Master's thesis

Software Engineering and ICT

2021

Tommi Nurmi

NETWORK DETECTION AND REACTION

CASE STUDY: PROOF ON CONCEPT FOR VECTRA IMPLEMATION

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

MASTER'S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Software Engineering and ICT

2021 | 54 pages

Tommi Nurmi

NETWORK DETECTION AND REACTION

CASE STUDY: PROOF OF CONCEPT FOR VECTRA IMPLEMENTATION

Network threats today are very critical issues in every industry where there are digital services. All systems use ICT services. As a result, network attacks target every device connected to the network. This thesis provides an idea of how a network-based monitoring and response system adds value to threat mapping and prevention.

In my thesis work, I also go through how different knowledge security models work as part of a system that makes devices, people, and processes work together. As a result of new observation tools and machine learning, anomalies can be searched in the data to reveal anomalous events that contradict the behavioral pattern.

Visibility is no longer the only thing that can guarantee environmental safety. With the help of machine learning and the development of tool software, it is possible to detect very sophisticated intrusion patterns. However, this requires extensive expertise and familiarity with the possibilities of the tools. Therefore, this requires concentration and dedication. Processes need to be strongly involved when things do go as planned. Risk management must also be part of the process of keeping a company afloat.

In my work, I want to point out why it is good to gather online information also into threat mapping. To get the right picture, the network is the surest source of information that can be used to see patterns of behavior on how an attacker reaches an object.

KEYWORDS:

Network Detection and Reaction, Security Operation Center, Mitre Matrix framework, Threat Hunting, cybersecurity

OPINNÄYTETYÖ (YAMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Ohjelmistotekniikka ja ICT

2021 | 54 sivua

Tommi Nurmi

VERKON HAVAINNOINTI JA REAGOINTI

Tapaustutkimus: Käyttöönotto Vectra työkaluilla

Verkkouhat ovat nykyään erittäin kriittisiä asioita jokaisella saralla, jossa on olemassa digitaallisia palveluita. Kaikki järjestelmät käyttävät ICT-palveluja. Tämän vuoksi verkkohyökkäykset kohdistuvat jokaiseen laitteeseen, jotka ovat yhdistetty verkkoon. Tämä opinnäytetyö antaa kuvan siitä, miten verkkopohjainen seuranta ja reagointijärjestelmä antaa lisäarvoa uhkien kartoittamiseen ja estämiseen.

Opinnäytetyössäni käyn läpi myös miten eri tietoturvamallit toimivat osana järjestelmää, jolla saadaan laitteet, ihmiset ja prosessit toimimaan yhdessä. Uusien havaintotyökalujen ja koneoppimisen johdosta datasta voidaan etsiä poikkeavuuksia, jolla voidaan saada käyttäytymismallin vastaisesti poikkeavia tapahtumia esille.

Näkyvyys ei ole enään ainoa asia, jolla voidaan taata ympäristön turvallisuus. Koneoppimisen avulla ja työkalujen ohjelmistojen kehittyessä on mahdollisuus havaita erittäin hienostuneita tunkeutumistapoja. Tämä vaatii kuitenkin laajaa asiantuntemusta ja perehtymistä työkalujen mahdollisuuksiin. Tämän vuoksi tämä vaatii keskittymistä ja omistautumista asiaan. Prosessit pitää olla vahvasti mukana kun asiat eivät mene suunnitellusti. Myös Riskienhallinta pitää olla osana prosessia, jonka avulla pidetään yrityksen toiminta pystyssä.

Työssäni haluan tuoda esille, että miksi on hyvä kerätä verkkoinformaatiota myös osaksi uhkien kartoittamista. Ison kuvan saamiseksi verkko on varmin information lähde, jolla voidaan nähdä käyttäymismalleista miten hyökkääjä saavuttaa kohteen.

ASIASANAT:

Verkon havainnointi ja reagointi, tietoturvakeskus, Mitre Matrix framework, uhkien kartoitus, kyberturvallisuus

CONTENT

FIGURES

LIST OF ABBREVIATIONS

API	Application Programming interfaces
NDR	Network Detection and Reaction
SIEM	Security Information and Event Management
SOC	Security Operation Center
NBA	Network Behavior Analysis
ISE	Cisco Identity Services Engine
EDR	Endpoint Detection and Response
ZT	Zero Trust
SOAR	Security orchestration, Automation and Response
UEBA	User and Entity Behavior Analytics
IPS	Intrusion Prevention System
IDS	Intrusion Detection System
CMDB	Configuration Management Database
AI	Artificial Intelligence
MFA	Multi Factor Authentication
IT	Information Technology
RPC	Remote Procedure Calls
DNS	Domain Name System
SSH	Secure Shell
SPAN	Switch Port Analyzer
DHCP	Dynamic Host Configuration Protocol
BYOD	Bring Your Own Device
IOT	Internet of Things
NIST	National Institute for Standards and Technology
POV	Prof of Value

1 INTRODUCTION

1.1 Description of the problem and challenges

The subject of this thesis is network anomaly and behavior detection from network traffic. There are several layers of a company network with different security systems. One of the clearest layers is the network where all critical the information exists. The data communication network has all the information you need to get the right information about how the environment works. A data communication network is a collection network of devices, users, and applications that communicate with each other.

At the network level, there are several individual security devices / systems that perform security tasks at various levels. Usually, the systems are not products of the same manufacturer and therefor there are security information and event management (SIEM) systems that can combine data from different products. However, the amount of data is so large that the response is problematic.

There are significant innovations in data science, machine learning and behavioral analysis, that, when combined, make it is possible to automate real-time threat detection and response. Automated threat management detects all phases of an active cyber-attack, including command and control, internal reconnaissance, lateral movement, data exfiltration, and botnet monetization. Automation is the only way threat management can scale the rapid increase and diversity of modern cyber-attacks. It is not humanly possible to analyze massive volumes of alerts and logs to find the breadcrumbs of threats that make their way inside networks. Having automated threat management software working throughout a distributed network is like having a top-shelf security analyst at headquarters and every remote location – except it works around the clock, watches all traffic and never takes a vacation.

Historically, the methods for detecting anomalies are derived from statistics. Changes in traffic volumes have been detected by the systems and have been detected / analyzed according to the system specifications. This model, as a sighting, gives a rough picture of events that do not catch the users and

applications themselves. Attacking techniques have become more diverse, so the ability of the system to see and learn is important.

With machine learning, network traffic analysis has become more diverse. The principle of machine learning is to teach the system to understand what people are doing and machine learning is part of a broader field of artificial intelligence.

Often the problem is that a lot of data is collected from many sources. As a result, a single product cannot provide a complete solution that provides a fully secure and automated security solution. The thesis focuses on one area, which is the analysis of network traffic. Network traffic gives you a view that gives you a true picture of the situation. The problem is that the environment is multileve There are several switching points, and the applications are nowadays in multiple locations. As a result, tracking your network traffic from one place is no longer an effective security solution. This hybrid cloud/datacenter environment is a big challenge around this topic. Clients are now found basically anywhere, and they can have many different devices with different security points and policies.

Many network traffic analytics companies are working to make their product Application Programming Interfaces (API) accessible to everyone, allowing systems to be integrated effectively. Historically this was a rather problematic issue because the systems did not work very well with each other. This led to the launch of SIEM systems, the first security operation center (SOC) tools to track security incidents from various sources. The challenge with SIEM is that you need to create the policy yourself. It requires a lot of human input to follow and analyze data. Also, another issue is that systems produce a lot of false positive alarms. That is a big problem, because then it is not possible to follow the data which you should follow and react to the real security incident.

Another challenge is data itself. The trend now is that businesses collect a lot of data and try to manage that somehow. Data and visibility are key words in this security market area. There are two different product names. There is network detection and reaction (NDR), which we normally see and the other one is network behavior anomaly detection (NBAD). This thesis will concentrate on both, because those three products which I have tested work under both names.

Network traffic analyze is basically a protocol anomaly detection product. It follows how protocol works between client and application and it measures network traffic load from different places on your network. NDR is the continuous monitoring of a network for unusual events or trends. NDR is an integral part of Network Behavior Analysis (NBA), which offers security in addition to that provided by traditional anti-threat applications such as firewalls, intrusion detection systems, antivirus software and spyware-detection software [1].

Also is important to follow common frameworks. Example NIST (National Institute for Standards and Technology) framework is designed to protect organizations from attacks. In NIST framework there are three principles [2]:

- Confidentiality: Information should only be accessible to those who need access to it.
- Integrity: Information should be protected from unauthorized modification, destruction and loss
- Availability: The information should be accessible to authorized person as and when necessary

These kinds of frameworks and tools give the possibility to see and react when a real situation occurs. NIST core functions are identity, protect, detect, respond and recover. Framework also assumes that a breach will happen at some point. Then organizations need well planned process and documentation how to recover after attack [2].

1.2 Security threat landscape overview

The Enisa threat report provide a good visual overview to see and understand the current status in this field as well [3]. Network behavior anomaly area is a good point to gather data and with Artificial intelligence (AI) analyze tools, to create some policies to follow the right areas of your environment.

Figure 1 summarizes the top 15 cyber threats and trends.

Top Threats 2019-2020		Assessed Trends	Change in Ranking
1	Malware	—	—
2	Web-based Attacks	—	↗
3	Phishing	↗	↗
4	Web application attacks	—	↙
5	Spam	↙	↗
6	Denial of service	↙	↙
7	Identity theft	↗	↗
8	Data breaches	—	—
9	Insider threat	↗	—
10	Botnets	↙	↙
11	Physical manipulation, damage, theft and loss	—	↙
12	Information leakage	↗	↙
13	Ransomware	↗	↗
14	Cyberespionage	↙	↗
15	Crytojacking	↙	↙

Legend: Trends: ↙ Declining, — Stable, ↗ Increasing **Ranking**: ↗ Going up, — Same, ↙ Going down

Figure 1. Top cyber threats report from Enisa [3]

There have not been tremendous changes. The most common cyber threat is malware. It is the most often encountered cyberthreat in these reports. Below (figure 2) one can see the type of assets for malware attack

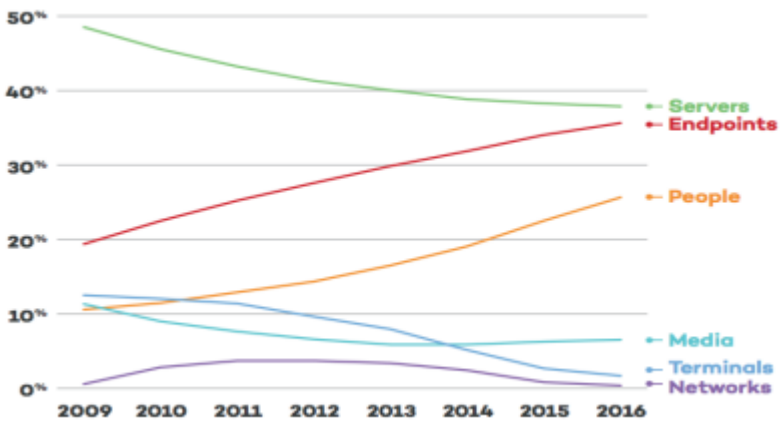

Figure 2. Percentage of threat detection per asset type [3]

The information in the ENISA report provides mitigation measures to take against malware attacks.

Here are some mitigation actions for Malware attacks [3]:

- Update the malware mitigation controls and adapt to new attack methods/vectors regularly (preferably using MITRE's ATT&CK framework109)
- Monitor the logs via a SIEM solution. Indicative log sources should be Anti-Virus alerts, endpoint detection and response (EDR) detections, proxy server logs, Windows Event and Sysmon logs, IDS (Intrusion Detection System) logs
- Relying exclusively on endpoint or server malware detection and mitigation is not sufficient. Malware detection should be implemented for all inbound/outbound channels, including network, web and application systems in all used platforms (i.e. servers, network infrastructure, personal computers and mobile devices).

