



Detecting Insider Threats Using User and Entity Behavior Analytics

Petri Hakonen

Master's thesis

October 2022

Information technology

Master of Engineering in Information Technology, Cyber Security

Hakonen, Petri

Detecting Insider Threats Using User and Entity Behavior Analytics

Jyväskylä: JAMK University of Applied Sciences, October 26, 2022, 72

Information technology, Master of engineering in information technology, cyber security, Master's thesis

Permission for web publication: Yes

Language of publication: English

Abstract

Information technology advancements made during the past decade have made detecting adversaries extremely hard and almost impossible, so detection mechanisms have also evolved from old signature-based systems to look at the behavior of users, entities, and software.

The purpose of this master's thesis is to research and gather the basic knowledge of insider threat taxonomy, what are the common indicators in human behavior, how those indicators could be potentially detected via technical logs (machine data) with user and entity behavior analytics tools and what are the prioritized use cases. In my master's thesis process I utilized a mixed method approach of research. Background information was gathered through literature review, interview and familiarizing myself with the use cases of User and Entity Behavior analytics tool developed by Splunk Inc.

The findings of my research indicate that traditional security methods relying on rules and known patterns are not going to disappear, but they will remain as a key part of the layered defense. The effectiveness of these solutions will be multiplied by adapting AI driven user behavior analytics on top of them. User behavior analytics tools are providing a different approach to anomaly detection and relying on a range of analytical approaches. These are usually a combination of basic analytics methods and advanced analytics. Basic analytics means simple statistics, signatures, and pattern matching. Advanced analytics are relying in AI capabilities, and this allows the tool to learn and adapt faster to changes and does not require a similar level of human intervention. The changes are seen as anomalies from usual behavior, whether it is based on learning from individual behavior over times or from predefined role-based baselines.

Keywords/tags (subjects)

Security, cyber security, insider threat, user behavior analytics, artificial intelligence

Miscellaneous (Confidential information)

n / a

Hakonen, Petri

Detecting Insider Threats Using User Behavior Analytics

Jyväskylä: Jyväskylän Ammattikorkeakoulu, lokakuu 26, 2022, 72

Tietojenkäsittely ja tietoliikenne. Tieto- ja viestintäteknikan tutkinto-ohjelma, Master's Degree Programme in Information Technology, Cyber Security. Opinnäytetyö YAMK.

Verkkojulkaisulupa myönnetty: Kyllä

Julkaisun kieli: englanti

Tiivistelmä

Viime vuosikymmenen aikana saavutetut tietotekniikan edistysaskeleet ovat tehneet vastustajien havaitsemisesta erittäin vaikeaa, ellei jopa lähes mahdotonta, joten myös tunnistusmekanismit ovat kehittyneet perinteisistä sääntöpohjaisista järjestelmistä tarkastelemaan käyttäjien, entiteettien ja ohjelmistojen käyttäytymistä.

Tämän opinnäytetyön (YAMK) tarkoituksena on tutkia ja kerätä perustiedot sisäpiirin uhkien taksonomiasta, mitkä ovat yleisimmät indikaattorit ihmisten käyttäytymisessä, kuinka ne voitaisiin mahdollisesti havaita teknisten lokien (konedatan) avulla käyttäjien ja entiteettien käyttäytymisanalytiikalla ja mitkä ovat ensisijaisia käyttötapauksia. Opinnäytetyö (YAMK) prosessissani käytin tutkimukseen sekamenetelmää. Taustatietoa kerättiin kirjallisuuskatsauksen, haastattelun ja Splunk Inc:n kehittämän User and Entity Behavior Analytics -työkalun käyttötapauksiin tutustumisen kautta.

Tutkimukseni tulokset osoittavat, että perinteiset sääntöihin ja tunnettuihin malleihin perustuvat turvallisuusmenetelmät eivät katoa, vaan ne säilyvät keskeisenä osana kerrostettua puolustusta. Näiden ratkaisujen tehokkuus moninkertaistuu lisäämällä tekoälyyn perustuvaa käyttäytymisanalytiikkaa niiden päälle. Käyttäytymisen analytiikkatyökalut tarjoavat erilaisen lähestymistavan poikkeamien havaitsemiseen ja luottavat useisiin analyttisiin lähestymistapoihin. Nämä ovat yleensä yhdistelmä perusanalytiikkamenetelmiä ja edistyksellistä analytiikkaa. Perusanalytiikka tarkoittaa yksinkertaisia tilastoja ja ennalta määriteltyjä sääntöjä. Kehittynyt analytiikka tukeutuu tekoälyyn, mikä mahdollistaa työkalun oppimisen ja sopeutumisen muutoksiin nopeammin, eikä se vaadi samantasoista ihmisen puuttumista. Muutokset nähdään tavanomaisen käyttäytymisen poikkeavuuksina, perustuivatpa se sitten yksilöllisen käyttäytymisen oppimiseen ajan mittaan tai ennalta määritellyistä roolipohjaisista lähtökohdista.

Avainsanat (asiasanat)

Turvallisuus, kyber turvallisuus, sisäinen uhka, käyttäytymisen mallintaminen ja analytiikka, keinoäly

Muut tiedot (salassa pidettävät liitteet)

n / a

Contents

1	Introduction	7
1.1	Purpose and objectives of research	8
1.2	Research methods	9
1.3	Literature review process	11
1.4	Interview process and familiarization to Splunk UBA/UEBA tool	13
1.5	Ethicality and reliability of research	14
2	Insider threat	15
2.1	Approach to insider threats	17
2.2	Insider threat taxonomy	17
2.3	Intentionality and reason	18
2.4	Profile	19
2.5	Indicators	22
2.6	Attack statistics	24
3	User Behavior Analytics (UBA) / User and Entity Behavior Analytics (UEBA)	26
3.1	Technology	28
3.2	Analytics methods	29
4	Detecting insider threats	32
4.1	Background, physical and digital indicators	34
4.2	Use cases and log sources	38
4.2.1	Account Misuse	39
4.2.2	Compromised User Account	42
4.2.3	Compromised and Infected Machine	45
4.2.4	Data Exfiltration	48
4.2.5	Lateral Movement	52
4.2.6	Suspicious Behavior / Unknown Threats	56
4.3	Prioritization	61
5	Conclusion	63
	References	67

Figures

Figure 1. Insider threat types, (adapted from Intelligence and National Security Association, 2019)	16
Figure 2. Insider threat types (Adapted from Jääskeläinen, 2018)	17

Figure 3. Intentionality (Adapted from Jääskeläinen, 2018).....	18
Figure 4. Insider threat profiles (Adapted from Jääskeläinen, 2018)	20
Figure 5. CMU research statistics (Miller, 2016).....	22
Figure 6. Affected devices of insider attacks (Miller & Pickering, 2020)	26
Figure 7. Log / event data sources (Splunk Inc, 2022)	30
Figure 8. UEBA Dashboard (Splunk UBA/UEBA screen capture).....	33
Figure 9. UEBA watchlist (Splunk UBA/UEBA screen capture)	33
Figure 10. Account information from HR data (Splunk UBA/UEBA screen capture)	34
Figure 11. Authentication data views (Splunk UBA/UEBA, screen capture).....	40
Figure 12. Account misuse example 1 (Splunk UBA/UEBA, screen capture)	40
Figure 13. Account misuse example 2 (Splunk UBA/UEBA, screen capture)	41
Figure 14. Suspicious data access (Splunk UBA/UEBA screen capture).....	41
Figure 15. AD data views (Splunk UBA/UEBA, screen capture)	43
Figure 16. Data exfiltration by compromised account (Splunk UBA/UEBA screen capture)	44
Figure 17. Land speed violation (Splunk UBA/UEBA screen capture).....	45
Figure 18. DNS data views (Splunk UBA/UEBA, screen capture)	47
Figure 19. Compromised machine (Splunk UBA/UEBA screen capture).....	47
Figure 20. Suspicious network traffic (Splunk UBA/UEBA screen capture)	48
Figure 21. DLP data views (Splunk UBA/UEBA, screen capture).....	49
Figure 22. Data Exfiltration by suspicious user or device (Splunk UBA/UEBA screen capture) .	50
Figure 23. Unusual USB activity (Splunk UBA/UEBA screen capture).....	51
Figure 24. Excessive data printed (Splunk UBA/UEBA screen capture).....	51
Figure 25. Excessive data transmission (Splunk UBA/UEBA screen capture)	52
Figure 26. Network data views (Splunk UBA/UEBA, screen capture).....	53
Figure 27. Unusual scanning activity (Splunk UBA/UEBA screen capture)	54
Figure 28. Malicious AD activity (Splunk UBA/UEBA screen capture)	54
Figure 29. Unusual machine access (Splunk UBA/UEBA screen capture).....	55
Figure 30. Badge access data views (Splunk UBA/UEBA, screen capture).....	57
Figure 31. User dashboard with risk score (Splunk UBA/UEBA screen capture)	57
Figure 32. User facts and summary (Splunk UBA/UEBA screen capture)	59
Figure 33. Suspicious badge activity (Splunk UBA/UEBA screen capture).....	60
Figure 34. Unauthorized login (Splunk UBA/UEBA screen capture)	61

Tables

Table 1. Background, physical and digital indicators associated to different threat types (Kont et al., 2014; Proofpoint US, 2021).....	38
Table 2. Log source prioritization based on Splunk use cases	63

1 Introduction

The digital battlefield is changing and expanding fast and there are no more distinct organizational borders to defend within information technology field. Organizational networks are rapidly expanding through cloud services and remote work, which open new attack vectors to monitor and defend, since people are accessing data outside corporate perimeters, storing machines and for example USB-media at their home offices and utilizing vulnerable personal wireless networks (Hartline, 2017). All these changes have made it harder to detect an insider threat. This is especially true, if one does not have a proper insider threat management program in place, which includes everything from executive buy in, assessment, plan, training, and monitoring (Krishnan, 2022). Adversaries are becoming better equipped, well-funded and in some cases, the criminals are either backed by or working directly for nation-state players. It is a multi-billion-dollar business, so, for the defenders it is becoming almost impossible to defend the IT environments they are paid to protect, or at least it is impossible with old fashioned perimeter and signature-based security solutions like for example basic antivirus and firewalls (Mehan, 2016).

Based on a recent report from Ponemon (2020 Cost of Insider Threat Report | Proofpoint UK, 2020), cybercrime costs are expected to grow by almost 15 percent per year over the next four years and reaching the mindboggling \$10 trillion USD annually by 2025. At the same time, the increase of cybersecurity incidents caused by insiders, have grown from 2018 by staggering 47%. The monetary impact of these insider caused incidents has been estimated to be averaging around \$11,5 million annually including direct financial impacts but also the impact caused by loss of reputation (2020 Cost of Insider Threat Report | Proofpoint UK, 2020).

There are multiple types of insider threats ranging from discontent employee wishing to penalize the employer from being mistreated, all the way up to a nation-state sponsored espionage, resulting into a fact that all insiders are not created equal. Some of them pose a bigger risk than others and therefore organizations need to be able to identify those that are considered as a bigger risk. Organizations need to be able to identify the people, soon-to-depart employees, contractors etc. who have the high-level privileged access to sensitive data or to proprietary information. Their access and movements need to be monitored closely and organizations need to have a strict procedure for exiting the organization. Unfortunately, processes are not enough to

mitigate the threat, but organizations also need to implement required technological solutions as well (Thompson, 2018).

Traditional security methods relying on approach of rules and known patterns, solutions like firewalls, intrusion detection systems, antivirus, next generation endpoint protection and Security Incident Event Management (SIEM) tools are not going to disappear, but those will remain as a key part of the layered defense. The effectiveness of these solutions will be multiplied by adapting AI driven user behavior analytics on top of them. Why we need the mix? As the tools and strategies of the attackers change, us people tasked to defend are not able to keep up and create the necessary rules from past events in time to detect them in the future. Even if we can develop those rules in short amount of time, the attackers have already changed their methods just slightly and are able to bypass the perimeter.

User behavior analytics tools are providing a different approach to anomaly detection and relying on a range of analytical approaches. These are usually a combination of basic analytics methods and advanced analytics. Basic analytics are simple statistics, signatures, and pattern matching and advanced analytics are relying in Artificial Intelligence (AI) capabilities. These AI advancements allows the tool to learn and adapt faster to changes in behavioral features and doesn't require similar level of human intervention. The changes are seen as anomalies from usual behavior, whether it is based on learning from individuals over a long period of time or from predefined roles-based baselines. These analytics tools analyze multiple different aspects and log sources, for example access to systems and facilities, changes in networks or transfer of data, to evaluate activity of entities and users against learned baseline. These log sources can be for example hosts, login information from networks and applications, network traffic and data storages and this information is used to detect potential incidents that are planned or executed by insiders or outside attackers that cannot be detected by traditional methods (Beardsley et al., 2021).

1.1 Purpose and objectives of research

The Insider threat topic has been my personal interest for years, but the encouragement to research this topic further also came from my employer. In my organization, we have identified a

long time ago the problematic nature of malicious insiders and the difficulty to detect the potential actions indicating such behavior. Though this is an important for my organization, this is a universal issue impacting all, regardless of industry or the size of the organization.

The purpose of this master's thesis was to research and gather the basic understanding of insider threat taxonomy, what are the common indicators in human behavior, how those indicators could be potentially detected via technical logs (machine data) with User behavior Analytics (UBA) or User and Entity Behavior Analytics (UEBA) tools and what are the prioritized use cases.

Objective is to research the topic purely from internal security perspective and concentrating on the employees, who for some reason decide to do the wrong thing, bypass rules, and endanger the environment, steal something, and share/sell it to people or organizations that are looking to profit from it. Reasons behind such a decisions and actions are diverse and not always malicious, but nevertheless bad decisions that put the organization at risk. For organizations to be able to detect, prevent and investigate these types of cases, they need to understand the person, means and motivations behind the action. Through understanding the insider threat and corresponding technology to mitigate it, the result of this master's thesis could be used as a prioritized blueprint for organizations battling against this threat, to plan, improve and build their defenses. This blueprint is again universal and applicable to all organizations regardless of size, location, or trade. It is prioritized, so based on available resources, every organization can scale according to their appetite.

Research question driving the master's thesis: How can one utilize User and Entity Behavior Analytics tools to detect different indicators of insider threats?

1.2 Research methods

In my master's thesis process I utilized a mixed method approach. The reason why I chose this approach was the requirement to research quantifiable facts, for example studies that prove certain types of indicators being associated to different types of insider threat actors, and also statistics related to attacks executed by these insider threats, but also the to provide more in-depth view and subject matter expertise on the UBA/UEBA tool itself, I needed to conduct an interview and review case studies which are methods associated with qualitative research. Additionally, to

my personal view on this methodology, according to Tuomi & Sarajärvi, utilizing both qualitative and quantitative methods together provide a good assurance, that the research is not missing any factors or points of views, that could be missed by utilizing just one method (Tuomi; Sarajärvi, 2018).

In this thesis, the theoretical information is gathered through multiple different methods including literature review, using scientific publications, case studies, semi-structured subject matter expert interview, and through studying use cases from UBA/UEBA tool test environment built by Splunk Inc.

A literature review means studying available information published in different sources and targeted to a specific topic. In certain cases, the literature sources could be contained to a time frame or a region to narrow down the search and material. As simple as summary from multiple reviewed sources can be accounted as a literature review, but usually there needs to be a proper structure, analysis, and synthesis to present acquired knowledge and conclusions compared to other research and theories (McCombes, 2019). Theoretical Information gathering and literature review to this thesis is conducted from publications from different databases like janet.finna.fi, mpkk.finna.fi and open-source (Google Scholar etc.) utilizing search terms criminal behavior, computer security, risk management, internal threat, user behavior analytics, cyber security, advanced threats.

A semi-structured interviews are utilized to gather qualitative open-ended data and highlights the interviewees meanings and interpretations and how those are formed. Semi-structured interview process and questions are not set in stone, but rather based on the interaction between the interviewer and interviewee (Tuomi & Sarajärvi, 2018). In my thesis process, I conducted this interview with Splunk Inc's regional sales engineer during my introduction to the UBA/UEBA tool. This approach allowed me to familiarize myself with the functionalities of the tool, but also to acquire a Splunk UBA/UEBA subject matter experts view on the insider threat phenomena and to the capabilities to detect associated indicators. As a part of subject matter expert review, I was allowed to study and utilize Splunk Inc. UBA/UEBA test environment to gather use case examples, related logs and information on what exactly the solutions are looking for from the logs (Splunk Inc., 2022). This was important to visualize the solution and its capabilities and because

building this type of test environment would be impossible due to the requirement of logs, the quantity of samples and the complexity of the solution.

For information source evaluation I used the P.R.O.V.E.N methodology (Carey, 2021). The process of evaluating a source according to P.R.O.V.E.N, requires fact-checking and analyzing the source itself. This is especially true when we are talking about open-source information from internet. One needs to examine, if the information can be verified by another source, analyze if the information itself is relevant and what is the expertise of the author to make claims. Also, one needs to verify the authors objectivity, purpose of the resource and there is a method to confirm the findings.

P.R.O.V.E.N acronym derives from the first letters of six step process to help the writer to evaluate and verify the sources which are planned to be utilized in the writing process (Carey, 2021):

- **Purpose**, why and how was this source created and who is the planned audience?
- **Relevance**, what is value and usefulness of the source and how does it compare to others? More importantly, does it answer writer's questions?
- **Objectivity**, Is the information complete, reasonable, and presented professionally without a strong personal agenda?
- **Verifiability**, is the information accurate, truthful, and backed up with factual evidence that can be verified from another source?
- **Expertise**, what is the authority of the authors? Are the sources reviewed or peer reviewed?
- **Newness**, what is the age of the information and are there newer sources available?

1.3 Literature review process

There are multiple research papers written about insider threats (Homoliak et al., 2019) and several papers on user behavior analytics (Salitin & Zolait, 2018), so there is plenty of good research and documentation to review and study to have the basic knowledge of both topics. User behavior technology is relatively new in the world of information technology, and it is evolving with great speed with artificial intelligence. UBA/UEBA systems first appeared in the early 2000 and were mainly used as market analysis tools. Technological advancements have created new opportunities for achieving better visibility and detection capabilities, thus resulting also for further

research, including combining the UBA/UEBA technology in the context of insider threat detection.

As mentioned in the research methods section the theoretical information to this master's thesis was gathered through multiple different methods including literature review using scientific publications, books, white papers, and case studies. For internal threats, I concentrated more on sociology related research, but also documentation and guides written by governmental security entities. Jääskeläinen, (2018) Cybersecurity and Infrastructure Security Agency, (2020), Greene-meier, (2007), Whitty, (2021), to mention few, who have done extensive research on the threats. Key question from the existing research is what is an insider threat, what are the motivations behind the actions and more importantly to me, what are the potential indicators?

From technical UBA/UEBA perspective there is a good amount of documentation, but also the use cases are extensive. UBA/UEBA is utilized in so many different areas of business, so the problem becomes to find the right sources for writer specific requirements. In my literature review, I tried to concentrate on utilizing appropriate and as accurate as possible search words to avoid overloading the results. During my review I found good sources like Krasznay & Hámornik, (2018), Shashanka et al., (2016), who were looking at the UBA/UEBA capabilities on detecting behavioral patterns of a cyber-attack as a part of bigger enterprise security framework. In my opinion this is important aspect, since the monitoring of internal threat indicators from UBA/UEBA tools will usually be tasked to the same people monitoring the enterprise cyber-security in security operations centers. During my review I was also able to discover previous thesis's from Seppänen, (2021) and Jääskelä, (2020) that were looking into the task and challenges of designing and implementing UBA/UEBA solution. Both papers were taking a deeper dive to a specific vendor solution or looking at the detailed mechanisms on how the learning happens within the technology.

