

Use case creation and management

Mikko Iso-Oja

Master's thesis

April 2021

School of Technology

Information and Communication Technology

Master of Engineering, Cyber Security

Author(s) Iso-Oja, Mikko	Type of publication Master's thesis	Date April 2021 Language of publication: English
	Number of pages 47	Permission for web publication: Yes
Title of publication Use case creation and management		
Degree programme Master of Engineering, Cyber Security		
Supervisor(s) Kotikoski Sampo, Hautamäki Jari		
Assigned by Telia Cygate Oy		
Abstract <p>The main goal of the thesis was to start the implementation of a use case library database application and to gain insight into the use of Sigma format.</p> <p>In the beginning discussions were held on the direction of the work: What should be accomplished and how to limit the scope of the work? Sigma format was the only mandatory component of the work. Otherwise, free options were given to develop the application.</p> <p>The application was developed with the use of the following methods, technologies, and programming languages. Python3, MySQL, GitHub, Linux, Bash and Sigma and its Sigmac conversion tool.</p> <p>Sigma allows easy conversion of alert use case templates to different security monitoring and event management platforms (SIEM). This can be beneficial in avoiding a vendor lock. Also, as a MSSP Telia Cygate might have in its control multiple different SIEM platforms from different vendors and Sigma allows easy conversion of an alert use case to multiple formats.</p> <p>The work was presented to Telia Cygate's cybersecurity development team. Discussions and a survey were conducted to gather opinions about the developed app and to gather the development team's opinions on Sigma format.</p>		
Keywords/tags (subjects) Alert, Use case, SIEM, Sigma, ATT&CK		
Miscellaneous (Confidential information)		

Description

Tekijä(t) Iso-Oja, Mikko	Julkaisun laji Opinnäytetyö, ylempi AMK	Päivämäärä Huhtikuu 2021 Language of publication: englantia
	Number of pages 47	Verkojulkaisulupa myönnetty: Kyllä
Työn nimi Use case creation and management.		
Tutkinto-ohjelma Master of Engineering, Cyber Security		
Työn ohjaaja(t) Kotikoski Sampo, Hautamäki Jari		
Toimeksiantaja(t) Telia Cygate Oy		
Tiivistelmä Työn tarkoituksena oli aloittaa käyttötapaus kirjasto tietokantaohjelmiston teko, sekä saada tietoa Sigma formaatin käyttämisestä hälytys käyttötapausten dokumentointiin. Työ alkoi keskusteluilla sen tulevasta suunnasta ja päämääristä. Oli päätettävä mitä tavoitellaan ja mitkä asiat kuuluvat projektiin. Ainut ennalta päätetty kohde oli Sigma formaatin käyttäminen, muuten suunnitteluun annettiin vapaat kädet. Sovellus kehitettiin käyttämällä seuraavia metodeja, teknologioita ja ohjelmointikieliä. Python3, MySQL, GitHub, Linux, Bash and Sigma ja Sigma projektin kehittämä Sigmac konversio työkalu. Sigman avulla voidaan helposti konvertoida hälytys käyttötappauksia useiden eri valmistajien alustoihin. Tästä voi olla hyötyä, mikäli on pakottava tarve suunnitella hälytyksiä useiden eri valmistajien alustoilla. Työ esitettiin Telia Cygate:n kyberturvallisuus kehitys ryhmälle. Keskusteluita ja kysely työstä suoritettiin, jotta saataisiin kerättyä mielipiteitä kehitetystä ohjelmasta ja Sigma formaatin käytöstä.		
Avainsanat (asiasanat) Alert, Use case, SIEM, Sigma, ATT&CK		
Muut tiedot (salassa pidettävät liitteet)		

Contents

1	Introduction	5
2	Research question and methods	5
3	Managed security service provider	8
	3.1 Security operations center	8
	3.2 Challenges faced by managed security service provider.	9
4	Advanced Persistent Threat	9
	4.1 What is an Advanced Persistent Threat actor?	9
	4.2 Who are APT actors?	12
	4.3 Example of APT targets	12
5	Kill Chain frameworks.....	15
	5.1 Kill chain.....	15
	5.2 Lockheed Martin’s Kill chain.....	16
	5.3 MITRE ATT&CK for Enterprise	16
	5.4 How to use ATT&CK for Enterprises.....	17
6	Detecting the adversary.....	19
	6.1 SIEM.....	19
	6.2 Log management.....	21
	6.3 Alerts	22
	6.4 Sigma and Sigmac.....	22
	6.5 Use of Sigmac	25
7	Implementation.....	26
	7.1 Scope	26
	7.2 Out of scope	27
	7.3 Database.....	28

	2
7.4 GIT Version control.....	29
7.5 Programming.....	31
8 Conclusions	34
9 Discussion	35
References.....	38
Appendices	42

Figures

Figure 1. Concept for the flow of data at the start of the project.	6
Figure 2. Spiral loop of reactive research.....	7
Figure 3. Advanced persistent threat lifecycle.....	11
Figure 4. ATT&CK for Enterprises.	17
Figure 5. Techniques used by APT19.....	18
Figure 6. SIEM solutions as illustrated by LogPoint.	20
Figure 7. Converting Sigma rules.....	23
Figure 8. Sigma example for clearing the PowerShell History.	24
Figure 9. Use of Sigmac.	25
Figure 10. LogPoint rule done with Sigmac.....	25
Figure 11. Splunk rule done with Sigmac.	26
Figure 12. Implementation plan. Dashed lines represent airgaps.	27
Figure 13. Terminology differences in Git platforms.	30
Figure 14. Git provider market shares.	31
Figure 15. Use of mysql.connector.	33
Figure 16. Example of GitPython.....	34

Tables

Table 1 Patterns of APT attack.	10
--------------------------------------	----

Acronyms

APT	Advanced Persistent threat
ATT&CK	Adversarial Tactics, Techniques, and Common Knowledge
FFRDC	Federally funded research and development center
IOC	Indicators of Compromise
MSSP	Managed Security Service Provider
NOC	Network Operations Center
POC	Proof of Concept
PRC	People's Republic of China
SIEM	Security Information and Event Management
SOC	Security Operations Center
SQL	Structured Query Language

1 Introduction

The goal of this project was to build a proof of concept for a use case database application that would allow for the archival and data management of use cases in a managed security service provider (MSSP) environment. The database should allow management of security information and event management (SIEM) use case alerts. The database should be able to inform data of the use case and to inform to which SIEM environments does it apply to.

The database should help with threat hunting specially related to advanced persistent threats. Later it could be adapted to help in the provision of new SIEM environments. Threat use cases can be searched from MITRE ATT&CK, implemented as SIEM alerts with the help of Sigma format and then their data stored into the database.

This project also aimed to gather information about the usability of Sigma signature format. The use case database must utilize the Sigma format to evaluate its usability. The main question was that can it be used in the conversion of the use cases to multiple different SIEM vendor platform formats.

2 Research question and methods

A MSSP has under its control multiple different SIEM platforms on multiple different customers. The platforms might not be connected together and even a large corporate network might have more than one SIEM but under the supervision of the same MSSP. The implementation and documentation of different security use cases into these SIEM platforms can be difficult. There needs to be some kind of a system where to mark what use cases are in use in what platforms. Also, the system should help in the storage of the use case alert code. This research aims to answer the following question:

What improvements can a database application bring to the implementation of SIEM use cases in an MSSP environment?

This can further be refined into sub questions:

1. If there is a need to implement a SIEM alert based on a use case, where do we store it and how do we access it later?
2. How to know what use case does customer X have implemented in their SIEM?
3. Can this process be one "pipeline" and how does one maintain it?
4. Can multi-vendor support be achieved?
5. How can we find new use case scenarios?

The aim is to identify useful use cases from MITRE ATT&CK: to create an alert script based on the use case and store it in a database and then implement that script into the customers' SIEM. Once the ATT&CK use case has been scripted and stored into the database application, can it be easily taken from that database and implemented into a SIEM platform? The preliminary concept of the data flow can be seen in Figure 1.

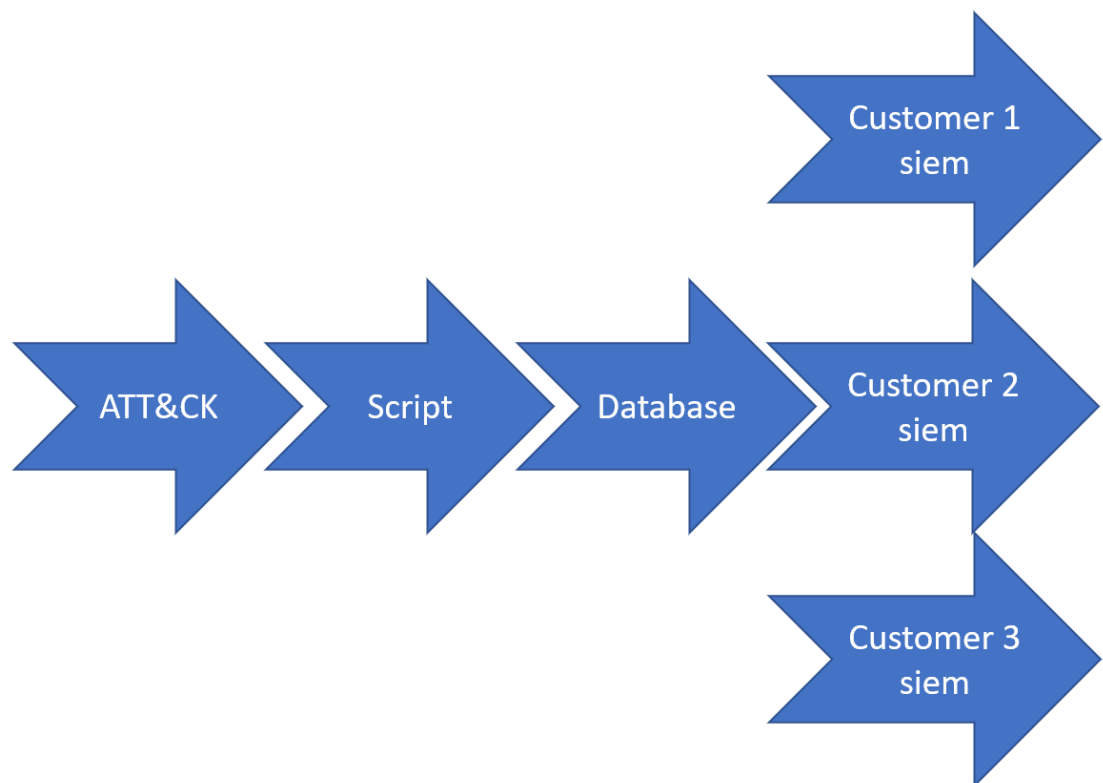


Figure 1. Concept for the flow of data at the start of the project.