This brief description says that you need to have EDR, NDR and SOC services in place. In Section 2. I will go through SOC related issues. It is the best place way to monitor and see when you have traffic, logs and user behaviors in one place.

1.3 Description of solution for threat hunting from network

In this thesis I show how a NDR solution provides more data and information from a company network and how integration with different devices work together. The NDR solution is just a passive device. That means that the solution is not able drop or stop attack itself. There is different way to create active integration with different product and for example Vectra NDR product uses Microsoft EDR product to isolate devices in your network [4]. It collects data and uses different methods to analyze how different devices and user behavior look in a real environment. There are different methods to create an active detection system. For example, Cisco identity services engine (Cisco ISE (Identity Services

Engine)) or firewalls can be integrated to this setup. That is one important thing around this topic. Integration to other systems is a key issue. I will cover different integration possibilities with SIEM and different security enforcement points as well. Also, SOC has its own area in my thesis. SOC is an extremely critical piece of large information security field. Without SOC, it is difficult to know what is happening in your environment. Ability for SOC is a very essential part of reduce reaction time.

There are also some common frameworks, for example MITRE framework, which describe how cyberattacks work. In Section 3, I descripe how MITRE enterprise framework [5] works and why we need example NDR solutions to get more data and visibility to see attacks against your environment. The goal is to stop cyber attack before it causes problems for your environment. Another framework example is Zero Trust framework (ZT) [6] which is often used term these days. It is a collection of many security areas, and you can not buy just one product directly. Execution of this framework combines advanced technologies such as multi factor authentication (MFA), identity and access management (IAM), identity management and next-generation endpoint security technology to verify the user's identity and support system security. Zero Trust extended also requires consideration of encryption of data, securing email, and verifying the hygiene of assets and endpoints before they connect to applications [7].

1.4 Why NDR is a required component for Zero Trust framework

Adopting a Zero Trust (ZT) security paradigm, one that focuses on protecting resources (assets, services, workflows, accounts) and not network segments, has become a more popular approach.

ZT relies heavily on continuous and accurate monitoring of the interactions between these resources on the network to evaluate and control access based on their behaviors. In fact, as noted in the NIST report, "An enterprise implementing a ZT should establish a continuous diagnostics and mitigation (CDM) or similar system."

With a Continue Diagnostic and Mitigation (CDM), or network detection and response (NDR), security analysts can answer questions like:

- What devices, applications and services are connected to the network and being used by the network?
- What users and accounts, including service accounts, are accessing the network?
- What traffic patterns and messages are exchanged over the network?

The ability to address these questions underlines the importance of organizations to have visibility into all actors and components on their network so they can monitor and detect threats.

Traditional detection models attempt to find exploit code, a known sample of malware or malicious code. That is why NDR brings values of detection and reactions. For example, every attack must establish some form of hidden communications. Attackers want some internal resources and lateral movements are not easy to find If you just use EDR or some other basic security tools such as firewalls.

Sophisticated cyber attackers constantly invent and reinvent more effective ways to mount their assaults. Their evasive behaviors and the invisible footprints they leave behind change with unsteady frequency. Traditional legacy security designed to keep out attackers are blind to these changing threat behaviors, giving cybercriminals free rein to spy, spread and steal. What is needed is a reliable way to detect hidden attackers who get inside and respond instantly to stop in-progress threats from becoming a data breach. One that proactively hunts for evasive threats, augments your existing security investments, keeps up with the changing threat landscape, and offers exceptional scale across cloud, data center, IT and IoT networks.

Figure 3 shows current ways to compare signatures and data science methods. Data science is how NDR is working nowadays.

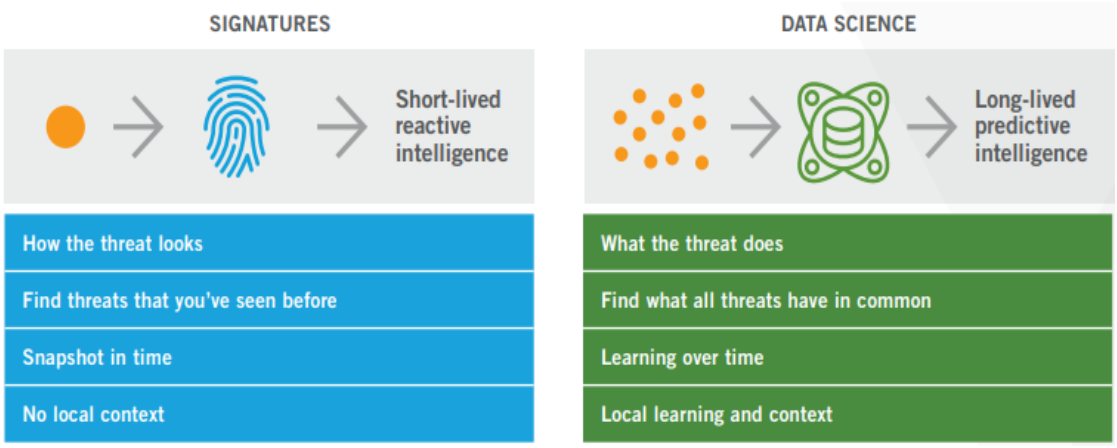

Figure 3. Signature and data science threat hunting method

In section 3 I will explain how difficult it is to find the right attack path using MITRE frameworks. Machine learning with the understanding of what, when and how is key issue to detect threats. This is a critically major difference when using data science.

2 SOC WITH NDR SOLUTION

A Security Operations Center (SOC) is a collection of people, technologies and processes where cybersecurity professionals are responsible for monitoring, analyzing and protecting a business from cyber-attacks. A SOC is a centralized function within an organization that employs people, processes and technology to continuously monitoring different systems. There are many ways to do and build SOC services and that is one challenge to bring some values of business to build right level of SOC.

History shows that there have been SOC services used by some electric and gas utility companies. They use example monitors different activities from their CCTV monitors[8]. Normally there was one person per shift, but this kind of setup is not true for SOC. Today there are multiple people, technologies, automation and process behind a SOC.

There are many ways to utilize SOC in your business. The basic idea is just protecting your data, business continuity and understanding your risks and threats. A SOC team is one tool for your business. That protects your data and assets in your environment.

Normally SOC is an outsourced service that is completely focused on following company security incidents. There are many levels and areas that SOC can be implemented. The first thing is to decide what type of support you need from the SOC team. Also, it is important to define that the SOC does not focus on physical security, because that is normally a different service for the company. Of course, that could be also added to SOC monitoring, but then you need to define that in your monitoring system as well. SOC acts like a hub or central place gathering logs and information from different assets, such as your network, devices, appliances and information stores. Essentially, the SOC is the correlation point for every event logged within the organization that is being monitored. For each of these events, the SOC must decide how they will be managed and how to react [8].

The key importance area of a SOC is to have a clear understanding of what would have the most negative impact on the business, such as downtime of a critical system. This is one key issue for proper SOC service. There are a lot of different cases which require you to prioritize time, attention and effort. Also, SOC should be integrated into your IT (Information Technology) and business process. That means the SOC organization model should cover people from different areas like risk management sectors which have a good understanding of risks from a business perspective. SOC is gathering a lot of data from various sources, so it is important that you have the right context of data. You need to ignore alerts, chase false positives and try not to make any mistakes during analyst work. This kind of work is like a circle. Continually, you must check your data context over again, because your SOC services must be top of data all the time.

Figure 4 shows a Lifecycle for SOC services. There are separate phases which walk through the reasons and needs why a company needs SOC services. Normally you see just technology components, but most of actions are to collaborate between people and process. Technology and tools are important issues, but when you need to take care of business risk management as well. You need to have proper plans on how to mitigate risks as well and how to manage business continuity [9].

Figure 4. Lifecycle for SOC service [9]

IT, business units, security systems, as well as apps and devices are in use throughout the organization and synthesizes it to produce a higher set of false positive alerts. A SIEM facilitates the detection, management, investigation, search, containment, and remediation of threats and other high-security issues. In some instances, these alerts will need to be reviewed by humans, and in other

instances they can be handled by the technology solution, but overall, organizations can expect to see a rapid increase in their ability to detect and respond to security threats.

Monitor at the speed of business – in real time. Business is running at warp speed and your security operations need to keep pace. Integrating advanced analytics into the equation enables your SIEM to deliver your SOC and SecOps team a powerful assist, starting with managing and accessing network traffic and intrusion data [10]. A SIEM provides endpoint protection, delivers threat intel and malware authentication, processes wire data, and analyzes assets and identities. As part of a SOC, analytics driven SIEM can monitor all security activity, correlate and sequence events, confirm alerts and then prioritize, review, and investigate security instances, and can even decide the best path to resolution.

Threat detection is only one part of the results. Organizations also need smart incident response. For enterprises, the pairing of SIEM and security orchestration, automation and response (SOAR) is the true formula for success. Together, they allow teams to gain deeper insights and shorten incident response times. Security teams can automate tasks and workflows — the entire SOC flows more efficiently [10].

The success of any SOC is dependent on an enterprise’s ability to carefully bring together security technologies, tools and talent with the devices, processes and applications it must protect. There are many choices when it comes to the framework or platform on which a SOC can be designed, as well as the how the SOC will be used or managed. It is recommended that an organization should become “the boss of” their SOC. Everything you do, and every decision you make should be with a view toward an end situation where your SOC will work smarter, not harder. Achieving this requires a proactive, not a reactive, SOC model. You’ll want it to be plug-in ready and have critical automation and machine learning tools, along with robust analytics. A single suite SOC that integrates third-party solutions, minimizes user uncertainties, support calls, and work interference is crucial.

2.1 SOC factors

SOC includes three factors' people, process and technology (figure 5). Normally in cybersecurity world there is lot of discussion under technology part, but People and process are important pieces in this puzzle also [11]. Automation and data are a key element also for prober SOC-services. SOAR is nowadays the name for this kind of service. Security Orchestration, Automation and Response Platform (SOAR) is a new element for SOC services. That gives a much faster way to do incident response from different data sources. You can easily automate repetitive, manual, time consuming tasks, enrich the data, investigate, detect, prioritize and respond. It is easy to automate workflows with bots and playbooks. These automations shorten response times to human centric decision needed cases. API first approach provides hundreds of pre-defined and two-way integrations. Vendor-free integration capability is empowered with free plugin services. SOAR is an independent platform so there is no limit or barriers to integrate any security tools that you use in your SOC operations [11].

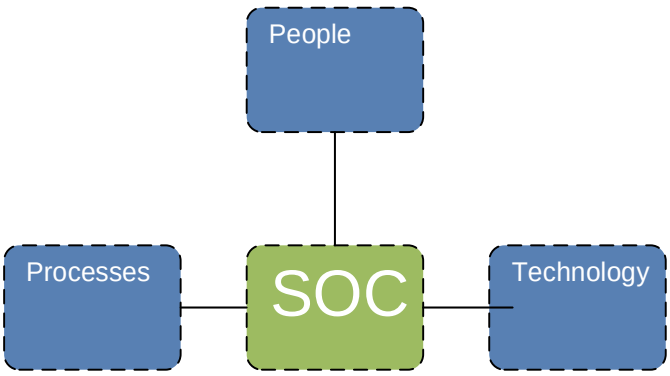

Figure 5. SOC factors

2.1.1 People

The SOC staff have a challenging job with several designated roles to be fulfilled. The roles and duties of the SOC staff can be summarized as follows. Figure 6 shows elements for Tier model

- **Tier 1 Security Analyst** – Continuous monitoring of systems and alerts in place, from all sensors and endpoints.