So, it is obvious there is a lot of research to review, but still I found that significant amount is still concentrating either on the human side or purely on the technology itself and what are the next evolutions. Documents that are looking in to detecting insider threats with UBA/UEBA technology exist, but the ones I found were concentrating on pure technical requirements, or a very detailed technical challenge for example detecting a foreign keyboard in network traffic. Also,

these research papers do not dive into details on what insider threat is, what are the physical indicators and what are the corresponding technical indicators of such behavior, to further explain the reasons and indicators from physical to digital and vice versa.

1.4 Interview process and familiarization to Splunk UBA/UEBA tool

Interview with Splunk Inc. subject matter expert was conducted online simultaneously while I was taught to use the Splunk UBA/UEBA tool in their online test environment. Interview was conducted as a semi-structured interview which aims to gather qualitative open-ended data and highlights the interviewees meanings and interpretations. During the interview, we were able to dive into the mechanics of the tool itself, but also to the experiences of the subject matter expert.

I have had the privilege to utilize UBA/UEBA tools during my career about 4-5 years ago, but during then the use cases were far less complex than they are now. Also, the technology has developed vastly from those days and now I saw an opportunity at my current employer's environment to potentially utilize this technology to enhance our internal security capabilities, so I had to seize the moment. This master's thesis topic gave me the perfect excuse to spend more of my time to expand my knowledge on this technology and to present the findings as a basis and reasoning why we should embark on this journey as an organization.

Being able to utilize and explore the Splunk test environment gave me a lot of information to advance this research, but also provided good illustration to better explain what the tools is looking at with different insider threat scenarios. Part of my daily life is to develop methods and means to detect, prevent, and investigate insider threats. I have spent over 20 years within the ICT-industry and from all those years, majority has gone within security and cyber security domains. My specialty has been on operational side of things, trying to perfect the art of detecting bad things and what to do, when something is detected. When nation state actors, organized crime or internal threats gain access to the information one is trying to protect, they do not use malware or any similar malicious software which could be detected by traditional means. They utilize the target environments IT-tools or previously gained privileged access to gather information or whatever is on their specific agenda. So, one needs to look for other kinds of indicators of

compromise, like behavioral patterns of a user, weird login times, locations etc. This is especially true, when it comes to internal threats, whether they are intentional or not (Brancik, 2007).

To be able to do that I need to document what internal threats are, what are the common physical indicators and corresponding technical indicators. Also, we need to look at where the UEBA technology came, where is it now and especially what are the future enhancements that will be the game changers for our ability to detect those internal threats.

1.5 Ethicality and reliability of research

To guarantee quality and ethics of my research the process was defined in detail before initiating the research. Mixed method was chosen as the main methodology as it provides both qualitative and quantitative data, which is gathered through different sources including literature review, interview and utilizing a test environment to further provide proof for conclusions. The quality of the sources for theoretical information was checked with P.R.O.V.E.N methodology (Carey, 2021) and the level and depth of questions used in the interview were explained before initiating the interview itself. Result and conclusions from the capabilities of the Splunk UEBA tool, was shared with the Splunk subject matter expert to verify that authors conclusions were correct from technical perspective and truthful to the capabilities of the Splunk UBA/UEBA tool.

This thesis is based on non-classified open-source information, earlier research, scientific publications and for example vendor specific white papers. The semi-structured subject matter expert interview and vendor demo environment data will not include any proprietary and/or personally identifiable data that would require heavy data management process and safe keeping. The vendor supporting the thesis through interviews provided only public data and did not require non-disclosure agreements. The vendor specific information shared in this master's thesis was sent for review and approval before finalizing the thesis.

Human error caused by erroneous interpretation is possible. This is since the analysis and conclusions of the gathered data was conducted by the author alone.

2 Insider threat

Insider threats are one of today's most challenging cybersecurity issues alongside with nation state threat actors and organized crime organizations. These challenges are not well addressed by commonly employed perimeter or signature-based security solutions. To be able to understand how to utilize UBA/UEBA to detect insider threats, the organization first needs to understand who the insiders are, what motivates them and what are the potential indicators. Insider threats are one of the most challenging attack models to detect and deal with in real life. The malicious insiders have the advantage against outside threat, as they already possess legitimate access to the environment in some extent and it is easier and less noticeable to gain additional privileges. Insiders that are working with information technology, often have detailed knowledge of the flaws, vulnerabilities and security controls allowing them to bypass basic type of monitoring. So, it can be easy to commit a fraud and for this reason, even trusted, and honest individuals can succumb to temptation or lured with a substantial payoff (Hamin, 2000). According to some recently done surveys (2020 Cost of Insider Threat Report | Proofpoint UK, 2020), approximately 27% of all cybercrime incidents were estimated to be carried out by insiders. Additionally, the same survey ((2020 Cost of Insider Threat Report | Proofpoint UK, 2020) suggested that roughly around 30% of responses indicated that the damage caused by insiders was more severe than the similar attacks initiated by outside threat actors. This increasing numbers of insider attacks has raised the awareness and initiated a new requirement for security planning, which is insider threat programs. These programs have been tasked to identify the potential targets, vulnerabilities and aligning threat and mitigate them. Programs like this are always a sensitive topic because the organization is monitoring their employees and to a certain extent their personal lives. It is crucial, that these programs are transparent, respect privacy rights and laws, and have the understanding and support of personnel (NITTF Produced Guides & Templates, 2017).

What is an insider and what means insider threat? An insider does not mean that it must be an employee of the organization. Insider can be basically anybody with an authorized access to organizations information, premises, and assets, like a contractor, consultant or outsourced service staff like developers, cleaners, even vendors selling organizations products, and so forth (Cybersecurity and Infrastructure Security Agency, 2020). Being an insider does not mean that one is bad. Insider threat on the other hand means that one is.

I like the Intelligence and National Security Alliances (INSA) definition, where it is stated that the insider threat is a threat resulting from someone who has, or had, authorized access to classified information, facilities, networks, people or assets, and who intentionally or unintentionally commits actions contrary to law or organizational policy which contribute to or may contribute to harm by causing the loss or destruction of classified information, facilities, networks, people or assets (Intelligence and National Security Association, 2019).

To understand the relevant approach to insider threats, organizations need to take consideration what is the environment that they are approaching this topic from. One of the widely used models is the definition from Intelligence and National Security Associations (2019), that in my personal view provides a good starting point to describe this phenomenon in easily understandable high-level format. INSA approach is to define five different types of insider threat, see Figure 1:

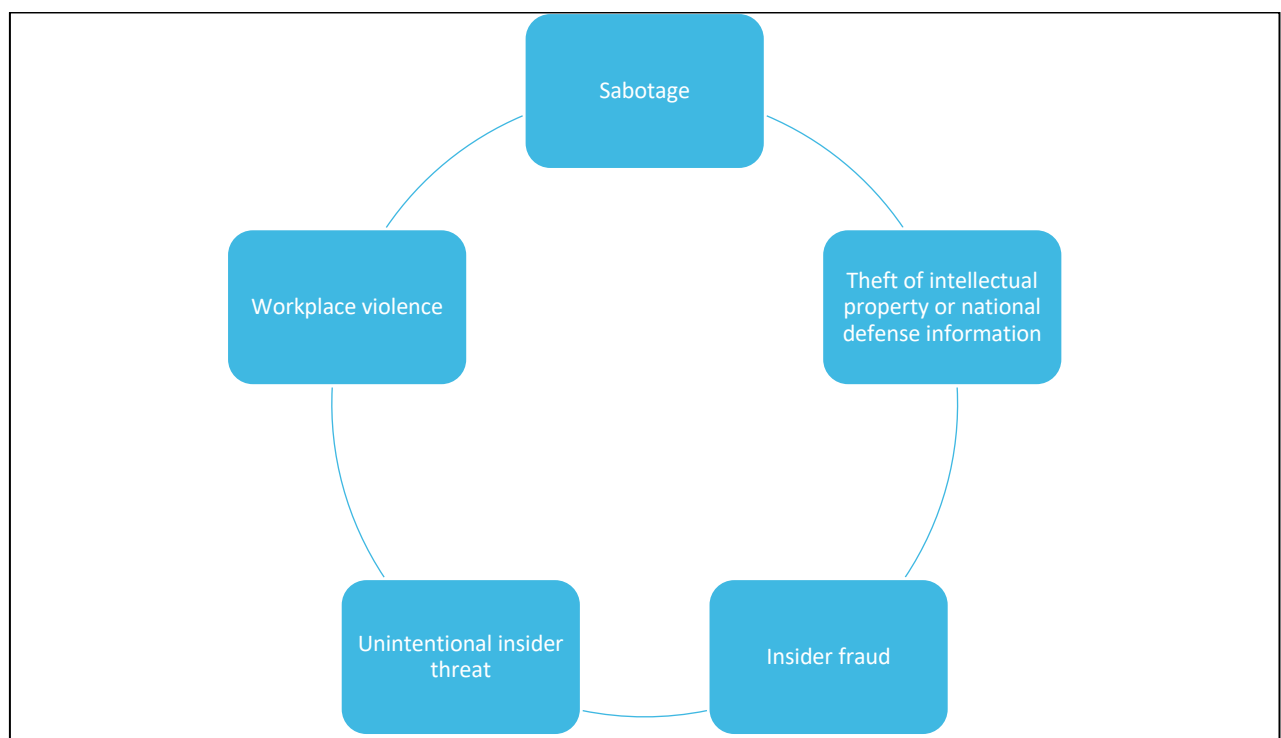


Figure 1. Insider threat types, (adapted from Intelligence and National Security Association, 2019)

2.1 Approach to insider threats

As mentioned, this is a high-level approach and a good starting point, but for my personal preference, is lacking some depth on describing the different nuances, drivers, and motivations behind the activity. Finnish Security Intelligence Services published a paper which was based on Jääskeläinen research, where the author utilizes a more in-depth approach on looking at this topic from perspective of securing proprietary information (PI) from insider threats (Jääskeläinen, 2018). This approach expands the point of view and provides a more comprehensive definition, that takes in consideration more than just the threat type. It also includes different variables like if the act was intentional or unintentional, what were the potential reasons behind the act and what is the profile of the person in question. This taxonomy model described in the FSIS publication is applying the research from Cappelli et al (2012) and Gelles, (2016). Cappelli added the layer of intentionality and Gelles further introduced the variables disregard and ignorance. We will dive deeper into this insider threat taxonomy in following sections.

2.2 Insider threat taxonomy

Insider threat taxonomy in this thesis is mainly based on the earlier research done by Jääskeläinen (2018). The threat types in Jääskeläinen (2018) are categorized similarly as in model from Intelligence and National Security Association (Intelligence and National Security Association, 2019). The five main threat types are:

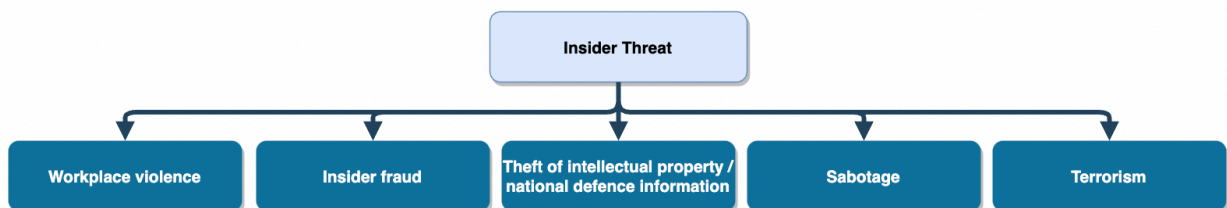


Figure 2. Insider threat types (Adapted from Jääskeläinen, 2018)

Workplace violence: This contains all forms of violence, abuse, intimidation, bullying, offensive jokes, or other threatening behavior, that occurs in a persons place of employment, whether it is physical intimidation or psychological harassment.

Fraud: In this case, the insider is deleting, adding, modifying, or using inappropriately organizational information, tools, or systems to usually gain personal benefits. Traditional example comes from financial world in a form of insider trading, embezzlement etc. This can also be done by a trusted business partner, who has access to these systems or information.

Theft of intellectual property, sensitive and/or classified materials or information: This is probably one of the most common types of insider attack. In this case, the insider is stealing information or material for example to benefit financially by selling it forward. Motivation behind this can also be political, espionage or forced by outsider entity.

Sabotage: This means the purposeful / Intentional destruction of material, whether it is in physical or electronical format to cause harm to the organization and / or individuals within.

Terrorism: United Nations, have their own definition of terrorism manifested in Security Council's resolution 1566 (2004), but I am more drawn into Northern Atlantic Treaty Organizations (NATO) version which in my opinion is more descriptive and usable (Yalcinkaya, 2021). NATO considers all unlawful threats to use violence, instill terror and fear against individuals or property, with the objectives driven by political, religious, or other ideological agendas, to gain control over a population by threatening governments and societies as acts of terrorism (Yalcinkaya, 2021).

2.3 Intentionality and reason

Whatever the type of the insider threat turns out to be, there is always the potential for the actions to be either intentional or unintentional.



Figure 3. Intentionality (Adapted from Jääskeläinen, 2018)

If we look at the unintentional act, which is by no means lesser evil, there is diverse set of reason behind it. Unintentional insider threat is a person that bends the rules, whether it is within organizations networks, systems, data, or even physical premises, thus resulting into destruction, harm, and costs to the organization. This can be due to lack understanding, laziness or just being plain negligent, but nevertheless through action or inaction these persons, without any malicious intent, cause massive harm through for example accidental disclosure of classified information, opening phishing emails or even losing physical items containing sensitive information. Sometimes, this kind of unintentional malicious behavior, that undermines security can be a symptom from badly designed or unsuitable tools, for example difficult procedures or applications that does not function as planned. For organization to be able to detect such behavior, resulting from unsuitable procedures or tools, can act as a driver for a change, thus resulting in better operations and security. Organizations are also battling these unintentional insiders via education and training programs, spending a lot of time, effort, and money, to make employees understand the importance of security. The main causes for these programs to fail is either too complex and heavy material or the lack of accountability from users and management (Blowers, 2015).

Intentional act can also be driven by multiple reasons and not all are malicious. Example from intentional, but not necessarily malicious in the true sense of the word. Whistleblowing, where the insider might leak information, that he/she feels necessary to reveal. Behind such a decision, to turn against one's own organization can be personal views and opinions that are against what the person is tasked to do or what the organization represents and the policies it holds. Intentional and malicious insiders are performing their acts usually to benefit from those. More often the sought benefit has a monetary value which is achieved through stealing classified information and selling it forward. Other common driver behind an intentional malicious act is revenge, which is caused by grudge for being bypassed in promotions, being furloughed, or let go (Nurse et al., 2014).

2.4 Profile

According to Jääskeläinen the profiles of malicious and intentional insider threat can be divided into three distinct categories presented in Figure 4.



Figure 4. Insider threat profiles (Adapted from Jääskeläinen, 2018)

Self-driven and independent threat actors are so called lone wolves, malicious intentional insiders who are performing their acts without any external manipulation or influence. This type of a threat is especially dangerous, due to their access levels. Very often the self-driven threat actor, who decides to act against his/her organization is motivated, has a good understanding of the environment, security features and has plenty of time to plan and execute their actions and most importantly, they are already in and usually in a trusted position and armed with high-level privileged access rights. One of the most notorious examples would be Edward Snowden, who utilized his position and access to leak sensitive NSA information.

Infiltrator on the other hand, is initially an outsider, whose main goal is to gain access to an organization and to its information, with an intention to steal it or destroy it. The Infiltrator can portray to be a vendor or a partner for the organization or for example a contractor or even an employee. Motivation behind infiltration can vary from personal vendetta, corporate espionage to terrorism.

Recruited insider threats are either employees, contractors or partners who for example a competitor, criminal organization or a nation-state threat actor has identified or targeted as a potential source of information. Targeting takes place through intelligence gathering utilizing different methods from open source to human intelligence. Through this process the threat actor identifies the potential resource, with the right kind of knowledge or access. Recruited insiders act because a monetary compensation received from the recruiter or for example due to blackmail, when the recruiter holds some information about them that could damage their business or reputation (Goldstein, 2020).

Carnegie Mellon University (CMU) has ongoing project (Carnegie Mellon University, 2017) that is concentrating on everything related to insider threats. One of the topics within the research, is

sabotage of information technology. As a part of the ongoing research, the CMU is updating a list of example cases, where the IT staff of an organization have performed intentional malicious acts. This list showcases again, the correlation between privileged access and successful internal malicious action. Below some examples of listed cases (Carnegie Mellon University, 2017):

- An energy company reported over \$1 million losses in revenue, after a disgruntled system architect deleted data and reset the organizations servers utilizing a remote access. Employee also utilized on-site access to disable cooling systems from data center. These activities were performed as a revenge after job contract was terminated due to sharing classified material.
- IT-company spent over 30-days recovering from an insider attack executed by their system administrator. It took less than half an hour for the former employee to make the network unusable. If there were no backups, the organization might not have been able to recover from the attack at all.
- After receiving a poor performance review, a technical staff employee decided to revenge and inserted a malicious code into organizations network causing approximately 90% of the network to fail. The attacker utilized privileged on-site access and attack was executed just before major holidays, thus delaying the response time for maximum damage.
- After being asked to resign, an employee of telco company sabotaged the employers IT systems by shutting it complete down and blocking for example 911 services in multiple major cities the telco company was providing services to.

Going through the attacker characteristics of insider threats from CMU's list, we can see some similarities between different attackers (Miller, 2016):

- Vast majority of the attackers had a technical role, like system administrator, developer, and / or a programmer.
- Majority of the attackers had privileged access either online and/ or on-site to critical assets and information.
- Most frequently attacked systems were the systems the inside attackers were already working with in their day-to-day job.
- Very often, the insider attackers hold grudge towards their employer, due to termination of contracts, poor performance reviews and performed their sabotage as an act of revenge.
- Most inside activities were planned well in advance. According to research, almost 25% of the time, other employees had information about the activities of the insider threat.

