Luke Torri

MICROSOFT SENTINEL DEPLOYMENT AND EVALUATION

Bachelor's Thesis

Bachelor of Engineering

Information Technology

2022

South-Eastern Finland
University of Applied Sciences

South-Eastern Finland University of Applied Sciences

Degree title	Bachelor of Engineering
Author (authors)	Luke Torri
Thesis title	Microsoft Sentinel deployment and evaluation
Commissioned by	Marskidata Oy
Time	2022
Pages	41 pages, 0 pages of appendices
Supervisor	Matti Juutilainen

ABSTRACT

This thesis was a research and implementation of Microsoft Sentinel a cloud-based security information event management tool. An opportunity for the thesis work came from a company called Marskidata where Microsoft products were heavily used, but Sentinel was still unknown. My goals were to demonstrate how to implement Microsoft Sentinel to an existing company environment, and to evaluate how useful Sentinel is, and in what situations.

All the work was done in Marskidata Azure cloud environment. The first implementation of Sentinel was done in my own demo 365 Office environment, and after learning and studying Sentinel there, a fully functional version was configured to a working Marskidata cloud environment. Documentation was done as I learned new skills and concepts on the way. Microsoft Sentinel is relatively easy to deploy to an existing Azure cloud environment. All the surface level and default tools are simple to understand and use, but the actual hunting and incident response work begins to get complicated for an unexperienced user. Microsoft Sentinel turned out to be an excellent tool for responding to new to threats.

Sentinel is not for every network or organization; it is hard to use, and it is relatively costly. I wanted to get an idea of where Sentinel suits the best, in what size and type of organization. Generally bigger the environment, the more value Sentinel brings with some exceptions.

Keywords: Microsoft, SIEM, information security, cloud

CONTENTS

GLOSSARY

Term	Definition
Virtual private network (VPN)	An encrypted connection to a remote network.
NT Authority\ System	Highest privileged access on a windows machine.
IP address	Internet protocol address used to identify machines across networks.
Command-line interface (CLI)	Used to insert commands onto a system from a user in the form of lines of text.
Hypertext Transfer Protocol (HTTP)	Main protocol to communicate between web browsers and web servers.
Uniform Recourse Locator (URL)	Mechanism used by browser to retrieve any published information.
SMB protocol	Used to share files and recourses on a network.
Zero-day	A vulnerability that is currently wild and in action without a patch.
Python	Is an interpreted, object-oriented, high-level programming language with dynamic semantics.
Kernel	A core of an operating system with full control over it.
Firewall	A firewall is a system that helps protect a computer or network from unauthorized access.
Anti-virus	An anti-virus is a computer program that is designed to protect a computer against viruses and malicious software.

1 INTRODUCTION

The decision to write my thesis about Microsoft Sentinel came from my own interest in cyber-security and a great opportunity at Marskidata company. Sentinel is still unknown territory and research is needed. Cyber threats are developing fast and new threats rise every day. Large networks need fast and agile responses to counter these threats. It is not enough to install a simple antivirus to sit back and relax.

The thesis consists of two main goals. First was to demonstrate deployment of Microsoft Sentinel in a functioning business environment with existing data connections. The deployment and functionality part are made in a how-to-guide sense. Second was to review Sentinel capabilities and security information value and use the working version to counter and respond to modern threats. This is done by critically evaluating the cost versus efficiency of Sentinel and using Sentinels hunting capabilities to counter threats. There is an huge amount of information security tools to protect assets and one of my intentions was to find where Microsoft Sentinel or SIEMs in general play their role.

The whole thesis process was done and documented by self-learning Microsoft Sentinel step-by-step and discovering topics along the way. I have a good understanding of Azure cloud environment, Microsoft Defender, and Microsoft Purview. Defender and Purview are Office 365 apps to protect one’s cloud, network, and sensitive information. Microsoft Sentinel is a natural step further for me on the Microsoft information security field.

2 THEORY

The theory section starts with a discussion of basic cyber-security concepts, and from there gradually moving on to more complicated topics. Not everything from Information security can be explained, so I have prioritized subjects that I feel are the most important to understanding Microsoft Sentinel and the subjects discussed later.

Most of the research was done by using Microsoft services. Microsoft Docs and learn were heavily used to find information and tutorials. You can find information about SIEMs in many different places, but specifically about Microsoft sentinel the only trusted source is Microsoft Docs and the official Sentinel GitHub page. Finding the latest threats, one must keep a close eye to some cybersecurity information channel like kyberturvallisuuskeskus.fi.

2.1 Information security, modern attacks, and threats

Let's start by comparing some key concepts about information security to physical world and look at what kind of threats we face nowadays. Attack vector is a pathway or method which through harmful actions is conducted to a defending system. Unlocked backdoor to your home or network route with misconfigured firewall could be an attack vector. Defending system can be anything, one computer with an external server or a private company network with 100 devices.

Threats are possible harmful events or misconfigurations in your defending system. A missing key to your home or compromised user in a company network is a threat. Vulnerabilities and exploits are the means used by bad actors to cause threats though attack vectors. Vulnerability can be an old and weak lock to your storage which a thief could picklock, or outdated software used by company which can be exploited to gain remote access to sensitive information. Exploits are specially crafted applications or functions using vulnerabilities.

It is important for everyone not just cyber security professionals, to understand what kind of attacks are happening nowadays. Mitre CVE is a catalog of all publicly disclosed cyber security vulnerabilities. When vulnerabilities are discovered partner publishers and organizations around the world publish them to CVE catalog. Point is to ensure the best coordination and efforts to prioritize vulnerability mitigation (Mitre, 2017).

Every vulnerability is categorized by CVE-YEAR-Unique ID in CVE catalog. CVE-2022-30190 Microsoft Windows Support Diagnostic Tool (MSDT). Using

a weakness in MSDT attacker could run custom code and execute PowerShell commands with privileges of the program used. In a worst-case scenario bad actor could gain access to target computer just by the victim clicking a word document with the exploit executed with it. Microsoft Word uses MSDT, which causes it to be a potential attack vector. Patch has been issued by Microsoft on 14.6.2022 update and it's not a threat anymore to up to date systems (MSRC, 2022b).

Vulnerabilities and exploits are discovered all the time everywhere. That's why we simply can't trust software or hardware to protect our systems. We need security methods such as zero trust and principle of least privilege. In a zero-trust environment defending system is designed to trust no one and assume breach all the time. This can be enforced by network segmentation, access control or monitoring internal networks and systems for suspicious activity such as enumeration and privilege escalation.

When a bad actor gains access for example through click of a word document, the first action is to enumerate a target. An attacker scans and looks ways to escalate their privileges and access using vulnerabilities and exploits. Enforcing a principle of least privilege by giving users as minimum access as possible for their required duties, we make it harder for an attacker to find ways of gaining more access and thus protecting valuable assets.

In general, there is a lot more to discuss, such as CIA triad, defense in dept, phishing, social engineering, malware, or ransomware. I don't want to focus too much on general concepts or ideas. The goal for this thesis is not to teach everything about information security, just the concepts mostly used with Microsoft Sentinel.

2.2 Cloud environment and Azure portal

Why use a cloud environment and what are the advantages? Azure cloud environment is a platform as a service (PaaS). It means users have complete deployment and development capabilities in the cloud to create everything

from simple apps to enterprise applications. A simple app can be a virtual machine or enterprise application a security information event management (SIEM). Idea is to support scalability and reliability (Lyon, 2019b).

Azure portal is a centralized tool to manage everything from web apps to cloud deployment. Users can create customized dashboards for all kinds of data and resources. Microsoft Sentinel is a dashboard with many kinds of functions and tools (Lyon, 2022a).