Research method

Action research aims to generate solutions to practical problems. This can be achieved through a repeatable process of iterations. The iteration can be described as a spiral as illustrated in Figure 2. One process loop is gone through and after the reflection the research continues to another loop, this can continue to spiral “downwards” endlessly. After each reflection new data based on the observations are added to the plan and then acted accordingly. Action research along with constructive research is often used in the research projects of new computing and information technology. (McGregor, C. 2018)

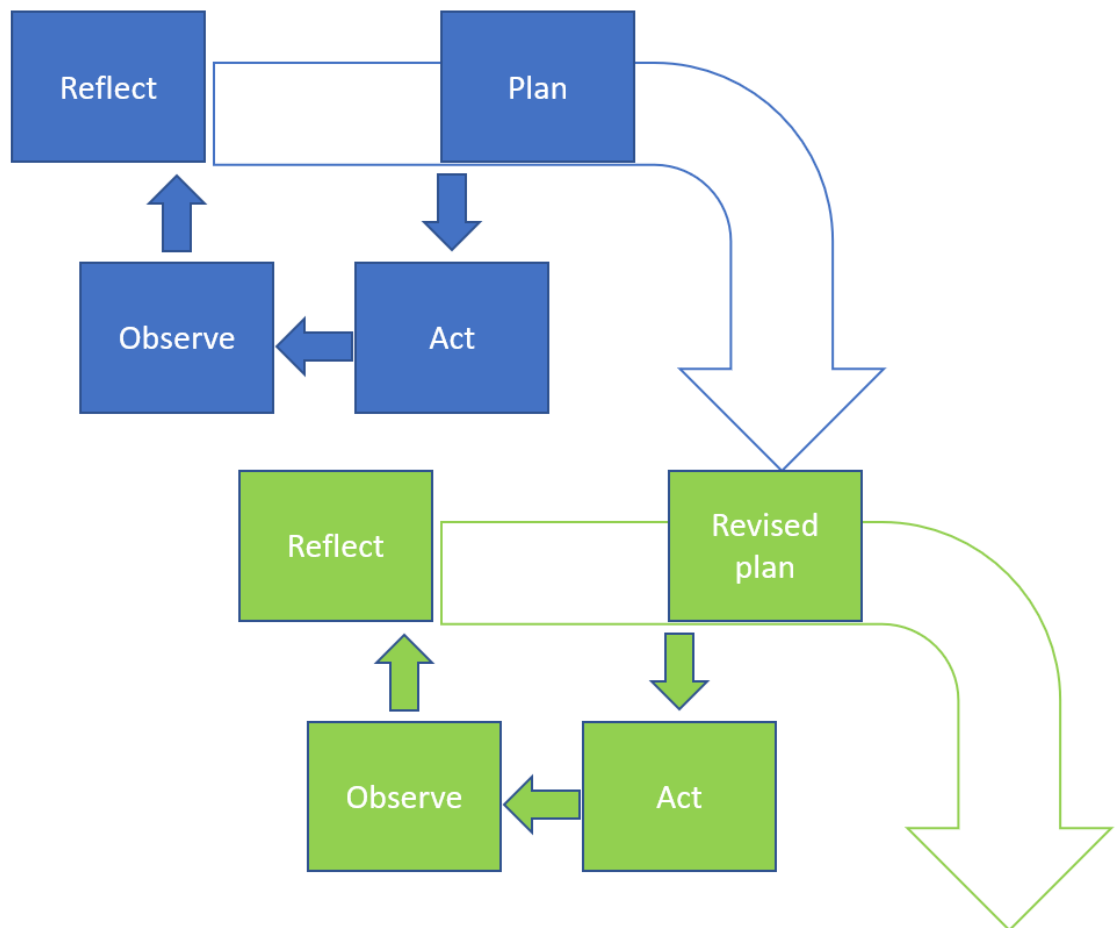


Figure 2. Spiral loop of reactive research.

Action research was suitable for this project because it was decided that there would be periodic checks during the development phase. Progress of the work was

showcased to the development team in bi-weekly meetings and the application was changed based on the review given by the team.

3 Managed security service provider

A managed security service provider (MSSP) is an outsourced cyber security service provider. A MSSP can provide some services to a customer for example event monitoring or device management. Increasingly the whole network / security operations center (NOC / SOC) can be operated by the MSSP. Usually, managed security service providers have multiple different customers from different fields of industry. (Logpoint 2020)

3.1 Security operations center

Security operations center (SOC) can be managed by an individual company as an inhouse department, or it can be bought from a MSSP as a service. SOC monitors, reacts, detects, and investigates security threats detected in an organizations network. A SOC usually operates 24/7 but due to financial restraints this can be limited to normal business hours.

SOC security analysts handle the monitoring of alerts and reacts to possible incidents. Monitoring is done with cybersecurity systems like a security incident management system (SIEM). Security engineers handle the administration, upkeep, and development of SOC platforms. Additional personnel can be dedicated threat hunters and digital forensics and incident response (DFIR) personnel.

Companies that have taken SOC as a service from a MSSP still have limited security personnel of their own. This can be example network engineers, IT managers, dedicated CIRT-teams or just a chief information's security officers. SOC communicates important incident data to the customer security personnel immediately or in the case of non-critical incidents typically on weekly basis as post incident reports.

The reasons affecting a company's decision to outsource its SOC-operations are lack of talented cybersecurity employees, threat landscape becoming more advanced, and costs associated in keeping and developing an own dedicated 24/7 security operations center. (Fortinet 2019)

Threats are becoming increasingly more complex. Advanced threat actors are trending towards persistent attacks. This trend is driving the customer and their MSSP towards a more integrated security architecture. Customers are not looking for individual security tools but a security partner that can provide a full-scale monitoring and protective service to counter these threats. (Matteson, S. 2019)

3.2 Challenges faced by managed security service provider.

The customer bases of a MSSP can contain multiple companies from multiple different fields. This creates a unique threat landscape where the MSSP must be aware of general cybersecurity threats but also be able to anticipate and counter the threats targeting their specific customers.

Inadequate alerts and lack of integration with the client's IT infrastructure can increase this challenge. To counter the unique threats faced from the customers side the MSSP should develop unique alerts to detect the threats and distribute them to the systems monitoring the customers IT infrastructure. However, this can be challenging due to the lack of communication between the different systems and in worst cases the system manufacturer can vary depending on the customer. (Francis 2019)

4 Advanced Persistent Threat

4.1 What is an Advanced Persistent Threat actor?

Advanced Persistent Threat (APT) is a threat actor (group) that uses continuous, clandestine, and sophisticated hacking techniques to acquire access to a system and lingers there for an extended period of time. APT groups normally target high value

targets like governments and large companies. New trend is that they have started to target smaller scale companies that are part of the supply-chain of their primary target. (Kaspersky 2020)

APT attacks usually follow a set of patterns or sequences. There are no exact definitions of the sequences and they vary bit according to the publisher of the information, but the general pattern remains the same. Table 1 shows the attack stages as defined by cyber security companies Kaspersky, Carbon Black, and Cynet.

Table 1 Patterns of APT attack.

Kaspersky	Carbon Black	Cynet
	Develop a specific strategy.	
Gain access	Gain access	Initial access
Establish a foothold	Establish a foothold and probe	First penetration and malware deployment
Deepen access	Stage the attack	Expand access and move laterally
Move laterally	Take the data	Stage the attack
Look, learn and remain	Persist until detected	Exfiltration or damage infliction
		Follow up attacks

Table 1. Patterns of an APT attack.

The overall chain of events remains the same for each attack pattern, but there are some slight differences. According to Carbon Black the attack already starts in the strategy development phase while Kaspersky and Cynet considers the act of gaining an initial access as the first step. Cynet lists the possible follow up attack as a separate part while the two other companies state the possibility of a follow up attack to be part of the remain / persist stage. Kaspersky lists no separate attack /

data exfiltration step but states that the attacker might remain or withdraw once their objective has been completed. (Kaspersky 2020; Carbon Black 2020; Cynet 2020)

Patterns of an advanced persistent threat actor attack can also be illustrated by an APT attack Lifecycle wheel as illustrated in Figure 3. The loop does not end until the threat actor has been detected and removed from the system. (Kaspersky 2018)



Figure 3. Advanced persistent threat lifecycle.

4.2 Who are APT actors?

There are no official definitions to who are the APT actors, but a common definition is that an APT group is one that receives direction and support from an established nation state. (FireEye 2021)

Some groups like APT 1 has been linked to a certain national military unit by another nation state. APT 1 is claimed by cybersecurity company Mandiant (now part of FireEye) to be the People's Liberation Army Unit 61398. (Mandiant 2014)

APT 1 has targeted several companies around the world to steal trade secrets and to conduct cyber espionage. Some of APT 1 targets have been US based metal, nuclear and solar companies. This has led the US Department of Justice to charge five People's Liberation Army members with multiple charges and are now wanted by the FBI. Foreign ministry of the People's Republic of China has stated the charges to be "made up". (Reuters 2014; FBI 2014)

PRC has also been the target of APT groups themselves. In 2015 Russian cybersecurity company Kaspersky exposed some of the operations done by a group named Equation Group. In their report Kaspersky implicated that Equation Group is a US spy agency. The actual perpetrator was not named but it is commonly thought to be US National Security Agency. (Goodin, D. 2015)

Exact number and origin of APT groups cannot be stated. MITRE lists 122 different groups, some stated to be linked to a certain ministry or military unit and others as a cybercriminal group. Lists also show some bias based on the origin of the list. Example FireEye a US cybersecurity company does not state any US based threat actors.