During 2016 the CMU reviewed over 100 insider attacks that were categorized as sabotage targeting organizations IT systems. The researchers were able to quantify the following statistics illustrated in Figure 5, showing the percentages of different levels of access (Miller, 2016):

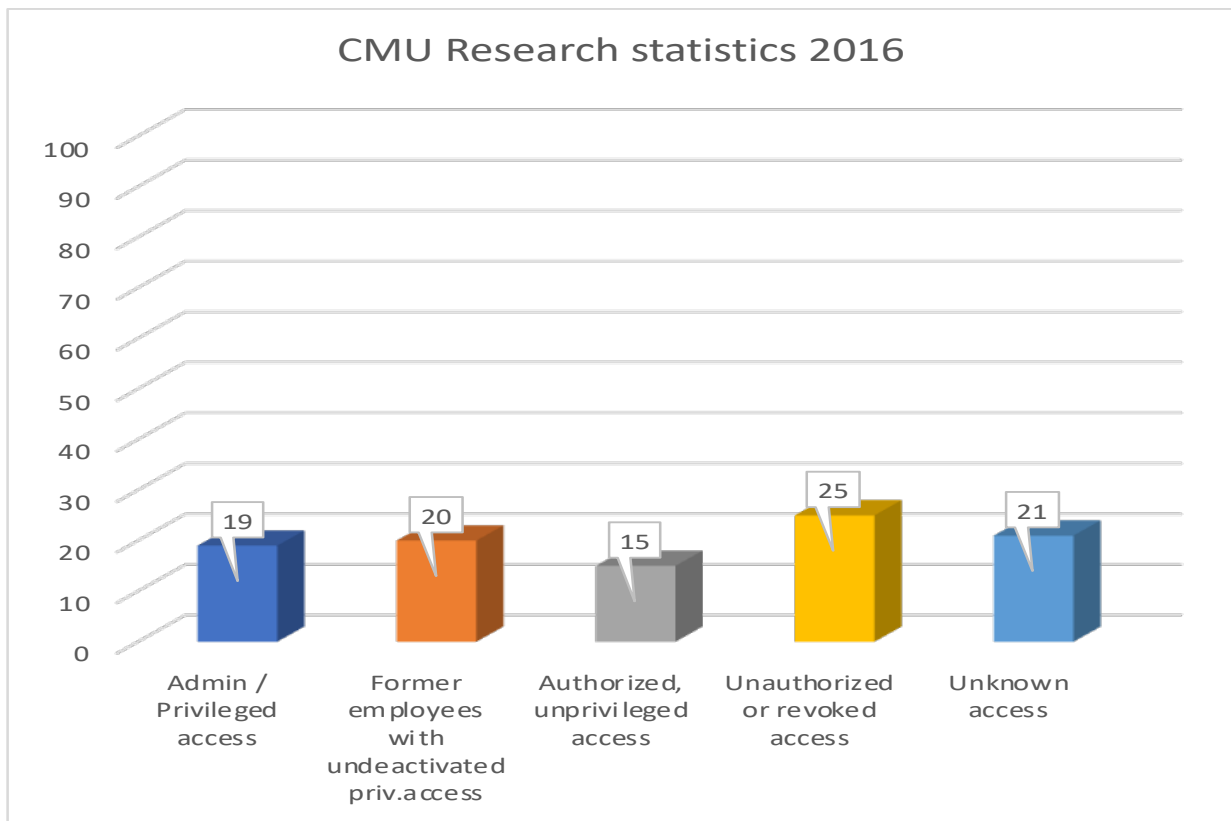


Figure 5. CMU research statistics (Miller, 2016)

2.5 Indicators

Majority of cyber security tools and, more precisely, threat intelligence tools are looking at technical indicators of compromise for internal threats. The common sources for information are applications, computers, servers, and network devices. These solutions can also monitor for example a privileged and authorized access of a person, but how it defines what is good or potentially bad for each specific user. This is the reason for monitoring the behavior of users and assets to detect the anomaly and possible indicators of compromise.

Based on research from NATO Cooperative Cyber Defence Centre of Excellence (Kont et al., 2014), often the cause of actions taken of the malicious insider is originating from their personal lives, that are often troubled. Personal problems can be due to financial, family or even mental health issues. Also, one of the biggest issues arise from work related problems, like demotion, poor reviews or un-social behavior that results into personal vendetta and sabotage. Whatever the reason is, in many cases the team members or security personnel should be able to detect

the physical and technical indicators in time to intervene. Below is listed some of the most common patterns in the behavior of the malicious insider that were identified in this thesis. This is not an all-encompassing list, but rather a starting point for every organization to develop their own indicators that suit their environment and business specific needs (Kont et al., 2014):

- Frequently occurring violations of organizational rules for compliance and data protection.
- Anti-social or even malicious behavior against co-workers, management, or other employees of the organization.
- Verbal and / or physical conflicts with other employees
- Personal performance is continuously deteriorating and / or well below average.
- Misuse of company funds or assets. For example, utilizing company credit cards for personal use or reimbursing personal costs through travel and expense claims.
- Falling behind in personal job-related assignments and overall lack of interest in personal daily routines.
- Increasing interest in other projects that are not part of personal assignments. Especially increase in projects that require access to sensitive or classified data.
- Increasing number of sick leaves or un-explainable absences during the office hours.

Many of these indicators and changes in behavior could also be explained by something that is not malicious. But being able to detect and investigate is still a critical capability to protect the environment from malicious insiders who hide within the non-malicious personnel.

To be able to monitor and analyze behavior, the organization needs to gather large quantities of data from multiple sources, and they need to gather it for a quite some time to be able to formulate a good baseline on how the employees and asset act within the organizational environment and this baseline needs to be tuned to acceptable false positive and false negatives ratio. Some of the insider threat indicators are technical in nature and require technical solutions to monitor. Some indicators are physical and can be observed by for example co-workers, managers, and HR-employees. These physical indicators are more difficult to monitor, since those require proper procedures due to their usually sensitive nature, but also due to the manual effort comparing to analyzing log data. Physical indicators that have been identified as similarities between detected malicious insiders are the following (Kont et al., 2014):

- Employee or a resource has been associated with organizations or groups, that support a vision or a cause, that is against the values of the employer.
- Employee or a resource has been involved in activities that creates a potential conflict of interests between the employers.

- Employee has been detected to be prone to different addictions, like alcohol, drugs, gambling, etc.
- Employees work history is filled with un-explained short-term employments.
- Criminal record
- Business relationships with suspicious organizations and personnel or direct association to nations of concern.
- Concerning professional or social networks.

Nowadays, it is very common to do background checks with various levels of detail for people being considered or hired for roles that have privileged access to classified information. This background data is extremely valuable and should be part of continuous analysis when trying to identify potential malicious insiders. While doing a background check, some indicators might not be suspicious at the time, but a change in situation, change in threats towards organization and when trying to identify potential risks associated to a new threat actor, some earlier indicators for example from a background check can arise. This allows the organization to adjust to the new situation and provide time to implement additional countermeasures or detection capabilities to counter this new identified threat, but also provide a tool to profile potential insider groups. To give a few profiles as an example: employees with large number of short-term employments could entail unreliability, personal problems with addictions or monetary issues could be a reason to steal classified information for monetary gain. These indicators can easily be from non-malicious acts and not automatically meaning that somebody is doing something wrong, but again, it is better to detect these and investigate to be false positives, rather than being completely blind to this type of indicators and threats.

There should be no difference in security policies for employees, contractors, and business partners alike. Same rules should apply to all, because during this day and age of outsourcing, more and more of even critical roles are being transferred outside the corporate borders. This means, that organizations system admins can be sitting across the globe in a country that does not follow the same code of conduct (Kont et al., 2014).

2.6 Attack statistics

With the current amount of data, the organizations generate, the log management, SIEM, and UEBA tools can become extremely expensive and though the importance of information and

cyber security has been elevated to a higher level through publicly disclosed breach cases the security departments are still fighting for funds and resources. If the resources are not available in the extent needed, that leaves only one option and that is to prioritize.

As a starting point, it is good to look at historical data and conducted research. The basics of any security function is to understand what the organization is protecting and what are the targets commonly associated to insider attacks. Based on research conducted by the CERT National Insider Threat Center, which included the study of over 500 cases of categorized affected assets, they have created a taxonomy to identify and classify the most common targets of insider attacks. The research also studied the quantities of affected assets per attack, to better understand the nature of the threat. According to the research (Miller, 2020):

- Over 75% of insiders targeted only a single asset.
- About 17% of insiders targeted two separate assets.
- Approximately 5% of insiders targeted three or more assets.
- Only one of the cases, had the insiders targeting 10 or more assets.

Through the cases studied, the researchers were able to identify the most common targets for insider attacks. These numbers include all different types of insider threats mentioned in this thesis as well (Miller & Pickering, 2020) which are illustrated in Figure 6.

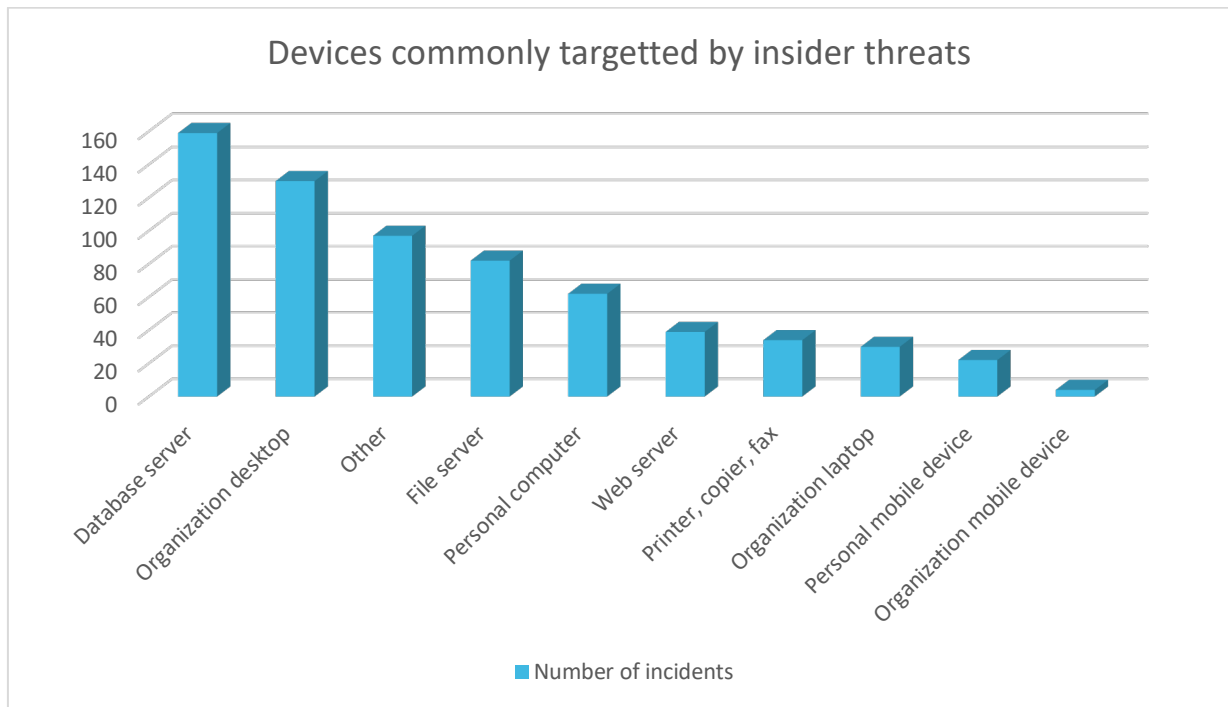


Figure 6. Affected devices of insider attacks (Miller & Pickering, 2020)

Though these statistics provide a basic understanding of the potential targets, these numbers could vary from organization to another depending on geolocation, industry and or for example size. Also, some of the cases could involve attacks towards multiple assets when the attacker has conducted lateral movement to achieve their main target. These research statistics can still be used to correlate against assets identified in the user's own organization as the most critical assets to protect and assess whether they are monitoring and protecting the correct things.

3 User Behavior Analytics (UBA) / User and Entity Behavior Analytics (UEBA)

User Behavior Analytics (UBA) and User and Entity Behavior Analytics (UEBA) are familiar terms for most people within the IT-industry, regardless of the business one is working for. These solutions have a wide variety of use cases ranging from, but not limited to (Frankenfield, 2019):

- E-commerce and retail the use case types evolve around helping to create for example product recommendations or predict future sales trends based on consumers' previous orders, clicks, downloads etc. Being able to utilize historical data from previous customer behavior can allow the organization to adapt and for example scale their e-commerce infrastructure during the peak days. This especially applies to cloud infrastructure which is based on rapid scalability.

- In online gaming industry it is important to predict trends in usage and preferences for future development and offerings. As we have seen lately the gaming companies are moving away from “old” standard monthly sub-subscription packaged products to use behavioral analytics to monitor their gamers and provide targeted specific in-game upsells.
- Application development businesses utilize this solution to figure out how, when and where people use apps that they provide to forecast future trends. As with online gaming analytics, application development will utilize this information to provide more targeted user experience by offering different kinds of upgrades within the app that are based on individual behavioral patterns.
- For security industry, whether it is a security service provider or internal organization providing security, these types of analytics enable them to detect compromised information and/or malicious behavior (intentional or un-intentional) by finding the unusual activity from the normal day to day stuff. This allows security teams to track those advanced threat actors or insiders who rarely use for example malicious software after gaining a foothold which are potentially detectible via old fashioned perimeter defense.

Also, these solutions are utilized to streamline production and lower costs in low tech industries like transportation. Use cases are endless when the requirement is to predict the future based on behavioral history and everybody wants to know today what happens tomorrow.

Like mentioned in this thesis, in security context, which is my area of interest, UBA/UEBA technology is used for searching and modelling the behavioral patterns of the users to create a baseline of what could be called normal behavior. This baseline is again used to detect any unusual behavior whether those are caused by hackers, insiders or malicious software changing processes within the IT-environment. Like perimeter defense, UBA/UEBA won't prevent or block bad things from happening, but it allows the security teams to detect and react to those and minimize the potential damage (Green, 2020). After the initial detection, the security teams can then apply the human judgment, holistic understanding of the environment and organization to provide further analysis whether the detected anomaly was suspicious or not (Amoroso, 2011).

To be able to understand why user behavior tools were invented and implemented as part of security operations, we need to consider where the current perimeter and signature-based solutions came short. If we look at the past 10 years and the breaches that have made the headlines, those report that almost in all the cases, the target organizations basically gave the keys to the front door for the attackers (Verizon Business, 2022). Basic security operations rely on monitoring logs from anti-malware, intrusion detection and firewall solutions and collecting and correlating the gathered logs in Security Incident and Event Management (SIEM) solutions. This style of monitoring is usually able to detect the obvious attacks and unintentional mishaps of users, but

not the serious threats or internal threats. Therefore, organizations need to utilize both traditional and UEBA technologies for better visibility.

3.1 Technology

The scale and complexity of the environments that security operations are required to monitor, have grown significantly during the past decade. Requirements for cost efficient scalability, remote capabilities etc. have introduced multiple game changing technologies like cloud services (IaaS, PaaS, SaaS) and these technologies require new security skill sets. Unfortunately, the demand is higher than what can be delivered now. These services have expanded the perimeter outside of the organization's control and made it difficult to monitor and defend. Now adversaries are targeting the weakest links in the chain to gain access to the main target, and those weak links usually are the smaller companies providing some specific services as subcontractors. Gaining access to these partner environments allows attackers to send, for example, phishing emails, SharePoint links with malicious contents from a trusted source, thus bypassing multiple different perimeter security technologies (Beardsley et al., 2021).

As illustrative example, there are breaches that have made the tabloid headlines and are still talked about even today. What comes to case Snowden and Wikileaks, a classic insider example where a disgruntled employee decides to a revenge on employer or due to personal agenda decides to expose the secrets to public. Nobody really needed to hack anything, since the insider had all the access he needed. The Target breach was about bad password policy and failed monitoring. Attackers apparently simply guessed the password and were able to remote login to the environment. And finally, maybe the biggest blunder, if one looks at it from the national security perspective, the USA's Office of Personnel Management breach, where the attacked was initiated via something as simple as a phishing email. None of these cases had any fancy zero-day vulnerabilities being exploited or massive armies of hackers cracking the code. Whether it is an insider or outsider, after gaining the foothold, they do not utilize malicious software or tools to expand their presence or to access the data they are looking for. They utilize legitimate tools such as the IT support does.

So, when we look at this insider threat dilemma, it makes no sense to rely solely on legacy perimeter defense, because it was never meant to solve this challenge, but rather to keep bad outsiders out of the Intranet. Even nowadays, the bad outsiders can easily bypass these border controls by using simple and cheap measures like massive phishing campaigns and open-source intelligence relying on bad password policies and bad administrative security, the foot hold is gained, the attackers will appear as any random user from the organization.

I am not saying that perimeter-oriented security and even the new anomaly-based solutions are useless. They do serve a purpose and are still valid today, but for the insider or APT context, they are just looking for the unusual activity from the wrong places (Green, 2020).

3.2 Analytics methods

How does user behavior analytics work and why it is the primary tool for future security operations and for tackling the insider threat? First, it is good to understand the difference between UBA and UEBA. Though we are talking about similar technologies and the terminology *user behavior analytics* is used to describe both approaches, there are some differences in the technology and analysis methods. What UEBA does compared to UBA is, that it extends the analytical capabilities also to entities and events, rather than just users. These entities can be devices such as endpoints, servers, and routers, resulting in a much improved and more powerful platform than the earlier approaches concentrating to just users. These additional capabilities allow more advanced analytics and better visibility to for example fraudulent activity. User behavior analytics used to be a standalone solution, but nowadays it is more often acquirable as an add-on module / feature to SIEM or log management tools. Depending on different vendor strategies and capabilities obviously. It is a software solution that uses different kinds of algorithms and types of AI to analyze machine data ranging from standard log formats to pictures, videos, and sounds (Splunk approach presented in Figure 7) to learn what is considered normal interaction with people, IT systems and facilities of the organization.



Figure 7. Log / event data sources (Splunk Inc, 2022)

With user and entity behavior analytics solutions utilizing the AI capabilities and collected data organizations can baseline what is the normal behavior and react and investigate when an anomaly occurs. As mentioned earlier, the insider or the Advanced Persistent Threat (APT) with foothold in the environment, usually appear as any other normal user. Though malicious threat actors use the same tools, but usually to carry out what they want to do, they need to do it hidden,

meaning odd hours and odd locations. Especially with APT's, they need to do their actions remotely. This is something that the user and entity behavior monitoring can detect. Something out of ordinary is happening:

- Why is Petri logging in from an IP from Russia?
- Why is Petri logged in at Helsinki office IP-range, while the physical access tells us that he just walked in at Tampere office?
- Why is Petri accessing this data base and downloading data to USB, even though his role does not require access to this data?

User and entity behavior analytics software can detect these anomalies via individual behavior baseline or role-based baseline. These baselines are either learned by utilizing unsupervised machine learning where the solution just follows each user id or asset tags to create a behavioral model through a long period of time, or the baseline is based on predefined role-based models where the user id or asset tag is just "glued" to the role they are expected to follow. Both approaches have their advantages and disadvantages, but nevertheless, both take time to achieve a good false positive and false negative ratio (Legg et al., 2017).

User behavior analytics tools are providing a different approach to anomaly detection and relying on a range of analytical approaches. These are usually a combination of basic analytics methods and advanced analytics. Basic analytics means simple statistics, signatures, and pattern matching. Advanced analytics are relying in AI capabilities, and this allows the tool to learn and adapt faster to changes and doesn't require a similar level of human intervention. The changes are seen as anomalies from usual behavior, whether it's based on learning from individual behavior over time or from predefined role-based baselines. These analytics tools analyze multiple different aspects and log sources to evaluate activity of entities and users. These log sources can be for example hosts, login information from networks and applications, network traffic and data storages and this information is used to detect potential incidents that are planned or executed by insiders or out-side attackers that cannot be detected by traditional methods. This is the optimal situation, though it requires a lot of work to get there (Reciprocity, 2021).