- **Tier2 Security Specialist** – In-depth analysis of incidents based on correlated data, impact analysis, and remediation recommendations.
- **Tier 3 Subject Matter Expert** – In-depth knowledge of network events with forensics and malware reverse engineering skills. Actively involved in threat detection analytics.
- **SOC Manager/Director** – Responsible for the technology strategy to meet Service-Level Agreements (SLAs), with a deep understanding of incidents. Acts as the organizational coordinator for business-critical incidents while providing input to the overall security strategy.

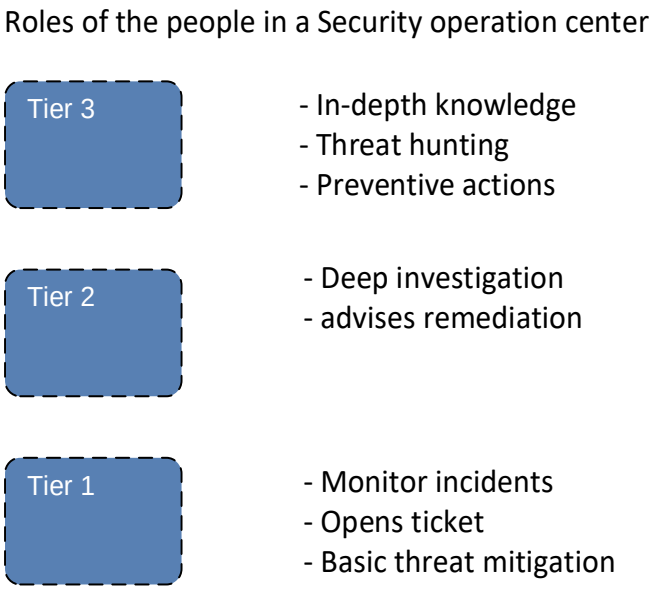

Figure 6. SOC Tier analyst model

SOC analyst duty is to ensure that the organization's digital assets are secure and protected from unauthorized access. That means that you are responsible for protecting both online and on-premises infrastructures, monitoring data to identify suspicious activity and identifying and mitigating risks before there is a breach. If a breach does occur, an SOC analyst will be on the front line, working to counter the attack.

2.1.2 Processes

The processes and procedures in place in a SOC are figured out by its scope. More specifically, because of the number of services offered, the number of customers being supported, and the different technologies being used. According to McAfee, the following is a list of the basic procedures needed for supporting a SOC:

- Monitoring Procedure
- Notification Procedure
- Escalation Process
- Transition of Daily SOC Services
- Shift Logging Procedures
- Incident Logging Procedures
- Compliance Monitoring Procedure
- Report Development Procedure
- Dashboard Creation Procedure
- Incident Investigation Procedure

However, this is only an example and a small sample of the procedures that may be needed. The above list is subject to customizations based on the types of technologies in use.

In figure 7 it shows how security incident process workflow should go. It is always important to use lesson learned phase because that gives effective way to create better security and learn those incidents which do not end well.

Figure 7. Security incident process workflow [6]

2.1.3 Technology

Data collection, correlation, monitoring and real-time analysis are the core technologies of a successful SOC. The data collection is performed across several varied systems including logs from various sources. Figure 7 shows how SOC services use different sources to get the right data from different places.

Data collection and correlation should not only be able to go back and trace an incident but also enable real-time response. Thus, visibility and response are tied to the correlation of network events originating from network traffic, system logs, endpoint data, threat intelligence feeds, and security events.

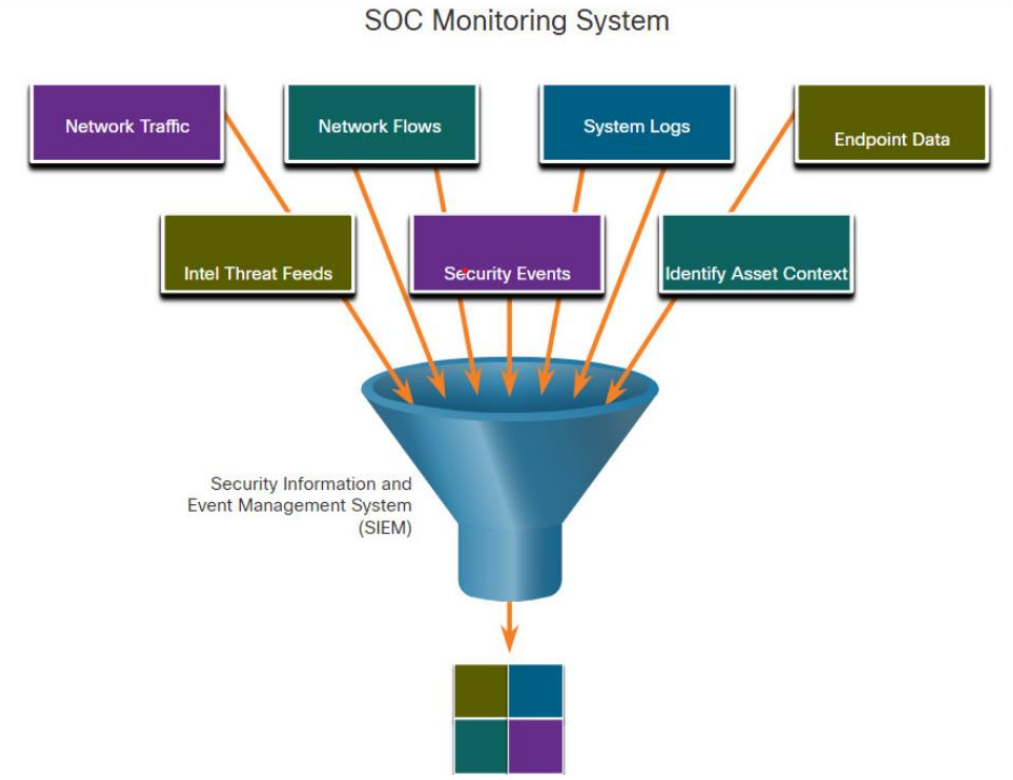

Figure 7. SOC Monitoring System [12]

SIEM and security orchestration, automation and response (SOAR) are often paired together as they have capabilities that complement each other.

SOAR platforms are like SIEMs (Security and Information Event Management) (Security Information and Event Management) in that they aggregate, correlate, and analyze alerts. However, SOAR technology goes a step further by integrating

threat intelligence and automating incident investigation and response workflows based on playbooks developed by the security team [12].

SIEM systems necessarily produce more alerts than most SecOps teams can realistically investigate in order to conservatively capture as many potential exploits as possible. SOAR will process many of these alerts automatically and will enable security personnel to focus on more complex and potentially damaging exploits.

2.2 SOC operations and Tier model

The function of a security operations team and Security Operation Center is to monitor 24/7 cyberthreats. SOC team has responsibility for monitoring and protecting business assets. Typically, SOC is built like hub and spoke architecture. Where security information and event management (SIEM) systems collect and correlates data from your security feeds. Spokes of this model can incorporate a variety of systems, such as vulnerability assessment solutions, governance, risk and compliance (GRC) systems, application and database scanners, intrusion prevention systems (IPS), user and entity behavior analytics (UEBA), Endpoint-based detection and response (EDR), Network detection and response (NDR) [12].

In this thesis I focus on network-based detection and reaction system, but this product has many added integration opportunities. The SOC specialist can choose the toolset they need. In Chapter 5 there is a practical example of how the SOC specialist can use different tools to analyze different sources. Also, in the same chapter there is information on how Vectra products integrate into other security tools as well. Normally SOC specialists use many tools, but integration gives more flexibility to identify incidents faster. There are also other issues to do before you add any technologies to your SOC system. Quite often it is easy to just focus on the technology part, but first you need to focus to do framing assessments. Framing assessments are one key component. When you start SOC-services. You should receive general indications of where your security gaps are. You should get a specific heat map from your assets in your

environment which allows you to se a baseline. Then you can really focus on the right areas for your security environment.

2.3 SOC visibility triad

As showed by unprecedented cybercrime, traditional security defenses have lost their effectiveness. Threats are stealthy, acting over long periods of time, secreted within encrypted traffic or hidden in tunnels. With increasingly sophisticated threats, security teams need quick threat visibility across their environments [13].

In the Gartner research report “Applying Network-Centric Approaches for Threat Detection and Response” authors introduced the concept of the SOC Visibility Triad [13]. In this article, they state: “The escalating sophistication of threats requires organizations to use multiple sources of data for threat detection and response.

“Network-based technologies enable technical professionals to obtain quick threat visibility across an entire environment without using agents”[13].

Here is Gartner view on around SOC visibility area (figure 8). NDR together with SIEM and EDR delivers several dimensions needed in a modern-day SOC.

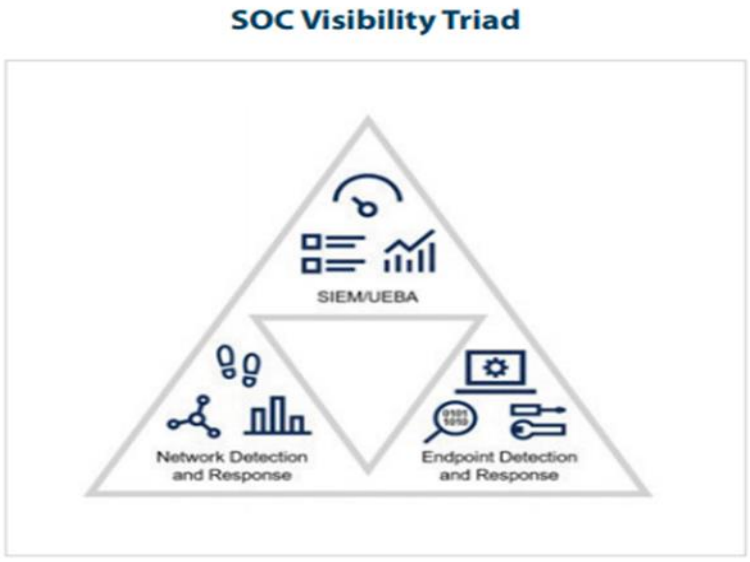

Figure 8. SOC Visibility Triad [13]

Parts of SOC visibility Triad:

- SIEM (Security information and event management)
  Normally when a company starts with SOC it is SIEM system. In my thesis, I use Splunk for. SIEM collecting data from host, machines, devices, users, accounts and credentials.
- EDR (Endpoint-based detection and response)
  EDR is an endpoint-based detection and response agent. EDR can detect and alert if the host is compromised in any way.

- NDR (Network-based detection and response)
  Network-based threat detection and response is a platform that uses network data for visibility, detection and, most importantly, context. Security products in this platform leverage network data to detect threats based on:
  - Artificial Intelligence (AI): detects anomalies across thousands of hosts and devices on the network.
  - Analysis of Network Packet Data: analyzes actual files downloaded on a device or a file sent as an email attachment identifying malicious files such as malware, ransomware and more.
  - Attacks from an External Network (Internet): discovers compromises such as phishing attacks to stop the download of malicious files on machines, especially those communicating on the network with Command-and-Control servers.

Traditionally, Security Operations Centers relied heavily on endpoint detection and response (EDR) and security information and event management (SIEM) tools for incident management and response. But those tools could not provide real-time visibility into east-west, or internal, traffic that's essential for protecting the enterprise.

NDR solutions are the missing piece of the triad. When true NDR became technologically possible, the triad became the go-to structure for providing visibility across complex IT environments [13].

This combination uses SIEM, EDR and NDR are empowered to answer a broader range of questions when responding to an incident or hunting for threats. For example:

- Whether one feature may behave strangely after the other is functioning normally
- What service and protocol were used?
- What other assets or accounts may be affected?
- Has any other property accessed the same external command and control IP address?
- Has your account been accessed in an unexpected way by another device?

2.4 SOC Triad with Network-based Detection and Response

According to Gartner: “Your SOC triad seeks to significantly reduce the chance that attackers will operate on your network long enough to accomplish their goals” [13]. Logs, endpoint data and network data provide full visibility of the environment and reduce each other’s weaknesses. Using them together severely reduces the chance that an attacker can evade you for extended periods of time [13].

