removing the root-cause of the incident and denying attackers access to the environment.

	Microsoft 365 Defender - Product suite:
	• **Microsoft Defender for Endpoint**
	  • Capabilities extend to Azure through Defender for Servers (Microsoft, 2023aa).
	  • Helps with for example malicious file removal and other EDR capabilities (Microsoft, 2023o).
	• **Microsoft Defender for Office 365**
	  • Remove email-based threats to protect Azure identities (Microsoft, 2023p)
	• **Microsoft 365 Defender for Businesses**
	  • Similar capabilities as Defender for Endpoint (Microsoft, 2023f).
	Microsoft Defender for Cloud - Product suite:
	• **Microsoft Defender for Servers**
	  • Utilizes capabilities and features of Defender for Endpoint (Microsoft, 2023aa).
	Azure Active Directory
	• Eliminate, delete, deny access for cloud resources and identities (Microsoft, 2023ag).
	Azure Automation
	• Utilize to automate eradication response (Microsoft, 2023ah).
	Azure Backup
	• Remove malicious artifacts from the environment by reverting to a previous good state (Microsoft, 2023bb).
	Azure Functions
	• Utilize Azure Functions to automate eradication actions (Microsoft, 2023j).
	Azure Logic Apps
	• Utilize Azure Logic Apps to automate eradication actions (Microsoft, 2023an).
		AWS Backup
		• Remove malicious artifacts from the environment by reverting to a previous good state (AWS, 2023r).
		AWS CloudFormation
		• Delete resources or entire environments that have been compromised and create new ones (AWS, 2023e, p. 7).
		AWS Config
		• Apply and roll back changes to the environment to eradicate the root-cause of the incident (AWS, 2023e, p. 43)
		AWS Elastic Block Store (EBS)
		• Eradicate by restoring data and environments to a known good state from snapshots (AWS, 2023e, p. 33).
		AWS EventBridge (CloudWatch Events)
		• Trigger automated eradication measures (AWS, 2023e, p. 43)
		AWS GuardDuty
		• Utilize and integrate with APIs, CLI tools, or CloudWatch events to trigger automated eradication actions with for example AWS Lambda or Step Functions (AWS, 2023bf).
		AWS IAM
		• Remove access to compromised accounts or resources (AWS, 2023bc).
		AWS Lambda
		• Utilize to automate eradication actions (AWS, 2023e, p. 45).
		AWS Security Hub
		• Can integrate with other tools to automate response actions when findings are observed

	Azure Policy • Eradicate the root-cause of the incident by bulk and automated remediation of non-compliant resources (Microsoft, 2023ap) **Azure Resource Manager** • Create, update, and delete Azure resources (Microsoft, 2023aq). **Microsoft Sentinel** • Automate and orchestrate eradication actions (Microsoft, 2023az). **Azure Update Management** • Apply patches and updates eradicate the root-cause of the incident if the incident is related to a vulnerability (Microsoft, 2023ac). **Azure support** • Azure support can potentially assist with incident root-cause eradication	such as eradication actions with automation tools (AWS, 2023s). **AWS Shield** • Automatically mitigates DDoS attacks (AWS, 2023w). **AWS Step Functions** • Utilize to automate eradication actions (AWS, 2023e, p. 45). **AWS Support** • AWS support can potentially assist with incident root-cause eradication (AWS, 2023aa). **AWS Systems manager** • Automate operational tasks across AWS resources such as eradication actions (AWS, 2023e, p. 46). **AWS WAF** • Utilize WAF rules to block malicious traffic (AWS, 2023g)
	Recovery use Cases - Microsoft Azure **(Larger Microsoft cloud ecosystem impact considered)** The requirements were related to restoration, confirmation of restoration, and the ability to improve the environment.	**Recovery use cases - Amazon Web Services** The requirements were related to restoration, confirmation of restoration, and the ability to improve the environment.

	Microsoft 365 Defender - Product suite:
	• **Microsoft Defender for Endpoint**
	  • Capabilities extend to Azure through Defender for Servers (Microsoft, 2023aa).
	  • Helps with for example removing malware-based threats, or confirming that the threat has been removed, and applying policies to detect similar signals in the future (Microsoft, 2023o).
	• **Microsoft Defender for Cloud Apps**
	  • Potentially helps with identifying any changes that were made during the incident and confirming that the restoration actions were completed.
	• **Microsoft 365 Defender for Businesses**
	  • Similar capabilities as Defender for Endpoint (Microsoft, 2023f).
	• **Microsoft Defender Vulnerability Management**
	  • Vulnerability remediation (Microsoft, 2023aw).
	Microsoft Defender for Cloud - Product suite:
	• **Microsoft Defender for Servers**
	  • Utilizes capabilities and features of Defender for Endpoint (Microsoft, 2023aa).
	Azure Active Directory
	• Restore cloud resources and identities (Microsoft, 2023ag).
		AWS Backup
		• Restore cloud resources and data to a previous good state (AWS, 2023r).
		AWS Billing
		• Some account administration tasks such as resetting the AWS root password can be done via the billing console (AWS, 2023ai).
		AWS CloudFormation
		• Restore and rebuild environments consistently to resemble the pre-incident environment (AWS, 2023e, p. 7).
		AWS Config
		• Restore resources and environments to their previous state (AWS, 2023e, p. 43)
		AWS EC2
		• Recover virtualized resources to a known good state from snapshots (AWS, 2023bi).
		AWS Elastic Beanstalk
		• Restore applications and services to their pre-incident state (AWS, 2023aj).
		AWS Elastic Block Store (EBS)
		• Recover data from snapshots (AWS, 2023e, p. 33).
		AWS Elastic Disaster Recovery
		• Recover AWS resources (AWS, 2023bb).
		AWS EventBridge (CloudWatch Events)