4 Detecting insider threats

Like the normal SIEM solutions, the UBA/UEBA solutions provide customizable dashboard views for security teams to improved situational awareness as illustrated in a figure 8. For this to work efficiently, organizations need to monitor relevant log sources, have correct policies in place within the organization, have resources and personnel with a holistic understanding of the IT-environment and what is acceptable and what is not. Implementing a UBA/UEBA solution takes time and effort and especially in the beginning it is very prone to produce false positive and false negative alerts in massive quantities. Security professionals need to prepare to spend a lot of time tuning the solution to meet the requirements and the baseline behavior of the organization's personnel and assets. There are multiple reasons for false positive and false negative detection when it comes to behavior analytics. As one might expect, the behavior of people and/or assets will change over time, so the organization need to prepare to continuously modify the set up as time goes. People change roles, change in the number of employees or a peak season in business can change the amount or schedule of traffic (Micro Focus, n.d.).

Most of the UBA/UEBA tools provide a certain set of off-the-shelf use cases and I will be reviewing few examples from Splunk UBA/UEBA later in the following sections. This basic set of use cases will provide a good starting point for almost any organization and from there, organizations can develop their own thresholds or group or role-based baselines. As mentioned earlier, the user behavior baseline is individual to different organizations and there are no one size fits all solutions.

Technology is one thing, but the organization needs to know what they are monitoring, why they are monitoring it, what is the organizational policy about what is allowed and what is not. There are limitations in multiple countries regarding what information and data one can gather. To have the concrete building blocks for effective insider threat detection capability, one needs to have an organization wide policy. Security professionals need to understand their IT environment and tune the system to meet the needs of the organization from technical, but also from policy point of view (Wall, 2012).

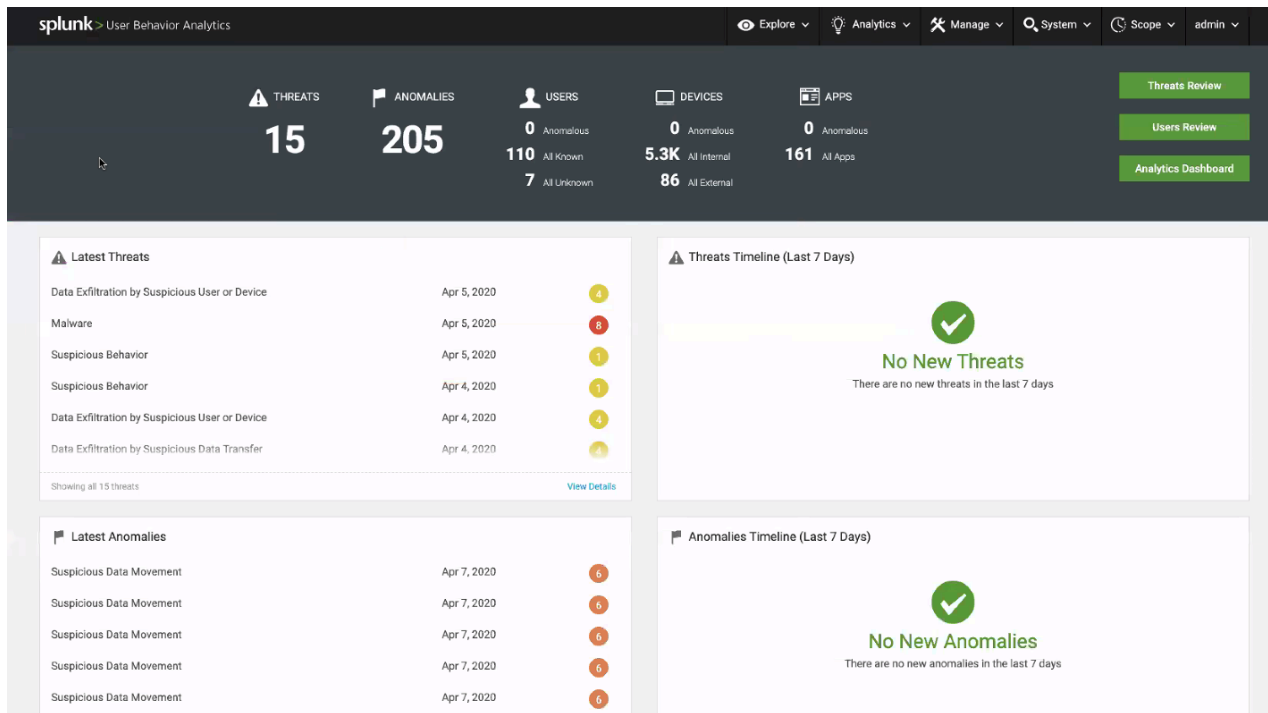


Figure 8. UEBA Dashboard (Splunk UBA/UEBA screen capture)

UBA/UEBA tools can utilize the manual and analogic knowledge of the organization which is not generated by machines. Like described in section 2.4 of this thesis, the indicators could be driven from for example background checks, interview notes, whatever HR related information the organization is allowed to gather, and store based on local legislation. This information, though manually inputted to HR systems, can then be utilized for a security perspective, to create watchlists or other custom alerts, like shown in Figure 9.

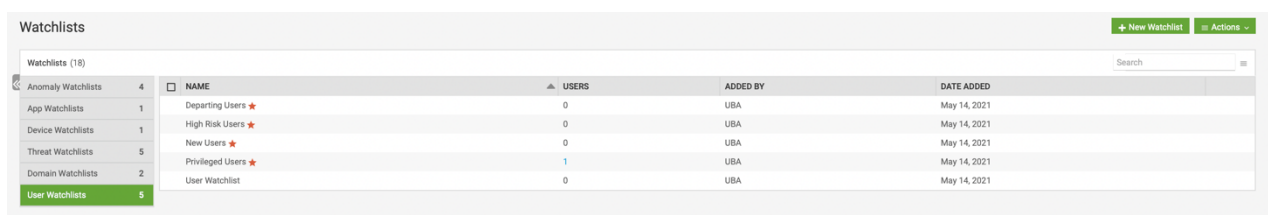


Figure 9. UEBA watchlist (Splunk UBA/UEBA screen capture)

This information from HR systems can also be utilized, to provide additional context. An employee might have had some difficult circumstances earlier in life, that has risen to attention during interviews. This does not mean, that he or she is automatically bad, because we all do make

mistakes during our time here, but this can be something that needs to be taken in consideration, while giving privileged access or participation to sensitive and classified projects. This information regarding the employee's background will also enrich the potential indication of detected malicious insider activity. An alert, that might be lower in severity score for other user, could be raised to higher level due to something in the recorded background information of some other user. Figure 10 showcases, the examples of imported HR data in Splunk UEBA. The scale and depth of the HR data is obviously dependent on the HR system and the ability for providing the relevant information. In this Figure 10 example, we can see the users ID information, groups the user belongs to and peer's.

The screenshot displays the account information for Bill Lundquist in Splunk UEBA. At the top, the user's profile is shown with a name, last update time, watchlists, and account status. Below this, the account details are organized into several sections:

- Account Type:** Normal
- Login ID:** blundquist
- Email Address:** blundquist@acme.com
- AD Groups (3):** ACME-Engineering, ACME-US, ACME-Users
- User Account Control:** Normal Account
- Dormant [90Days]:** No
- Domain and LoginID:** blundquist

Below the account details, there are two main sections for peer groups:

- Engineering (38) OU User Group:** A table showing user names and their HR records.

USER NAME	USER HR RECORD
Aaron Rando	Known
Aimee Moege	Known
Angelina Smith	Known
Apama Kumar	Known
Beau Struthers	Known
Bill Lundquist	Known
Brandon Hines	Known
- ACME-Users (109) AD Account Group:** A table showing account login IDs and account types.

ACCOUNT LOGIN ID	ACCOUNT TYPE
akumar	Normal
Apama Kumar	Normal
amcclean	Normal
Albert McClean	Normal

Figure 10. Account information from HR data (Splunk UBA/UEBA screen capture)

4.1 Background, physical and digital indicators

In this section, we look and compare different background, physical and digital insider threat indicators which have been, according to research from NATO Cooperative Cyber Defence Centre of Excellence (Kont et al., 2014), highly repetitive and associated in detected incidents to different threat types of malicious insider's describer earlier in this thesis. This combined Table 1 gathered from NATO Cooperative Cyber Defence Centre of Excellence (Kont et al., 2014) research is not meant to be all inclusive, but rather to give a high-level of understanding of what types of

indicators have been usually associated with different types of insider threats. It is easy to conclude, that majority of the indicators can be applicable to threat types with different levels of association and likelihood, but it does not make them irrelevant or useless, but rather showcases the complexity of detecting the insider threat from different layers of indicators.

Background indicators	Physical indicators	Digital indicators	Associated threat types
Employees work history is filled with unexplained short-term employments	Unwillingness to follow organizations policies and procedures Continuously trying to find shortcuts or bypassing chain of command	Utilizing unauthorized offensive tools Modification or destruction of stored log data or files Continuous anti-malware alerts	Sabotage Workplace violence
Proven history of either emotional or mental disorder	Anti-social and or aggressive behavior towards co-workers Poor social skills Increasing number of sick leaves or unexplainable absences during the office hours	Connections from organizations workstations initiated outside of normal office hours Accessing organizations network, assets, or applications outside of normal office hours	Sabotage Workplace violence

<p>Employee or a resource has been associated with organizations or groups, that support a vision or a cause, that is against the values of the employer</p>	<p>Concerning statements, jokes, or bragging</p> <p>Access attempts to physical location, digital assets, or information that is not associated with his/her role</p>	<p>Downloading unauthorized software or execution of blacklisted or malicious programs</p> <p>Access attempts to restricted digital assets of information without permit</p> <p>Attempted escalation of privileges</p> <p>Attempts to bypass organizational security procedures and technology (for example disabling anti-malware etc.)</p>	<p>Sabotage</p> <p>Espionage</p>
<p>Criminal record</p>	<p>Continuous unexplained use of tools to create copies of classified information (for example copy machine, camera, etc.)</p>	<p>Use of unauthorized and/or blacklisted files and tools such as offensive hacker tools</p> <p>Connecting unauthorized devices to</p>	<p>Theft</p> <p>Espionage</p> <p>Fraud</p>

		organizational networks and/or workstations	
Financial problems	Increasing interest in other projects that are not part of personal assignments. Especially increase in projects that require access to sensitive or classified data.	Sending emails with usually large amount of attachments / data outside of organizational networks Attempts to copy and or print documents that contain confidential information	Theft Espionage Fraud
Employee has been detected to be prone to different addictions, like alcohol, drugs, gambling, etc.	Excessive overtime work Unexpected and unexplained absences	Continuous and unexplained correspondence with competitors	Theft Fraud Workplace violence
Employee or a resource has been involved in activities that creates a potential conflict of interests between employers.	Access attempts to location not associated with his/her role Change in behavior and or presence in for example social media	Use of personal software on organizational assets to hide activity. For example, VPN solutions or Tor Unexplained logging in to a on-premises workstation or asset	Theft Fraud Espionage Fraud

		<p>outside of official office hours</p> <p>Modification of log data</p> <p>Connecting unauthorized and or unidentified devices into organization assets or networks. Such as USB, CD-ROM etc.</p>	
--	--	---	--

Table 1. Background, physical and digital indicators associated to different threat types (Kont et al., 2014; Proofpoint US, 2021)

4.2 Use cases and log sources

This chapter reviews the different use cases, required log sources, and examples that are based on the Splunk UBA/UEBA tool. I utilized this tool as the source for examples, since my familiarity with other products from this company, mainly Security Incident Event Management (SIEM) and Log Management solutions. Splunk UBA/UEBA tool is a separate solution, which utilizes the Splunk Enterprise or Splunk Cloud as the platform where it collects the configured and required data for behavioral analysis. Splunk Inc. allowed me to utilize their UBA/UEBA demo environment, to capture relevant examples to cover six different use cases and required data sources, which I have listed below. Each use case provides a description of the expected activity / behavior and what are the log sources relevant to detect such activity. Without the Splunk demo environment the examples would have been almost impossible to capture and visualize, since the UBA/UEBA tools require large quantities of data, and some use cases require specific log sources which are not that easy to build in a personal test environment.

To avoid creating an exhausting list, I wanted to look further into few examples, that I found interesting and with the best return of investment, because these are applicable to both internal

and external threats and for a security organization that very commonly has limited resources, the organization need to be able to multitask and use their resources intelligently.

4.2.1 Account Misuse

Account misuse is a complex use case and contains types of acts that can be accidental or deliberate. These similar behavioral patterns can be detected with internal and external threats when the threat actor has access to resources or for example superuser accounts. When dealing with intentional privileged account misuse that is based on either insider utilizing his/hers access to data or outside threat that has penetrated the perimeter security, the threat actors usually utilize similar tactics to achieve their target and avoid detection. These tactics include using service accounts to do VPN logins, accessing highly confidential information, and then deleting audit logs from systems they have accessed. These privileged access rights can also be used for destructive behavior from a disgruntled employee or a contractor that is deleting valuable assets and / or information for personal revenge (Fimin, M. 2018).

The key thing is to monitor authentication and access, who is doing it, where it is happening, what time, which location and what are the actions taken. To be able to monitor this organization need to have sufficient visibility to the IT environment. Required log sources for authentication and access monitoring could be authentication logs from different applications and systems, file integrity monitoring solution, physical access data (badge), cloud data, email, endpoint, external alarm, VPN and Active Directory (Windows Security Events). This is where the UEBA learning capabilities come in. Different types of use case for authentication in Splunk UEBA tool are shown below in Figure 11:

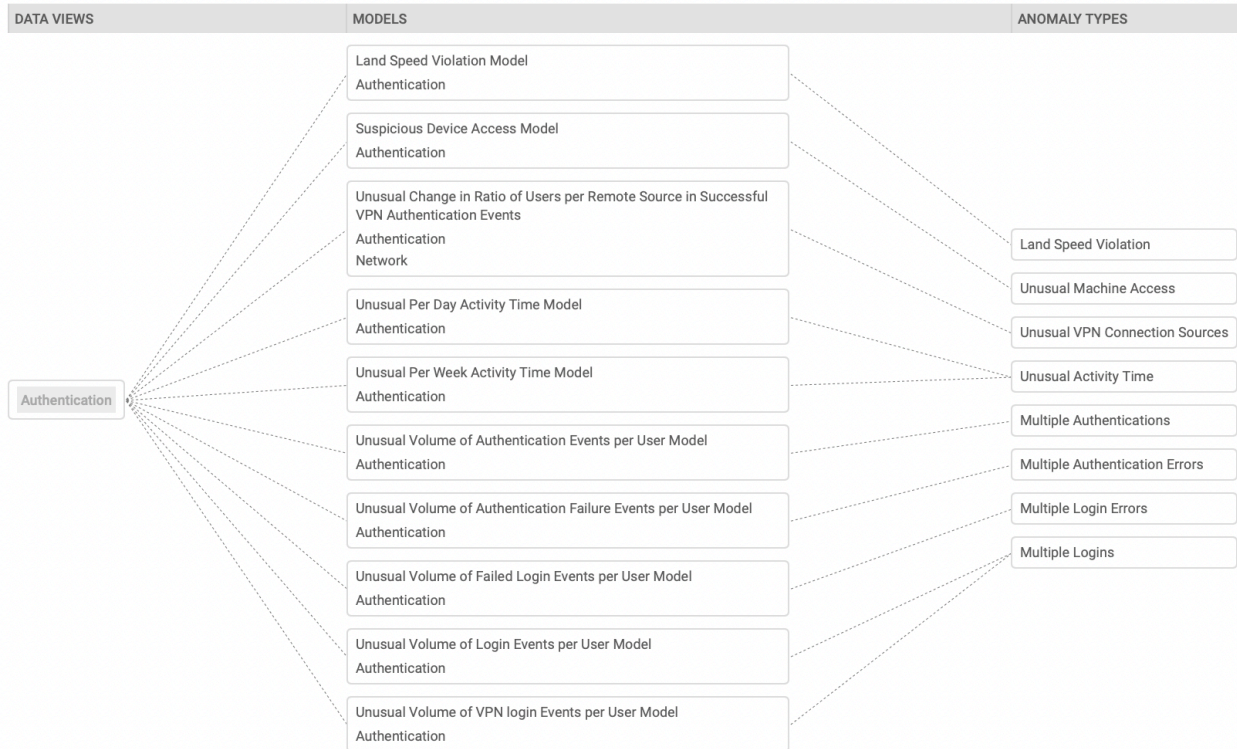


Figure 11. Authentication data views (Splunk UBA/UEBA, screen capture)

Suspicious account activity can present itself in many forms. It can be something as simple as logging in to weird places, during odd hours, accessing data that is not required in the specific job, adding new access permits to users own id which should not be required or admin accounts with a short lifespan. There is always potential that these detections can be non-malicious and are caused by change of role or a location, but still worthwhile checking and can be easily verified. But at the end of the day, whoever is stealing or trying to steal the data, the bottom line is that the attacker needs the access. To get to the classified information, usually the person needs to have or attain higher privileges and if the user wants to continue malicious activities in the future, the user needs to keep his/her activities hidden, and the user need to be able to hide his or her tracks. Below in Figures 12 and 13 are few examples of Splunk UBA/UEBA commercial of the shelf technology (COTS) use cases.

ANOMALY TYPE	PARTICIPANTS	SUMMARY	START DATE	SCORE
Suspicious Account Activity	<ul style="list-style-type: none"> reprsv32 Service acme-srv-10251862 	Interactive login using service account	Apr 5, 2020 12:00 AM	4
Suspicious Account Activity	<ul style="list-style-type: none"> Donna Callister 	Account created and deleted in short span by same user	Apr 5, 2020 12:00 AM	4

Figure 12. Account misuse example 1 (Splunk UBA/UEBA, screen capture)

ANOMALY TYPE	PARTICIPANTS	SUMMARY	START DATE	SCORE
Malicious AD Activity	Donna Callister	Audit log has been cleared	Apr 5, 2020 12:00 AM	7
Malicious AD Activity	Gowri Vignesh	Audit log has been cleared	Apr 4, 2020 12:00 AM	7
Malicious AD Activity	db-backup scl-s-dc01	User performs a security sensitive operation on himself.	Apr 5, 2020 6:56 AM	9

Figure 13. Account misuse example 2 (Splunk UBA/UEBA, screen capture)

In Figure 12 and 13 we can see different kinds of detected anomalies ranging from interactive logins from service accounts, accounts with short lifespan, and users performing security sensitive operations on himself/herself like audit log and backup clearance. UBA/UEBA tools give a threat score for each event, but also correlates these different events together if there is a common nominator, like a user id, IP address (destination/source), or an asset name. Like in these examples the actions of the user are outside the learned baseline or outside the agreed role and have created alerts in the console. Having multiple alerts from the same user increases the risk score, thus creating a more urgent need to investigate further.

Suspicious Data Access 4

Detected a combination of actions performed in a data store with possible security implications.

Anomaly Creation Time Apr 7, 2020 1:13 AM
Last Scored Time Apr 7, 2020 1:13 AM
Last Scored by AnomalyScoringRules
Event Start Time Apr 3, 2020 12:00 AM **Event End Time** Apr 4, 2020 12:00 AM

Watchlists * -

Categories Cloud Data | Data Destruction | Network Detection | Signature

A user has deleted a high number of files or files from several directories.