When working with Azure portal there are different tiers of management. This is important when working in large environments, administrators can group and label resources, apps and cloud deployments. Working with Microsoft Sentinel most interactions happen in the resource group and resource tier of management. Before going any further on Microsoft Sentinel, it is beneficial to understand the hierarchy and connections in Azure portal as shown in Figure 1.

Figure 1. Hierarchy of management tiers (Lyon, 2021c).

Starting from the bottom, resources are for example cloud applications or virtual machines. Sentinel is a resource that displays specially crafted information from other resources or external connections. Resource group is a container for all related recourses in a solution or only for those a user wants

to manage. Group resources with same lifecycle and what makes most sense in given organization (Gao, 2022).

Subscription is the management tier that holds all the licenses to your Microsoft services. It's an agreement with Microsoft to use services and resources, it charges per resource used or on cloud base resource consumption. Organizations can have multiple subscriptions running same time with different services. Subscription administrators assign permissions to use certain resources for example Azure portal subscription to use and deploy Microsoft sentinel. Administrators don't need to have own licenses to assign them, and they should not. It is good practice to separate administrators from users in case of breach and to protect from privilege escalation (Vice, 2022).

Management groups are for handling multiple Azure subscriptions for large environments. Subscriptions can be organized into management groups for efficient policy and governance assignments. All subscriptions in a management group must be under single tenant. As an example, policy to only deploy virtual machines to north Europe region can be done with in managements group. If this policy is applied it affects all subscriptions, resource groups and recourses under that management group (Warner, 2022).

Finally, a look at what is a tenant. Single dedicated and trusted representee for an organization, identity, or a person. Tenant is automatically created when first signing up for any Microsoft cloud services. Organizations can create more tenants, but one tenant can only have one Azure active directory. When looking at Figure 1 a tenant is the entity above all, and everything below trusts only that one tenant (Kumar, 2022).

2.3 SIEM

Security information and event management (SIEM) is combination of two separate security systems SIM (security information management) and SEM (security event management). SIEM takes the functions of SIM and SEM into

one management system. Basic function of SIEM is data collection and analyzation. More advanced SIEM systems include UEBA (user and entity behavior analytics) and SOAR (security orchestration, automation, and response). Microsoft Sentinel is a combination of SIEM and SOAR systems. Sentinel also offers UEBA services under Entity behavior menu, some additional charges may apply for UEBA usage.

Data collection is done by deploying many connection agents to gather security-related events from end-user devices, servers, network equipment, cloud applications and some specialized security equipment like firewalls, antiviruses or intrusion prevention systems (IPS). Data is forwarded to centralized management console, where security analyst can query data and find security incidents.

As an example, user account that makes 25 login attempts in 25 minutes would cause an alert. SIEM would categorize this low priority because most likely it was done by user who forgot it's password. User account that does 150 login attempts in 2 minutes would be categorized as high-priority incident. This type of behavior is most likely caused by brute-force attack. Brute-force attack refers to an attacking method where in this case passwords are guessed by every possible combination of characters or by usually using a wordlist of most common passwords.

SIEM is important for managing large amounts of security related data. Generally, it shortens the time it takes to find true positive alerts and filter false positive. True positive means that alert is triggered with real threat and false positive means that the alert is triggered but does not contain real threat. Additionally, since SIEM collects data across the whole IT infrastructure when attacks do happen a company can determine the cause, nature, route, and impact much more effectively. General downsides of SIEM are cost, difficult implementation and it requires some expert knowledge. Some SIEM systems are managed by a security operation center (SOC). SOC is an information security team to deal with organizations’ security events and issues.

Before going into Microsoft Sentinel, also investigate other software included in SIEM space. SPLUNK full on-premises SIEM system. IBM QRADAR can be deployed as a hardware, virtual or software appliance or as a cloud service SIEM product. LOGRHYTHM is a good SIEM for smaller organizations. EXA-BEAM offers many capabilities like UEBA. RSA NETWITNESS PLATFORM includes threat detection and data acquisition response tool, RSA is also a SOAR. Choosing a SIEM for organization depends on multiple factors. Budget and overall company security posture should be at least considered. When looking at specific SIEM product following capabilities should be looked for; compliance reporting, incident response, database and server access monitoring, internal and external threat monitoring, intrusion detection system (IDS) and IPS, threat intelligence and user activity monitoring (UAM) (Rosencrance, 2020).

2.4 Microsoft Sentinel and SOAR

Security orchestration, automation and response SOAR is the more complex part of Microsoft Sentinel. SOAR systems aim to respond and automate security related events. When data is collected and security incident alerted, SOAR triggers playbooks that automate a response or workflow. Figure 2 shows a visual representation of playbook function when detecting malware. Playbook retrieves the target data and analyzes, reports and updates databases.

Figure 2. SOAR playbook analysis lifecycle (Palo Alto Networks, n.d.).

A combination of machine and human learning is used to prioritize automated incident response actions. As a result, an effective and efficient way to handle cybersecurity problems is created. Playbooks are discussed and demonstrated more deeply in chapter 3.5.3 Automation rules and playbooks. By looking at what is happening in Figure 2 we can understand the basic function of SOAR systems (Palo Alto Networks, n.d.).

Microsoft Sentinel is a self-evident choice for organizations that use Azure and Office 365 platforms. As said previously, SIEMs are costly but when partnered with Microsoft 365 E5, A5, F5, and G5 customers get discounts and free data connections. Connections to other 365 products are easy and usually done with a single click.

Sentinel combines the SIEM and SOAR systems to one management console. Microsoft describes Sentinel as a bird’s-eye view of your organization’s information security. Sentinel collects data using built-in connectors or using common event format, Syslog or REST-API. To monitor one’s data in Microsoft Sentinel, use built-in workbook templates to display data in easily readable formats. Custom workbooks can be created to fully utilize given data. Using multiple connectors Sentinel will generate a lot of noise. This is reduced by using analytic rules and correlating alerts into incidents. Incident means multiple related alerts that indicate a possible threat. In Sentinel it is possible to map out an organization’s network activity using machine learning rules and start looking for anomalies across. When Sentinel starts to find anomalies and incidents, playbooks can be created to automatically to respond. Again, built-in playbooks exist and can be modified further to add custom logic. Playbooks work best with simple tasks and do not require coding knowledge.

Microsoft Sentinel allows hunting of security related threats. Hunting is based on Mitre framework and database. Idea is to find vulnerabilities before they cause incidents. When successfully done, these hunting queries can be added to detection rules to automate the process. To extend the capabilities of Sentinel, Jupyter notebooks can be used to create custom analytics, data visualization and data integrations. Notebooks are meant for advanced users and re-

quire a higher learning curve and coding knowledge. Microsoft Sentinel provides community collaboration in official GitHub repository at their website https://github.com/Azure/Azure-Sentinel. Custom workbooks, hunting queries, notebooks and playbooks are available for everyone's use (Levin, 2022b).

3 DEPLOYMENT, FUNCTIONS AND EVALUATION

Chapter 3 is the practical part of this thesis. It includes detailed instructions to deploy Microsoft Sentinel to a working company infrastructure with all necessary connections. An idea is to investigate most of the Sentinels functions starting from simple concepts like workbooks and gradually explore the harder concepts like threat hunting. Also, a more in depth look at certain vulnerabilities and exploits.

For the deployment process I first installed Sentinel on my own demo environment in which I got familiar with all the settings and functions. After that I was confident enough to deploy a working version on the Marskidata cloud environment and from there I started the documentation.

Most of the demonstration in the practical part is done with real events and incidents from Marskidata cloud environment. The original plan was to create simulated incidents, but Sentinel was generating enough incidents from the real data to investigate. To clarify, all incidents and alerts observed were false positives, and no real malicious activities were found.