4.3 Example of APT targets

APT actors target a wide range of targets. Government entities, Non-governmental organizations, universities, and companies. Goal of an APT actor can be to acquire intellectual property, classified data, personal information, infrastructure data, credentials, and other sensitive information or to conduct sabotage. (Cynet 2020)

Below are some examples of APT activities targeting different types of targets. Each example has a different motive to illustrate the different activities done by APT actors. Common for each example is also the lack of exact proof into the identity of the culprit. In some cases, the suspect and the target both deny any involvement into the incident.

Each of the target examples can be a customer of a MSSP and usually a MSSP will have customers from multiple customer categories for example universities, corporations, and government entities. This makes it important for the MSSP to be aware of the threat landscape and to know the possible adversaries they could encounter.

Non-governmental organizations

Targets like non-governmental organization and individual persons indicate state sponsorship due to the lack of financial gains. One such instance is an attack campaign targeting the Tibetan and Uyghur NGOs. The campaign was dubbed by threat intelligence company Recoded Future as RedAlpha. Publicly available malware and tools were observed in the beginning of the campaign, most likely to obstruct the origin of the attacks. Later a malware called FF-RAT was observed. FF-RAT has been known exclusively used by APT actors from People's Republic of China. ThaiCERT lists this attack as being linked to a wider campaign targeting NGOs that are related to the "Five Poisons" of The Communist Party of China. (Recoded Future 2018; ThaiCERT 2020)

Universities

Silent Librarian is an APT group that has been targeting universities since 2018. By late 2019 the group was known to have targeted at least 60 universities from multiple different countries and more targets were identified in autumn 2020 (the start of the academic year). (Paganini 2019)

According to the US Department of Justice the organization behind the Silent Librarian group is an Iranian based company called the Mabna Institute. US Department of Justice claims that the Mabna institute is instructed on behalf of the Islamic Revolutionary Guard Corps of Iran to conduct a cyber theft campaign.

Department of justice has charged nine individuals from Iran with computer intrusion and other crimes. (Department of Justice 2018)

Sanctions to Iran have been said to be the motives behind the attacks. Stealing research and development data from around the world is a way to hamper the effectiveness of the sanctions that have been poised to Iran. (Muncaster, P. 2020)

Companies

As with universities companies are the targets of APT actors due to advanced research and development material. Companies can also be targeted for political reasons. In 2014 Sony Pictures was hacked by a group calling them Guardians of Peace. The aim of the hackers was most likely to stop the release of a movie called The Interview and to cause damage to Sony Pictures, due to the making of the movie. The hackers released among other things confidential and personal data, including employee's private information and future plans of Sony Pictures. (Peterson, A. 2014)

US investigation into the incident pointed to a group known as Lazarus Group. Lazarus Group is believed to be a military cyberwarfare unit operating in the Democratic People's Republic of Korea. Lab 121 (Bureau 121 on some reports) of the Reconnaissance General Bureau of the General Staff Department. (FBI 2018)

US federal arrest warrant was issued for Park Jin Hyok and he is thought to be a member of the Reconnaissance General Bureau. The warrant also states that his hacking group is labelled by some private cybersecurity researchers as the Lazarus Group. (FBI 2018)

Government entities

In spring of 2020 Vietnam survived the initial covid19 pandemic without major outbreaks even though it is located relatively close to Wuhan, starting place of the covid19 pandemic. Vietnam acted fast and closed its borders. Also, it set up a quarantine camp system for people arriving to the country. (Reuters 2020)

According to FireEye an APT group started to target officials from the city of Wuhan and the ministry of emergency management of the People's Republic of China in early January 2020. FireEye claims the group to be APT32 also known as Ocean Lotus.

Suspected to be a cyber espionage group of the government of Vietnam. (Reuters 2020)

It has been suspected that information gathered through this campaign was used by the government of Vietnam to uncover classified information about the early phases of the covid19 outbreak, revealing the true scope of the danger. This led Vietnam to take a more aggressive stance against the virus in the early phases of the pandemic. (Reuters 2020)

Both Vietnamese and PRC officials are denying claims of this campaign. Vietnam denies being the attacker and officials in PRC are not commenting on possible incidents. (Reuters 2020)

5 Kill Chain frameworks

5.1 Kill chain

Kill chain is originally a military concept developed by the United States Navy and Air Force for use in their AirSea Battle doctrine. One of the key aspects of the doctrine is to identify kill chains that can be used to defeat enemy anti-access capabilities.

Modern weapons systems require a complex chain of actions before they can be used. Kill chain aims to identify this chain of actions and tries to target the weakest point in the chain, in order to disrupt or end the use of the system. (Greenert, J. & Welsh, M. 2013)

In 2011 Lockheed Martin defined the term in a cyber security context in their whitepaper called "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains". (Sans 2019)

The paper argues that conventional defensive methods like, intrusion detection systems, software patching and anti-virus software's are not enough to counter APT intrusions. To counter an APT actor, one needs to identify the intrusion, identify the kill chain, and disrupt that chain. (Amin, R. Cloppert, M. & Hutchins, E. 2011)

5.2 Lockheed Martin's Kill chain

Lockheed Martin's original Intrusion kill chain is not a standard set of tools. Each APT case is customized and adapted according to the target. However, an intrusion kill chain can be broken down to the following steps:

1. Reconnaissance – Information about the target needs to be gathered. This can be achieved by collecting information from public sites (names, phone numbers). Web crawling and trying to find hidden information from the target's website or by port scanning and looking for open ports and collecting data on used systems / software's.
2. Weaponization – Designing a malware / hostile payload for example by embedding a hidden spyware or remote access tool into a seemingly harmless file. For example, a PDF file. The payload can be designed to use a known vulnerability in a software the target is using.
3. Delivery – The weaponized payload needs to be delivered to the target. This can be achieved for example by email, www-site or with USB drive.
4. Exploitation – Exploit a known vulnerability in the targets system.
5. Installation – escalating the users' privileges, increasing persistence inside the environment, gaining lateral access.
6. Command and Control – APT actors usually need a command and control (C2) channel for their operations.
7. Action on Objectives – each of the previous steps are required for the intruder to achieve their objectives. Objectives might be for example data exfiltration, violation of data integrity or negative impacts on system / data availability.
(Amin, R. Cloppert, M. & Hutchins, E. 2011)

Lockheed Martin's cyber kill chain was the first one to be developed but after that the idea has been adopted and modified into several other kill chain frameworks.

5.3 MITRE ATT&CK for Enterprise

The MITRE corporation is funded by the federal government of the United States and functions as a not-for-profit organization. MITRE operates six different research and development centers. Each center is funded by a different federal agency.

Cybersecurity research is conducted by MITRES National Cybersecurity FFRDC (federally funded research and development center) funded by the U.S. National Institute of Standards and Technology (MITRE 2021)

In 2013 MITRE started a project called Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK). Aim of the project was to document common tactics, techniques, and procedures (TTPs) used by APT actors in Windows enterprise networks. (Storm, B. 2018)

The current framework is called ATT&CK for Enterprise and it is an adversary model that refines the kill chain model to better facilitate the needs of an enterprise network, also the current model contains multiple different operating systems. ATT&CK for Enterprise contains 11 tactic categories that describe the kill chain. The 12 phases are illustrated in Figure 4 under the ATT&CK for Enterprise. Additionally, PRE-ATT&CK can be used as a separate framework. (MITRE 2021)

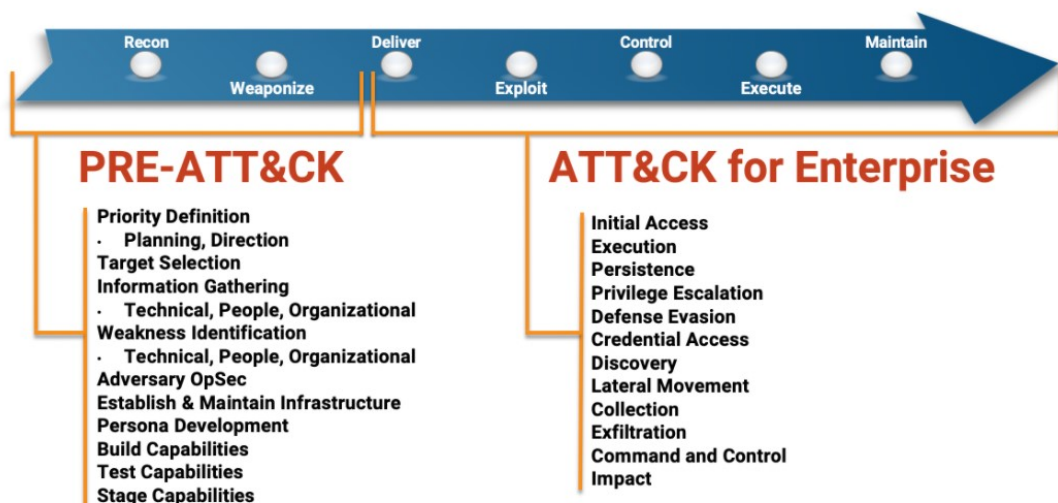


Figure 4. ATT&CK for Enterprises.

ATT&CK framework is updated bi-annually, and its update are based on publicly published threat intel data and incident reporting. The incidents are analysed and updated TTPs are developed out of the processed data. (MITRE 2021)

5.4 How to use ATT&CK for Enterprises

MITRE advises three different layers of competency when using ATT&CK.

- Level 1 for those just starting out who may not have many resources.
- Level 2 for those who are mid-level teams starting to mature.

- Level 3 for those with more advanced cybersecurity teams and resources. (Applebaum, A. 2019)

For this example, we will be concentrating on Level 1, also MITRE advises by starting small and concentrating first on just one technique and gradually expanding to other cases.