Vectra network detection and response network metadata is the most authoritative source for finding threats. Only traffic on the wire reveals hidden threats with complete fidelity and independence. Low-resolution sources, such as analyzing logs, only show you what you have seen, not the fundamental threat behaviors that attackers simply can not avoid as they spy, spread and steal. An

NDR solution collects and stores key network metadata and augments it with machine learning and advanced analytics to detect suspicious activities on enterprise networks. NDR builds models that reflect normal behavior and enriches the models with both real-time and historical metadata. NDR supplies an aerial view of the interactions between all devices on the network. In-progress attacks are detected, prioritized and correlated to compromised host devices. NDR supplies a 360-degree, enterprise-wide view—from public cloud and personal data center workloads to user and internet-of-things devices [13].

3 ANALYZE OF CYBERATTACK WITH MITRE MATRIX ENTERPRISE FRAMEWORK

MITRE ATT&CK stands for MITRE Adversarial Tactics, Techniques and Common Knowledge. It is a curated knowledge base of adversarial behavior based on real-world observation of APT campaigns.

The original idea for the project was to answer the question, “How are we doing at detecting documented adversary behavior?” MITRE ATT&CK v1 was released in 2015 [14], and since then, it has seen rapid growth and adoption across multiple domains such as risk management, threat intelligence, incident response and threat hunting, secure configurations and security engineering, among others.

The main components of ATT&CK, adversarial behaviors, are structured as a taxonomy of tactics, techniques, and sub-techniques with other components such as software, APT groups and mitigations standing in various relations between each other and the behaviors. Techniques and sub-techniques are abstracted from actual procedures used by adversaries, while tactics represent a classification of adversary goals like a kill chain but nonlinear. These provide a common vocabulary to categorize specific attacking or defending behavior [14].

Basic idea for this framework is that offense is the best driver for defense. Defending an enterprise network against an advanced persistent threat (APT) stays a progressively difficult challenge that requires, among other things, advanced technologies and approaches to prevent enemy goals. In current enterprise networks, it is unlikely that organizations have the talent or the resources to detect and defend against every method an enemy might use to gain access to their networks and systems.

Help with that challenge. MITRE’s approach was that public information on cyber intrusions suggests that enemies tend to show consistent patterns of behavior while interacting with endpoint or victim systems. The goal of MITRE’s research was to show that automated measuring of endpoint data or telemetry could be used to detect post-compromise operations in a useful way that distinguished

such behavior from the typical noise generated through normal system use. The results of this research showed that using analytics based on a combination of host and network behaviors supplies a useful way to detect post-compromise adversary behavior. This idea is to collect data from EDR and NDR system to get better visibility and more rich data for detection phase.

MITRE framework one key issue is to find security gaps from the company's environment. If you just follow the framework itself and try to see what's reality. That's not giving truthful information from your security things. There is a need to clarify with your personals what you have in your environment. Figure 9 presents what is needed to identify things from different areas. Real heatmap from your services needs a lot of analyzing and interviews from different people and vendors. Output should cover heatmap, prioritization plan and recommendations for company. Also, the idea is to produce SOC capabilities for companies. This framework gives tools, process and methodology for SOC services.

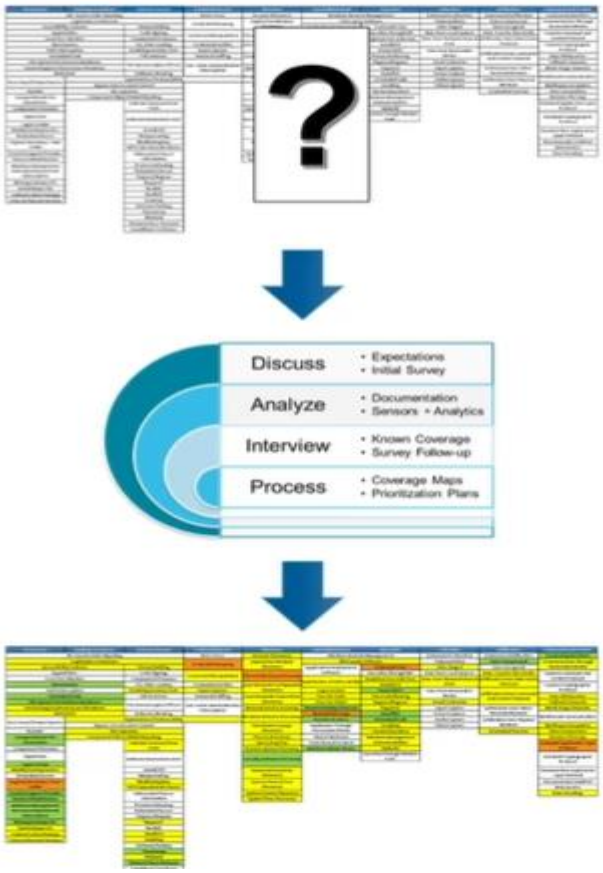

Figure 9. MITRE framework with heatmap results [15]

This kind of information is important to see in reality for your environment. But you also need tools to provide visibility to all pieces in your puzzle. There are some products that give visibility to using this framework, example MITRE ATT&CK® Threat Heatmap - Huntsman [15] tool can show Live dashboard that changes color progressively, shows changes in tactics such as lateral movement and privilege escalation as they occur.

3.1 Threat-based security approach.

MITRE's threat-based approach to network compromise detection uses a behavioral method and is followed by five principles that MITRE framework is produced [14]. These principles describe critical ideas of an effective threat-based approach to network security. They are summarized here in (Figure 10).

Figure 10. Threat base approach to network security [14]

- Include post-compromise detection

  In a real network environment, you need to have the possibility to minimize damage. Because there are always ways to penetrate even the most well-defended network perimeter. Any effective network security should consider post compromise adversary behavior in order to minimize damage caused by an attacker. Who able to successfully penetrator your network defense [14]

- Focus on Behavior.

  In modern defenses, they normally focus on signatures and basic indicators. That is normally known as malicious software or activity. Nowadays it is easy to bypass modifying malware or change some other indicators. An intrusion detection program incorporating behavioral detection analytics is more resilient to attempts by adversaries to avoid signature-based detection through indicator modification. Behavioral detection approaches help identify the common behaviors that are highly likely to be performed across many adversary groups during an intrusion and are independent of specific changes to indicators that adversaries

make. This is the premise that drove the development of ATT&CK-based analytics [14].

- Use a threat-based model

  It is important to have processes. When you try to do prober security defense things in your environment. Threat-Base Model give a possibility to follow security process in a best way [14].

- Iterate by design

  An iterative process is critical to creating an effective behavioral analytics and detection system aligned with the ATT&CK model. Another benefit of iteration is the ability for network defenses to adapt to a changing threat landscape [14].

- Develop/test in a realistic environment

  This is especially a major area, because to get a reality picture of your situation. Need to do and create ongoing test activities. Normally that means. That company orders testing from external parties. They great red team activities and same time try to see what happen during a test attack [14].

The Enterprise ATT&CK framework consists of 12 tactics areas. Under every tactic area are techniques and procedures (TTP). That means that every attack is collected from different tactics and techniques. Listed below are the 12 tactics areas. In Figure 11 introduced how this playbook work like real cyberattack situation [14].

- Initial access: The adversary is trying to get into your network.
- Execution: The adversary is trying to run malicious code.
- Persistence: The adversary is trying to maintain their foothold.
- Privilege escalation: The adversary is trying to gain higher-level permission.
- Defense evasion: The adversary is trying to avoid being detected
- Credential access: The adversary is trying to steal account names and passwords.
- Discovery: The adversary is trying to figure out your environment.

- Lateral movement: The adversary is trying to move through your environment.
- Collection: The adversary is trying to gather data of interest to their goal.
- Command and control: The adversary is trying to communicate with compromised systems to control them.
- Exfiltration: The adversary is trying to steal data.
- Impact: The adversary is trying to manipulate, interrupt, or destroy your systems and data.

Figure 11 shows how MITRE framework collects data to matrix table which produce real attacks scenarios for this matrix table. They are collected to playbook that is easy to follow how different cyberattacks work in a real environment. In other words this database is just behavior profiles how attacks works at different phases in real cases.

Enterprise Matrix

Below are the tactics and technique representing the MITRE ATT&CK® Matrix for Enterprise. The Matrix contains information for the following platforms: Windows, macOS, Linux, AWS, GCP, Azure, Azure AD, Office 365, SaaS.

Last Modified: 2019-10-09 18:48:31.906000

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Application Access Token	Bash History	Application Window Discovery	Application Access Token	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Application Deployment Software	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact

Figure 11. MITRE Enterprise framework [14]

Basic example for remote execution via scheduled tasks using schtasks.exe. This example shows how a contextual way of viewing indicators provides the best way to gather effective information about the use of adversary techniques and how to relate them to other data points to form useful analytics [14].

Requirements for attacker:

1. Credentials or existing domain permissions providing SMB (Server Message Block – the Windows file sharing mechanism) access to the remote system.

2. Ability to move a file to the remote system for execution by the scheduled task.

3. Permission to run schtasks.exe on the local system. Any user can run schtasks.exe by default.

4. Administrative access to the remote system to schedule the task over Remote Procedure Calls (RPCs).

Cause:

1. Invocation of schtasks.exe at a command-line interface with arguments to execute a file on a remote system.

Effects:

1. The schtasks.exe process starts on the local system.

2. An RPC (Remote Procedure Calls) connection is established from the local system to the destination system.

3. An entry for the task is made under the remote system's "%SystemRoot%\Tasks\"

directory.

4. The file on the remote system is executed at a specified time as a child process of

taskeng.exe.

5. Subsequent system changes are caused by execution of the binary or script. For example,

if the program is a remote access tool, the resulting process may attempt to open a

network connection.

3.2 Threat hunting with MITRE's ATT&CK framework

Threat hunting is not just that you have good defense tools or services from SOC. You should also know how an attacker works and what the behavior looks like in a real situation. NDR system is one way to see that kind behavior. Figure 12 shows how that works with the MITRE Framework. This example is from Vectra Cognito platform [16].

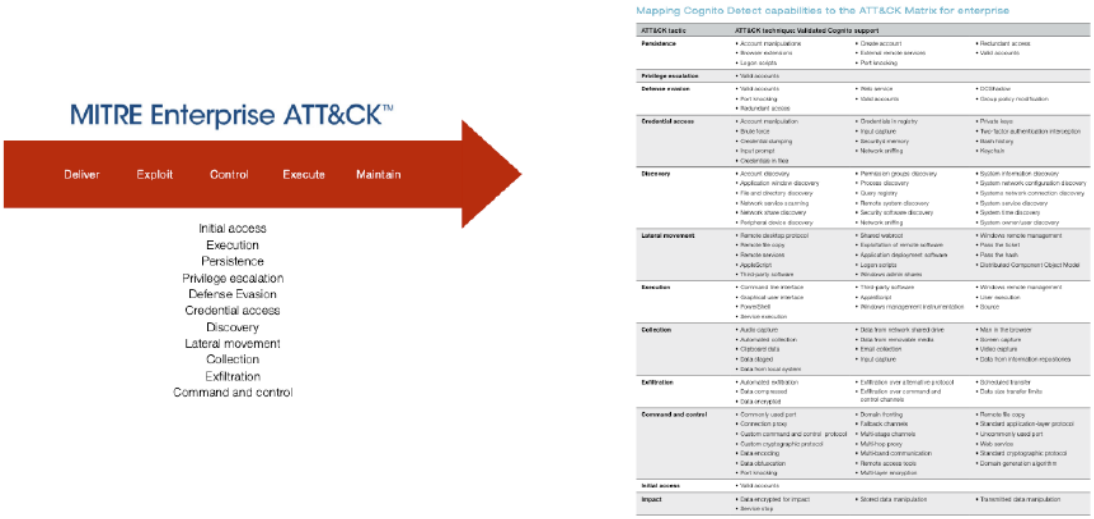

Figure 12. Vectra and MITRE Framework [16]

NDR with behavior analyzis is a key value. When you have the possibility to understand how an attacker works with different phases. Figure 13 shows one example. There are five different attack methods or categories. In section 4 there is more information about this topic with practical examples. How attack uses different phases and how example of Vectra can see this in dashboard view.