3.1 Azure pricing, costs, and payments

All the data for an analysis and querying are stored in Microsoft Sentinel Log Analytics Workspace. Microsoft Sentinel bills for a data stored in a workspace and an amount of data analyzed or queried in Microsoft Sentinel. Data can be ingested in two types of forms, analytic logs, and basic logs. Analytic logs are flexible, support all types of data and offer full capabilities to query data. These are the logs that are monitored proactively using hunting and analytics

rules. Basic logs contain a mix of high volume and low security value data without all the capabilities of analytic logs. These logs are not frequently used and are accessed with normal methods 8 days, and after that when demanded. They are then archived and stored for a much lower price than an analytic logs.

When Sentinel is deployed, it comes with free 31-day trial period with 10 gigabytes of data ingestion. This discount is always subject to new workspaces no matter what the subscription is. After the trial, Sentinel costs 2,50 € per gigabyte ingested as pay-as-you-go pricing model. When handling huge amounts of data, customers can pay a fixed price per day to save money. As an example, 100 gigabytes per day, customers can pay a fixed price of 125 € and save half as they would in a pay-as-you-go model (Microsoft Azure, 2022).

3.2 Log Analytics workspace

When deploying Sentinel, a good practice is to create one's own workspace and not use some existing one. Start by selecting or creating an active Azure subscription. For that subscription, select an existing resource group or create a new one just for this workspace.

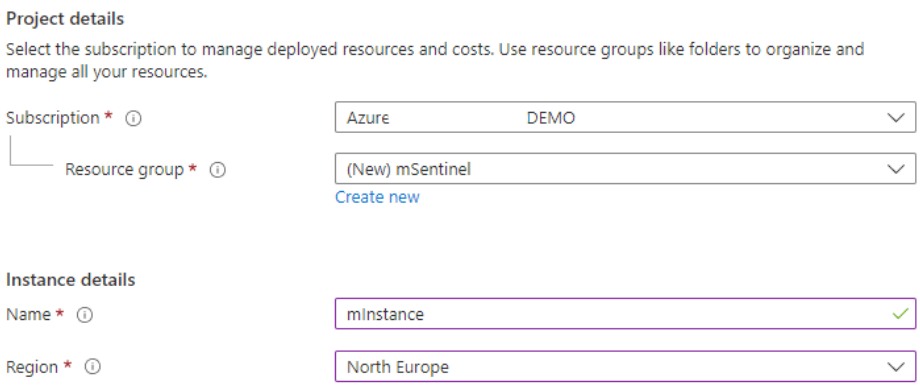

Figure 3. Workspace

When planning and creating a workspace consider a design criteria and strategy. Workspaces should be designed with efficiency and complexity in mind. If there are more resources in the same workspace as Sentinel, all the data in that workspace is subject to Sentinels pricing (Wild, 2022). If your organization

is paying a fixed price per mount, it might be beneficial to group multiple resources in the same workspace to achieve certain data ingestion for a discount. When a workspace has been created as in Figure 3, Microsoft Sentinel does not support moving the workspace to another subscription or resource group.

At this point of the deployment process tagging should be done, but it's not mandatory. When managing a large IT environment with a lot of infrastructure, tagging your resources can a be good practice. Figure 4 shows that the tags are like properties or values that you can assign to your resources.

Figure 4. Tags

Tags help to identifying correct assets when searching something specific and adds a layer of documentation. After a workspace is created and proper tags set, it's time to add it to Microsoft Sentinel. This process takes a few minutes.

3.3 Azure permissions

To enable Microsoft Sentinel, at least a contributor permission is needed in the Azure subscription. When using Sentinel an user needs contributor or reader permissions on the workspace where Sentinel is running. Other permissions might be needed when further connecting Sentinel to specific data sources (Levin, 2022a).

When assigning a permission or giving access to a resource or resource group an administrator is required to consider the principle of least privilege, by giving users access only to the resources they require to do their jobs. When a user does not need given privileges anymore, those extra rights should be taken away immediately. When access is given to users thoughtfully and carefully, it can limit or stop attackers from damaging the system. A same principle also applies when creating secure software. Only give adminis-

trator or root privileges when necessary and remove immediately when not required anymore (Gegick and Barnum, 2005). Common attack vector for privilege escalation is software with higher privilege level than necessary.

Administrators can deny user access to certain files like password hashes or local user lists. Using enumeration tactics an attacker that uses compromised user account can find software with elevated privileges. As an example, text editor VIM could have higher privileges than the user account and could have read permission to password hash file. Thus, attacker can open and read the restricted files using vulnerable software, in this case VIM.

3.4 Enable Microsoft Sentinel

Microsoft Sentinel does not provide anything itself. To enable Sentinel data connectors need to be configured. There are hundreds of connectors available, and it is administrator's duty to pick the most useful ones. For every bit of data there is a price tag, and one must prioritize for an optimal cost efficiency. When there are no data connections to other sources, there is really nothing a user can do with it as shown in Figure 5.

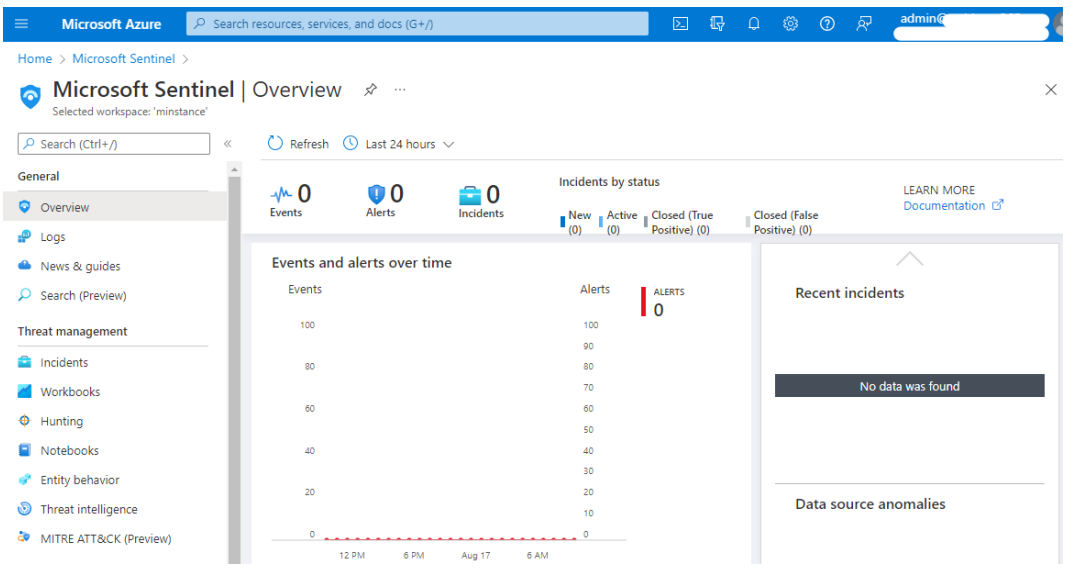

Figure 5. A blank Sentinel deployed by author.

On the left side there is a scroll down menu where we navigate through Sentinel. On the overview page is an overall picture of recent events and alerts. After connecting Sentinel to data sources and enabling analytics rules, this page starts showing the relevant information.

3.4.1 Data connectors

After active subscription, permission, resource group and workspace are configured next step is to enable data connectors. Found on the left side menu under configurations, users can find a list of all available connectors. Following data connectors are always free for Microsoft Sentinel users and should be enabled regardless of subscription plan. Offer includes Azure activity logs, Office 365 audit logs, Microsoft 365 Defender, Microsoft Defender for Cloud, Microsoft Defender for Office 365, Microsoft Defender for Identity, Microsoft Defender for Endpoint, and Microsoft Defender for Cloud Apps (Microsoft Azure, 2022).