APT19 is a Chinese group that has targeted for example telecommunications companies. By selecting APT19 from ATT&CK's group database, one can see the different techniques used by that group. Figure 5 shows a portion of techniques used by APT19.

Techniques Used ATT&CK® Navigator Layers -

Domain	ID	Name	Use
Enterprise	T1043	Commonly Used Port	APT19 used TCP port 80 for C2. ^[1]
Enterprise	T1132	Data Encoding	An APT19 HTTP malware variant used Base64 to encode communications to the C2 server. ^[4]
Enterprise	T1140	Decfuscate/Decode Files or Information	An APT19 HTTP malware variant decrypts strings using single-byte XOR keys. ^[4]
Enterprise	T1073	DLL Side-Loading	APT19 launched an HTTP malware variant and a Port 22 malware variant using a legitimate executable that loaded the malicious DLL. ^[4]
Enterprise	T1189	Drive-by Compromise	APT19 performed a watering hole attack on forbes.com in 2014 to compromise targets. ^[4]
Enterprise	T1143	Hidden Window	APT19 used <code>-WindowStyle Hidden</code> to conceal PowerShell windows by setting the WindowStyle parameter to hidden. ^[1]
Enterprise	T1031	Modify Existing Service	An APT19 Port 22 malware variant registers itself as a service. ^[4]
Enterprise	T1112	Modify Registry	APT19 uses a Port 22 malware variant to modify several Registry keys. ^[4]
Enterprise	T1027	Obfuscated Files or Information	APT19 used Base64 to obfuscate commands and the payload. ^[1]
Enterprise	T1086	PowerShell	APT19 used PowerShell commands to execute payloads. ^[1]
Enterprise	T1060	Registry Run Keys / Startup Folder	An APT19 HTTP malware variant establishes persistence by setting the Registry key <code>HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Windows Debug Tools=150C8A5FFDCA11</code> . ^[4]
Enterprise	T1117	Regsvr32	APT19 used Regsvr32 to bypass application whitelisting techniques. ^[1]
Enterprise	T1085	Rundll32	APT19 configured its payload to inject into the rundll32.exe. ^[1]

Figure 5. Techniques used by APT19.

On the list we can see that hiding the PowerShell window is one of the techniques used by the group. Hidden power shell is defined by MITRE to be a defence evasion tactic. This can be used to conceal malicious activities from the user. This can be achieved by giving the command `powershell.exe -WindowStyle Hidden`. (MITRE 2019)

The successful detection of this phase in the kill chain would alert the defenders that a malicious attack is underway and could potentially lead to a successful defensive campaign against the threat actor.

MITRE advises as a detection method to enable PowerShell logging and to monitor the logs for command like `-WindowStyle Hidden`. This is one of the ways of doing it,

but you are not forced to follow MITRE's example. If you can develop another way to accomplish the task, then that could also be used. For Windows, this technique contains only a detection guide but for MacOs the guide also contains a mitigation suggestion. Both detection and mitigation should be considered if available. (MITRE 2019)

This technique is just one of the use cases used by APT19. To cover the threat caused by APT19, all or most of the different techniques should be covered. Although the detection of just one TTP will lead to the conclusion that an attack is underway. It should also be noted that the method can be used by multiple different groups, not just by APT19.

6 Detecting the adversary

MITRE ATT&CK gives us an idea on what to look for but it does not provide us with the tools to detect the threat. Tools come in the form of different software. One such is Security information and event management software (SIEM).

6.1 SIEM

Security information and event management (SIEM) is a software that is used to centrally collect log information out of a network. Computers, networking devices and software can be configured natively or with the help of a separate log forwarding software to send their logs into a SIEM.

SIEM allows the processing of the collected log data. Alerts can be configured to alert if unauthorized events are monitored, and dashboards can be set up to show the current state of the network being monitored. All this can be done centrally from one endpoint by using a SIEM. (LogPoint 2020)

Networks without a SIEM are vulnerable to malicious attacks due to the lack of visibility. SIEM gives visibility into the whole network. For SIEM to function as intended, alerts and dashboards need to be set up to give the initial indication of compromise (IOC). After a triggered alert, the SIEM allows for a centralized analysis

of the incident. Before SIEM's one had to individually connect into the system being investigated and go through the logs, now the whole network can be analysed from one portal. (LogPoint 2020)

Popularity of SIEM-software has also increased due to heightened compliance needs due to laws, regulations and to comply with certificates. Regulations mandate the maintenance of an audit trail that must be kept for example for half year to two years. These logs can be stored and later handled if needed in a SIEM platform. (Stratozen 2019)

The visibility given by SIEM's into the network mean that they can be utilized for other tasks than just cyber security. Threat detection and investigation remain as the core features. Other tasks can be for example compliance, IT-operations, and business analytics as is illustrated in Figure 6.

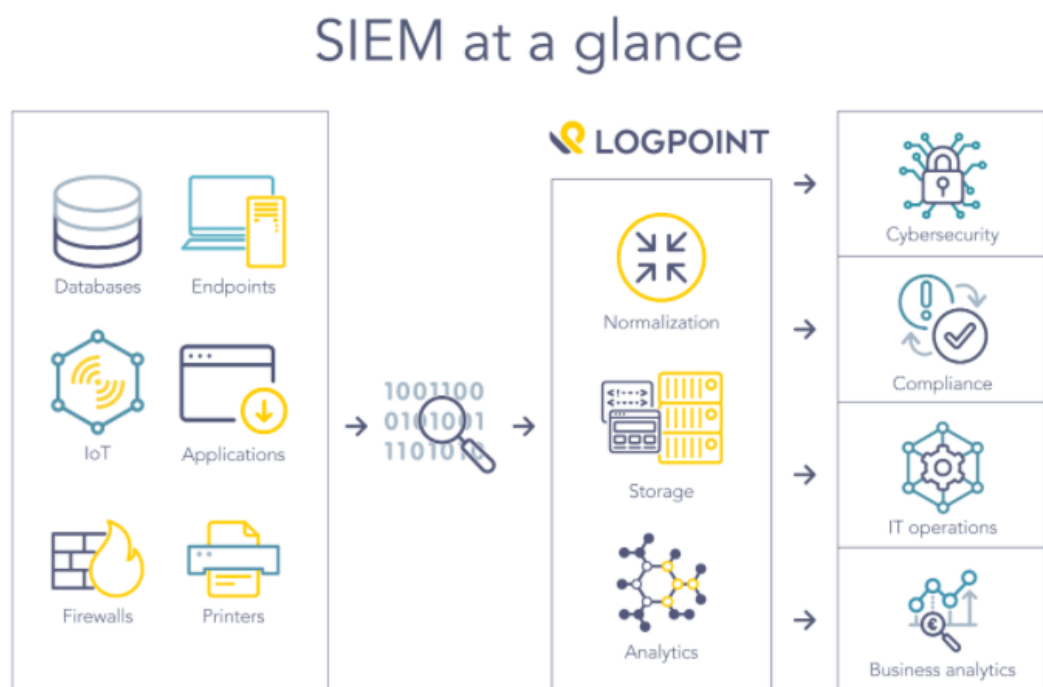


Figure 6. SIEM solutions as illustrated by LogPoint.

Taking a SIEM into use is a large project that can be divided into two tasks.

1. What to collect and how. (Log management)
2. How to use the data.

The data (logs) need to be first collected by the SIEM and then alerts need to be set up so that the data can be utilized. Usually, the data also needs to be first converted into a format the SIEM understands (data normalization).

6.2 Log management

Log management is the process of defining what logs should be stored and how long should they be kept, also reporting can be a criteria of log management. Many SIEM platforms can be used as a log management tool and therefore there is no need for a separate log management program. (Sumo logic 2020)

Some SIEM platforms are built on top of a Log management platform and a separate layer on top of the log management can be used to “upgrade” the log management platform to a SIEM platform. Example is Azure Log Analytics that can be used to store and query log data but if the user wants SIEM features then Azure Log Analytics with Azure Sentinel must be used. Sentinel uses the data located in Azure Log Analytics to create dashboards and to enable alerts.

Expenses need to be considered with log management. Some log management / SIEM platforms have their billing based on the number of logs ingested and the fee is based on the data sent to the platform. Physical storage limitations and costs remain as an issue even if there is no ingestion-based billing.

Log retention can be categorized with the amount of log coming into the system. A suitable retention time needs to be enacted. According to FireEye the average attacker dwell time was 56 days in 2020. This means that to detect a threat the logs need to be kept at least 56 days. Also, plenty of time should be left for further investigation. Each organization need to set a log retention policy that reflects the threat landscape they face. (FireEye 2020)

Insufficient log management can lead to an incident not being detected due to not ingesting the right log into the log management / SIEM platform. Also, insufficient data retention time can cause the full details of the incident to be left uncovered even if the attack is detected.

6.3 Alerts

Alerts are template scripts that can be written into a SIEM. An alert could be triggered when a new Admin is created or if a user copies files from a monitored location. Typically, these alerts are monitored by the security operations center (SOC). Alerts can be created based on the need of the organization.

In order to detect advanced threats one needs to first know the tactics and techniques used by the threat actor. These can be for example built based on the MITRE ATT&CK framework. Techniques listed in the framework can directly be made into SIEM alerts. One kill chain can be broken down into multiple use cases and each use case can be developed into a SIEM alert. The detection of one of these steps will lead to the discovery and hopefully eventually prevention of the attack.

6.4 Sigma and Sigmac

Each SIEM platform has a different template on how to build an alert. Alerts from one vendor are not interchangeable with another vendor's SIEM. This brings some issues, example:

- The community cannot easily share alerts with each other if the alerts can't be directly transferred into another SIEM.
- This can be a hindrance if an organization is contemplating on changing the SIEM vendor.
- If the organization uses multiple different SIEM vendors. This could happen during a vendor change or in a large MSSP with multiple platforms.

An open-source generic signature format called Sigma has been developed to help with these issues. Main goal of the Sigma project was to develop a structured open-source way for researchers or analysts to share and present the detection methods they have developed. (Sigma 2021)

A tool called Sigmac has been developed by the Sigma project. Sigmac allows the conversion of Sigma rules into the format of different SIEM vendors. Sigma rules are first written in accordance with the project's format and then converted with the converter as illustrated in Figure 7.