Score Breakdown:

- Multiple (26) files show the pattern
- Files from multiple directories (6) show the pattern

[Actions](#)

Users (1)

Simon Roma

Devices (1)

External
24.5.189.76

Threats (0)

This anomaly is not included in any threat

Event Drilldown

Advanced Identity Lookup [Generate Contributing Events Link\(s\)](#)

Activity Breakdown (26)

Actions that contributed to the pattern or may help explain it.

FILE	ACTION	DIRECTORY	SOURCE IP	FILE SIZE	TIME	USER	TARGET USER	CLIENT USED
projc_4	Delete	backup	24.5.189.76	85.8 MB	2020-04-03 00:00:00	Simon Roma		
user_portal.zip	Delete	source	24.5.189.76	59.4 MB	2020-04-03 00:00:00	Simon Roma		
mcguffin_gen.tgz	Delete	source	24.5.189.76	67.4 MB	2020-04-03 00:00:00	Simon Roma		
src_main.tgz	Delete	source	24.5.189.76	116 MB	2020-04-03 00:00:00	Simon Roma		
projc_2	Delete	backup	24.5.189.76	72.5 MB	2020-04-03 00:00:00	Simon Roma		
ai_matrix.zip	Delete	projects	24.5.189.76	111 MB	2020-04-03 00:00:00	Simon Roma		
projext_k_proposal.ppt	Delete	projects	24.5.189.76	98.2 MB	2020-04-03 00:00:00	Simon Roma		

Figure 14. Suspicious data access (Splunk UBA/UEBA screen capture)

After the threat actor has gained required information successfully, they need to hide their tracks to keep their identity hidden and to be able to continue utilizing the gained foothold. In this Figure 14 we can see the UBA/UEBA tracking a user deleting multiple files from different directories including backups. This could indicate hiding the malicious activities performed or it

could also be an insider with a different motivation than stealing data. One of the potential threat types and motivations for an insider is sabotage from a disgruntled employee.

4.2.2 Compromised User Account

Compromised user account means that someone other than the legitimate owner of the account is either attempting or is using those credentials. Both insider and outsider threat actors, try to hide their malicious acts and point of ingress. In the case of insider threat, the perpetrator could be hiding his/her identity, by committing malicious acts via for example co-worker's user account. Also, this type of user account compromise can be a part of gaining a higher privileged access for the insider, instead of trying to get the access privileges to his/her own account.

For outside threat actors, for example hackers and criminal organizations. The easiest and most common way to gain access to organization's network is to steal credentials. Most common methods are via different forms of social engineering like phishing, whaling, etc., where the user is tricked to provide those credentials willingly. Utilizing these stolen credentials allows the attacker to bypass majority of the basic security controls and stay hidden for quite some time (Ekran, 2019). With Insiders, one of the key dilemmas is co-workers sharing credentials, weak password policies, and still the negligent behavior of using post-it notes under keyboards, which is still too familiar even now in 2022.

To detect this type of activity, we need to look at what are the potential anomalies in the behavior of the user account. UBA/UEBA monitors and identifies what is the expected behavior of the user or application and compares that to detected changes and raises notable events and alerts. These anomalies in behavior can be time and or locations based, but this use case can also detect shared account abuse when same account are utilized in multiple assets and multiple combination of previously mentioned. Other examples of unusual activity could be Active Directory (AD) related actions on self or changes on terminated users. AD (dataflows presented in Figure 15) and authentication logs play a key role in this use case, but additional value add log sources are VPN, endpoint, badge access, and cloud data.

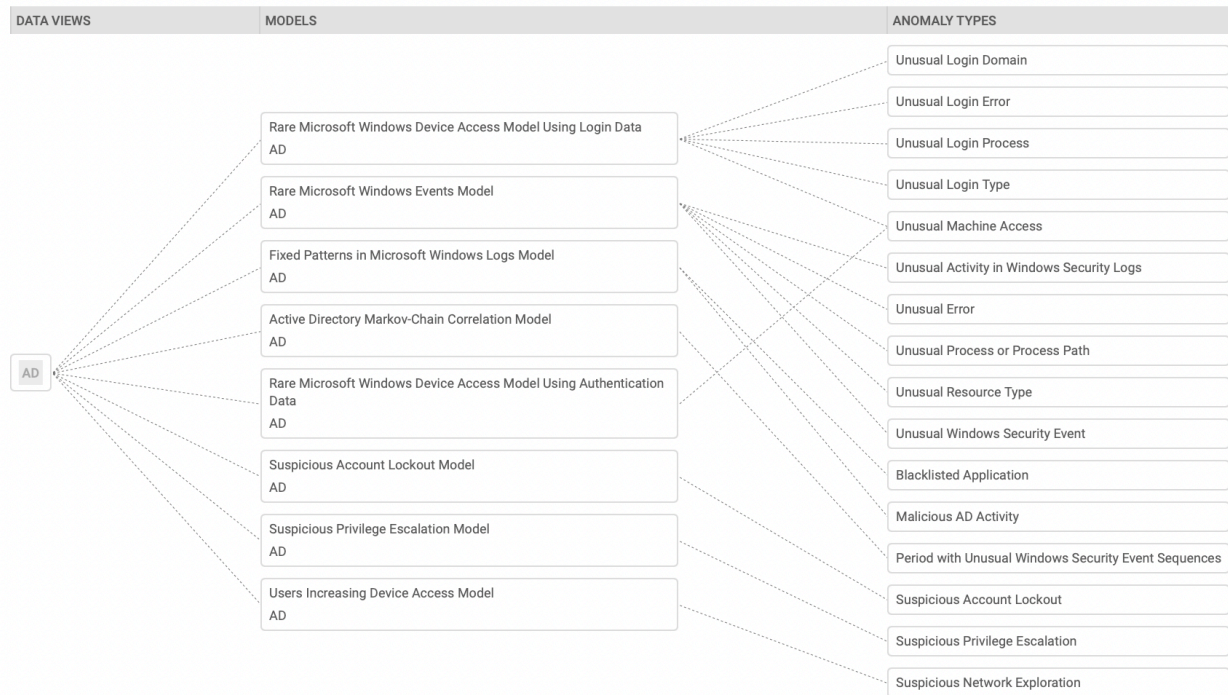


Figure 15. AD data views (Splunk UBA/UEBA, screen capture)

There are multiple potential indicators that could imply that the user account has been compromised. In the example illustrated in Figure 16, we can see different indicators that are familiar to different phases of an attack. Initial detection, called land speed violation, comes from unusual login activity from Bill Lundquist's account, which indicates that the account has been accessed from multiple geographical locations simultaneously within a short period of time (which we will cover more in detail in the next example), other detected strong indicator is machine generated traffic (beacon) which is common command and control behavior, where the compromised account is trying to connect to outside source. In this example the beacon is connecting to similar external IP range as the detected unusual login came from. There is an alert for lateral movement where the compromised account is scanning additional resources to gain further access, but also to exfiltrate stolen data. This type of activity would apply also to insider threat attempting to commit fraud or to steal (espionage) confidential information, who is looking to hide his/her identity, if the exfiltration would be detected, since that is detectable even with basic security monitoring tools.

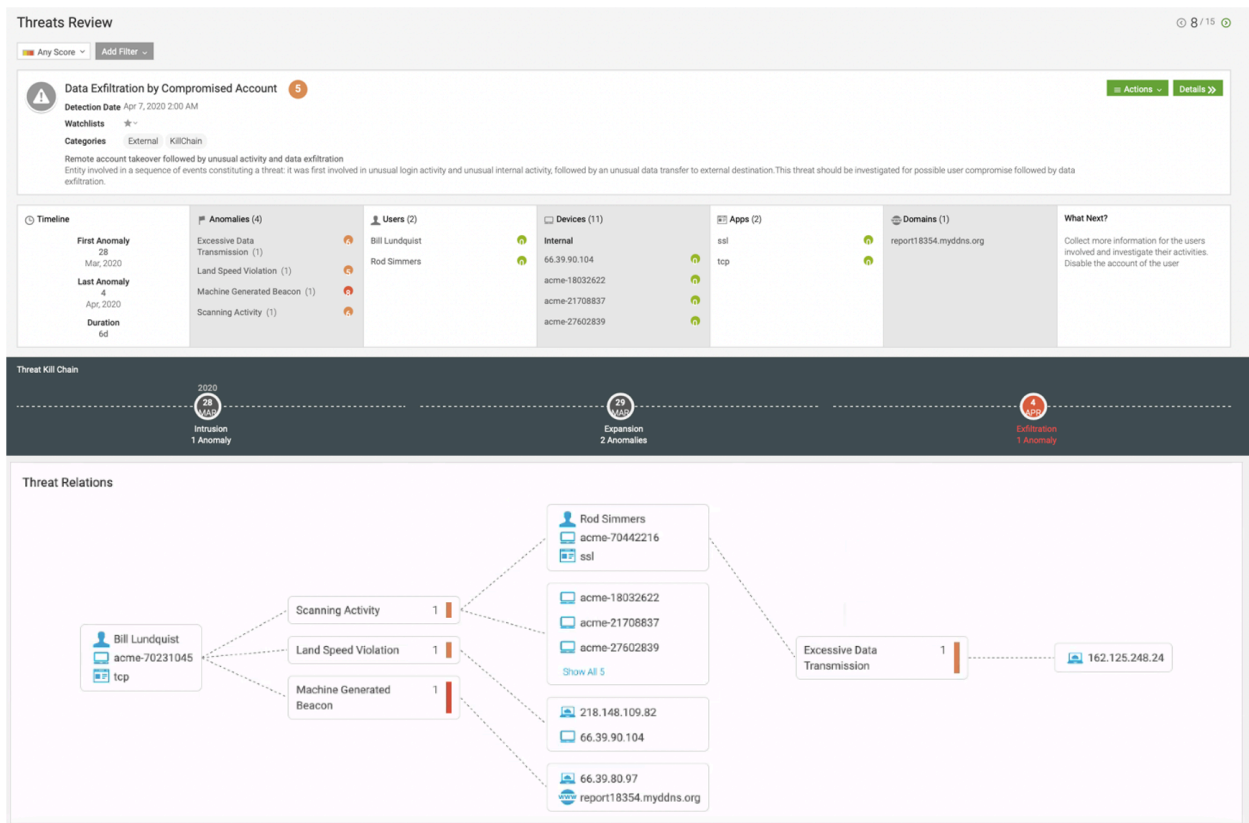


Figure 16. Data exfiltration by compromised account (Splunk UBA/UEBA screen capture)

Previously mentioned land speed violation (Splunk terminology) is a common use case and can be found from Microsoft O365 tools, where the detection is based on anomaly in geography. Though organizations need to keep in mind, that some of these solution specific tools are commonly limited to be used only within the solution itself and cannot import and utilize data from other log sources unlike Splunk UBA/UEBA. Figure 17 illustrates the geographical impossibility for a user to login within two locations separated by thousands of kilometers and with two different assets and IP addresses. This could be explained by use of personal VPN that are common nowadays, but more often these are forbidden in the corporate assets by policy and rules, so detecting a use of personal VPN, could be an indicator or insider threat trying bypass data loss prevention or perimeter security mechanisms. This similar use case could be applied within the confines of an office when user account is being utilized within multiple different assets simultaneously.

Land Speed Violation 5

Users logging in from locations that are too far apart.

Anomaly Creation Time Apr 6, 2020 11:16 PM
Last Scored Time Apr 6, 2020 11:16 PM
Last Scored by AnomalyScoringRules
Event Start Time Mar 28, 2020 5:00 PM **Event End Time** Mar 28, 2020 5:10 PM

Watchlists ★
Categories Allowed | Credential Access | Incoming | Rare Location | Signature

The previous location , US and the new location KR are 6787 miles apart but the time difference between the two activities is only 64.0 minutes

Users (1)
 Bill Lundquist

Devices (2)
Internal
 66.39.90.104
External
 218.148.109.82

Threats (1)
 Data Exfiltration by Compromised Account (1)

Anomaly Relations

Bill Lundquist — Land Speed Violation — 218.148.109.82, 66.39.90.104

Event Drilldown
 This is a sample contributing event
 Mar 28 17:00:00 10.152.249.246 : %ASA-6-113839: Group <SSLVPN> User <blundquist> IP <218.148.109.82> AnyConnect parent session started

Advanced Identity Lookup | Generate Contributing Events Link(s)

Device Locations (2)

Map | Satellite

Map showing locations in North Korea, South Korea, Japan, and the United States.

Figure 17. Land speed violation (Splunk UBA/UEBA screen capture)

4.2.3 Compromised and Infected Machine

In the previous chapter we covered the compromised account, which is a different scenario to compromised machine. One talks about user accounts, which are often not tied into a specific machine. Compromised machine on the other hand means that the machine itself is compromised and it does not really matter who is logged into it. Also, there is a difference on what means compromised vs. infected and it makes sense to clarify that as well. When for example a computer is running malicious software such as a virus, the machine is considered as infected and infected machines can still usually be cleaned. When someone outside the organization has some sort of remote control of the asset the asset is considered compromised. Compromised machines cannot be cleaned, because the organization does not know what changes has been made to the machine after the initial access, because the initial compromise could have happened a long time ago, thus making it difficult to investigate. This undetected compromise is also

the reason why it is critical to monitor traffic to potentially detect call home traffic. A malicious insider could utilize these tactics to steal classified information from the organization as part of personal agenda, for example compromising an asset that he/she has access, thus allowing a backdoor or a remote access for later use. Or a disgruntled employee's personal revenge to create a logic bomb, that executes on a specific date after the insider has left the organization and infect assets with destructive malware. Also, this type of machine compromise can be utilized to exfiltrate data to a predefined destination by an insider that has knowledge about technical security controls, meaning he/she knows what could be detected. We cannot exclude espionage, when a recruited insider is given a task to Install malicious software and allow an external entity to take control and gain access to the environment.

SIEM tools can monitor and create alerts when they detect potential call home traffic, but these detections are based on signature created on threat intelligence of malicious indicators from past. What UEBA does, it identifies potentially infected and or compromised assets from the change in behavior and nobody needs to be logged in to the systems. For UEBA, it does not matter what the initial infection mechanisms were, but it can detect the changes in communication patterns of assets.

Valuable log sources to detect potentially infected and or compromised assets are DNS, firewalls, network-based IDS/IPS, DLP and AD logs (Windows security events). Figure 18 showcases the basic models and anomaly types for DNS data, which is one of the key log sources for this use case.

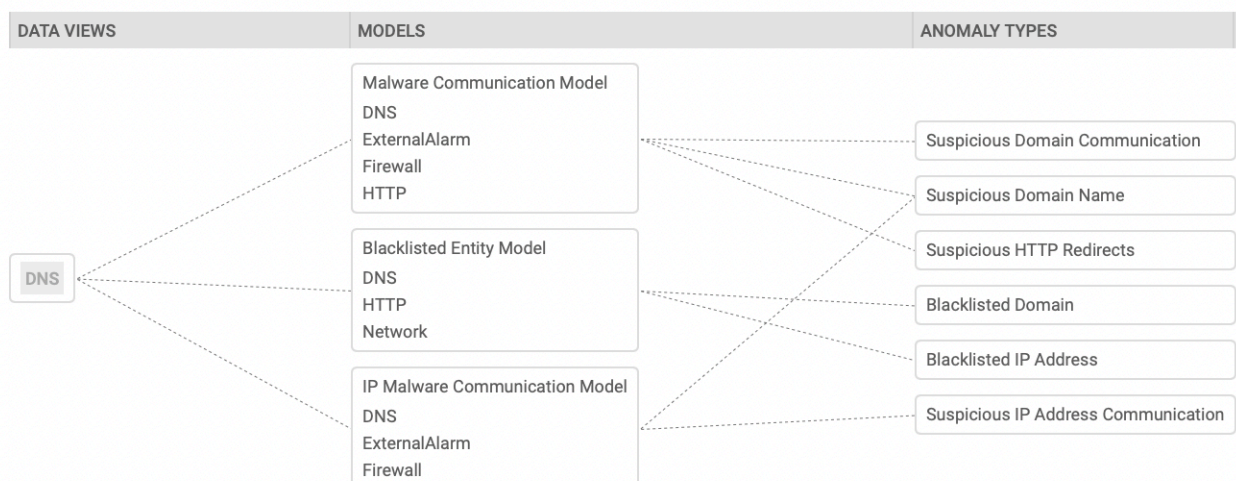


Figure 18. DNS data views (Splunk UBA/UEBA, screen capture)

In the example pictured in Figure 19, we can see two different indicators being detected from the host illustrated in the anomalies section. One can also notice that the criticality changes due to different activities, but one can also see that the user, asset, applications, and or the source and destination addresses are not considered malicious or have a history of being associated with malicious activity. This alert originates from the change in the behavior of the asset or the user. This asset is creating a Secure Shell (SSH) connection outside the organization's network and this type of behavior is associated with potential malicious behavior. SSH protocol has been detected in the past breaches of being used to create proxies to bypass other security controls. This also creates a problem from logging and monitoring perspective since one is not able to scan and investigate the outbound traffic and this allows a way for a malicious insider to exfiltrate confidential data via compromised asset.

The second anomaly came from PowerShell usage. This tool is used by admins almost everywhere and due to this reason, it is not considered malicious. This tool is not for the average user, and this is the reason why this detection could have been alerted upon together with the suspicious SSH connections. Attackers utilize PowerShell for multiple different reasons and one of the reasons is that it is considered legitimate, thus it is not stopped or alerted upon even when it is detected by basic endpoint defenses. It also can download and execute content from another system and provides privileged access to Windows systems. The PowerShell has been used or built on for several offensive tools like Metasploit. (Chettiar, 2019)

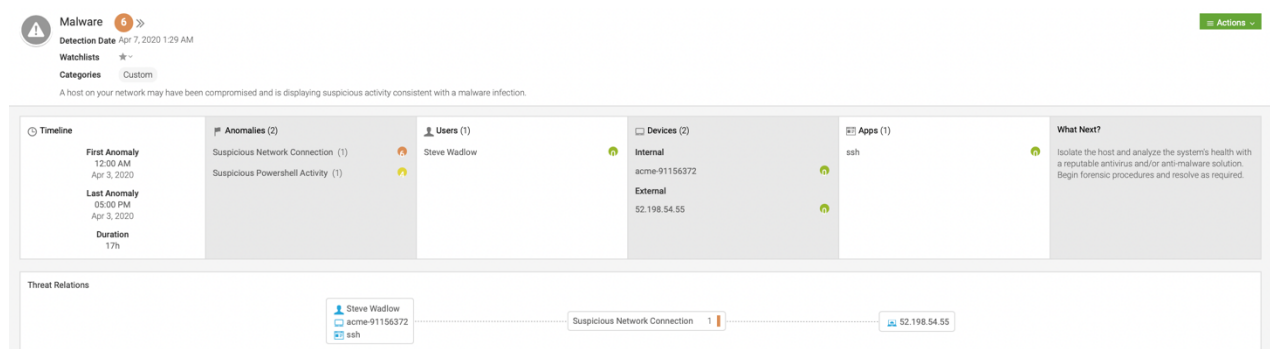


Figure 19. Compromised machine (Splunk UBA/UEBA screen capture)

The second example in Figure 20 is also potential malicious network connection. In this example we can see an asset creating out of the ordinary traffic via port reserved for NTP traffic. This alert is created because the packets size and interactive nature of the traffic is not normal for the well-defined model NTP is known for. This type of unusual behavior could indicate that the asset has been compromised and being used for data exfiltration or other types of potentially malicious covert communication by an inside or outside threat.