Most of the connections are made with single click. Outside resources that are not included in the Azure -Microsoft platform might require specific installation wizards and some work to successfully configure. Connecting resources should not be done without a care and users should prioritize what data they want to ingest. Configuring every possible data connection that there is available might skyrocket the cost and not offer the security value one might be paying for. It is important to prioritize the most important data sources. When opening to the data connector page, users are prompted with over 100 default connections offered by Sentinel and more connection can be found from community resources.

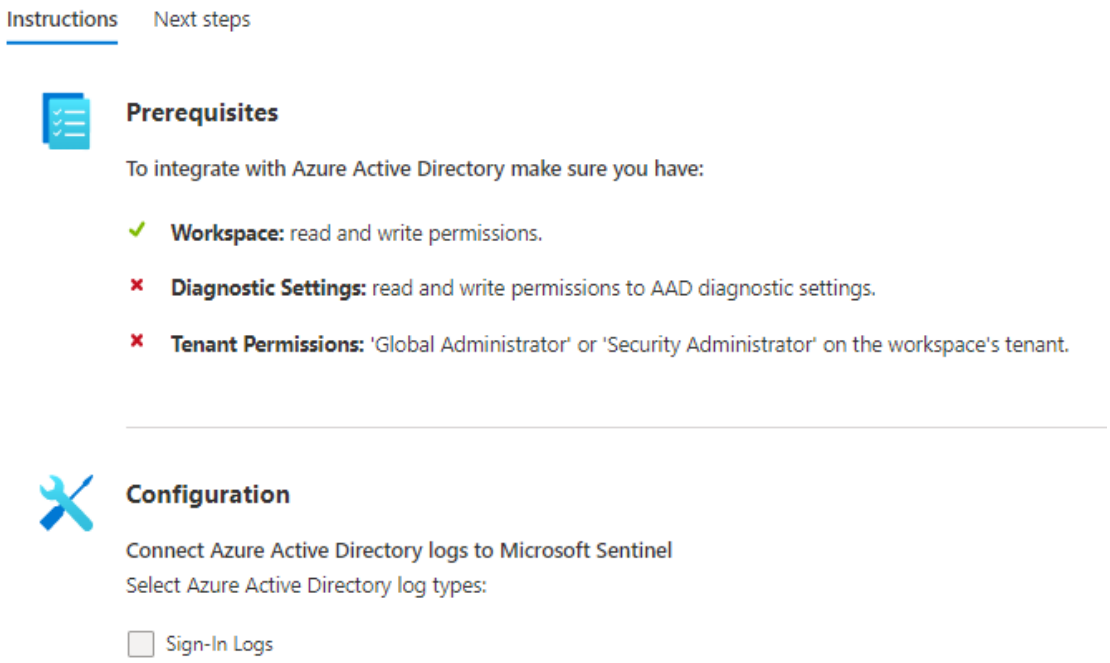

Figure 6. Data connection permissions and configuration.

Every data connector has a connector page and when opened user is prompted with a page like in Figure 6. Connectors have certain prerequisites and a configuration instruction. Prerequisites as a default require the user to have full administrator rights to the given data connection. As shown in Figure 6, my read and write permissions to Sentinel do not allow me to connect the Azure Active Directory. Below that is the guide to install your connector. If not configuring Microsoft resource, users can find more detailed instructions how to set up a connection. Most Microsoft connections are connected in the connector page by just clicking enable.

3.5 Functionality

To make Sentinel operational, it is not enough to make the data connections. Analytics rules need to be installed to generate alerts into incidents. Workbooks are a good tool to view data in a more user-friendly way. Microsoft Sentinel Cost workbook is a great example where users can view and evaluate current and estimated future pricing. Users need get familiar with KQL Kusto Query Language to be able to observe and investigate logs, and to modify analytics rule logic. For more advanced use there are notebooks and hunting that require some coding knowledge and deeper understanding of the current threat environment.

3.5.1 Workbooks and querying logs

After Sentinel is connected to data sources and data has been ingested, it is possible to start investigating even if there are no alerts or incidents. Ready-made workbook templates are a good starting point. Users can select workbooks best suited for the connections that were made. In Figure 7 there is Exchange Online workbook already saved, indicated by the green line.

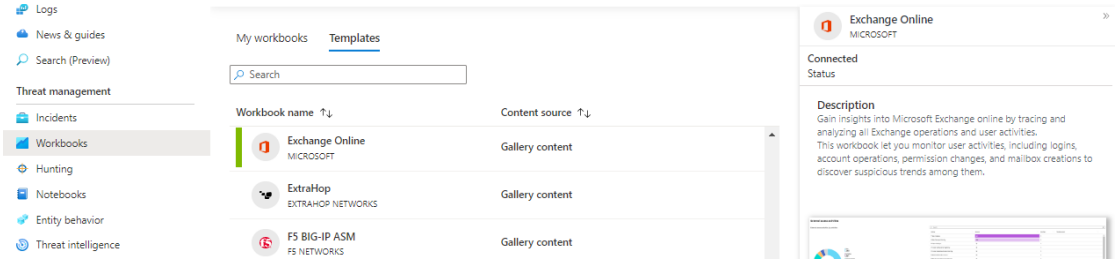

Figure 7. Workbooks page overview.

Custom workbooks can also be made, the best practice is to use readymade ones and customize from there. A main purpose is to get insight to activities and visualized data from data connections. Viewing a workbook template might give us many different graphs and formats to investigate. Figure 8 shows 208 suspicious activities. With a quick look most of them are normal actions done by Microsoft.Exchange.Servicehost. The actions were done with NT AUTHORITY\SYSTEM privileges which most likely caused suspicions.

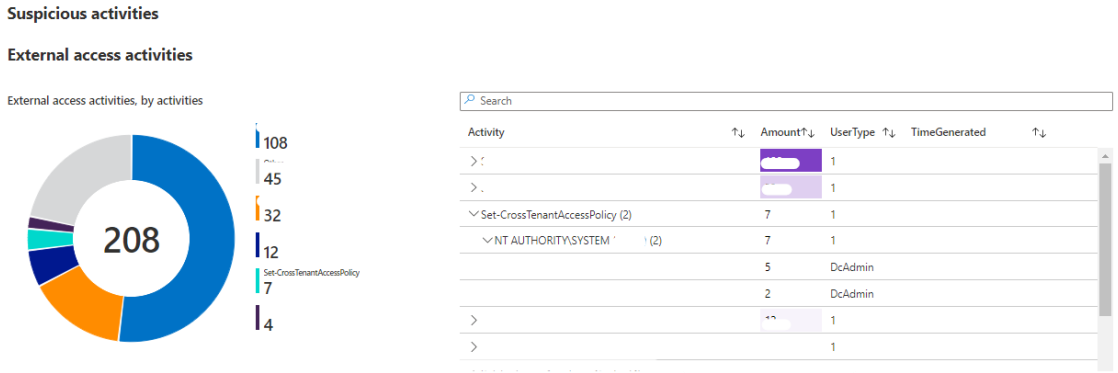

Figure 8. Suspicious activity at Exchange Online workbook.

From Figure 8 I have singled out an action Set-crossTenantAccessPolicy which was made by executable that have had in the past known vulnerabilities

and is also working with SYSTEM privileges. This workbook does not give us any further insightful information. To investigate these actions further, we can query Exchange Online data in the Logs section and find more information. Microsoft Sentinel uses Kusto Query Language (KQL) for querying log data. In my opinion KQL language is very easy to understand, the editor shown in the Figure 9 is beginner friendly and auto-suggests most of the needed values and parameters.