- Command and control:
  A command-and-control [C&C] server is a computer controlled by an attacker or cybercriminal which is used to send commands to systems compromised by malware and receive stolen data from a target network [16].

- Reconnaissance:

  Active reconnaissance is a computer attack where hackers communicate with a target system to collect information. The process involves probing a network for weaknesses, such as open ports or other possible entry points that include vulnerable routers [16].

- Lateral movement:

  Lateral movement refers to the techniques that a cyberattacked use, after gaining initial access, to move deeper into a network in search of sensitive data and other high-value assets. After entering the network, the attacker maintains ongoing access by moving through the compromised environment and obtaining increased privileges using various tools [16].

- Exfiltration:

  A common data exfiltration definition is the theft or unauthorized removal or movement of any data from a device. Data exfiltration typically involves a cyber-criminal stealing data from personal or corporate devices, such as computers and mobile phones, through various cyberattack methods [16].

- Botnet activity:

  A botnet [short for bot network] is a network of hijacked computers and devices infected with bot malware and remotely controlled by a hacker. The bot network is used to send spam and launch Distributed Denial of Service [DDoS] attacks and may be rented out to other cybercriminals. Botnets can also exist without a command and control (C&C) server by using peer-to-peer [P2P] architecture and other management channels to transfer commands from one bot to another [16].

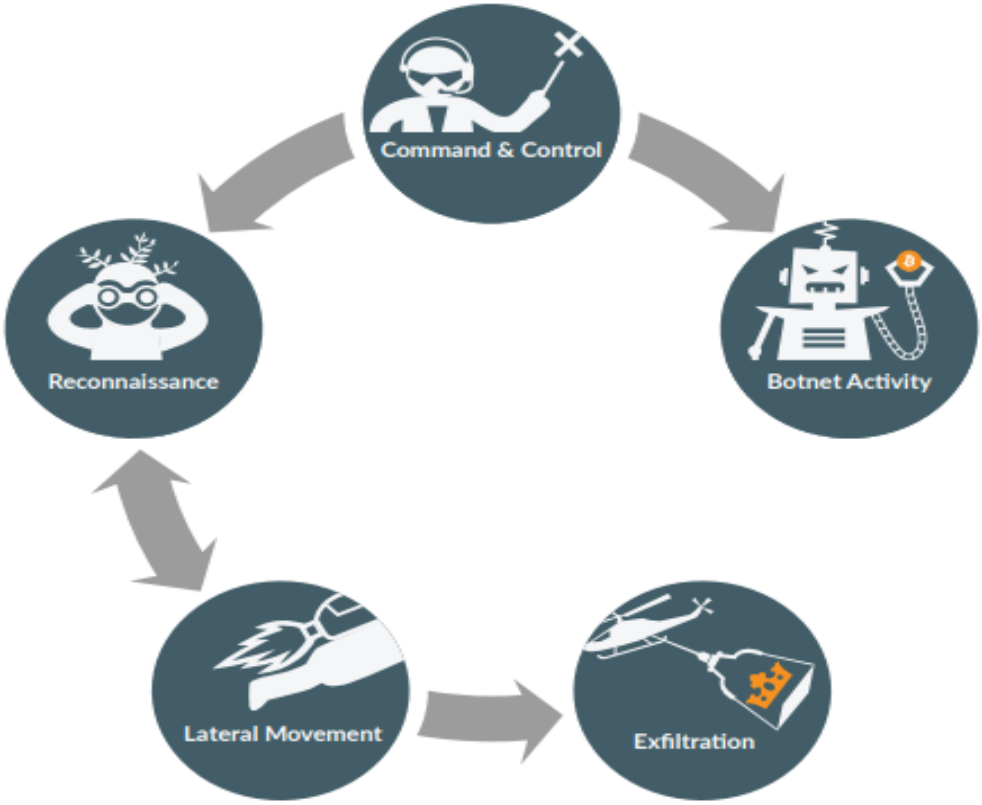

Figure 13. Attack phases in Vectra tool [17]

After an initial exploit, the malware will contact its Command & Control server from which it will be remotely controlled in an automated fashion or by a human. The attack usually progresses (figure 13) along the opportunistic path – the malware joins the host to a botnet and the bot herder steals information from the infected host and makes use of your resources to make money by attacking other systems across the Internet (Botnet Activity). The attack may also have you as its intended target, something that is rarer, but also more threatening – in this case, the infected host will orient itself in your network (Reconnaissance), spread laterally to get closer to your crown jewels (Lateral Movement) and steal your data and send it to an outside system (Exfiltration).

4 PROOF OF CONCEPT VIA VECTRA SOLUTIONS

4.1 Definition of solution criteria

When I start to find different solutions under network behavior analyze tools and systems it is important to identify what solution needs to be done and what is the value obtained? Scenarious and parametres for the proof-of-concept (POC) are defined below:

List for soluion definition:

- Performance and scalability
    - ability to monitor traffic at least 10Gbps ingress/egress points
    - ability to work under SPAN [26] interfaces
- VMWare integration
    - ability to capture all traffic the VMWare vSwitch
- Detection and analysis automation
    - Solution should automatically identify and classify all threats, including attack phase and risk, without requiring any manual intervention
    - Solution should aggregate and prioritize threats over time by physical host, even across IP and user identity changes
    - Solution should differentiate key assets from other hosts for risk prioritization
    - Solution should prose a mechanism to automatically show the confidence of detection when threats are detected based on anomalies
    - Solution should have the ability to automatically differentiate between general botnet behaviors and those that are more likely to be targeted threats
- Prioritization and investigation of threats
    - Solution should automatically score and prioritize each individual attacker behavior detected

  - Solution should have the ability to notify staff based on the threat score
  - Solution should provide visibility into host interconnectivity
  - Solution should provide packet captures of identified attacker behaviors for analysis

- Detection method
  - Solution should directly identify threats based on packet-level analysis of network traffic
  - Solution should have the ability to detect network-based threats within encrypted traffic
  - Solution should detect custom or unknown threats, where there is no signature or IP/domain reputation history
  - Solution should be applicable across all user and infrastructure devices (Windows, Mac, mobile devices, byod, IoT, routers, firewalls)
  - Solution should use multiple behavior techniques (Supervised Learning, Unsupervised Learning, Heuristics, Deep Learning)
  - Solution must have the ability to analyze all traffic: North, South, East, West traffic
- Global modeling of threats
  - Solution should incorporate learnings from global attacker behaviors and techniques to detect threats on the local network whenever possible
  - Global modeling of threats should be combined with local network learning to improve accuracy and relevance for the local network
- Local modeling of threats
  - Solution should detect potentially malicious anomalies based on deviation from learned on the local norms within the network
  - Solution should continually learn as the network and usage evolves

    - Solution should have the ability to detect threats within new devices or devices that were already compromised when baselined
- Analysis
    - Solution should maintain network packet captures of detected attacker behaviors
    - Solution must not decrypt the traffic in order to analyze
- Types of threats detected
    - Remote access tunnels used by attackers to control compromised systems
    - Hidden tunnels over HTTP, HTTPS, or DNS (Domain Name System) to communicate with C&C or to exfiltrate data
    - Web-based Command and Control (not relying on IP reputation or threat lists)
    - Malware using a fake browser
    - Malware being updated
    - Malware getting new instructions
    - Malware replicating a payload to / exploiting vulnerabilities against other hosts
    - TOR Anonymization
    - Peer-to-peer traffic
    - Botnet monetization behaviors: Click Fraud, Bitcoin Mining, outbound DoS, outbound SPAM
    - Ransomware activity: encrypting file shares
    - Network reconnaissance scans: port scans, port sweeps, scanning unused IP’s
    - Use of a stolen credential from a host it has not previously been used on
    - Use of a stolen credential from its normal system, but asking for unusual services or in excessive volume
    - A host trying many credentials to attempt to gain access to a server
    - Kerberos service scans
    - Fake Kerberos servers

  - Brute force attacks
  - Use of administrative protocols, including RDP, SSH (Secure Shell), and IPMI, where the target host is not typically administered by the source host on that protocol
  - Activation of a sub-OS rootkit using an ""knocking"" byte sequence on a common port
  - A host exfiltrating data to an unusual destination
  - A host gathering unusual volumes of data and then sending exfiltrating to an external IP
  - A host being used as a relay to exfiltrate data to an external system
- Integrations
  - Solution must provide API-driven access to all events, hosts, and scoring information for integration with other security solutions & operational systems
- Operations
  - The solution must have the ability to automatically update. To reduce the operational burden of the solution, software updates must be an automated process that does not require any human intervention.
  - Hybrid management model

4.2 Deployment of preparation

In this thesis I use one company real production environment. Main idea is to collect data from as many places as possible. The Vectra appliance automatically serves threatens in real time, for example connecting to port on the core network switch configured as switch port analyzer (SPAN) [18]. In our installation we use core switch deployment with s-series model. Figure 1 shows POV network deployment. One device is installed to the office network and other is installed to datacenter environment.

Here are principals for gathering data to Vectra system.

- User connect to internet: Purpose is to detect C&C connections, botnet monetization, click fraud and data exfiltration
- User connection to user: Purpose is to detect reconnaissance, lateral movement, data acquisition and data exfiltration
- User connection to datacenter: Purpose is to detect reconnaissance, data acquisition and data exfiltration
- User connection to authentication servers: Purpose is to detect brute force login attempt, lateral movements and used for host identification.
- DHCP (Dynamic Host Configuration Protocol): Purpose to identify hosts.

4.3 Network deployment for POC

Network placement of the Vectra is critical to ensure it detects different segments and traffic flows. It is important to understand how your client and servers traffic goes. Normally systems follow client behavior but also server to server traffic gives valuable information for anomaly behavior systems.

Here is a list for network deployment and installation for POC (figure 14)

- Office sensor
    - Vectra s2 sensor
    - gather data from network and send it to the data lake (Vectra x29)
    - client to internet traffic
- Datacenter sensor and data lake database and configuration management setting
    - Vectra x29 model
    - gathering data from datacenter
    - client to datacenter
    - server to server
- Cognito stream server

- send data to SIEM system (Splunk)
- Cognito Stream is deployed as a virtual machine (VM). Metadata flows from the Cognito Brain to Stream, which normalizes it to the Bro/Zeek format and sends the metadata to the SIEM (Splunk)

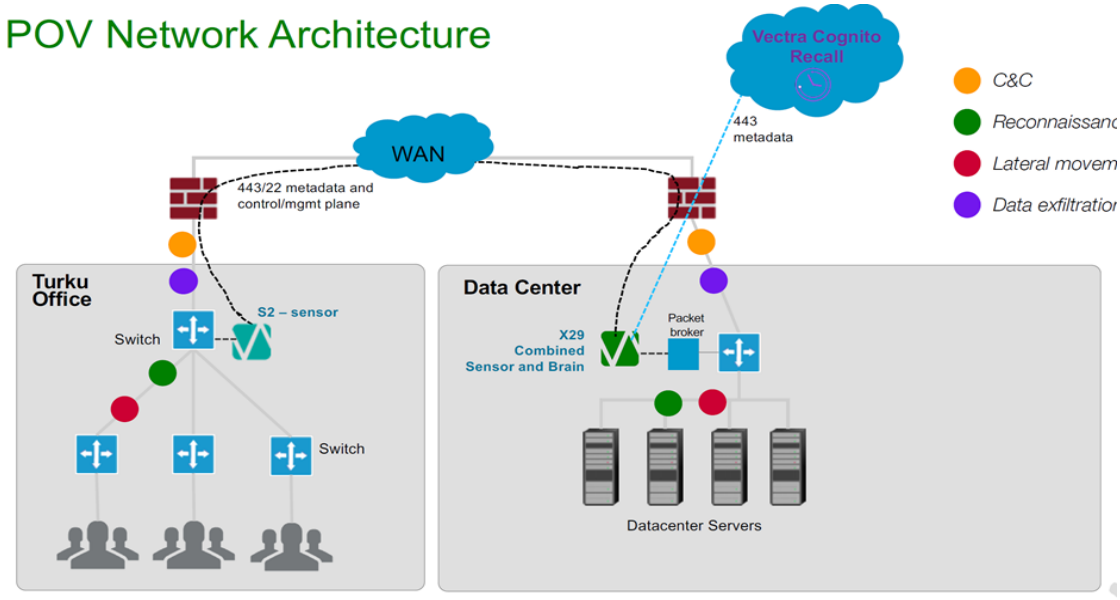

Figure 14. Network deployment for POV

Figure 14 shows principals how this kind solution needs to be done. There are two different phases:

- Onboarding activities
- Ongoing activities

It is extremely critical to cover example how network flow is working at customer network. Nowadays users can use many different devices, but still have the same credentials with different places from network level. Also, there are many other issues that you need to take care with your deployment installation. Process and continues training are the key issue that you can develop and to see real benefit in your product. Figure 15 shows how to implement Vectra deployment for customers [19].