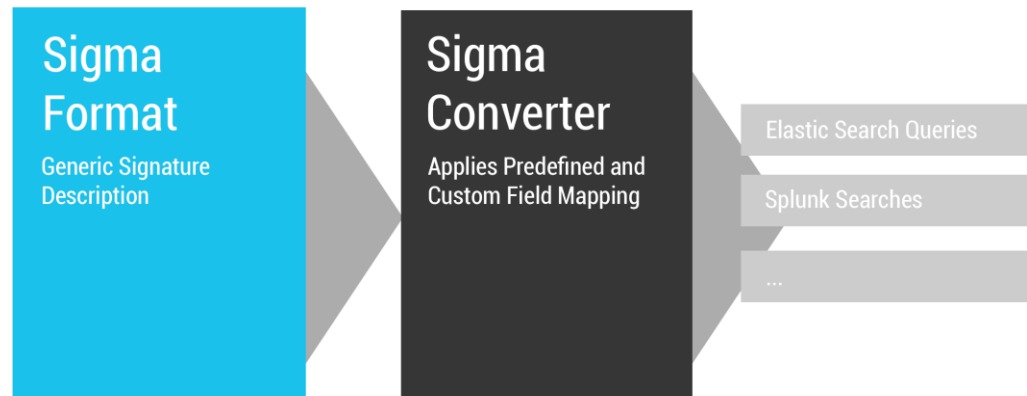


Figure 7. Converting Sigma rules.

Sigmac converter is programmed with Python and is available from the same GitHub repository as the Sigma rule. Sigmac converter supports 19 different platforms. List can be found in Appendix 1.

Sigma example

Sigma rules can be written by the user or ready-made Sigma rules can be used.

Figure 8 shows an example of a Sigma rule that can be downloaded from the Sigma repository at GitHub.

```

title: Clear PowerShell History
id: dfba4ce1-e0ea-495f-986e-97140f31af2d
status: experimental
description: Detects keywords that could indicate clearing PowerShell history
date: 2019/10/25
author: Ilyas Ochkov, oscd.community
references:
- https://gist.github.com/hook-s3c/7363a856c3cdbadeb71085147f042c1a
tags:
- attack.defense_evasion
- attack.t1146
logsource:
  product: windows
  service: powershell
detection:
  keywords:
  - 'del (Get-PSReadlineOption).HistorySavePath'
  - 'Set-PSReadlineOption -HistorySaveStyle SaveNothing'
  - 'Remove-Item (Get-PSReadlineOption).HistorySavePath'
  - 'rm (Get-PSReadlineOption).HistorySavePath'
  condition: keywords
falsepositives:
- some PS-scripts
level: medium

```

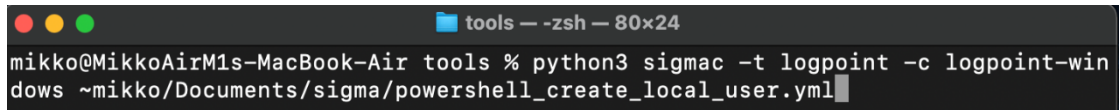
Figure 8. Sigma example for clearing the PowerShell History.

Information on how to write a Sigma rule can also be found from the wiki section in the GIT repository. All Sigma rules should start with a title and id section. The sections between id and log sources are optional. In the example the tags section describes what part of the ATT&CK framework does this rule detect. Tags section does not need to cover the ATT&CK framework. Optional information can be written in the section, but many rules found for example in GIT repositories are directly designed by the author to detect a threat falling into an ATT&CK category.

Because Sigma rules should be written in accordance with the instruction given on the GIT repository. This allows them to be translated through the Sigmac converter. The structured form of a Sigma rule also makes it easy to be read. This helps in sharing rules between developers even if no Sigmac converter is used. SIEM systems usually use a proprietary alert / query language that can be hard for the users of different systems to read.

6.5 Use of Sigmac

Sigmac can be used from the command line. The user must specify flags for the converter as demonstrated in Figure 9. In the example two flags are used, -t and -c flag.



```

tools — zsh — 80x24
mikko@MikkoAirM1s-MacBook-Air tools % python3 sigmac -t logpoint -c logpoint-windows ~mikko/Documents/sigma/powershell_create_local_user.yml

```

Figure 9. Use of Sigmac.

Full list of flags can be viewed from the documentation on GitHub or by giving the “-help” command. Minimum requirements are the -t flag that tells the target system followed by the path to the Sigma file that should be converted. With -c flag the user can specify a configuration file that can be used to give a more detailed conversion rule to the converter. Some target systems like the LogPoint does not require a configuration file but some example Splunk does require it.

The Sigma rule illustrated in Figure 8 can be converted with Sigmac converter into different forms giving the following examples. Figure 10 displays the rule in LogPoint format and Figure 11 in Splunk format.

```

("del (Get-PSReadlineOption).HistorySavePath" OR "Set-PSReadlineOption -HistorySaveStyle SaveNothing" OR "Remove-Item (Get-PSReadlineOption).HistorySavePath" OR "rm (Get-PSReadlineOption).HistorySavePath")

```

Figure 10. LogPoint rule done with Sigmac.

```
(source="WinEventLog:Microsoft-Windows-  
PowerShell/Operational" ("del (Get-  
PSReadlineOption).HistorySavePath" OR "Set-  
PSReadlineOption -HistorySaveStyle SaveNothing" OR  
"Remove-Item (Get-PSReadlineOption).HistorySavePath" OR  
"rm (Get-PSReadlineOption).HistorySavePath"))
```

Figure 11. Splunk rule done with Sigma.

Conversion into LogPoint format could be done without specifying a configuration file but the Splunk conversion required the use of splunk-windows configuration file. Even though this rule did not require the use of a configuration file for LogPoint conversion, it might be required if converting a non-windows or a non-standard Linux use case.

7 Implementation

7.1 Scope

To prevent escalating the project to be too big, a scope that defines the proof of concept (POC) had to be defined. The POC includes manual work phases and operations done through a software that has been done with Python and SQL. See Figure 12. Implementation plan for a visualization of the scope. Techniques and methods to be used were defined before any real work was started. Once the initial POC plan sounded feasible, then actual work was started.

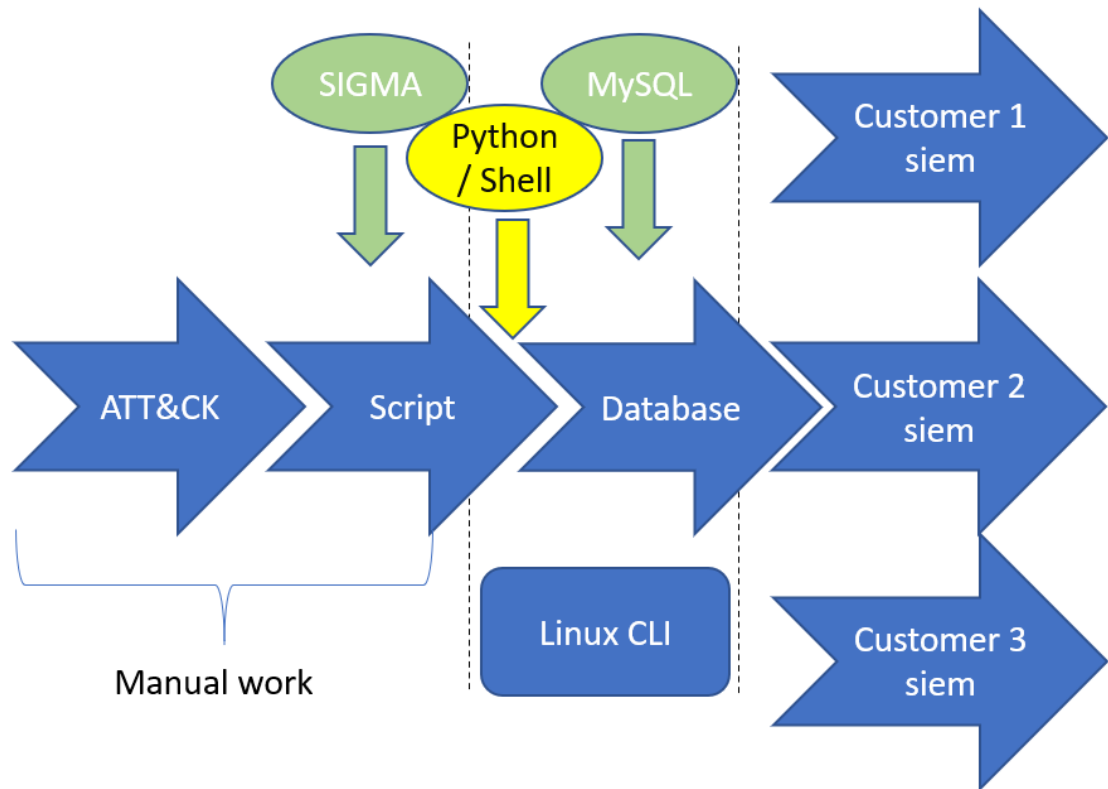


Figure 12. Implementation plan. Dashed lines represent airgaps.

7.2 Out of scope

Some features came into discussion already during the planning phase, but they were left out. Reason being that if the features would have been included then the scope would have grown to be too large and time consuming. These features can be added later if the original POC shows promise.

Features to be left out include:

- GUI – The goal is to provide a CLI based user interface. A further development is a HTML based interface that can be used in the local network.
- Extensive Use Case library – Collecting an extensive library of use case is time consuming. An extensive library is not needed, to prove the usability of this concept.
- API-integration – in the current concept there is an air gap between the SIEM systems and the Use Case library.
- User management – User authentication into the database allowing certain users to see only a limited amount of use cases.

7.3 Database

The initial idea was to use a database, but the scope of the database stayed unclear. It was not known that should the alert templates be stored in a database or should only some information be stored in the database.