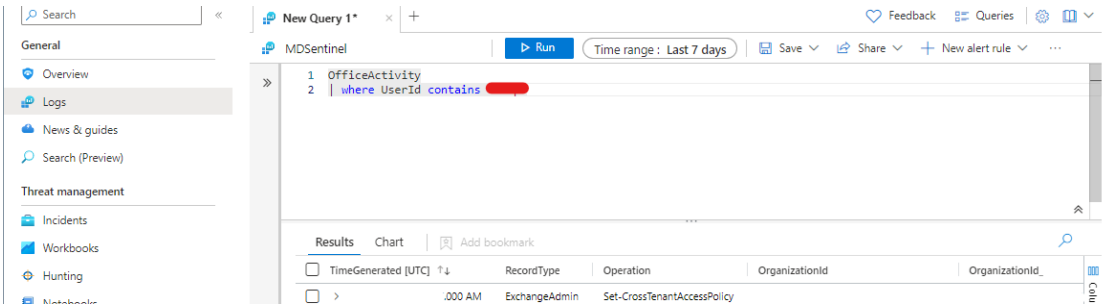

Figure 9. Simple query on the Logs page.

If a user has no previous coding experience, learning KQL is much harder. In Figure 9 I have written a simple query to find more information about the suspicious executable. First, we define the log space we need the information from. Exchange Online log data is under OfficeActivity. Giving the argument ***where UserId*** query looks for matching string in the column ***UserID***, the string is defined in ***contains "suspicious_executable_name"***. In this case same result can be achieved with ***where * has 'suspicious_executable_name'***. The argument **** has*** looks for any object, table, column, or value that contains the giving string. The second query goes through much more data and will take longer to execute but might return more relevant information. The first query only checks column ***UserId***, this query is faster and more precise if we only want results from a single column.

Every argument starts with ' **|** ' pipe operator and every query can have multiple arguments piped. KQL language filters given log data by these pipes starting from top to bottom. As a result, the order of the piped arguments matter and the outcome may differ depending on the order (Sagir, 2022).

3.5.2 Analytics rules and treat detection

To start discovering threats and anomalous behavior, create custom analytics rules in the analytics menu under configuration. Analytics rules are for searching specific events or multiple related event sets in the environment. When conditions specified in the rules are met, alert or incident is created and possibly automatically responded. Sentinel offers readymade rule templates that function on their own. These readymade templates can be modified to create custom rules for specific needs. Rules are constructed from rule logic, incident settings and automated response. A query is executed in a set period time for example every hour or ones in a day. It is advised to get familiar with KQL language before creating an own custom rule from rule templates.

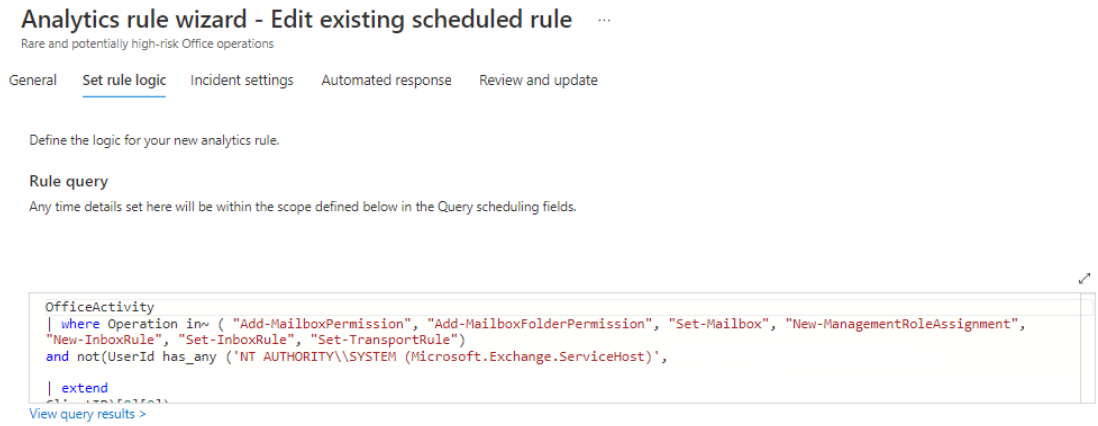

Figure 10. Rare and potentially high-risk office operations analytics rule wizard.

Figure 10 shows rule template with a pipe that finds operations done in OfficeActivity logs. This query is pipped again to exclude false positives like Microsoft.Exchange.Servicehost discussed in the previous chapter (Levin, 2022c).

Using a rule query shown in Figure 10 we can modify the first pipe ***where Operation in~*** to alert the Set-crossTenantAccessPolicy operation observed previously in Exchange Online workbook. A modified rule query shown in Figure 11 also creates alerts based on the new operation activities added.

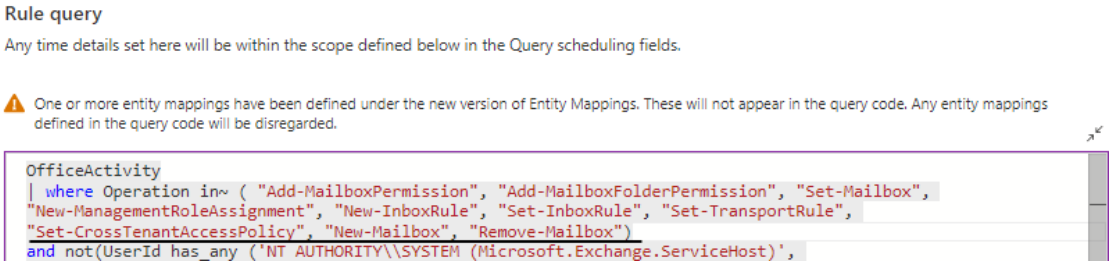

Figure 11. Rare and potentially high-risk office operations modified rule query.

The new activities underlined can be further filtered if for example, associating with Microsoft.Exchange.Servicehost to reduce possible false positives.

When an analytics rules are enabled, those rules can start generating alerts and incidents very soon. Every alert and incident should be manually reviewed, and a cause of action determined. Then make proper modifications to analytics rule query to filter false positives. Figure 12 shows an incident created by a default analytics rule template.

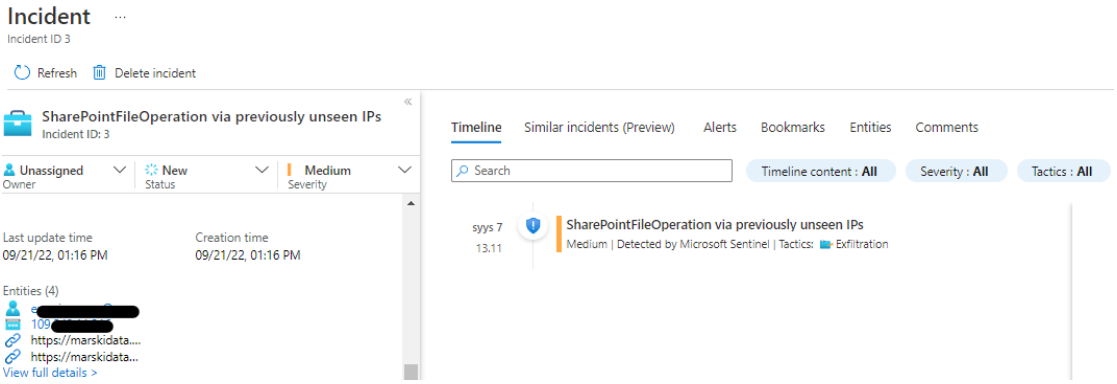

Figure 12. SharePointFileOperation Incident page

When observing the entities shown in Figure 12 bottom left, I can determine this as a false positive. Action was done by an employee who was not using a company VPN. An incident was triggered because this employee was operating from unknown IP address. Modifying the analytics rule to not alert false positives, open the KQL query command and study the logic behind it.