Suspicious Network Connection 9 Actions

Detected an unusual network connection or one with possible security implications.

Anomaly Creation Time Apr 6, 2020 11:16 PM
Last Scored Time Apr 6, 2020 11:16 PM
Last Scored By AnomalyScoringRules
Event Start Time Apr 4, 2020 10:48 AM **Event End Time** Apr 4, 2020 10:58 AM

Watchlists *-

Categories Allowed Behavior Command And Control Defense Evasion Firewall Data Network Detection Outgoing

NTP (Network Time Protocol) is a UDP based protocol that follows a request/response model. The protocol is well defined and has limited options. Legal packet sizes should be limited to 90 or 110 bytes (76 or 96 if source doesn't count the ethernet headers) In this case, the average packet size is 427. This is likely another application using UDP port 123. This session exchanged 12843254 bytes and is interactive. This may be a covert communication channel.

Relevant Features:

- Connection contained a High number of bytes
- Unusual Average Packet Size for NTP
- Connection appears Interactive
- Communication is with external address

Users (1)
Jillie Slade

Devices (2)
Internal
acme-72415241
External
67.168.140.28

Apps (1)
ntp

Threats (0)
This anomaly is not included in any threat

Anomaly Relations

Jillie Slade — acme-72415241 — Suspicious Network Connection — 67.168.140.28

Event Drilldown
This is a sample contributing event

```
Apr 04 10:48:00 CU-PAN-3020-1.acme.com 1,2020/04/04 10:48:00,001801028274,TRAFFIC_end,1,2020/04/04 10:48:00,10.2.10.53,67.168.140.28,0.0.0.0,0.0.0.0,Trap traffic from servers,jslade,ntp,vsys1,trust,Transit-WAN,ethermet1/5,tunnel.25,Acme1,2020/04/04 10:48:00,11051,1,19632,123,0,0,0x4000,udp,allow,12843264,8604986,4238278,30000,2020/04/04 10:48:00,7338,any,0,709566569,0x0,10.0.0.0-10.255.255.255,10.0.0.0-10.255.255.255,0,26672,3336,aged-out,0,0,0,0,,CU-PAN-3020-1,From-policy
```

Figure 20. Suspicious network traffic (Splunk UBA/UEBA screen capture)

4.2.4 Data Exfiltration

When a trusted insider or an outside entity is transferring or copying confidential information from organizations computer, cloud instance, or a server without an approval or authorization is called data exfiltration. Ultimately, this is the end goal and challenge for an attacker when the target is to steal data. How will the attacker get the data out without being detected? According to Proofpoint (2021) research, the malicious and non-malicious insiders are among the top reasons for unauthorized data exfiltrations. Though the non-malicious are usually not intentional and done in a purpose of causing harm to the organization, it is important to understand the importance to be able to detect this behavior, because those unintentional non-malicious acts can cause substantial and potentially unrecoverable harm both financially and reputationally just like the malicious and intentional ones.

Data is moving fast toward cloud, but this has not removed the old-school methods and threats associated with USB or other external drives. Also, the cloud service advancements and availability of personal massive online storage has opened a new means to transfer data outside the security of organizational borders. There are so many different services and service providers, so it is difficult to block all of them at the perimeter and it is usually impossible since these same services and service providers might be used by the organization itself.

In the following examples, we will look at a few scenarios for data exfiltration such as unknown devices, excessive printing, and excessive network transmissions. These detection mechanisms can be driven by behavioral change from the baseline or for example the sheer volume or transmission, or a combination of multiple smaller potentially suspicious indicators in users' or entities' behavior. One of the key log sources to detect potential data exfiltration is a data loss prevention solution, more commonly known as DLP. DLP can be a powerful tool, but due to certain regional legislative reasons, the implementation can be difficult, limited in scope or even prohibited. Also In real life, they are difficult to set up and maintain and they take a lot of resources from endpoints. Figure 21 shows different models for DLP based detections. Other good log sources for data exfiltration detection are for example endpoint, email, printer, firewall, IDS/IPS, cloud data and VPN (Proofpoint US, 2021).

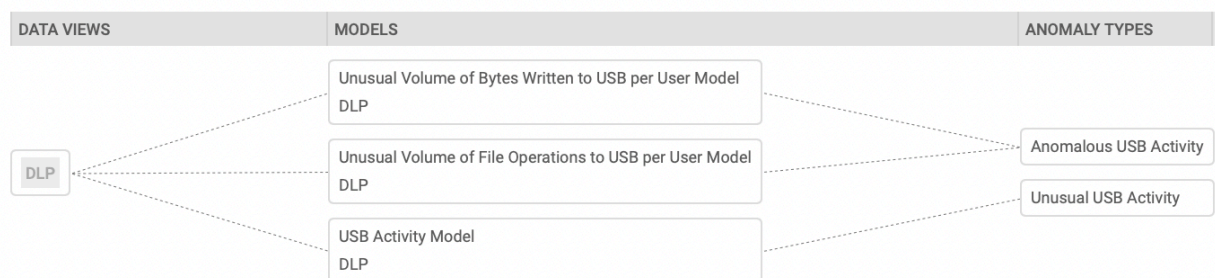


Figure 21. DLP data views (Splunk UBA/UEBA, screen capture)

In the first example illustrated in Figure 22, we can see that the UEBA tool has identified low severity level indicators for potential data exfiltration from multiple sources and combining the information to create an alert for further investigation. The user Bruce Yeager, his account has been identified to have been associated to unusual behavior outside of normal baseline, which includes multiple detections from network, endpoint, and database (cloud and or on-premises)

log sources. Additionally, the user has been identified in human resources information of being a flight risk, which basically means, that he has been either identified to be searching for a new employment opportunity or he has openly communicated this to co-workers, who then have notified management and HR. This type of HR data can be then retrieved by UEBA solutions to be added into the threat profile of the user. There are multiple cases that one can find online (Hoad, R., Neil, J., 2013), describing an employee leaving the organization taking confidential information with him/her, to benefit from those if transitioning to work for a competitor or just to cause harm if the contract was terminated. Like the case of utilizing DLP solutions, this type of activity of using HR information can be limited by regional legislation, so one needs to verify if the organization is able to execute this type of activity in monitoring.

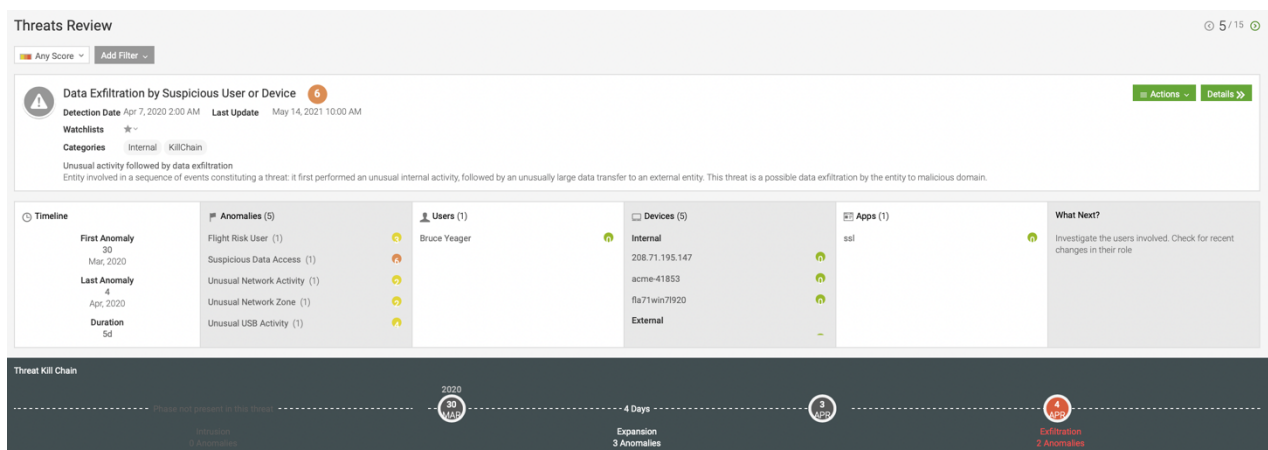


Figure 22. Data Exfiltration by suspicious user or device (Splunk UBA/UEBA screen capture)

Example two in Figure 23, is describing examples of detected unusual USB activities. Depending on the organizational policy, this can be a really good use case, especially if the organization do not have strict policies limiting the use of USB's and other external memory devices. Even though the data has been transitioned more and more into the cloud, the old-school USB's are a still relevant threat and it is unrealistic to try to ban all use of these devices. In UEBA use cases, one can detect again the unusual behavior, before unseen device are connected, using these devices more than before, or starting to use these devices for the first time even though this type of activity is not required in the specific role of the user.

ANOMALY TYPE	PARTICIPANTS	SUMMARY	START DATE	SCORE
Unusual USB Activity	<ul style="list-style-type: none">  Bruce Yeager  fla71win71920 	First time USB activity for the device	Apr 4, 2020 12:00 AM	4
Unusual USB Activity	<ul style="list-style-type: none">  Zeke Ratner  mktxsapc0020 	First time USB activity for the user	Apr 4, 2020 12:00 AM	2

Figure 23. Unusual USB activity (Splunk UBA/UEBA screen capture)

Printers still exist, though diminishing in numbers and heavily moving towards centralized network solutions. This course of development allows better monitoring and control for security personnel as well. Nowadays, it seems much simpler and user friendly for the insider to transfer data either to an external drive or even to an external online instance. There is a problem though, since the networks and endpoints are monitored better, so it still makes sense to try to exfiltrate confidential information via printed papers. In the example in figure 24, the detection originates from the change in the user's behavioral baseline. Based on the behavioral baseline gathered by the UEBA, the user Peter Venkman has never really used the printers and now suddenly there is a massive volume of documents being printed. There is the potential, that this is Peter just accidentally printing a few dozen copies instead of one or he was asked to do this, but still there is always a potential for malicious action and therefore it requires further investigation, made possible by this behavior-based detection.


ANOMALY TYPE	PARTICIPANTS	SUMMARY	START DATE	SCORE
Excessive Data Printed	<ul style="list-style-type: none">  Peter Venkman  follow-you 	Daily volume of data printed is 528739.0. Average is 0.0.	Mar 4, 2020 12:00 AM	6

Figure 24. Excessive data printed (Splunk UBA/UEBA screen capture)

Like mentioned earlier, the cloud service advancements and availability of personal massive online storages has opened a new means to transfer data outside the security of organizational borders. There are so many services and service providers, so it is difficult to block all of them at the perimeter, so the organization needs to be able to detect this. In Figure 25 we look at two alerts from two different users. These alerts are triggered due to the change in users baseline behavior. Both users are detected to exceed their average data transfer amount by large margin. These alerts could have also been triggered if the destination would have been unusual for their role or behavioral baseline or that these data transfers would have happened during unusual hours.









ANOMALY TYPE	PARTICIPANTS	SUMMARY	START DATE	SCORE
Excessive Data Transmission	<ul style="list-style-type: none">  Rithi Ravikummar  206.169.145.216  acme-91543286  google-drive-web 	Daily volume of data transmitted over the network is 242.8 MB. Average is 10.4 KB.	Apr 1, 2020 12:00 AM	7
Excessive Data Transmission	<ul style="list-style-type: none">  Rod Simmers  162.125.248.24  acme-70442216  ssl 	Daily volume of data transmitted over the network is 253.5 MB. Average is 628.9 KB.	Apr 4, 2020 12:00 AM	6

Figure 25. Excessive data transmission (Splunk UBA/UEBA screen capture)

4.2.5 Lateral Movement

It does not really make difference on what is the motive behind the actions, but for an attacker, whether it is an insider or outsider, the goal is to get access to classified and valuable data. Based on security by design, the more critical and valuable the data is, more complex and tighter the security is around it and that makes perfect sense. Unfortunately, this is not the case in real life and security is usually just added on to a ready solution making it less effective.

For an insider, the difficulty of the task is depending on what level of access the user has, and does the user know who has the access which is desired. The most critical information and data usually requires privileged access, and this is not and should not be given precariously. So, if the insider does not have the access, he/she needs to obtain it. This can be achieved via legitimate access requests, and if the organization does not have a strict policy or the approving authority is not paying attention, the access can be obtained easy and without triggering any alarms from basic detection mechanisms.

If the insider does not have the privileged access to the desired information and or data, then he/she will utilize techniques usually referred to as lateral movement. This is where the malicious insider will try to move through the network, assets, and accounts, to find the target and or acquire the access. If the insider is not familiar with the environment, then this is achieved by executing scans to identify resources he/she can further use to expand access and additionally compromise or utilize other assets or credentials. Log sources to detect this type of anomaly types are network solutions like Firewall, IDS/IPS, which are illustrated in Figure 26 and active directory (Windows security events).

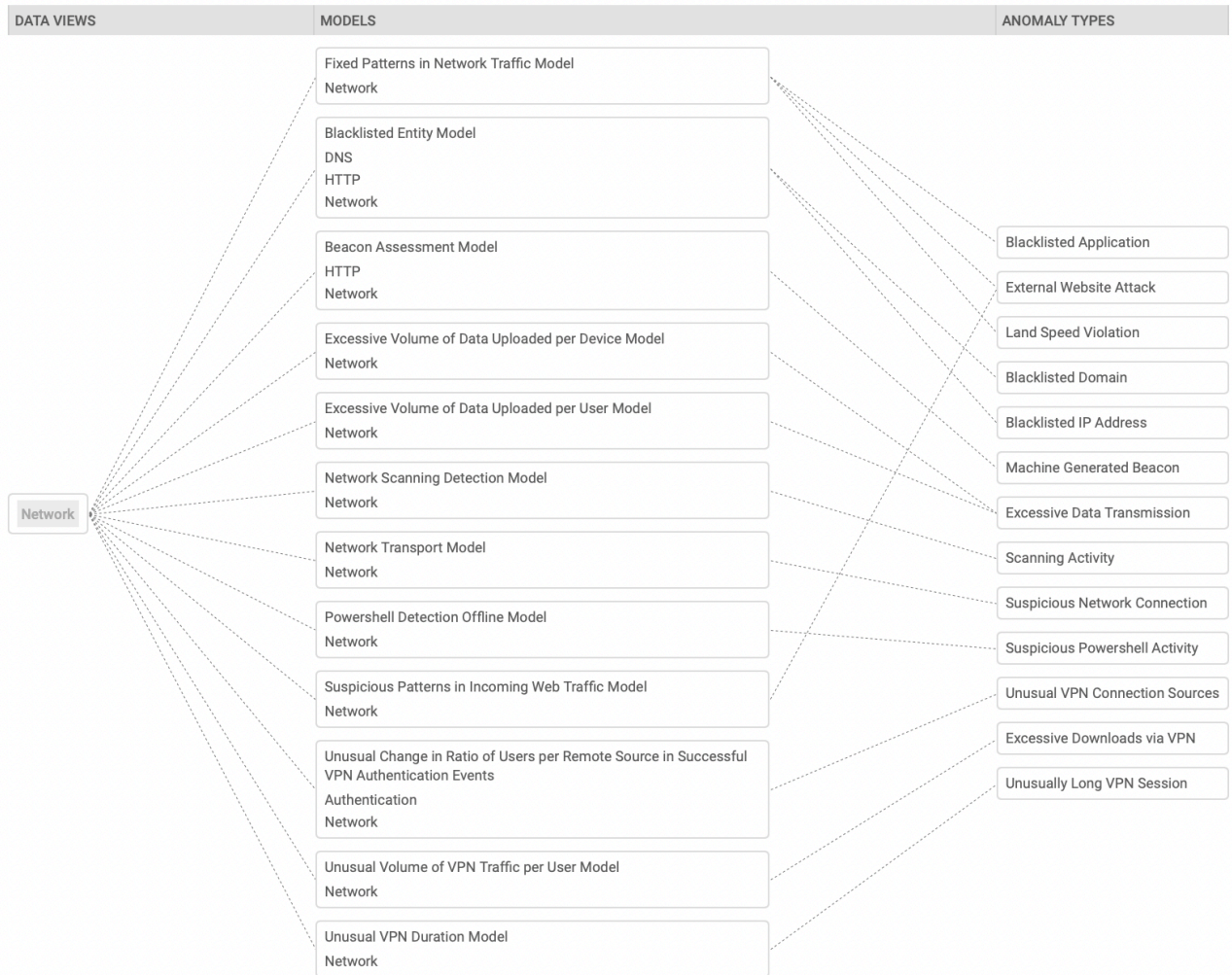


Figure 26. Network data views (Splunk UBA/UEBA, screen capture)

If the malicious insider does not have a good understanding of the environment, he/she needs to achieve this to be able to find the route to the desired asset or data. Basic scanning tools are easily available and are easy to use even with average IT skills, but if the organization has even basic security monitoring in place, this type of basic scanning should be detected when the average user scans the whole network from his/her workstation. If the scanning is done in a more covert way and the malicious insider has executed limited and long running scans to targets like hosts or applications, he/she is interested, then those can easily be bypassed by the standard monitoring tools. This requires UEBA capabilities to look at the change in behavior baseline, as illustrated in Figure 27.

Scanning Activity 6

Detected a possible horizontal or vertical scan over the network.

Anomaly Creation Time Apr 7, 2020 1:08 AM
Last Scored Time Apr 7, 2020 1:08 AM
Last Scored by AnomalyScoringRules
Event Start Time Mar 23, 2020 12:00 AM **Event End Time** Mar 23, 2020 12:00 AM

Watchlists *~

Categories Behavior Firewall Data Lateral Movement Recon

Device scanned multiple hosts looking for 2 particular services over the course of 15 days.
 It is likely that an attacker is attempting to locate a specific service or type of host on the network while avoiding detection with a long-running scan. A stealth service scan like this usually indicates that an attacker has an exploit for a service and is looking for available hosts to exploit.
 Device looked for 42 distinct destinations, sending 46 probes. 17 probes were acknowledged. 8 events are additional, non-probe connections. This might indicate an exploit that followed a scan.
 Device scan behavior shows regularity in the number of services scanned per day, but variations in the destinations scanned.
 The tables below show details about each service scanned. For each service scanned we show maximum 50 destinations.

Devices (38)

Internal

- acme-17122059
- acme-20082333
- acme-22559801
- acme-25749606

Apps (1)

- tcp

Threats (0)

This anomaly is not included in any threat

Anomaly Relations

acme3 tcp Scanning Activity acme-17122059 acme-20082333 acme-22559801 Show All 37

Figure 27. Unusual scanning activity (Splunk UBA/UEBA screen capture)

In this example pictured in Figure 28, the UEBA is using active directory logs to detect a potential malicious insider performing a security sensitive operation on his/her account. The user db-backup has been detected for adding his/her account to a global security enabled group. Also, this alert could have been raised because of the early hours of the action. Detection was made before 7 a.m., which could easily be out of the ordinary behavior of this user. This type of activity could entail, that the user is trying to achieve a privileged access via bypassing the organizational procedures or somebody has compromised this specific account and trying to use it as a steppingstone towards desired information and simultaneously hiding his/her tracs of the potentially malicious act.

Malicious AD Activity 5

Potentially malicious Active Directory activities.