At the start three different SQL options were discussed. MySQL, MariaDB and SQLite. It was felt that the selection of a well know platform would hasten the development and this fact guided into the direction of MySQL. SQLite also got support because it does not need additional infrastructure to be deployed. Issues regarding SQLite were raised during discussion:

- No prior experience.
- Unknown plugin / library support.
- Lack of user management.
- Full scope of the database implementation was unclear at this stage and SQLite was thought to be more suited for smaller scale projects.

SQLite has limited user management and it was discussed that a possible future development of the application could be the implementation of user management. This fact ultimately led to the rejection of SQLite.

MariaDB never rose to be a true candidate even though it was discussed. Lack of experience with MariaDB was the main driver against it. Also, MariaDB was deemed to be too similar to MySQL that no substantial benefit would be gotten out of using it.

MySQL was chosen because of its popularity in the community and familiarity to the team. Due to its popularity MySQL has a large user community. This popularity manifests as a large number of open-source libraries and plugins that can be integrated with MySQL, example being Python's MySQL Connector. MySQL is a full-fledged software platform with many features that can be taken into use if there is a need for example the support for user management.

MySQL development Environment

MySQL server was installed onto an Ubuntu server. MySQL server allows the construction of the database. To help with the design MySQL Workbench was installed to a Windows 10 workstation.

MySQL Workbench gives the developer a graphical user interface to allow for an easier design of the MySQL database. The workstation and the Ubuntu server were connected into the same network and this allows the workbench to push a new database schema directly into the MySQL database server. MySQL Workbench also allows the modification of an existing database with the push option. Tables, columns, and relations can be designed and altered in this way.

7.4 GIT Version control

During the development it became clear that storing the alert templates into the MySQL database would not be optimal. The storage of a long template where the template needs to stay intact proved to be problematic.

The decision was made to study the possibility of storing the template in a Git repository. Git is a distributed version control system that was originally developed by Linux Torvalds in 2005. (Atlassian 2021)

In Git's distributed version control system there is a remote repository server that contains the projects code. Each developer also downloads the code to their own work machines and start to work with the code downloaded to their machine. When the code is done then that developer does a pull request to merge his code into the remote repository server containing the master branch.

Git is the name of the technology and there are many different Git software providers. Popular Git platforms are GitHub, Bitbucket and GitLab. Because Git is a technology, the idea behind the different Git platforms stays the same. Differences come in the hosting options, licensing, user interface and even in the terminology as illustrated by Figure 13. (McNamee, H. 2016)



Comparing GitLab Terminology			
 Bitbucket	GitHub	 GitLab	So, what does it mean?
Pull Request	Pull Request	Merge Request	In GitLab a request to merge a feature branch into the official master is called a Merge Request.
Snippet	Gist	Snippet	Share snippets of code. Can be public, internal or private.
Repository	Repository	Project	In GitLab a Project is a container including the Git repository, discussions, attachments, project-specific settings, etc.
Teams	Organizations	Groups	In GitLab, you add projects to groups to allow for group-level management. Users can be added to groups and can manage group-wide notifications.

Figure 13. Terminology differences in Git platforms.

GitHub

GitHub is a cloud-based Git platform owned by Microsoft. GitHub is the market leader with a market share of 88% in Git source code management as illustrated by Figure 14. Because of its position as a large market leader and easy setup, GitHub was selected to be the Git provider for this POC. (Slintel 2021)

GitHub does not require any installations or setup except the registration of an account. After the registration, the user can immediately start to upload files to the Git repository (storage). The repository can be selected to be private or public depending on the nature of the development project.

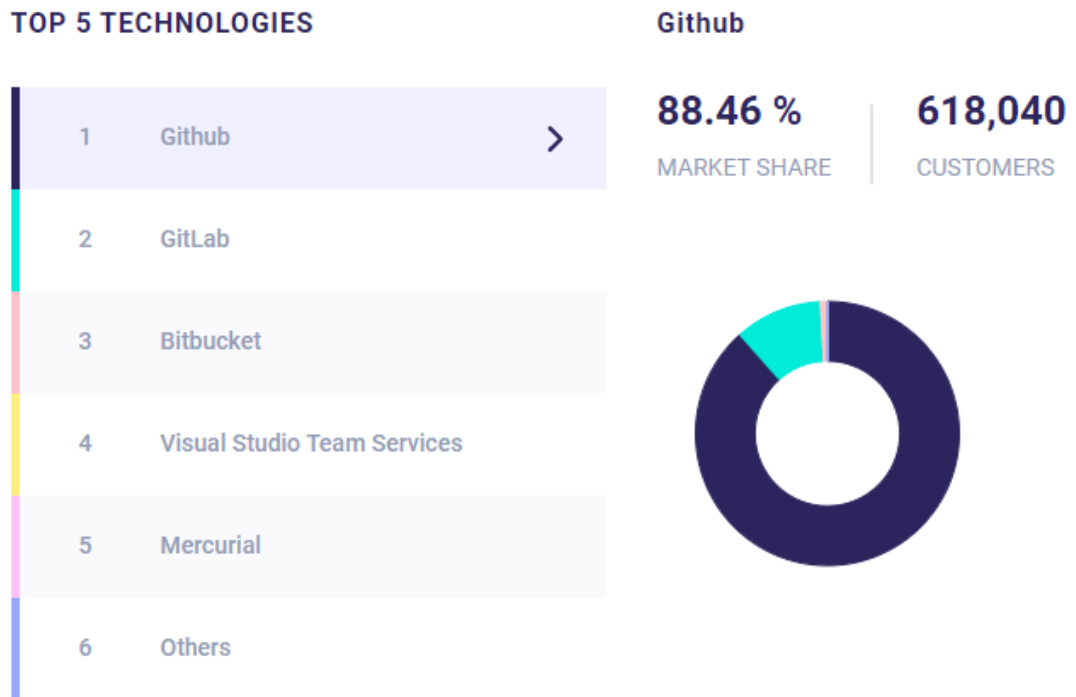


Figure 14. Git provider market shares.

7.5 Programming

The main programming language was selected to be Python. Python is a high-level programming language that does not need the use of a compiler. That makes python a good solution for scripting, also Sigmac converter has been done with Python so to avoid combability issues Python was the natural choice. (Python 2021)

There was no development environment in the start of the project, and everything had to be started from the beginning. This fact along with the Sigmac converter guided strongly to the selection of Python because it can easily be installed into a Linux machine and programming / scripting can be started with just the use of nano or vim.

Because python does not need to be compiled it allows the project to be started as separate script files that can be later brought together. Python 3 (3.8.2) was used to create the scripts in this work. Python 3 is the current version of Python.

Many of the instructions / documentations found are still in Python 2 format and this can cause problems because of the differences in the versions. Python 2 has reached End of Life status as of January 2020 and Python 2 is not compatible with Python 3. (Python 2020; Coghlan's Python Notes 2020)

Python also includes a standard package-management system called pip. Pip allows easy installation of python libraries and is maintained by the Python Packaging Authority. (PyPA 2020)

Libraries

Software libraries are ready-made set of functions, objects and modules that can be used in a software project. By using libraries, one quickens the development of a software project. Software libraries are used so that everything does not have to be started from the beginning. Usually, libraries concentrate around one specific operation. (GeeksforGeeks 2020)

MySQL Connector

MySQL Connector allows the connection and communication between a python application and a SQL database. The connector needs to be installed separately to the development machine and can be installed for example with pip. MySQL Connector is developed by Oracle. Oracle is also the developer of MySQL.

Connection into the SQL server must be made before typing any SQL commands. Minimum requirements are the importation of `mysql.connector` and the declaration of host, user, passwd (password) and database. Once these have been given then SQL-code can be embedded into the python script.

```

1  #!/usr/bin/env python
2  def AddCustomer():
3      print("")
4
5      import mysql.connector
6      from mysql.connector import Error
7
8      db = mysql.connector.connect(
9          host='localhost',
10         user='userXXX',
11         passwd='sadsad354asd!',
12         database='Test'
13     )
14
15     mycursor = db.cursor()
16
17     customer = input("Give the name of the customer: ")
18
19     sql = "INSERT INTO tbCustomers (customerName) values (%s)"
20     mycursor.execute(sql, (customer, ))
21     db.commit()
22
23     print("New customer added: ", customer)
24

```

Figure 15. Use of mysql.connector.

SQL-script can be placed inside a variable along with (%s) as illustrated in Figure 15.

The sign %s can be used to place user input inside the SQL-script. In Figure 15 the value of variable customer is placed into the INSERT statement. The variable is placed into the %s sign. SQL operations must end with the command db.commit() otherwise no commands will be carried to the SQL database.

GitPython

Git Python is a python library that allows the python project to communicate with git repositories. GitPython is compatible with GitHub. Usage of the GitPython starts by connecting into the Git repository. After the connection is made then additional interactions with GitHub can be made. Figure 16 shows an example where filename is supplied to the filu_sis variable and the file is then downloaded from the GitHub repository and printed into the console.

```
1 #!/usr/bin/env python
2
3 from github import Github
4 import base64
5
6 #Connecto to GitHub
7 g = Github("Username", "asffasbbs462")
8 for repo in g.get_user().get_repos():
9     print(repo.name)
10
11 #Get the contents and print it
12 filu_sis = repo.get_contents("WhoAmITest.yaml")
13 filu_data = base64.b64decode(filu_sis.content)
14 print (filu_data.decode('utf-8'))
15
```

Figure 16. Example of GitPython.

MySQL connector and GitPython operations can also be combined in a single python script. This allows content to be read out of the alert template located in GitHub and to store for example an id tag from the template into the SQL database. First part of the script is done with GitPython and the second part with the help of MySQL Connector.

8 Conclusions

During the POC a minimum viable product was built to demonstrate that is it viable to build a database for the administration of Sigma use cases. The use of Sigma format was wanted as an additional requirement for the project with the intended purpose of getting some familiarization into Sigma and to investigate its usability in a multi-vendor environment.

The POC was demonstrated to the cyber defence platforms team. Discussions and a survey were held about the concept after the demonstration. The survey received a limited number of answers. Therefore, no definite conclusion can be drawn based on the survey. Questions asked in the survey are presented in Appendix 2.