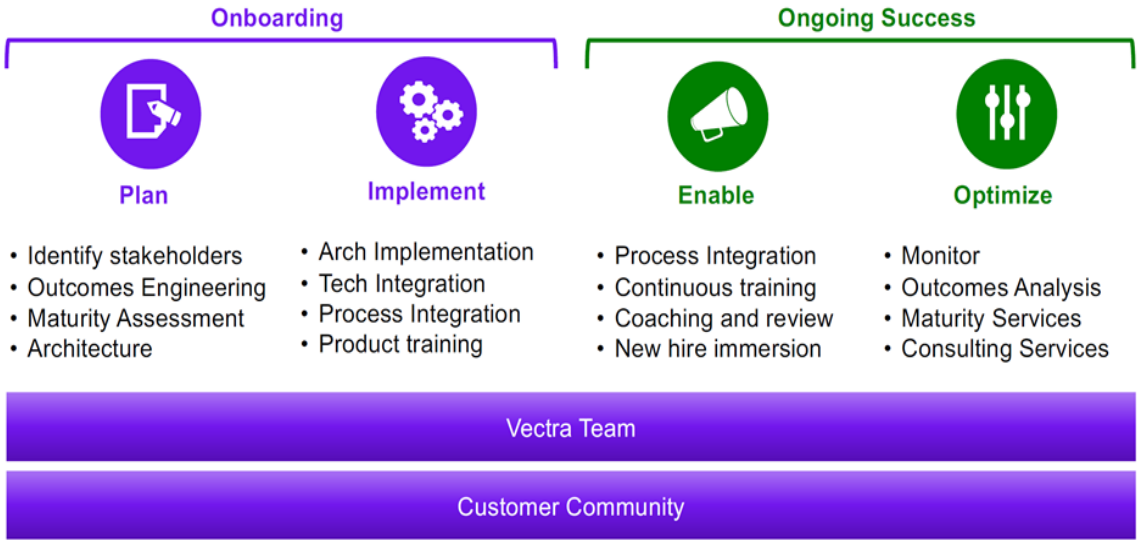

Figure 15. Vectra deployment model [19]

In this setup we focus on ongoing activities. Our goal was to see what benefits Vectra tools can bring to us in threat hunting. Monitoring and testing was a focus area. Normal situation is that you focus also onboarding tasks and try to get good overview environment and involve different stakeholders and systems.

4.4 Introducing Vectra solution

Vectra AI product idea is to collect data from network and from other systems. Figure 16 show areas what different sections are involved in this system. Rich metadata is key area. Which gives real-time visibility into network traffic. Vectra is extracting metadata from packets rather than do full packet analyze. This gives an effective way to handle large environment, because it is then you just send few bytes/packets to brain system.

Also, it is possible to extend visibility with laptops, servers, printers, BYOD (Bring Your Own Device), and IOT (Internet of Things) devices as well as all operating systems and applications. Integration is a key element to get a right understanding of how the environment is working. When your client or system works normally or if there is some unnormal behavior in your environment.

Collected metadata is a way to find hidden and unknown attackers. Machine learning with behavioral analytics in network traffic such a remote access tools,

hidden tunnels, backdoors, credential abuse and internal reconnaissance and lateral movements [19].

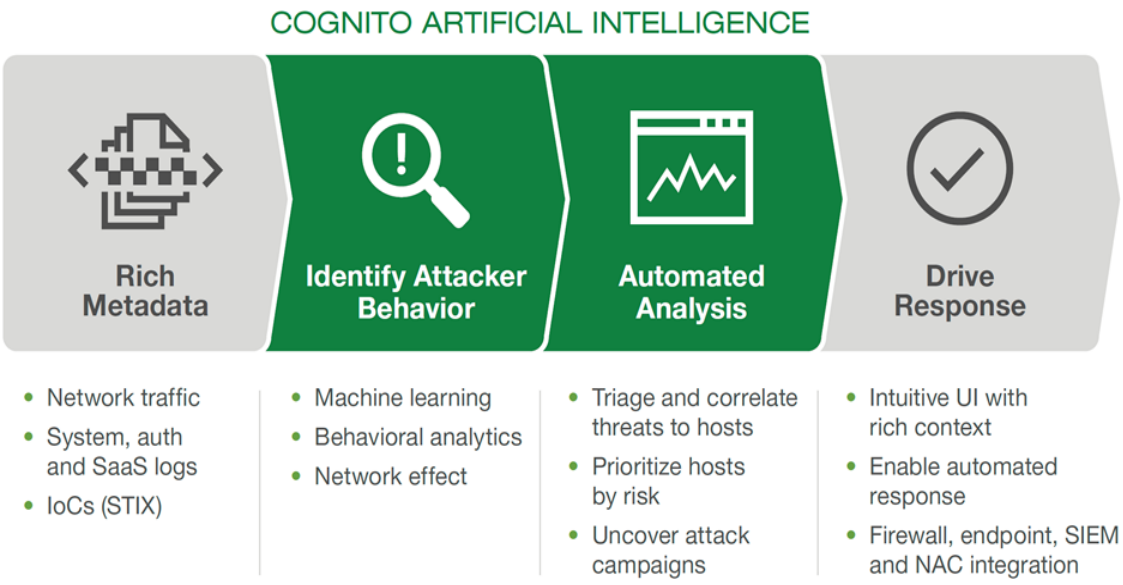

Figure 16. Vectra Detection Areas [19]

Here are the categories how Vectra products are used to identify threats on your environment:

- Botnet activity
- Command and Control and other hidden communications
- Internal reconnaissance
- Lateral movement
- Data exfiltration
- Abuse of account
- Attack campaigns

Figure 17 shows how, Vectra identified attack phases. This example (figure 17) tells how system has found some unnormal behavior [19].

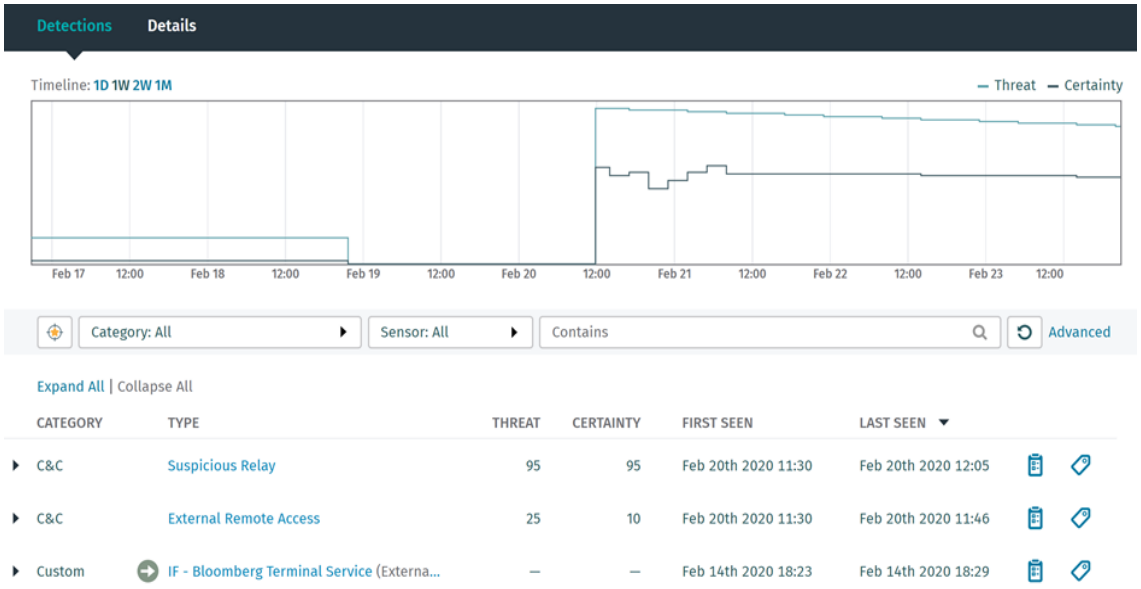

Figure 17. Unnormal traffic from Vectra dashboard

Dashboard shows overall situation at your network environment. There is an easy way to navigate different resources and try to recognize what might be an issue.

The first phase is to start to find host and accounts. In figure 18 shows a dashboard view. That shows in overall what type of issues there might have. First you should go through all critical issues and try to find example from your company CMDB (Configuration Management Database) more detailed information for host and users. CMDB is a key tool to identify your assets and owners as well.

Numerous hosts interacting with one each other are grouped together and can be expanded by clicking on the plus icon in the chart, with specific host information available by then clicking on the individual host (see Figure 18). This demonstrates the powerful threat hunting capabilities Cognito Detect provides analysts with little effort. Analysts can click individual hosts to get additional details about the host, such as the category of threats discovered, time of threat data and asset data (including admin sessions and data transform sessions).

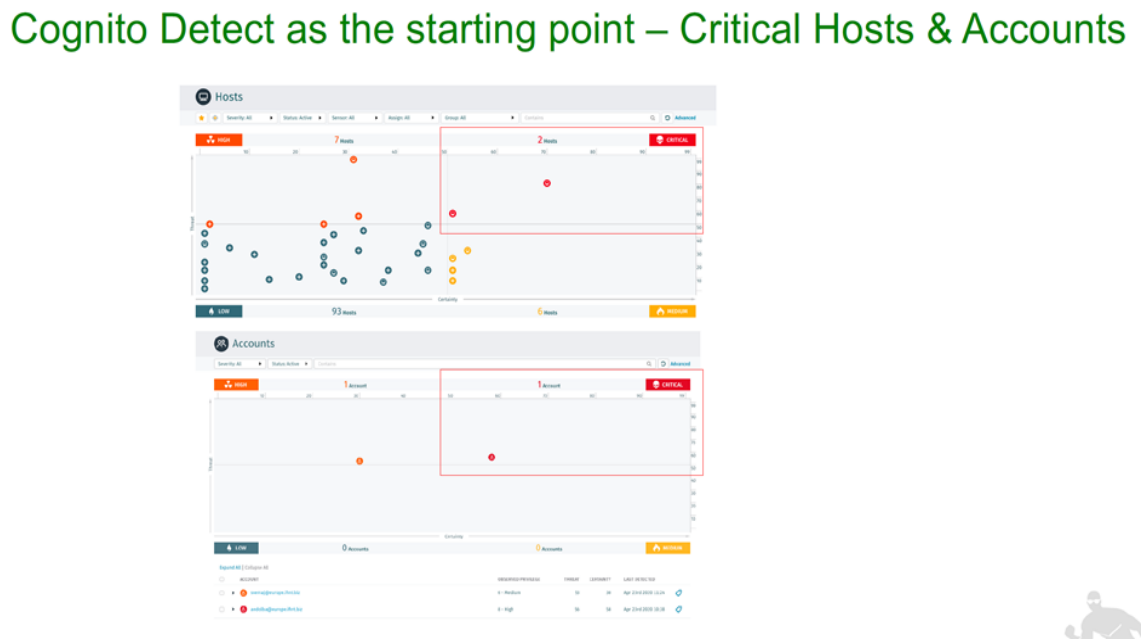

Figure 18. Host detection at Vectra dashboard

Figure 18 shows in overall situation from environment. Normally you should only check those critical cases, and normal environment there should be only few cases that you should go through. This kind result is important. That product not give too much alarms and falsepositivies. In some cases this is learning process and you need also put some input to system. What is valid and what is not.