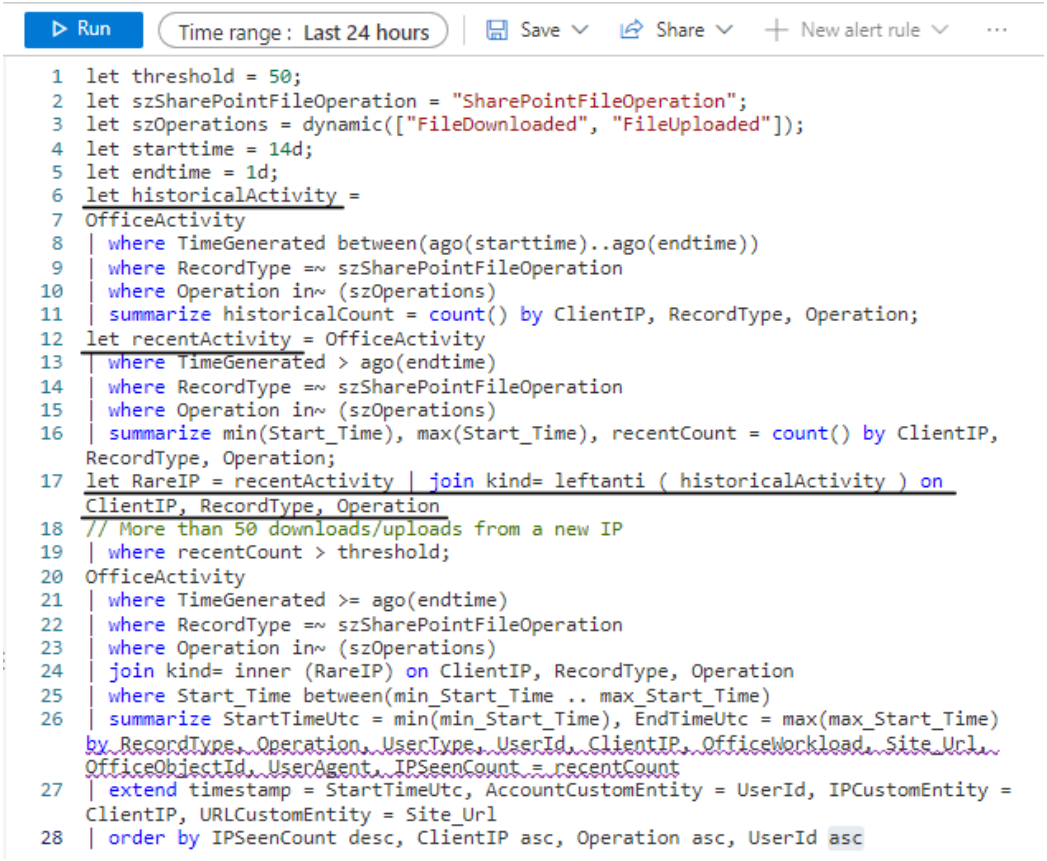

Figure 13. SharePoint file operation query KQL language.

In Figure 13, we can observe the command is in two sections separated by the comment on line 18. The first section defines variables to use in the second section starting from the line 19. This query scans the user activity defined in ***historicalActivity*** and ***recentActivity*** variable. Both variables have multiple pipes to filter log data. At the line 17 query returns if the IP is unseen or used. As a conclusion this query automatically filters used IP addresses, so changes do not have to be made. Next time the employee executes SharePoint operations from the same IP address, this query recognizes it from previous events and does not create a new incident.

One might consider the option to whitelist trusted users from the query shown in Figure 13. This can be achieved by adding a piped command ***where UserId !has 'trusted_user_name'*** between line 20 and 21. Operator ***!*** is the 'not' or negative command and thus excludes all listed users from this query. However, this is very much not advised. We want to follow the principle of zero trust, and not trust anyone and assume breach all the time. By whitelisting a user from threat detection queries we create possible attack vector if the user

account gets compromised. A better practice would be to enforce VPN policy, to only access a company resource in a private network.

3.5.3 Automation rules and playbooks

Automation rules let the user assign incident to right people, close known false positive incidents and change their severity. It is also the mechanism to execute playbooks in response to incidents. Playbooks are a set of functions or procedures that can be run in Microsoft Sentinel in a response to an alert or incident. They can be set to trigger automatically when a specific incident or alert is generated if being attached to an automation rule or analytics rule. Playbooks can also be run manually. To put it simple, an automation rule is the call to action and playbook is the set of actions to be executed.

With an automation rule you can create responses to incidents generated by analytics rules that detect compromised users to stop them to access your network. An example playbook for this job would alert and send messages to dedicated admins that had the option to block or ignore this incident. If ignored, the playbook would close the incident and let the user continue accessing the network. If blocked, playbook would send a command to Azure AD to disable the user and one command to a firewall to block the IP address user was using. To trigger this playbook, you would need an automation rule that changes the incident to active status and calls the example playbook to action.

Let’s recap the whole automation process. An alert or incident is generated. The incident has an automation rule attached to it. This automation rule triggers a playbook to handle the incident, and thus have hopefully resolved the issue by actions done by the playbook.

For this thesis, I will not be creating an actual playbook or automation rule to the working Marskidata environment. Setting these automated actions require high privileges of the network and are not to be created for “fun” or demonstrative purposes. However, we can investigate how they are made and configured.

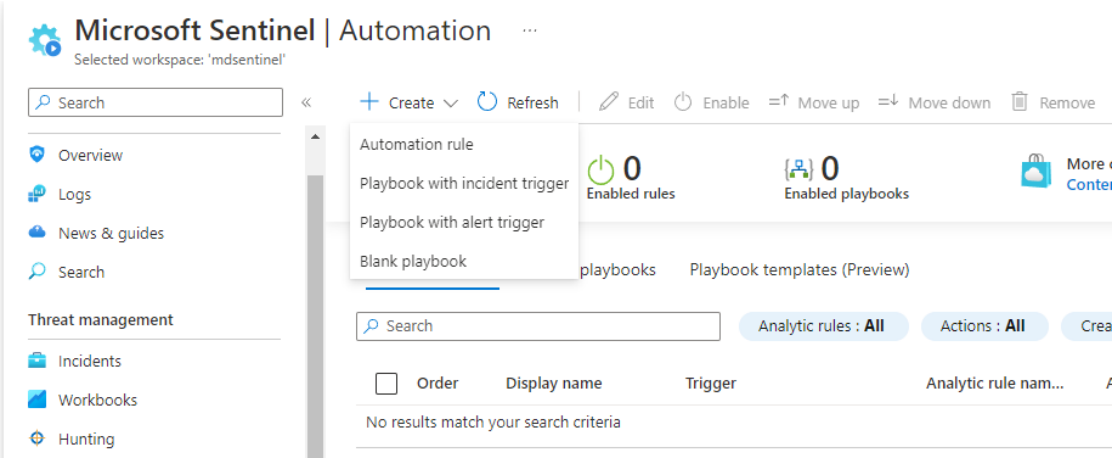

Figure 14. Where to create an automation rule.

Microsoft Sentinel has an own section under configurations for automation. There we can see all rules and playbooks that are enabled. In Figure 14 we can see a snippet of this page where to start creating your own rules. For demonstration purposes we are going to select automation rule and see what kind of configurations there are to set.