	Azure Automation • Utilize to automate recovery response (Microsoft, 2023ah). **Azure Backup** • Restore cloud resources and data to a previous good state (Microsoft, 2023bb). **Azure Blob storage** • Utilize blob storage for storing backups of Azure resources (2023ai). **Azure Cosmos DB** • Provides disaster recovery capabilities (Microsoft, 2023b). **Azure Functions** • Utilize Azure Functions to automate recovery actions (Microsoft, 2023j). **Azure Logic Apps** • Utilize Azure Logic Apps to automate recovery actions (Microsoft, 2023an). **Azure Policy** • Restore from incident by bulk and automated remediation of non-compliant resources (Microsoft, 2023ap) **Azure Resource Manager** • Create, update, and delete Azure resources (Microsoft, 2023aq). **Microsoft Sentinel** • Automate and orchestrate recovery actions (Microsoft, 2023az). **Azure Site Recovery** • Helps with recovery with automating and orchestrating replication of Azure resources between regions (Microsoft, 2023a). **Azure Traffic Manager** • Utilize load-balancing and automated failover models to recover from network-based attacks (Microsoft, 2023ba). **Azure Virtual Machines** • Recover virtualized resources to a known good state from snapshots (Microsoft, 2023ad). **Azure support** • Azure support can potentially assist with incident recovery	• Trigger automated recovery measures (AWS, 2023e, p. 43) **AWS Glacier (S3 Glacier)** • Utilize for long term data archiving, retention, and recovery (AWS, 2023af). **AWS GuardDuty** • Utilize and integrate with APIs, CLI tools, or CloudWatch events to trigger automated recovery actions with for example AWS Lambda or Step Functions (AWS, 2023bf). **AWS IAM** • Restore accounts and permissions to resources (AWS, 2023bc). **AWS Lambda** • Utilize to automate recovery actions (AWS, 2023e, p. 45). **AWS OpsWorks** • Restore and rebuild environments consistently to resemble the pre-incident environment (AWS, 2023bh). **AWS RDS** • Capabilities include automated backups and database snapshots that can help in recovering from incidents affecting database resources (AWS, 2023o). **AWS S3** • Can be used to restore critical data and backups (AWS, 2023ay). **AWS SNS** • Trigger automated containment actions with for example Lambda or Steps Functions (AWS, 2023e, p. 24). **AWS Security Hub** • Can integrate with other tools to automate response actions when findings are observed such as recovery actions with automation tools (AWS, 2023s). **AWS Service Catalog** • Helps recovery with the ability to redeploy standard configurations of affected resources and services (AWS, 2023ah). **AWS Shield** • Automatically mitigates DDoS attacks (AWS, 2023w). **AWS Step Functions** • Utilize to automate recovery actions (AWS, 2023e, p. 45). **AWS Support** • AWS support can potentially assist with incident recovery (AWS, 2023aa). **AWS Systems manager**

		• Automate operational tasks across AWS resources such as recovery actions (AWS, 2023e, p. 46). **AWS Route 53** • Monitor DNS traffic to identify if the recovery was successful (AWS, 2023e, p. 44). **AWS VPC** • Restore service availability and implement network level controls to prevent similar incidents from happening (AWS, 2023ba). Monitor network traffic to identify if the recovery was successful (AWS, 2023ba) **AWS WAF** • Utilize WAF rules to block malicious traffic and monitor that the recovery actions were successful (AWS, 2023g)
	Post incident use Cases - Microsoft Azure (Larger Microsoft cloud ecosystem impact considered) The requirements were related to learning from incidents and improving other incident response phases.	**Post incident use cases - Amazon Web Services** The requirements were related to learning from incidents and improving other incident response phases.

	Microsoft 365 Defender - Product suite:
	• **Microsoft Defender for Endpoint**
	  • Capabilities extend to Azure through Defender for Servers (Microsoft, 2023aa).
	  • Helps with for example applying policies to alert, contain, or eradicate indicators if similar signals from a known incident are observed again. (Microsoft, 2023o).
	• **Microsoft Defender for Office 365**
	  • Learn from education capabilities such as phishing campaign simulations (Microsoft, 2023p).
	• **Microsoft 365 Defender for Businesses**
	  • Similar capabilities as Defender for Endpoint (Microsoft, 2023f).
	Microsoft Defender for Cloud - Product suite:
	• **Microsoft Defender for Servers**
	  • Utilizes capabilities and features of Defender for Endpoint (Microsoft, 2023aa).
	Azure Active Directory
	• Automation learns and sets baselines for users and detects anomalous signals it has seen before (Microsoft, 2023ag).
	Azure DevOps
	• Utilize Azure DevOps collaboration tools to help with project management related to improving incident response capabilities, tracking, and learning from incidents.
	Microsoft Sentinel
		AWS Elastic Disaster Recovery
		• Perform non-disruptive testing and simulations (AWS, 2023bb).
		AWS GuardDuty
		• Improve and create custom detection rules and maintain and update own threat intelligence regarding known bad indicators to better detect and handle similar incidents in the future (AWS, 2023bf).

	• Improve analytics, automation, and orchestration capabilities based on previous incidents (Microsoft, 2023az).	