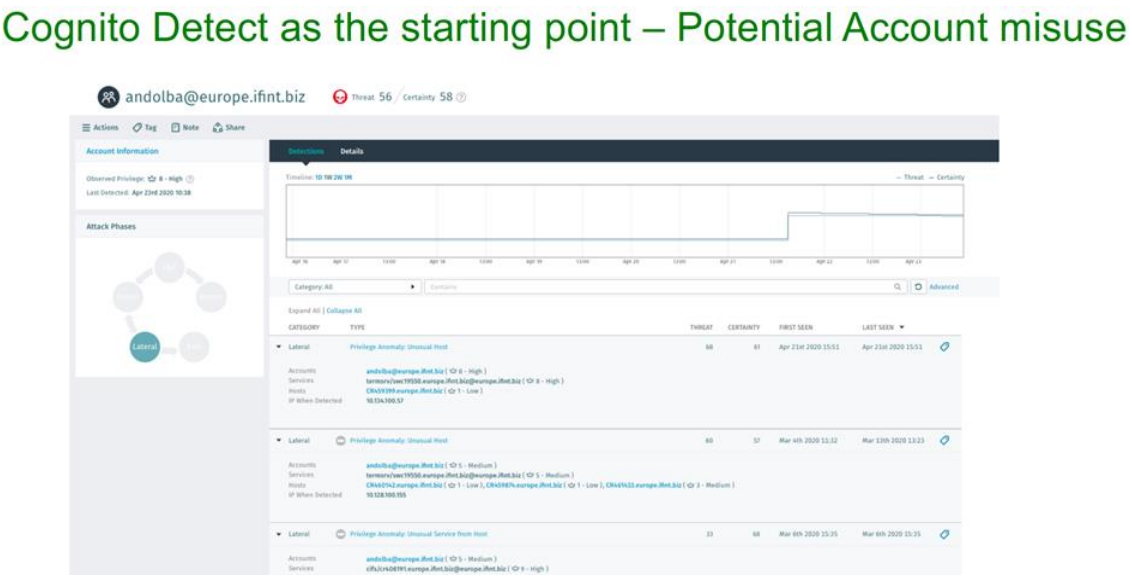

Figure 19. Account misuse case

Also, Vectra can follow account behavior for online (Figure 19). This gives good visibility for account misusage and gives more value for NDR. Example lateral movement with account misuse is exceptionally effective way to see. What different resources account use in your assets?

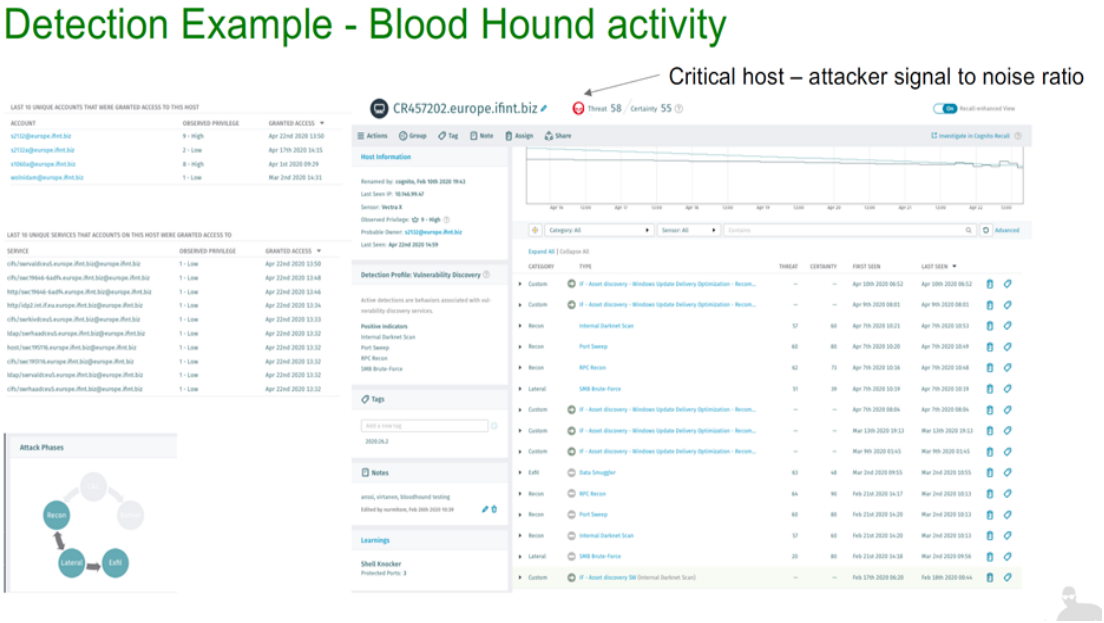

Figure 20. Test case for Blood Hound activity

4.5 Integrating Cognito with Splunk

The Vectra App for Splunk brings real-time, precorrelated attack detections to the operational intelligence of the Splunk platform. Integrating the Cognito platform's AI-based detection algorithms with Splunk enriches the context of threat investigations and speeds-up incident response.

There are two different phases. When you deploy integrations with Vectra and Splunk. First you need to add plugins to Splunk system and then configure metadata and forwarding config at Vectra Cognito system.

Cognito stream is deployed as a virtual machine (Vectra Server-Figure 14). Metadata data flows from Cognito brain devices to stream. Cognito stream

change metadata type to Bro/Zeek format and forwards metadata to SIEM or Splunk.

Here is a short description for config:

- Enable forwarding metadata settings (figure 21)
- Cognito stream VM needed sizing (figure 22)
- Select the metadata types (figure 23)
- Configure your SIEM or lake connector (figure 24)

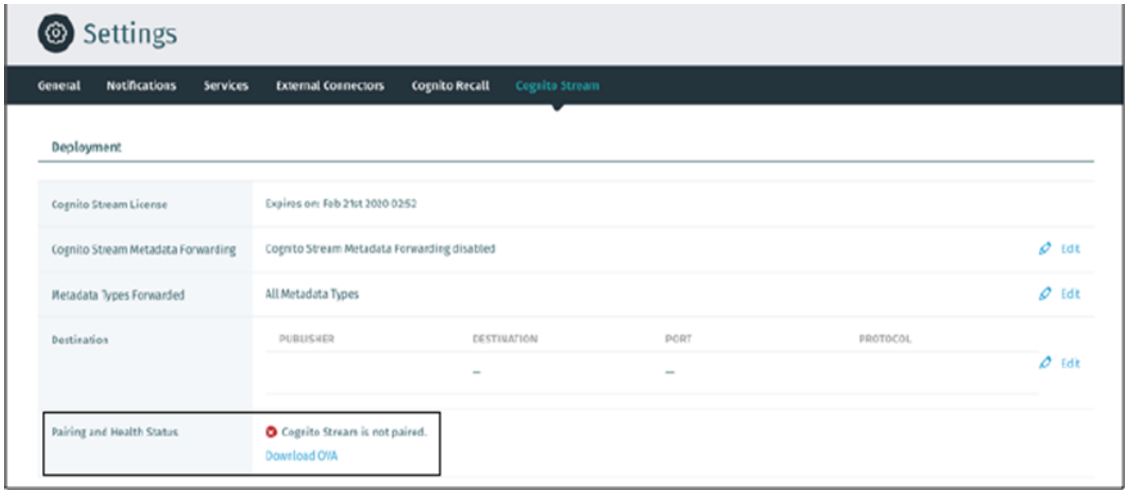

Figure 21. Enable forwarding settings

Resource type	Requirement		
Performance	Less than 10 Gbps	Greater than 10 Gbps, but less than 20 Gbps	Greater than 20 Gbps
CPU	8 vCPU	16 vCPU	Contact Vectra support
Memory	8 GB	16 GB	
Drive	50 GB	50 GB	

Figure 22. Cognito stream VM needed sizing.

Figure 22 shows how you need to use some performance settings when you deploy virtual server for Cognito stream server.

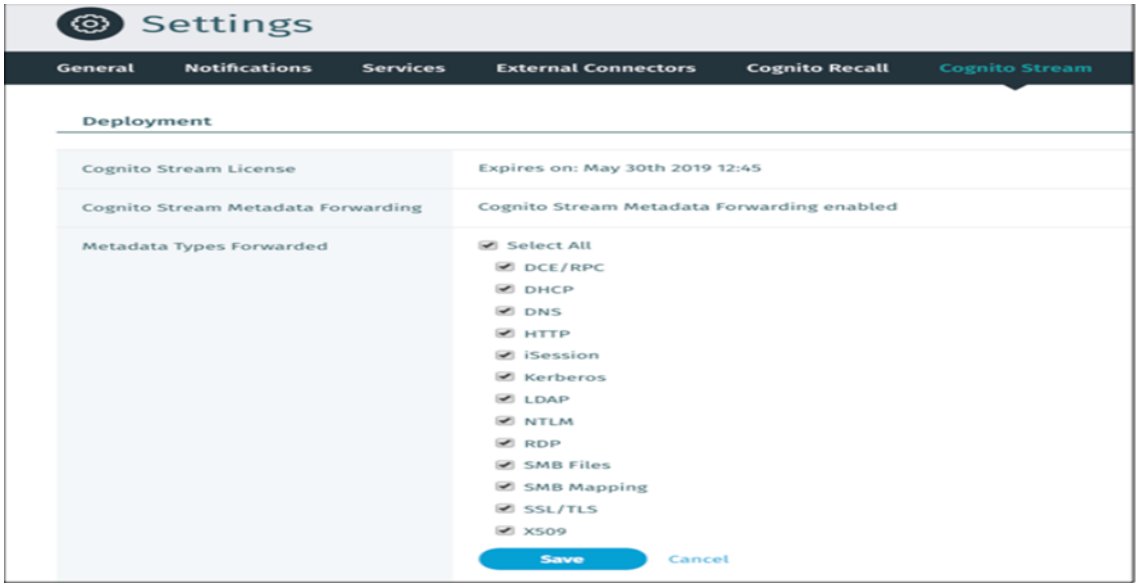

Figure 23. Select metadata types

With faster response and improved operational efficiency, the Vectra App for Splunk enables security teams to quickly mitigate and stop cyber-attacks before damage is done. Cognito prioritizes infected hosts that pose the highest risk and correlates threats with logs from devices in Splunk to provide greater context for every attack.