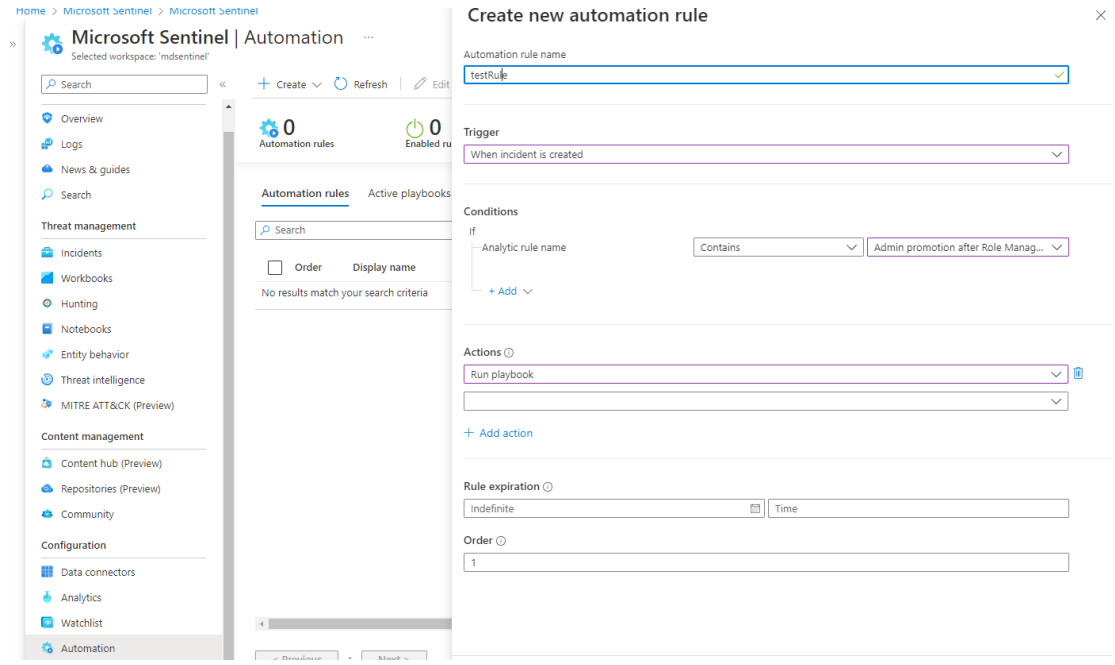

Figure 15. New automation rule configurations.

By looking at Figure 15 we can go step by step what is required to be configured. Use some meaningful name and choose whether to trigger from alert or incident. To recap the differences, incident is a set of multiple alerts. Next, we choose the conditions when this automation is triggered. We can choose from all your active analytics rules and set a negative, not containing certain rule.

This is the place where we would for example choose an analytics rule that detects compromised accounts. In the actions tab under conditions, we choose if we want to execute playbook or do some other less drastic action like change status or add tags. We can add as many actions as possible and conditions we want to our automation rule. Expiration data can be added if needed and the final number is the order which these rules a sequenced, the lowest numbers are executed first (Levin, 2022d).

3.5.4 Threat hunting, hypothesis and Jupyter notebooks

Hunting can be considered as proactive actions to find “not previously detected” cases. Differences can be easily seen in when comparing to incident response. When incidents are triggered, you are responding to something already happened. When hunting, you are trying to prevent the incident from happening. It is another step further to protecting an organization against cyber threats.

When hunting for “not previously detected” user must understand we are not waiting for a detection. When detection happens damages might already be done. If nothing is happening and no incidents are triggered, how is one supposed to start hunting? Every hunt is based on a hypothesis. A hypothesis might be a known attacking or enumeration tactic one can observe for traces. An idea is to search patterns and methods that are hard for a regular system to detect and to discover malicious activities before any damages are done. Threat hunting is an ongoing process as shown in Figure 16, and the first step is the hypothesis. It should answer to questions like what, where and how we are going to hunt.

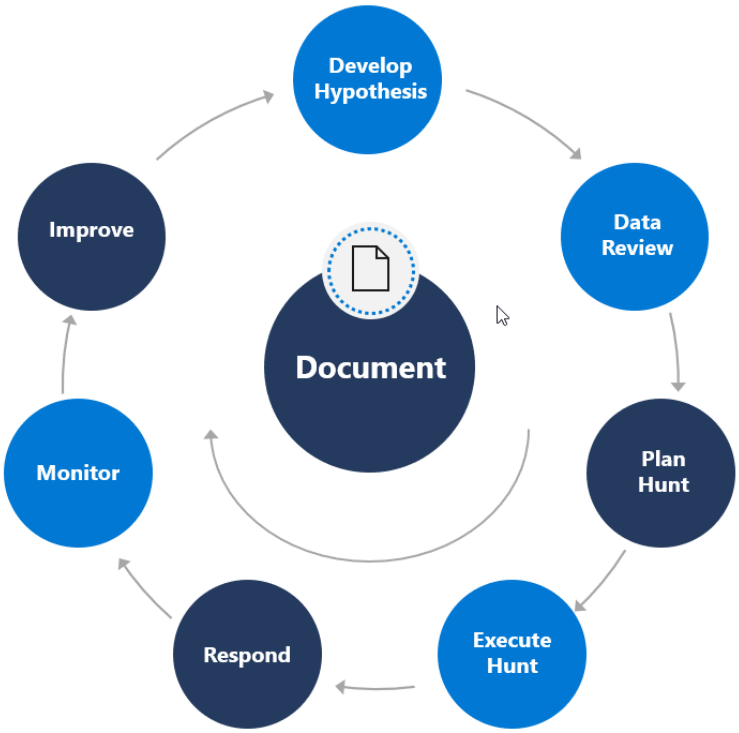

Figure 16. Hunting process and proper steps to success (Microsoft Learn, 2022).

We need to understand the data, tools, and expertise to achieve this. After an execution is done, there is still several steps to be conducted. Investigating results and doing proper improvements to your hunting queries. Even if nothing is found, routine tasks include setting up new monitoring and improving detection capabilities. When doing threat hunts, everything should be documented and should at least include what, how and why are you hunting, logic input and output, how to replicate the hunting process, and what to do next. To start hunting and building a hypothesis Microsoft Sentinel offers a visualized way view organizations security coverage shown in Figure 17.

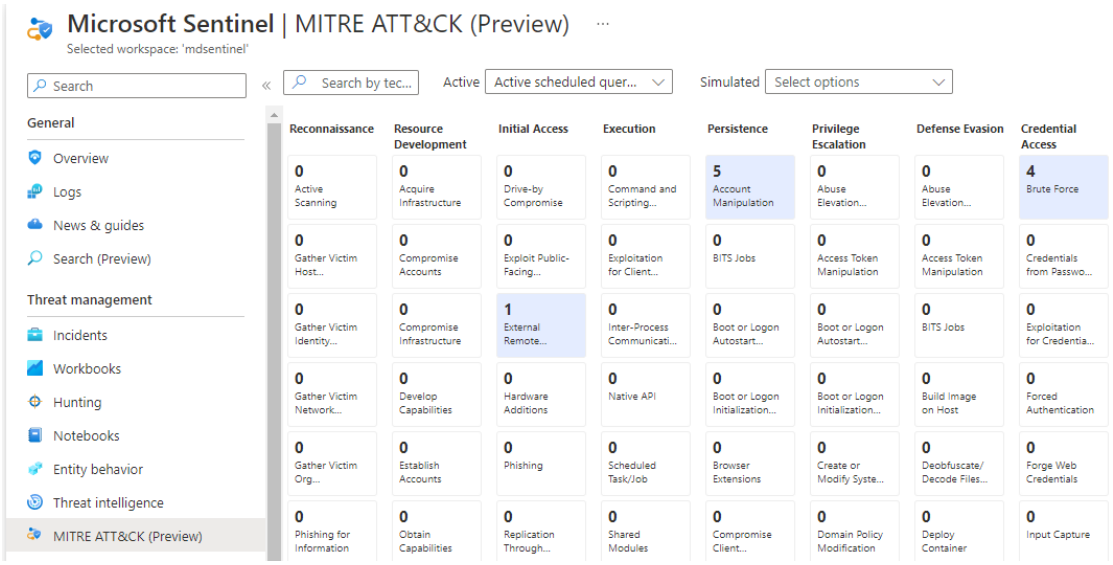

Figure 17. Mitre ATT&CK framework matrix by Microsoft Sentinel.