The thesis aimed to answer the following question:

What improvements can a database application bring to the implementation of SIEM use cases in an MSSP environment?

The implementation part of this thesis strived to answer the thesis question with the help of action research methodology. The iterative process used in action research methodology proved to be extra valuable due to the limited number of answers that was received in the end survey.

The strongest feedback was gathered during the biweekly control meetings and the application was developed according to the feedbacks received. This trend of oral feedback continued in the final presentation and is reflected in the survey's response quantity.

Many changes were done to the application during the development. The main force behind the changes in many cases was feedback that was received from the cyber defence development team. Feedback and the changes concerned both architecture of the application and its usability.

In a less flexible development method the problems would not have surfaced before the end presentation. The iterative process that is used in the action research methodology allowed the project to "live" and change during the development. At times there was a need to remind feedback givers of the scope of the project, due to their eagerness to describe future features that were clearly out of the scope of the project.

9 Discussion

The POC demonstration consisted of a demo on how to produce use cases in Sigma format and how to manage the Sigma files with the help of the database application. Sigmac converter was integrated into the database application with Python. This allowed Sigma format conversion to be run straight from the database application.

Sigma format and a demonstration on how to write use cases was showcased during the presentation. Feedback on Sigma was positive, and it was stated that Sigma should be taken into use, in the description of alert use cases.

The team felt that the best feature of the Sigma format is the easy readability of the format. This can also be seen in the survey results even though the survey received a limited number of answers. The answers are presented in Appendix 3.

The open-source community support was thought to be a benefit due to the availability of material, but it was also seen as a possible negative feature. Sigma use cases found from the internet should be taken with a grain of salt. Testing and critical review of the use case must be done before it is taken into production use.

The possibility of converting Sigma files into multiple formats was felt to be a significant benefit but it was felt to be more important to try to keep the customer SIEM base unified behind a single vendor. Sigma however gives the ability to integrate multiple SIEM vendors into the MSSP's systems or the ability to more flexibly change SIEM vendors, should there be a need.

Feedback of the database application concerned mostly the future direction of development. Improved database usability was raised as the most wanted future development direction both in the discussions and the survey.

Current "air-gaps" in the application should be removed and the command line interface developed so that it allows for a smoother uninterrupted flow of work. Only one of the survey responders wished for a graphical user interface, as seen in the results of the survey in Appendix 3.

The current database architecture did not get significant attention. No major flaws were noted in it by the development team. The architecture supports future modifications if there should be a need. Also, the tools used in the development (Python3, MySQL and Git) were felt to be the correct ones. They have support from the community, and they have no major limitations that could cause problems in the future.

Other categories for the use case classification were wished. The addition of product-based categories was raised as a future development subject that could be implemented quickly. This would allow queries to show use cases targeting only a certain product for example use cases concerning F5 Load Balancer. These product-

based categories can also be combined with the existing ATT&CK based use case categories.

References

Amin, R. Cloppert, M. & Hutchins, E. 2011. *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*. Lockheed Martin Corporation

Applebaum, A. 2019. *Getting Started with ATT&CK: Assessments and Engineering*. Accessed on 10.06.2020. Retrieved from <https://medium.com/mitre-attack/getting-started-with-attack-assessment-cc0b01769cb4>

Atlassian. 2021. What is Git. Accessed 13.02.2021. Retrieved from <https://www.atlassian.com/git/tutorials/what-is-git>

Carbon Black. 2020. *WHAT IS AN ADVANCED PERSISTENT THREAT (APT)?* Accessed on 10.06.2020. Retrieved from <https://www.carbonblack.com/resources/definitions/what-is-advanced-persistent-threat/>

Cynet. 2020. *Advanced Persistent Threat (APT) Attacks*. Accessed on 10.06.2020. Retrieved from <https://www.cynet.com/cyber-attacks/advanced-persistent-threat-apt-attacks/>

Federal Bureau of Investigation. 2014. Five Chinese Military Hackers Charged. Accessed 14.02.2021. Retrieved from <https://www.fbi.gov/news/stories/five-chinese-military-hackers-charged-with-cyber-espionage-against-us>

Federal Bureau of Investigation. 2021. PARK JIN HYOK. Accessed 14.02.2021. Retrieved from <https://www.fbi.gov/wanted/cyber/park-jin-hyok>

Finkle, J. Menn, J. & Viswanatha, A. 2014. U.S. accuses China of cyber spying on American companies. Accessed 14.02.2021. Retrieved from <https://www.reuters.com/article/us-cybercrime-usa-china-idUSKCN0J42M520141120>

FireEye. 2020. M-Trends 2020: Insights From the Front Lines. Accessed 14.02.2021. Retrieved from <https://www.fireeye.com/blog/threat-research/2020/02/mtrends-2020-insights-from-the-front-lines.html>

FireEye. 2021. Advanced Persistent Threat Groups. Accessed 14.02.2021. Retrieved from <https://www.fireeye.com/current-threats/apt-groups.html>

Fortinet. 2019. Fortinet Cybersecurity Solutions for Managed Security Service Providers. Accessed on 09.06.2020. Retrieved from <https://www.fortinet.com/content/dam/fortinet/assets/white-papers/wp-fortinet-mssp-cybersecurity-solutions.pdf>

Francis, A. 2019. Top 5 Challenges in Providing Managed Security. Accessed 21.02.2021. Retrieved from <https://www.channelfutures.com/mssp-insider/top-5-challenges-in-providing-managed-security>

- GeeksforGeeks. 2020. Software Framework vs Library. Accessed 13.02.2021. Retrieved from <https://www.geeksforgeeks.org/software-framework-vs-library/>
- Goodin, D. 2014. Accessed 14.02.2021. Retrieved from <https://arstechnica.com/information-technology/2015/02/how-omnipotent-hackers-tied-to-the-nsa-hid-for-14-years-and-were-found-at-last/>
- Greenert, J & Welsh, M. 2013. *Breaking the Kill Chain*. Accessed on 09.06.2020. Retrieved from <https://foreignpolicy.com/2013/05/17/breaking-the-kill-chain/>
- Kaspersky. 2020. *What Is an Advanced Persistent Threat (APT)?* Accessed on 10.06.2020. Retrieved from <https://www.kaspersky.com/resource-center/definitions/advanced-persistent-threats>
- Kaspersky. 2021. 5 Warning Signs of Advanced Persistent Threat and How to Prevent Advanced Persistent Threats. Accessed 14.02.2021. Retrieved from <https://www.kaspersky.com/resource-center/threats/advanced-persistent-threat>
- LogPoint. 2020. *What is MSSP (Managed Security Service Provider)?* Accessed on 09.06.2020. Retrieved from <https://www.logpoint.com/en/partners/what-is-an-mssp-and-why-choose-one/>
- LogPoint. 2020. What is SIEM. Accessed on 09.02.2021. Retrieved from <https://www.logpoint.com/en/understand/what-is-siem/>
- Mandiant. 2014. APT1 Exposing One of China's Cyber Espionage Units. Accessed 14.02.2021. Retrieved from <https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf>
- Matteson, S. 2019. To stay competitive, MSSPs need to grow and evolve. Accessed on 09.06.2020. Retrieved from <https://www.techrepublic.com/article/to-stay-competitive-mssps-need-to-grow-and-evolve/>
- McGregor, C. 2018. Using Constructive Research to Structure the Path to Transdisciplinary Innovation and Its Application for Precision Public Health with Big Data Analytics. Accessed 21.02.2021. Retrieved from <https://timreview.ca/article/1174>
- McNamee H. Comparing Confusing Terms in GitHub, Bitbucket, and GitLab. Accessed 13.02.2021. Retrieved from <https://about.gitlab.com/blog/2016/01/27/comparing-terms-gitlab-github-bitbucket/>
- MITRE. 2019. *Hidden Window*. Accessed on 10.06.2020. Retrieved from <https://attack.mitre.org/techniques/T1143/>
- MITRE. 2021. ATT&CK for Enterprise Introduction. Accessed 11.02.2021. Retrieved from <https://attack.mitre.org/resources/enterprise-introduction/>
- MITRE. 2021. Corporate Overview. Accessed 11.02.2021. Retrieved from <https://www.mitre.org/about/corporate-overview>
- MITRE. 2021. Frequently Asked Questions. Accessed 11.02.2021. Retrieved from <https://attack.mitre.org/resources/faq/>

Muncaster, P. 2020. Iranian APT Group Targets Global Universities Again. Accessed 14.02.2021. Retrieved from <https://www.infosecurity-magazine.com/news/iranian-apt-group-targets-global/>

Nick Coghlan's Python Notes. 2020. Python 3 Q & A. Accessed on 13.07.2020. Retrieved from http://python-notes.curiousericiency.org/en/latest/python3/questions_and_answers.html

Paganini, P. 2019. Iran-linked group Cobalt Dickens hit over 60 universities worldwide. Accessed 14.02.2021. Retrieved from <https://securityaffairs.co/wordpress/91157/apt/cobalt-dickens-targets-universities.html>

Peterson, A. 2014. The Sony Pictures hack, explained Accessed 14.02.2021. Retrieved from <https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/>

PyPA. 2020. Python Packaging Authority. Accessed on 13.07.2020. Retrieved from <https://www.pypa.io/en/latest/>

Python. 2020. PEP 373 -- Python 2.7 Release Schedule. Accessed on 13.07.2020. Retrieved from <https://www.python.org/dev/peps/pep-0373/>

Python. 2021. What is Python? Executive Summary. Accessed 11.02.2021. Retrieved from <https://www.python.org/doc/essays/blurb/>

Sans. 2019. *Applying Security Awareness to the Cyber Kill Chain*. Accessed on 09.06.2020. Retrieved from <https://www.sans.org/security-awareness-training/blog/applying-security-awareness-cyber-kill-chain>

Satter, R & Stubbs, J. 2020. Vietnam-linked hackers targeted Chinese government over coronavirus response: researchers. Accessed 22.02.2021. Retrieved from <https://www.reuters.com/article/us-health-coronavirus-cyber-vietnam-idUSKCN2241C8>

Sigma. 2021. Accessed 11.02.2021. Retrieved from <https://github.com/Neo23x0/sigma>

Slintel. 2021. Accessed 13.02.2021. Retrieved from <https://www.slintel.com/tech/source-code-management>

Storm, B. 2018. *Cyber Threat Intelligence: Post by Blake Strom*. Accessed on 10.06.2020. Retrieved from <https://www.mitre.org/capabilities/cybersecurity/overview/cybersecurity-blog/attck-101>

StratoZen. 2019. What is a SIEM and why do I need it?. Accessed 08.02.2020. Retrieved from <https://stratozen.com/what-is-siem-and-why-do-i-need-it/>

Sumo logic. 2021. SIEM vs Log Management: Capabilities and Features. Accessed 14.02.2021. Retrieved from <https://www.sumologic.com/glossary/siem-log/>

The United States Department of Justice. 2018. Nine Iranians Charged With Conducting Massive Cyber Theft Campaign on Behalf of the Islamic Revolutionary Guard Corps. Accessed 14.02.2021. Retrieved from <https://www.justice.gov/opa/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic-revolutionary>

Appendices

Appendix 1. Supported targets for Sigma.