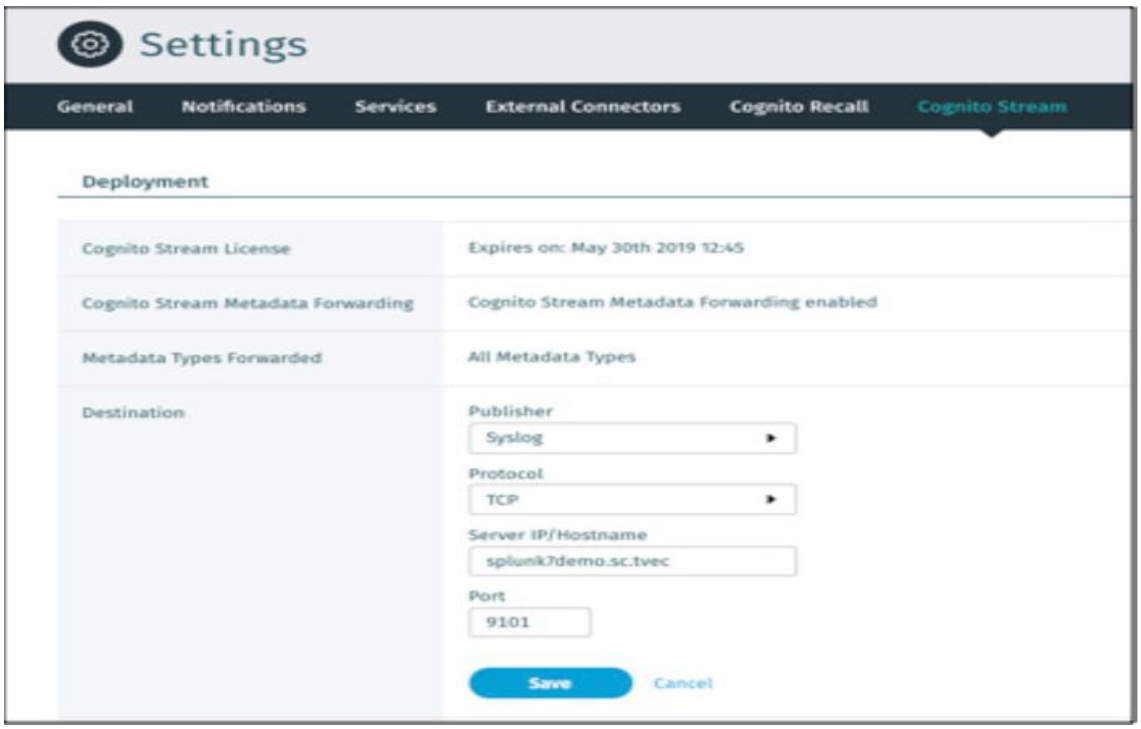

Figure 24. Configure SIEM cloud connector.

4.6 Cognito recall feature

Cognito recall is one way to follow how attacker traffic works at network level. There is a good dashboard view to see (figure 25) what different type of traffic that host sending and what services is used as well. Here is one example, where Vectra shows one workstation traffic figure 25 and figure 26.

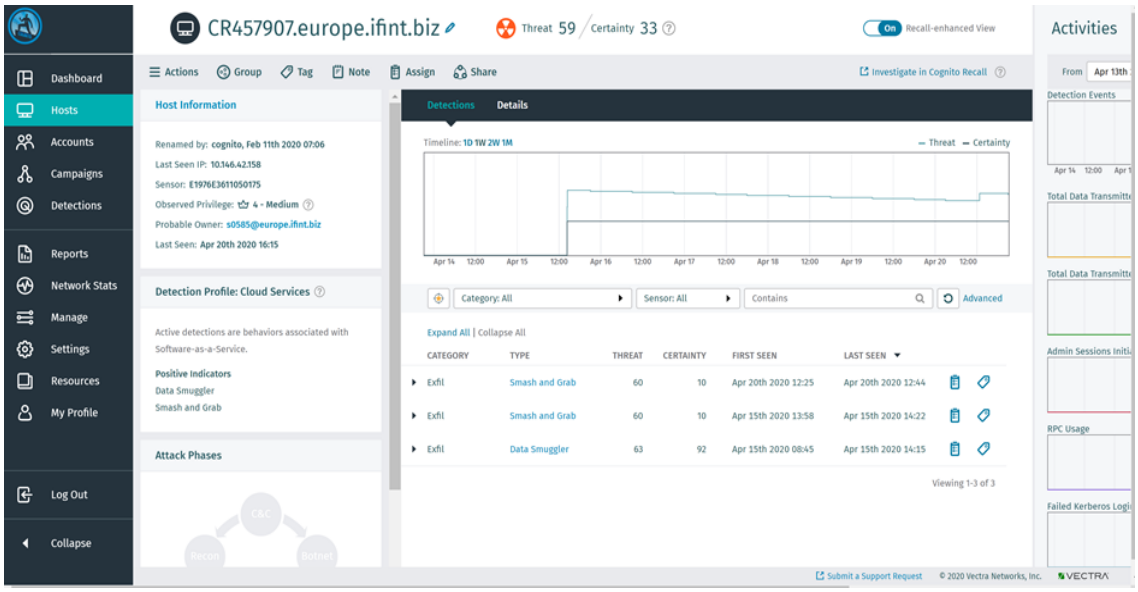

Figure 25. Host information from Vectra Cognito

Cognito Recall allows security analysts to identify the activity of host devices surrounding the time of a threat detection and reveal significant changes in the overall behavior of host devices. Through visual graphs and search capabilities, Cognito Recall exposes other host devices, accounts, and external domains and IP addresses, which enables security analysts to identify the full scope of the incident.

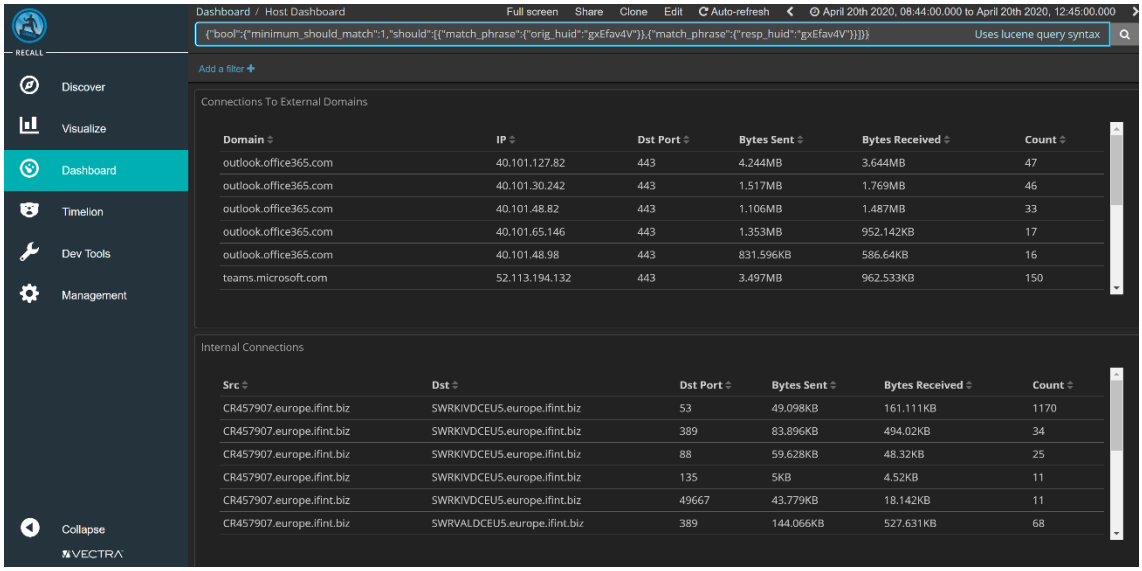

Figure 26. Vectra Recall dashboard (host info).

Cognito Recall enables security analysts to do deeper and more conclusive incident investigation with better efficiency. Security analysts can easily follow that chain of related events from attack detections found by Cognito Detect. With Cognito Recall, security analysts can investigate incidents with unprecedented efficiency using complete context about incidents, along with relevant details about associated devices, accounts and network communications.

This solution is the same as SIEM normally does. Collecting also third-party data from different vendors and sources.

CONCLUSIONS

Organizations are struggling to baseline behavior in their network environments and gain the proper visibility into what is happening at any given time. At the same time, simplifying security operations investigations across all analyst skill levels is a huge priority, given the shortage of skills available and the increasing pressures facing all security operations and investigations teams. I found that the Vectra and other NDR platforms succeeded in helping on both issues. The platform was fast and thorough and provided a wide range of options for searching and querying activity within the environment. On top of that, the interface was intuitive and easy to get started with, and that is one of the most critical factors in enabling security operations teams today. Also, I found the platform detailed and flexible for security operations teams that need better visibility into network behavior in their environment, with the benefits of deep investigation and hunting tools as well.

The starting point of my work was to gain better visibility into the operation of the network and to compare different products with their features that can add value to the way the security team works. Basically, visibility is at a sufficient level right now, but enriching information is one big step to better highlight real attacks. The way products bring out issues is key to being able to benefit from finding threats. Too often, products bring out false alarms, leaving SOC teams unable to handle the right things when the amount of data and false alarms cause unnecessary work.

The results of the work showed that it is possible to reap the benefits of finding threats. Visibility and product intelligence helped to find real abuses that the SOC team could investigate further. The starting point of the product was to know the behavior patterns of the network, devices and users. This reduces false alarms as learning becomes more accurate over time. The result of the work is that the benefits of the product are clearly visible. Now we are also considering other options from the market that would make the best possible product available to the company. I believe that my work will be of great benefit in providing additional tools for identifying and preventing threats.

REFERENCES

[1] Andre Perez 2014. Network Security. John Wiley & Sons, inc

[2] Alan Calder 2018. NIST Cybersecurity Framework. IT Governance Publishing

[3] Enisa 2021. Top Trends. Published on October 27, 2021 https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends

[4] Vectra 2021. Vectra and Microsoft EDR. Published on June 9, 2021 https://www.vectra.ai/partners/microsoft

[5] Mitre 2021. Mitre Framework. Published on July 23, 2021. https://attack.mitre.org/

[6] Jason Garbis, Jerry W.Chapman 2021. Zero Trust Security. Berkley, United States

[7] Crowdstrike 2021. Zerotrust strategy. Published on October 27, 2021 https://www.crowdstrike.com/cybersecurity-101/zero-trust-security/how-to-build-a-zero-trust-strategy/

[8] David Nathans 2014. Designed and Building Security Operations Center. Syngress Media USA

[9] Enisa 2021https://www.enisa.europa.eu/publications/how-to-set-up-csirt-and-soc. Published on December 10, 2020

[10] Exabeam 2021. SOC and Factors. Published on October 26, 2021 https://www.exabeam.com/siem-guide/the-soc-secops-and-siem/

[11] Swimlane 2021. SOAR introduction. Published on October 27. https://swimlane.com/resources/ebook-soar-capabilities

[12] Lastline 2019. SOC eBook_SOC_Triad_Strategy_eBook_Final.pdf. Published on August 2019

[13] Gartner 2019. Gartner resource page. Published on June 10,2021. applying-network-centric-approach-to-threat-detection-response-373460%20(2).pdf.

[14] Mitre 2017. Mitre resources. Published June 10, 2021. https://www.mitre.org/sites/default/files/publications/16-3713-finding-cyber-threats%20with%20att%26ck-based-analytics.pdf

[15] Huntsmansecurity 2021. Huntsmansecurity Mitre and heatmap. Published on June 10. 2021. https://www.huntsmansecurity.com/products/siem-features/mitre-attack-threat-heatmap/

[16] Vectra 2021. Vectra and Mitre framework. Published on October 15, 2021. https://content.vectra.ai/rs/748-MCE-447/images/SolutionOverview_MITRE.pdf

[17] Vectra webpage. Vectra and threat detection. Published on October 10,2021 https://content.vectra.ai/rs/748-MCE-447/images/Ebook_NewThreatDetectionModel.pdf.

[18] Networks Training 2020. SPAN interface deployment. Published on September 23. https://www.networkstraining.com/how-to-configure-cisco-span-rspan-erspan/

[19] Vectra 2021. Vectra NDR solution. Published on September 10, 2020 https://www.vectra.ai/resource-type/ebooks.