Anomaly Creation Time Apr 6, 2020 10:49 PM
Last Scored Time Apr 6, 2020 10:49 PM
Last Scored by AnomalyScoringRules
Event Start Time Apr 5, 2020 6:56 AM **Event End Time** Apr 5, 2020 7:06 AM

Watchlists *~

Categories Allowed Credential Access Internal Privilege Escalation Signature

User performs a security sensitive operation on himself.

Users (1)

- db-backup

Devices (1)

- Internal**
- scl-dc01

Threats (0)

This anomaly is not included in any threat

Event Drilldown

This is a sample contributing event

Apr 05 06:56:21 SCL-S-DC01.corp.acme.com/10.115.16.5/1.9.130.1 MSWinEventLog,1,Security,856175252,Sun Apr 05 06:56:21 2020,4729,Microsoft-Windows-Security-Auditing,,ACMEDOM\dcallister,N/A,Success Audit,SCL-S-DC01.corp.acme.com,Other,, member was added to a security-enabled global group. Subject: Security ID: S-1-5-21-753876628-205549372-1428518885-18651 Account Name: db-backup Account Domain: CORP Login ID: 0x17ae4159 Member: Security ID: S-1-5-21-753876628-205549372-1428518885-2701 Account Name: CN=db-backup,OU=Admin Accounts,OU=IT Operations,OU=Operations,OU=ATL,DC=corp,DC=xyz,DC=net Group: Security ID: S-1-5-21-753876628-205549372-1428518885-14805 Group Name: GRCA\Users Group Domain: CORP Additional Information: Privileges: ~ 3524343

Figure 28. Malicious AD activity (Splunk UBA/UEBA screen capture)

Lateral movement can also happen in the physical world. If the malicious insider does not have the tools or required IT skills to perform this activity in the network, it can be easier to just access the computer of somebody else who has the sensitive data he/she is looking for. Central storages and network drives have existed for ages and the implementation of cloud have made shared drives even more convenient and easy to access from wherever the user is. Still, multiple organizations struggle with the fact that users are still saving information on their desktops and computer hard drives. This brings problems from the backup perspective, but also it is more difficult to monitor if the data is present and accounted for and if the data is compromised in any way. If the data is stored in a way that another user can access it with his/her credentials, it would be difficult to detect without DLP solutions. UEBA provides an alternative approach to this, by monitoring the relationship of users and assets such as workstations, external memories USBs and printers, assets we use on daily basis. When something changes in the behavior baseline, the UEBA tool raises an alert. As seen in the Figure 29, where the user Ed Jones is accessing a device that is not usually associated with his account. Another indicator raising the severity of the detection is the fact that the device that was accessed is a domain controller which is usually categorized as a sensitive asset. Adding HR and or role-based information to this alert could provide additional information of Ed Jones, for example Ed being a cafeteria worker, thus having zero requirement of accessing organizations domain controllers.

Unusual Machine Access 2 Actions

Unusual interactions between accounts and devices.

Anomaly Creation Time Apr 7, 2020 2:31 AM
Last Scored Time Apr 7, 2020 2:31 AM
Last Scored by AnomalyScoringRules
Event Start Time Mar 25, 2020 12:00 AM **Event End Time** Mar 26, 2020 12:00 AM

Watchlists * -

Categories Active Directory Data Allowed Behavior Internal Lateral Movement Rare Device

An unusual interaction between an account and a device has been observed. The device may be unusual for the account given the account's history of device accesses, or the account may be unusual for the device given the history of accounts interacting with the device. In addition, other properties of the interaction may be unusual. An account can interact with a device in multiple ways: the device could be a destination of a login, the source of a login, or the device hosts services that the account attempts to authenticate for.

The account interacts with only few devices
 Multiple accounts interact with this device over multiple days
 The device is Domain Controller
 The device is considered sensitive because it is Domain Controller
 Found 2 rare value(s) over a period of 30 days.

1. Account [ejones] is uncommonly associated with Device [acme-dc01] in this environment – 5 occurrence(s) out of 44.8K. When observing Device [acme-dc01], most commonly observed values (up to top 3) are:

- [jgood] occurs 27.2K time(s) out of 44.8K (60.9%)
- [jevans] occurs 1.8K time(s) out of 44.8K (4.0%)
- [jmclean] occurs 1.5K time(s) out of 44.8K (3.4%)

2. Account [ejones] is uncommonly associated with Device Peer Group [Client-like behavior, Server-like behavior, involves Internal to Internal traffic, uses applications associated to Windows Machine] in this environment – 5 occurrence(s) out of 44.8K. When observing Device Peer Group [Client-like behavior, Server-like behavior, involves Internal to Internal traffic, uses applications associated to Windows Machine], most commonly observed values (up to top 3) are:

- [jgood] occurs 27.2K time(s) out of 44.8K (60.9%)
- [jevans] occurs 1.8K time(s) out of 44.8K (4.0%)
- [jmclean] occurs 1.5K time(s) out of 44.8K (3.4%)

Score Details

- The account is rare for the device and also a device peer group violation so it is interesting even though the device is accessed by multiple accounts
- Base score depends on the number of interesting rare values: 1
- Score increased (+1) since activity involves a sensitive device

Users (1)
Ed Jones

Devices (1)
Internal
acme-dc01

Threats (0)
This anomaly is not included in any threat

Anomaly Relations

Ed Jones — Unusual Machine Access — acme-dc01

Figure 29. Unusual machine access (Splunk UBA/UEBA screen capture)

4.2.6 Suspicious Behavior / Unknown Threats

Suspicious behavior and unknown threats are at least for me the most interesting and most complex use case. These use cases require massive amount of log sources and manually inputted data, thus making it difficult and potentially costly, but from my security professional point of view, maybe the most valuable for detecting insider threats. Especially detecting the skilled ones that either already have the access or know where to get it and have a plan how to execute their actions.

As presented earlier in this thesis, there is more to identifying and detecting a potential insider threat than just monitoring logs from different sources. Successful Insider threat detection program and or operations are a combination of technical surveillance based on different types of logs, but also a key component is the human factor. This human factor is compromised from background checks, continuously updated HR information and, not forgetting the employees, who are the eyes and ears in the organization. They are often situated in a way that they can detect a concerning change in a co-worker's behavior, personal life etc. and should be encouraged to report these findings forward to management or HR personnel. Not to penalize but to allow organization to either understand the context of the behavior or to intervene earlier and provide required support, if the issues are health, financial, family etc. related, before those escalate to a level, where this individual can become a liability and an insider threat to the organization (CISA, 2020).

The term unknown threat in cyber domain is often associated with zero-day vulnerabilities, but in insider threat context it can be described as a phenomenon for which there are no pre-defined clear indicators to which one could counter with signatures and correlation to be able to identify this potentially malicious scenario. In the following examples, we will look at different types of detected anomalies from various source domains. In the cyber world, we do not often monitor indicators from the physical world, information such as badge access or smart locks. In Figure 30 one can see the potential what monitoring of badge access could bring to insider threat monitoring capabilities. This is still a valid use case, since though we are moving more and more towards a digital society, there is still plenty of data in paper format that requires protection, but also, there are digital assets in high security environments that are not connected to networks, so getting access to those would require physical presence.

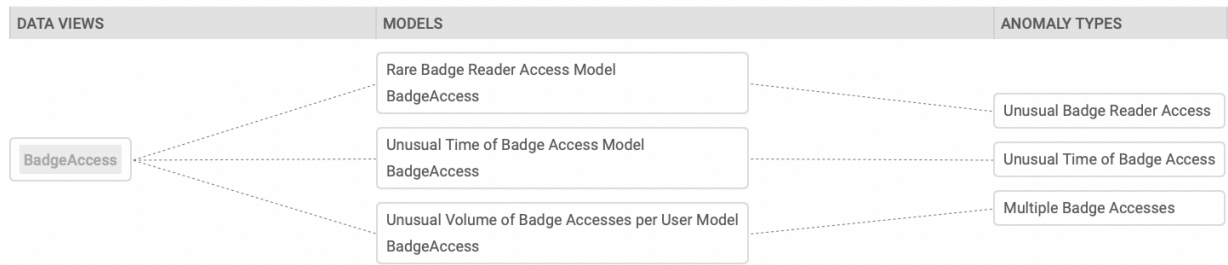


Figure 30. Badge access data views (Splunk UBA/UEBA, screen capture)

Gathering user information and especially information that is categorized within privacy is a touchy and heavily regulated topic in multiple regions. This requires great attention to detail and due diligence to be compliant with the regulations and laws. Gathering user information for insider threat management can still be achieved and used for preventative actions. When utilizing UEBA solutions we can combine multiple sources of information as pictured in Figure 31, to provide situational awareness for internal security personnel. This figure shows that with a single dashboard one can get a view on the status regarding potential internal threats whether those are users or entities. Dashboards are very similar to SIEM tool dashboards providing an overview of information security related events to security operation center analysts. In this example, the UEBA dashboard is combining information sources from HR to technical logs to provide a risk score for each individual.

All Users Actions

All Users Any HR Record Add Filter Save Clear Filters

Users (117)

NAME	HR RECORD	ACTIVE THREATS	ANOMALIES	EXTERNAL RISK PERCENTILE	INSIDER RISK PERCENTILE	ANOMALY RISK PERCENTILE	SCORE
Bryan Wilson	Known	0	4	0%	100%	93%	0
Terrance Jackson	Known	0	0	0%	99%		0
Albert McClean	Known	0	0	0%	98%		0
George Evans	Known	0	2	0%	97%	0%	0
Joseph Thierry	Known	0	0	0%	97%		0
Walter Smith	Known	0	0	0%	96%		0
Thomas Clarke	Known	0	0	96%	95%		0
Omar Smith	Known	0	4	0%	94%	89%	0
Angelina Smith	Known	0	2	0%	93%	0%	0

Figure 31. User dashboard with risk score (Splunk UBA/UEBA screen capture)

From the dashboard view, we can proceed to deeper analysis with the chosen target. In this example in Figure 32, the user Bryan Wilson is showing a high percentile in detected anomalies to be suspected of insider threat activity. This is where the security resources can utilize HR data, like background information from security interviews, checks or information provided by co-workers. If this specific user is recorded as being discontent, carrying a grudge and looking to leave the organization, but also the technical indicators are correlating with these human based indicators, then the likelihood of accurate detection is higher. In this specific example, we can see from the detected behavior, that the risk score for this user is coming from multiple different types of anomalies. There are several sources and destinations for large outbound data transfers, several login attempts and denied access to assets and or applications. This type of activity could be associated to committing a fraud or stealing confidential information, since these types of indicators are typically detected for user trying to gain privileged access and exfiltration of data. There is also detection for visiting job sites which could be an indicator for an employee at flight risk, but this type of monitoring will most likely be against privacy legislation in multiple regions, so the organization need to be aware of these limitations.

Bryan Wilson 0

Last Update Mar 25, 2020 8:44 AM

Watchlists ★

Account Normal (bwilson)

User Facts

THREATS		ANOMALIES	
0		4	

EMPLOYEE ID ACME-1017	OU Sales	USER STATUS Active	PHONE 408-555-2100
STREET 1735 Technology Blvd	CITY San Jose	STATE CA	COUNTRY US

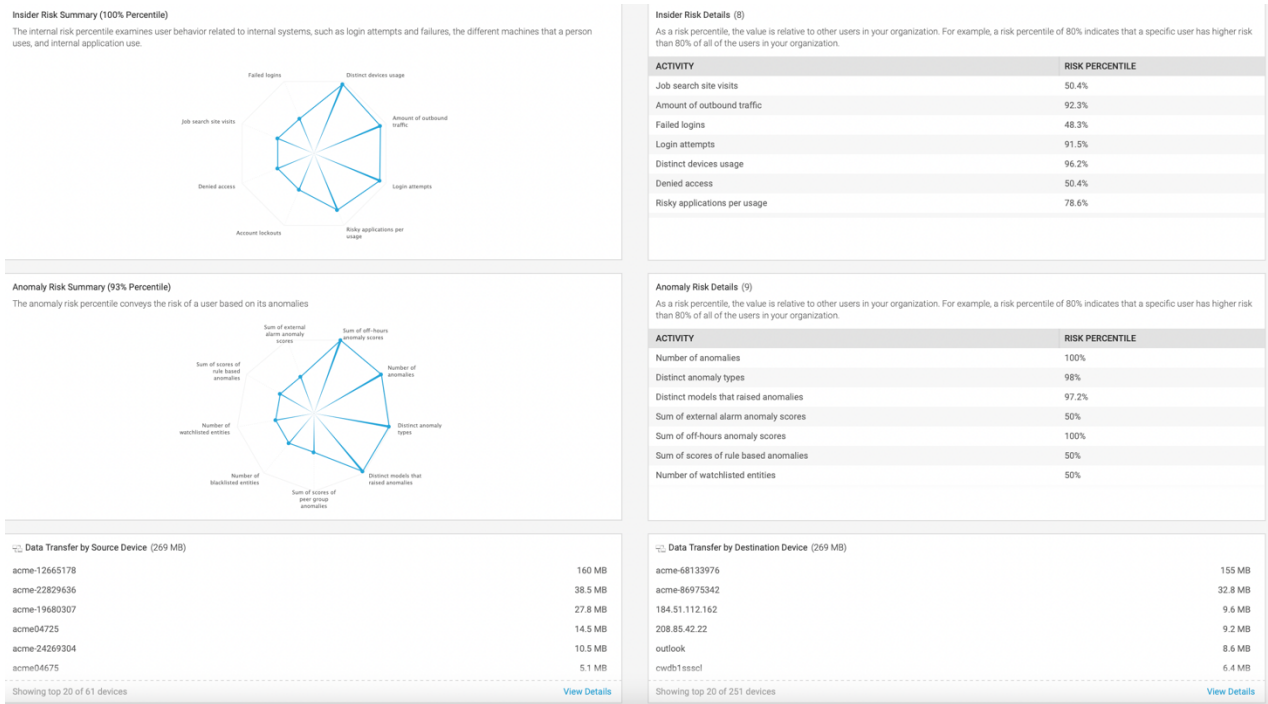


Figure 32. User facts and summary (Splunk UBA/UEBA screen capture)

As mentioned earlier, nowadays in this heavily networked and digital environment, we do not often monitor indicators from the physical world within the cyber security operation centers and SIEM tools. Information such as badge access or smart locks which are a commonly used de facto standards of the physical security. Figure 33 provides a good example of what kind of additional value could monitoring of badge access or smart locks provides yet as another input for detecting potential malicious insider threats. This is still a valid use case, since though we are moving more and more towards digital society, there is still plenty of data in paper format that requires protection, but also, there are digital assets in high security environments that are not connected to networks, so getting access to those would require physical presence. In this example we can see that UEBA has detected a change in the behavior of user Louis Manger. There are different types of detected anomalies or changes from the behavioral baseline, such as trying to access facilities to which the user does not have authorization, unusual times of access and trying to utilize a disabled badge. All these activities could be associated to insider activity where the individual is trying to achieve access to secure premises and protected assets and information that is not reachable via online methods.

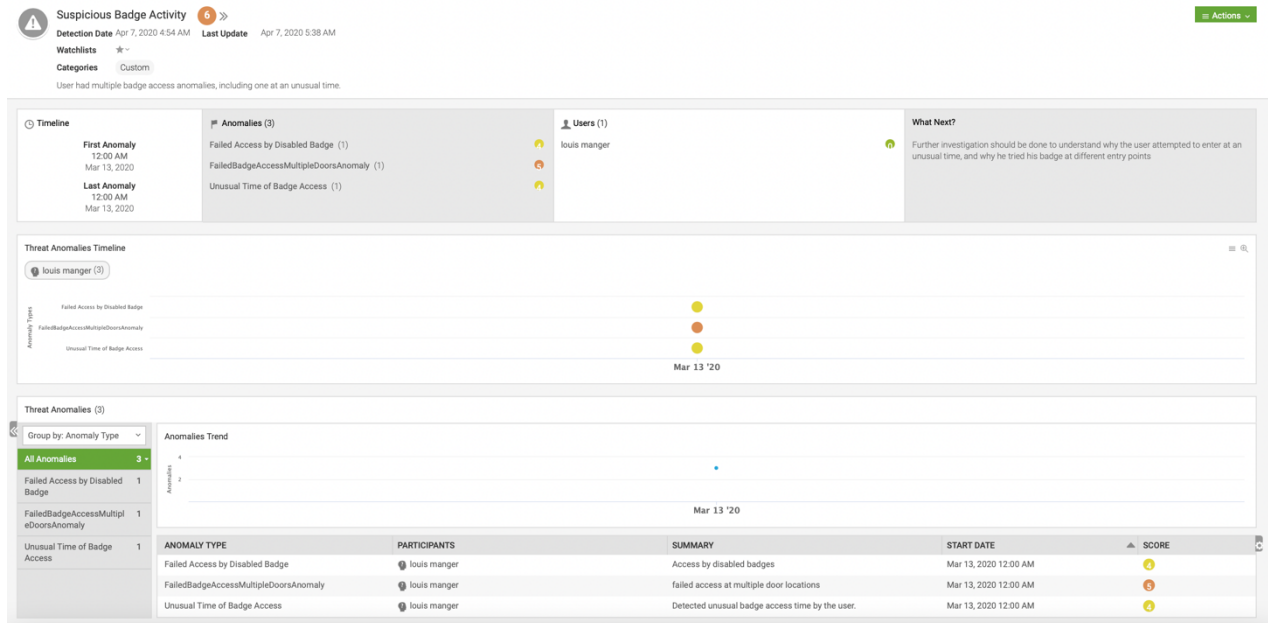


Figure 33. Suspicious badge activity (Splunk UBA/UEBA screen capture)

In high security environments, though they are usually separated from their own closed networks, those still need to be maintained and especially monitored. Otherwise, the organization will end up with outdated and unsecure environment. These lifecycle management and security monitoring capabilities can still be achieved in a secure fashion, though the network might not be accessible from outside. As an example, for monitoring, the log data can be gathered to a centralized storage within the closed network and then forwarded via data diode to SIEM and UEBA solutions within other organizational networks. These one-directional diode solutions have optical hardware separation and content inspection which allows a secure separation between different networks of equal level or different security levels.

These high security environments are often the crown jewel of the organization, thus requiring non-stop monitoring. We continue from the previous examples, where the malicious insider threat was detected trying to elevate his access and trying to achieve access to secure premises and protected assets and information. In detection presented in Figure 34, the user Monica Smith has either had or has achieved an elevated access to secure premises, but now has been detected trying to login and use a machine she is not authorized.

Unauthorized Login Type 3

User attempted an unauthorized AD login. This login was prevented due to login type.

Anomaly Creation Time Apr 6, 2020 11:52 PM
Last Scored Time Apr 6, 2020 11:52 PM
Last Scored by AnomalyRules
Event Start Time Apr 5, 2020 12:00 AM
Event End Time Apr 5, 2020 12:10 AM

Watchlists ☆ -

Categories Active Directory Data Blocked Credential Access Local Policy Violation Rare Device Signature

UBA identified 1 login failures on to the target machine. This was identified as suspicious because the error code 0xc0000070 indicated that the user was not authorized to login at this machine. These restrictions are usually set on Active Directory. Verify if this was a legitimate activity. If not, check for any other IOCs on this machine.

Users (1)
Monica Smith

Devices (1)
External
128.126.114.23

Threats (0)
This anomaly is not included in any threat

Unauthorized login activity
UBA identified 1 login failures on to the target machine. This was identified as suspicious because the error code 0xc0000070 indicated that the user was not authorized to login at this machine. These restrictions are usually set on Active Directory. Verify if this was a legitimate activity. If not, check for any other IOCs on this machine.