Splunk (plainqueries and dashboards)
ElasticSearch Query Strings
ElasticSearch Query DSL
Kibana
Elastic X-Pack Watcher
Logpoint
Microsoft Defender Advanced Threat Protection (MDATP)
Azure Sentinel / Azure Log Analytics
Sumologic
ArcSight
QRadar
Qualys
RSA NetWitness
PowerShell
Grep with Perl-compatible regular expression support
LimaCharlie
ee-outliers
Structured Threat Information Expression (STIX)
uberAgent ESA

Survey about Sigma and database application

Answer to all questions

*Pakollinen

What do you think is the most important feature with Sigma?

- Easy to read.
- Can be converted to multiple formats.
- Community support (Ready made rules easy to find).
- Muu: _____

Should Sigma be used even if there is just one SIEM vendor in use?

- Yes
- No / don't see any reason

Why yes / no? *

Oma vastauksesi _____

What are the negative features of Sigma?

Oma vastauksesi _____

Open feedback concerning Sigma.

Oma vastauksesi _____

Which future feature should be prioritised first?

- Improve database usability.
- Add API support
- Build a graphical user interface
- Improve conversion support for multiple SIEM vendors
- Muu: _____

What data should be added into the database (columns / tables)?

Oma vastauksesi _____

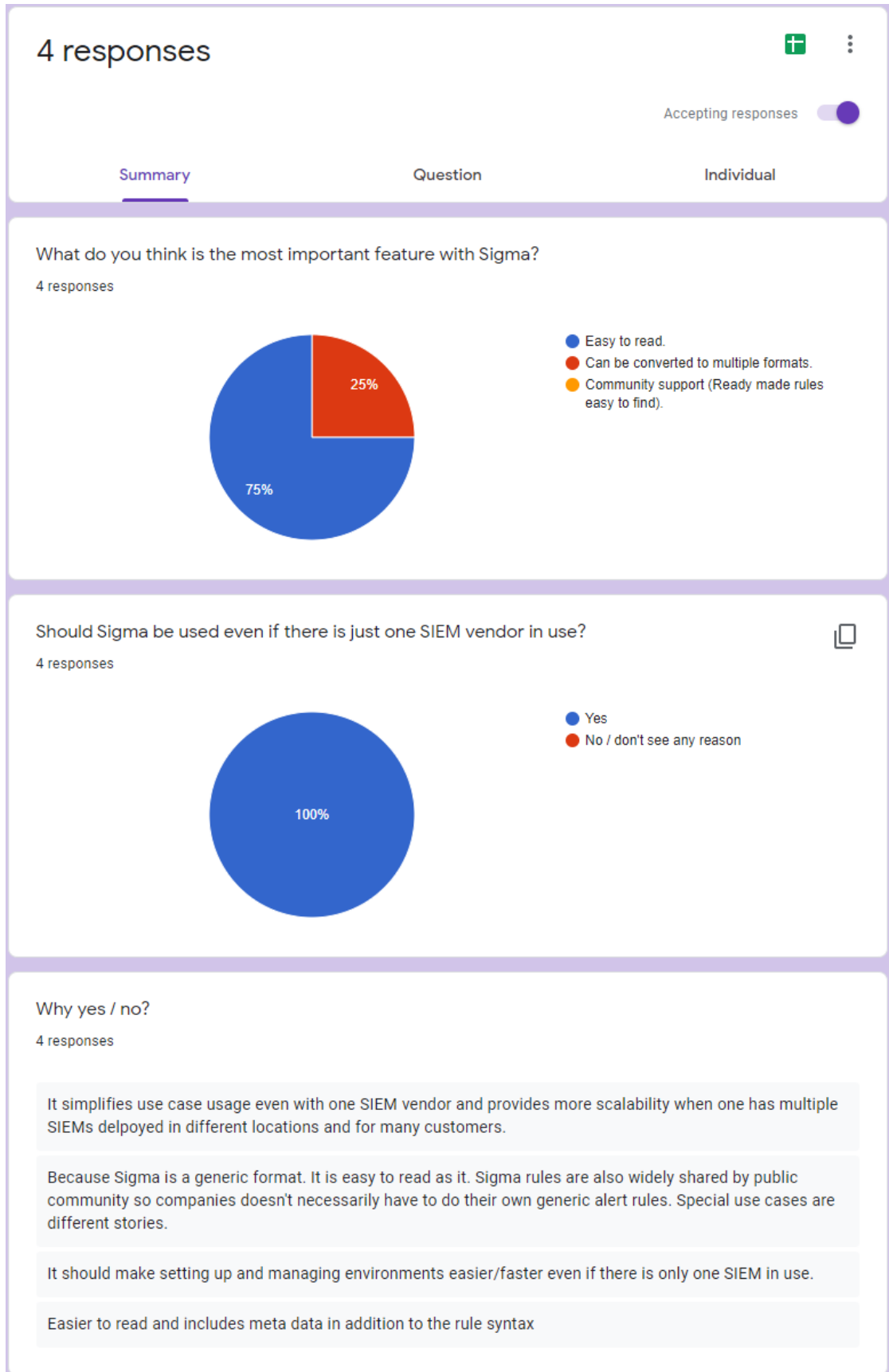
Categories were based on Mitre ATT&CK. What other categories would you want to see? Select the most important in your opinion.

- Based on SIEM environments Lifecycle (Example new project)
- Categories based on product. (F5 Load Balancer, Ironport, etc)
- Customer type (Government, bank, Factory, etc)
- APT groups
- Muu: _____

Database has been developed with Python3 and MySQL. Open feedback concerning Python3 / MySQL

Oma vastauksesi _____

Appendix 3. Results of the survey



What are the negative features of Sigma?

3 responses

Open-source and community projects usually do not have the same resources for development as commercial solutions, but both have their ups and downs.

Some of the Sigma rules that are compiled using the compiler may not work "out-of-the-box". The naming of the fields might not match so there will be some manual tuning needed.

Not of Sigma itself, but the quality and style of openly available Sigma rules vary greatly

Open feedback concerning Sigma.

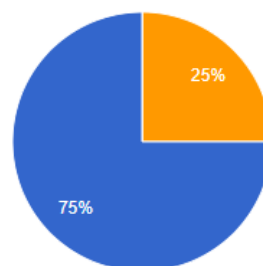
2 responses

It's great that these kind of open and community driven things happen from which everyone can benefit.

Looks very easy to use and understand even for someone who is not very familiar with the format. It also just seems quite useful in general if used properly.

Which future feature should be prioritised first?

4 responses



- Improve database usability.
- Add API support
- Build a graphical user interface
- Improve conversion support for multiple SIEM vendors

What data should be added into the database (columns / tables)?

3 responses

Not sure, would need more time spent on going through the design and other architectural things to consider about.

I think the database needs some further development so that the user doesn't have to do that much manual copying and pasting. The database could list all the available options for that specific operation. For example if we want to compile a rule, it could automatically list all the available .yaml rules in the console and then the user will select the rule he/she wants to compile simply by selecting the value (like 1). -> After selecting the rule, it should list all the available target formats that are supported and then the user selects which target system he/she wants.

Should be sufficient to only hold in database the information about what is in use and where. Could also include time stamps for enabling/disabling/changing for auditing purposes.

What data should be added into the database (columns / tables)?

3 responses

Not sure, would need more time spent on going through the design and other architectural things to consider about.

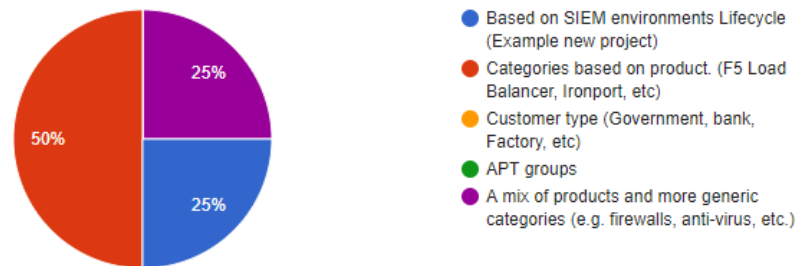
I think the database needs some further development so that the user doesn't have to do that much manual copying and pasting. The database could list all the available options for that specific operation. For example if we want to compile a rule, it could automatically list all the available .yaml rules in the console and then the user will select the rule he/she wants to compile simply by selecting the value (like 1). -> After selecting the rule, it should list all the available target formats that are supported and then the user selects which target system he/she wants.

Should be sufficient to only hold in database the information about what is in use and where. Could also include time stamps for enabling/disabling/changing for auditing purposes.

Categories were based on Mitre ATT&CK. What other categories would you want to see?

Select the most important in your opinion.

4 responses



Database has been developed with Python3 and MySQL. Open feedback concerning Python3 / MySQL

2 responses

Do both or especially MySQL support future expansion of the development or should other programming language or database used in the future.

I think python and MySQL are the correct choices for this database.