EVENTID	SUB STATUS DESCRIPTION/FAILURE REASON	ERROR CODE	FAILED LOGINS
[4625]	[User not allowed to login at this computer.]	[0xc0000070]	[1]

Figure 34. Unauthorized login (Splunk UBA/UEBA screen capture)

Looking at all these different layers of detection for unknown threats and suspicious behavior, ranging from background information to physical and technical indicators, one can see the strength and depth of behavioral analysis of the UEBA tools, but also gives a high-level understanding of the complexity and difficulty of detecting a trained professional utilizing tradecraft to avoid being detected.

4.3 Prioritization

If the resources are not available in the extent needed, that leaves only one option and that is to prioritize. Not all log and or indicator sources are created equal. Some of them provide more value than others. In this section I will try to summarize the value of different information sources based on research data covered in chapter 2.6 of this thesis, but also through quantifying the log source information from the use cases of the Splunk UBA/UEBA tool. Of course, this is not an absolute truth or the best way for every organization. Every organization is different, different level of maturity in security policies and with different risk appetite, so the organization needs to evaluate where they are with maturity etc. and through holistic understanding of the IT environment and naturally the tools that they will be using for user and entity behavior analytics. UEBA tools will have some similarities, but all vendors and manufacturers have their own approach and technology, so this is also something that the organization needs to take in consideration.

The statistics in section 2.6 can provide a basic knowledge of the potential targets, these numbers could vary from organization to another depending on geolocation, industry and or for example size. Also, some of the cases could involve attacks towards multiple assets when the attacker has conducted lateral movement to achieve their main target. Through holistic understanding of what are the critical assets, associated vulnerabilities, statistics of potential targets from researched insider attacks and use cases from the UBA/UEBA tool, we can look at what are the best log sources to provide best possible coverage for organizations environment. For the Splunk UBA/UEBA use cases we have covered in this master's thesis, the most valuable log sources for insider threat detection are presented in Table 2. The prioritization is based on the utilization of each log source per use case.

Use case → Log source ↓	Account Misuse	Compromised User Account	Compromised and Infected Machine	Data Exfiltration	Lateral Movement	Suspicious Behavior / Unknown Threats
Authentication	X	X				X
AD	X	X	X		X	X
Firewall			X	X		X
IDS/IPS			X	X	X	X
Endpoint	X	X	X			X
VPN	X	X		X		X
Cloud	X	X		X		X

DNS			X			X
Badge	X	X				X
DLP			X	X		X
Email	X					X
Printer				X		X

Table 2. Log source prioritization based on Splunk use cases

Based on Table 2, the five most valuable technical log sources would be AD, IDS/IPS, Endpoint, VPN and Cloud. These are the building blocks from which the organization can prioritize their own build based on the organization's resources and capabilities. But the two critical log sources that need to be implemented before any of these listed in Table 2, are HR data and up to date asset database (CMDB). For UBA/UEBA to work properly, the solution needs to be able to identify users and assets. Also from authentication perspective, though not high on the Table 2 usability, important log sources are DHCP and DNS.

5 Conclusion

The purpose of this master's thesis was to research and gather the basic knowledge of insider threat taxonomy, what are the common indicators in human behavior and background, how those indicators could be potentially detected via technical logs (machine data) with UBA/UEBA tools and what are the different threat types associated to each use case. The objective was to research the topic purely from an internal security perspective and concentrating on the employees, who for some reason decide to do the wrong thing or bypass the rules. Through understanding the insider threats and corresponding technologies to mitigate them, the result of this master's thesis could be used as a prioritized blueprint for organizations battling against this threat, to plan, improve and build their defenses. To guarantee quality and ethics of my research the process was defined in detail before initiating the research. Mixed method was chosen as

the main methodology as it provides both qualitative and quantitative data, which was gathered through different sources including literature review, interview and utilizing a test environment to further provide proof for conclusions.

The research indicates that the Insider threats are one of today's most challenging cybersecurity issues alongside with nation state threat actors and organized crime organizations that are not well addressed by commonly employed perimeter or signature-based security solutions. Insiders come in many shapes and forms and are motivated by different agendas. Sometimes the insider activity was not performed out of malicious intentions, but due to the actions taken, the result could be severe for the organization. On a high-level, we can categorize different types of insiders to five distinct categories, which are:

- Workplace violence
- Fraud
- Theft of intellectual property, sensitive and/or classified materials or information (espionage)
- Sabotage
- Terrorism

Insider threat is not just, somebody stealing confidential data and selling it to the highest bidder. Insider threats can also pose a physical risk to people, assets, and facilities, not to mention the reputational impact that any of these incidents would cause. This is the reason why this threat should be on every organization executive board agenda and not just an information technology issue. Managing these identified risks are the key for maximizing the preventative capabilities as stated in the Federal Bureau of Investigations report (*Making Prevention a Reality: Identifying, Assessing, and Managing the Threat of Targeted Attacks*, n.d.).

Information gathered through research indicate that as the outside threats have increased, so have the risks associated to malicious insiders. Compared to outsiders, the insider threats have the advantage that they are already inside the firewall. Most importantly, the malicious insiders already have certain level of access, they know where and how to further their reach towards the information, data, or asset they are after. If the insider is in privileged position, and is familiar with the organizational policies, network architecture, security capabilities, they have good chance of executing their malicious act, hide their tracks and avoid detection (Warkentin & Willison, 2009).

To combat these sophisticated outside and insider threats the security teams are required to shift their focus from legacy perimeter and signature-based defenses to look for the anomaly within their networks and assets. With user behavior analytics solutions utilizing the AI power and collected data organizations can baseline what is the normal behavior and react and investigate when an anomaly occurs. Like mentioned earlier, the insider or the APT with foothold in the environment, usually appear like any other normal user. Though they use the same tools, but usually to do what they want to do, they need to do it hidden, meaning odd hours and odd locations. Especially with APT's, they need to carry out their actions remotely. This is something that the user behavior monitoring can detect.

My findings indicate that majority of cyber security tools and more precisely threat intelligence tools are looking at technical indicators of compromise for internal threats. The common sources for information are applications, computers, servers, and network devices. These solutions can also monitor for example a privileged and authorized access of a person, but how can it define what is good or potentially bad for each specific user. This is the reason for monitoring the behavior of users and assets to detect the anomaly and possible indicators of compromise.

As can be seen from the research, the data that is required for insider threat detection is varied and ranging from background check interviews to digital logs from multiple different systems. UBA/UEBA is a complex solution, that requires a lot of funds, resources, knowledge, and dedication to make it work like it should. When implemented properly as a part of insider threat management program the UBA/UEBA can bring new capabilities to detect these internal threats and intervene in time. The organization does not need to implement a 100% coverage from the beginning, but rather from first understanding the organization specific environment, technical solutions, vulnerabilities, and threats, they can build this capability in smaller pieces and maximizing the fund and resources which the organization have at their disposal. This master's thesis provides a one version of log source prioritization based on a specific technology. The log source prioritization based on my research is not something that will fit every IT environment and organization, but it provides some ideas and a starting point, from which one can start building their own approach based on their organization resources and risk appetite, to tackle this growing threat.

How to continue the research on this topic? Based on the existing knowledge, the logical approach would be to document a real-life UBA/UEBA implementation and to verify the detection capabilities of the behavioral analytics tool. Based on the findings, this would be a challenging task due to the complex nature of the solution itself which will take time to implement properly. The target organization, their IT environment, related processes, personnel and existing log management and monitoring needs to be mature enough to allow a firm basis for more advanced capabilities such as UBA/UEBA.

Second option to advance this research could be a more in-depth look at a certain insider threat types or a type of indicators potentially associated to insider threats. For me personally, the topic would be to look at how to utilize information gathered from actions such as background checks and interviews in UBA/UEBA tools. This information is gathered from people by people, so it is different from standard log data which is more often utilized and can be a challenge to add to the system in a way that the UBA/UEBA solution is capable to utilize it. This type of personal information could potentially be extremely useful when correlated against low severity detections. If there are some background information that makes the specific user to be more vulnerable to for example outside influence, could raise the severity of the detection, thus resulting into further investigation. Due to legislative reasons, one needs to approach this topic carefully and examine local legislation before embarking on this research to avoid any privacy related issues.

References

- Amoroso, E. G. (2011). *Cyber attacks: protecting national infrastructure*. Butterworth-Heinemann.
- Beardsley, T., Carraig, S., & Nicholas, A. (2021, 10 20). BrightTalk. Viewed March 26, 2022. https://www.brighttalk.com/webcast/10457/511418?utm_source=brighttalk-portal&utm_medium=web&utm_content=user%20behaviour%20analytics&utm_term=search-result-2&utm_campaign=webcasts-search-results-feed
- Blowers, M. (Ed.) (2015). *Evolution of Cyber Technologies and Operations to 2035*. Springer International Publishing.
- Brancik, K. (2007). *Insider Computer Fraud An In-depth Framework for Detecting and Defending against Insider IT Attacks*. Auerbach Publications.
- Cappelli, D., Moore, A., & Trzeciak, R. (2012). *The CERT guide to insider threats: how to prevent, detect, and respond to information technology crimes (theft, sabotage, fraud)*. Addison-Wesley.
- Carey, E. (2021). *Research Guides: P.R.O.V.E.N. Source Evaluation*: Santa Barbara City College, Retrieved April 18, 2022. <https://libguides.sbcc.edu/PROVEN>
- Chettiar, R. (2019). *How to Prevent and Detect Malicious PowerShell Attacks | Rapid7 Blog*. Rapid7. <https://www.rapid7.com/blog/post/2019/08/08/the-importance-of-preventing-and-detecting-malicious-powershell-attacks/>
- Cybersecurity and Infrastructure Security Agency, (n.d.). *Insider Threat Mitigation*. [Www.cisa.gov . https://www.cisa.gov/insider-threat-mitigation](https://www.cisa.gov/insider-threat-mitigation)

Cybersecurity and Infrastructure Security Agency. (2020). *Insider Threat Mitigation Guide*.

https://www.cisa.gov/sites/default/files/publications/Insider%20Threat%20Mitigation%20Guide_Final_508.pdf

DBIR Report 2022, (2022). Verizon Business. <https://www.verizon.com/business/en-gb/resources/reports/dbir/2022/master-guide/>

Ekran. (2019, June 19). *Insider Threat Statistics for 2019: Facts and Figures*. EkranSystem.com.

<https://www.ekransystem.com/en/blog/insider-threat-statistics-facts-and-figures>

Fimin, M. (2018). *Privilege Abuse Attacks: 4 Common Scenarios*. Dark Reading.

<https://www.darkreading.com/endpoint/privilege-abuse-attacks-4-common-scenarios>

Frankenfield, J. (2019). *Inside Behavioral Analytics*. Investopedia. [https://www.in-](https://www.investopedia.com/terms/b/behavioral-analytics.asp)

[vestopedia.com/terms/b/behavioral-analytics.asp](https://www.investopedia.com/terms/b/behavioral-analytics.asp)

Gelles, M. G. (2016). *Insider threat: prevention, detection, mitigation, and deterrence*. Butterworth-Heinemann

Goldstein, J. (2020, July 16). *What Are Insider Threats and How Can You Mitigate Them?* Security Intelligence. <https://securityintelligence.com/posts/what-are-insider-threats-and-how-can-you-mitigate-them/>

Green, A. (2015, July 21). *What is User Behavior Analytics?* Inside out Security. [https://www.va-](https://www.varonis.com/blog/what-is-user-behavior-analytics/)
[ronis.com/blog/what-is-user-behavior-analytics/](https://www.varonis.com/blog/what-is-user-behavior-analytics/)

Greenemeier, L. InformationWeek, With, Sharon Gaudin. (2007). The Threat From Within -- Insiders represent one of the biggest security risks because of their knowledge and access. To head them off, consider the psychology and technology behind attacks. *Insurance & Technology*, 32(2), 38-40.

<http://ezproxy.jamk.fi:2048/login?url=https://www.proquest.com/trade-journals/threat-within-insiders-represent-one-biggest/docview/229199092/se-2?accountid=11773>

- Hamin, Z. (2000). Insider Cyber-threats: Problems and Perspectives. *International Review of Law, Computers & Technology*, 14(1), 105–113. <https://doi.org/10.1080/13600860054944>
- Hartline, C. L., Jr. (2017). *Examination of insider threats: A growing concern*. [Master's thesis, Utica College], ProQuest, <https://www.proquest.com/dissertations-theses/examination-insider-threats-growing-concern/docview/1984989687/se-2>
- Hoad, R., Neil, J., (2013). *Confidential information and departing employees - the threat from within*. Clayton Utz. <https://www.claytonutz.com/knowledge/2013/august/confidential-information-and-departing-employees-the-threat-from-within>
- Homoliak, I., Toffalini, F., Guarnizo, J., Elovici, Y., & Ochoa, M. (2019). Insight Into Insiders and IT. *ACM Computing Surveys*, 52(2), 1–40. <https://doi.org/10.1145/3303771>
- Intelligence and National Security Alliance (2019), *Categories of Insider Threats*. https://www.insaonline.org/wp-content/uploads/2019/10/INSA_WP_Categories_of_Insider_Threats-1.pdf
- Jääskeläinen, V. (2018). *Liikesalaisuuksiin kohdistuvien insider-riskien hallinta, Suojelupoliisin julkaisusarja 1/2018*. <https://ek.fi/wp-content/uploads/Liikesalaisuuksiin-kohdistuvien-insider-riskien-hallinta.pdf>
- Kont, M., Pihelgas, M., Wojtkowiak, J., Trinberg, L., & Osula, A.-M. (2014). *Insider Threat Detection Study*. NATO Cooperative Cyber Defence Centre of Excellence, https://ccdcoe.org/uploads/2018/10/Insider_Threat_Study_CCDCOE.pdf
- Krasznyay, C., & Hámornik, B. P. (2018). Analysis of Cyberattack Patterns by User Behavior Analytics. *Academic and Applied Research in Military and Public Management Science*, 17(3), 101–113. <https://doi.org/10.32565/aarms.2018.3.7>

- Krishnan, A., (2022). *Best practices for creating an insider threat program*. SearchSecurity. Retrieved May 1, 2022, from <https://www.techtarget.com/searchsecurity/tip/Best-practices-for-creating-an-insider-threat-program>
- Legg, P. A., Buckley, O., Goldsmith, M., & Creese, S. (2017). Automated Insider Threat Detection System Using User and Role-Based Profile Assessment. *IEEE Systems Journal*, 11(2), 503–512. <https://doi.org/10.1109/jsyst.2015.2438442>
- Making Prevention a Reality: Identifying, Assessing, and Managing the Threat of Targeted Attacks*. (n.d.). Federal Bureau of Investigation. <https://www.fbi.gov/file-repository/making-prevention-a-reality.pdf/view>
- McCombes, S. (2019, February 22). *How to write a literature review*. Scribbr. <https://www.scribbr.com/methodology/literature-review/>
- Mehan, J. (2016). *Insider threat: a guide to understanding, detecting, and defending against the enemy from within*. It Governance Pub.
- Miller, S. (2016, September 7). *Insider Threat Deep Dive on IT Sabotage: Updated Statistics (Part 1 of 2)* [Blog post]. Retrieved May 14, 2022, <http://insights.sei.cmu.edu/blog/insider-threat-deep-dive-on-it-sabotage-updated-statistics-part-1-of-2/>
- Miller, S. (2020, September 29). *Insider Threat Incidents: Assets Targeted by Malicious Insiders* [Blog post]. Retrieved May 14, 2022, <http://insights.sei.cmu.edu/blog/insider-threat-incidents-assets-targeted-by-malicious-insiders/>
- Miller, S., & Pickering, A., (2020, September 10). *Insider Threat Incidents: Most Commonly Affected Devices* [Blog post]. Retrieved May 14, 2022, <http://insights.sei.cmu.edu/blog/insider-threat-incidents-most-commonly-affected-devices/>
- NITTF Insider threat guide*. (2017). Wwww.dni.gov. Retrieved April 8, 2022, from <https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-nittf/ncsc-nittf-resource-library/nittf-produced-guides-templates>

- Nurse, J., Buckley, O., Legg, P., Goldsmith, M., Creese, S., Wright, G., & Whitty, M. (2014). Understanding Insider Threat: A Framework for Characterizing Attacks. *2014 IEEE Security and Privacy Workshops*. <https://doi.org/10.1109/SPW.2014.38>
- Positive Incentives for Reducing Insider Threat*. (2017). Carnegie Mellon University. Retrieved September 11, 2022, from https://www.sei.cmu.edu/our-work/projects/display.cfm?customel_datapageid_4050=6513&customel_datapageid_4050=6513
- Reciprocity (2021), *User Behavior Analysis 101*, <https://reciprocity.com/user-behavior-analysis-101/>
- Salitin, M. A., & Zolait, A. H. (2018). The role of User Entity Behavior Analytics to detect network attacks in real time. *2018 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT)*. <https://doi.org/10.1109/3ict.2018.8855782>
- Seppänen, M. (2021). *Methods for Managed Deployment of User Behavior Analytics to SIEM product*. JAMK. <https://urn.fi/URN:NBN:fi:amk-2021053112935>
- Shashanka, M., Shen, M.-Y., & Wang, J. (2016). User and entity behavior analytics for enterprise security. *2016 IEEE International Conference on Big Data (Big Data)*. <https://doi.org/10.1109/bigdata.2016.7840805>
- Thompson, E. E. (2020). *The insider threat: assessment and mitigation of risks*. Auerbach.
- Tuomi, J., & Sarajärvi, A., (2018). *Laadullinen tutkimus ja sisällönanalyysi*. Tammi.
- Wall, D. S. (2012). Enemies within: Redefining the insider threat in organizational security policy. *Security Journal*, 26(2), 107–124. <https://doi.org/10.1057/sj.2012.1>

Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: the insider threat. *European Journal of Information Systems*, 18(2), 101–105.
<https://doi.org/10.1057/ejis.2009.12>

What is an Insider Threat? Micro Focus. (n.d.). [Www.microfocus.com. https://www.microfocus.com/en-us/what-is/insider-threat](https://www.microfocus.com/en-us/what-is/insider-threat)

What Is an Insider Threat? Proofpoint US. (2021, June 9). Proofpoint.
<https://www.proofpoint.com/us/threat-reference/insider-threat>

What is Data Exfiltration? Proofpoint US. (2021, June 10). Proofpoint.
<https://www.proofpoint.com/us/threat-reference/data-exfiltration>

Which data sources do I need? - Splunk Documentation. Splunk Inc. Retrieved March 23, 2022, from <https://docs.splunk.com/Documentation/UBA/latest/GetDataIn/DataSources>

Whitty, M. T. (2021). *Developing a conceptual model for insider threat.* *Journal of Management and Organization*, 27(5), 911-929. <http://dx.doi.org/10.1017/jmo.2018.57>

Yalcinkaya, Haldun (ed.) (2021), *Good Practices in Counterterrorism*, (Centre of Excellence Defence Against Terrorism)

2020 Cost of Insider Threat Report. Proofpoint UK. (2020, March 3). Proofpoint.
<https://www.proofpoint.com/uk/resources/threat-reports/2020-cost-of-insider-threats>