Under threat management MITRE ATT&CK (preview) by default shows how many currently active and scheduled analytics query rules are operational and covering the given vulnerability. Looking at Figure 17 we can see there is 0 rule queries covering reconnaissance or enumeration and 4 rule queries covering credential access specifically brute force attacks. When creating new hunting queries or analytics rules specific techniques and tactics should be selected from MITRE ATT&CK matrix to keep your matrix up to data. The idea is to have overall look on to your Sentinels security state. (Microsoft Learn, 2022).

To go even further users can use Jupyter notebooks to have full programmability with machine learning, visualization, and data analysis. Most of the common tasks can be done in Microsoft Sentinel portal environment, notebooks are extension for high level users. I will not demonstrate how to create or use notebooks; this is a subject for another project. It is still beneficial to know the basics and capabilities.

Notebooks can be used when a user wants to perform analytics that are not provided by default from Sentinel, such as some Python machine learning features, or to create a data visualization such as custom timeline and process tree. Also, users can integrate data sources that are out of box and on-premise. Notebooks have two main components a browser-based interface and a kernel. This kernel is running on an Azure virtual machine. It can support

many instances of notebooks at once and can be upgraded for more powerful computer if your notebooks include complex machine learning models. Proper permission is required to use notebooks. Microsoft Sentinel notebooks are run on an Azure machine learning platform which is a separate from Sentinel. Users' need Microsoft Sentinel contributor permissions and owner permissions in Azure Machine Learning (Watson, 2022).

The next chapter contains simple and more concrete example of threat hunting as demonstrated with real zero-day vulnerability. This chapter was more theory based. These concepts are very hard to demonstrate and require some high-level expertise. I am also learning these methods and concepts as I'm making this thesis and getting to know Sentinel more.

3.6 Zero-day vulnerability in Exchange services

A new zero-day vulnerability affecting Exchange Online services was announced by Microsoft 30 September 2022. For me, it gave me a great opportunity to demonstrate Sentinel capabilities to deal with a real threat. Microsoft exchange email services had a vulnerability that allowed a signed in user to execute arbitrary code. Allowing an attacker to run any code they want on the affected email services. Microsoft had identified two zero-day vulnerabilities, which CVE identifications are CVE-2022-41040 and CVE-2022-41082 (TRAFICOM, 2022).

The first one CVE-2022-41040 is server-side request forgery (SSRF) vulnerability. SSRF allows a bad actor to cause a web server to make modified or edited HTTP requests to an affected resource. To demonstrate it very simply we can have a normal website URL as "*https://website.com/item/2?server=api*" that returns some intended function. When SSRF vulnerability is present we can modify the URL to "*https://website.com/**dir/users**?server=server*" to return something else useful to an attacker.

Second CVE-2022-41082 allows remote code execution (RCE) when Exchange PowerShell is available. RCE means the attacker can execute any malicious code they want on a remote device. Two infamous examples are Log4j exploit hosting multiple RCE vulnerabilities and WannaCry ransomware

in 2017 exploiting server message block protocol (SMB) vulnerability to run malicious code to encrypt data. CVE-2022-41040 SSRF can allow an authenticated attacker to trigger CVE-2022-41082 RCE. Both can also be used separately. Keynote here is the attacker needs authenticated user to use these vulnerabilities, thus reduces the attacks surface dramatically for example compared to Log4j that was devastating because of the huge attack surface it had.

Microsoft threat intelligence center (MSTIC) have been observing this threat already in August 2022 and concluded that attacks are done by a single group and with medium confidence assessed the group is state sponsored. Attacks were done by chaining CVE-2022-41040 (SSRF) and CVE-2022-41082 (RCE) to get initial access on the target and then installed a web shell. Web shells are malicious scripts that give administrative remote access to a remote server in a form of CLI. China Chopper web shell was used specifically in these attacks. It has been used by many groups and in many attacks tracing back to 2012 when first discovered (Wikipedia, 2022). Web shell gives the attacker a hands-on-keyboard access to enumerate the system and gather data.

Figure 18 demonstrates the MSTIC observed activity about these vulnerabilities in action. CVE-2022-41040 (SSRF) allows the attacker to send malicious HTTP request. Using CVE-2022-41082 (RCE) attacker deploys China Chopper web shell to gain hands-on-keyboard access. Now the attacker can enumerate the target to start lateral movement, escalate privileges and collect data (McCafferty, 2022)

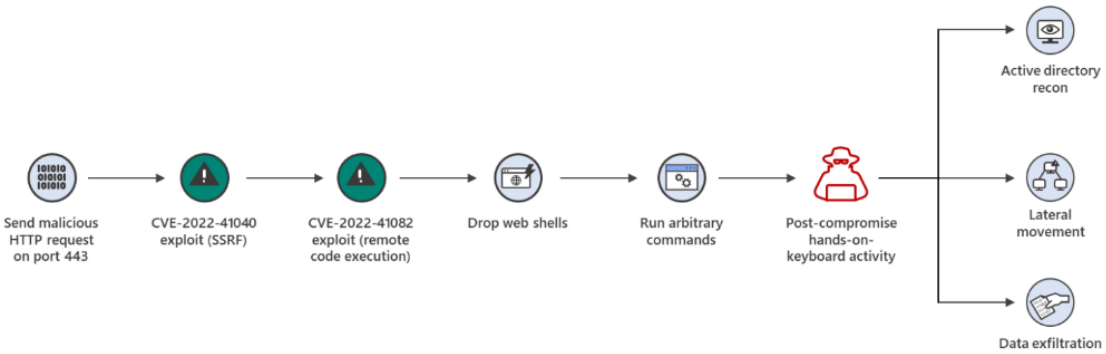

Figure 18. A pattern of attacks used with CVE-2022-41040 (SSRF) and CVE-2022-41082 (RCE).

After understanding the whole attack pattern, we can start hunting with Sentinel. Based on what we know about the attack, it would be wise start threat hunting on the China chopper web shell. MSTIC offers already readymade querie shown in Figure 19 to find this specific attack method.

```
1 DeviceProcessEvents
2 | where InitiatingProcessFileName =~ "w3wp.exe"
3 | where ProcessCommandLine has_any ("&ipconfig&echo", "&quser&echo", "&whoami&
echo", "&c:&echo", "&cd&echo", "&dir&echo", "&echo [E]", "&echo [S]")
```

Figure 19. China Chopper web shell hunting query.

The query in the Figure 19 looks for basic enumeration commands that are done when getting initial access. Command *whoami* return hostname of the system, *dir* and *cd* are basic directory traversal commands to move through the file system. Referring to Figure 18, this query would hunt actions done in “run arbitrary commands” section. Sentinel offers other similar hunting queries Exchange SSRF Autodiscover ProxyShell detection (Bryan, 2021), which was done to hunt ProxyShells, but its functionality is very similar to functions of China Chopper. Exchange Server Suspicious File Downloads (Bryan, 2022b) and Exchange Worker Process Making Remote Call (Bryan, 2022a) queries look for suspicious downloads or actions done in ISS logs. Internet Information services (IIS) is a web server host for Exchange Online and other Windows web resources. (McCafferty, 2022).

A more general approach would be to look for just web shell activity because it is a known core component in this attack. Looking through Microsoft Sentinel GitHub we can find a general web shell activity hunting query, which is much more general than the Chopper web shell hunting query (Trivedi, 2022).

To create one’s own custom query as shown in Figure 20, go to hunting tab and press top left “New Query”. Name the custom query, add your logic, and select “Tactics & Techniques”. For web shell activity tactics were persistence and initial access. Persistence means any action or access to a system that gives a bad actor long term presence in that system. Initial access refers to the attack vectors to get first foothold on a network. This way we categorize your custom query with the MITRE ATT&CK standards and update the matrix shown in Figure 17.

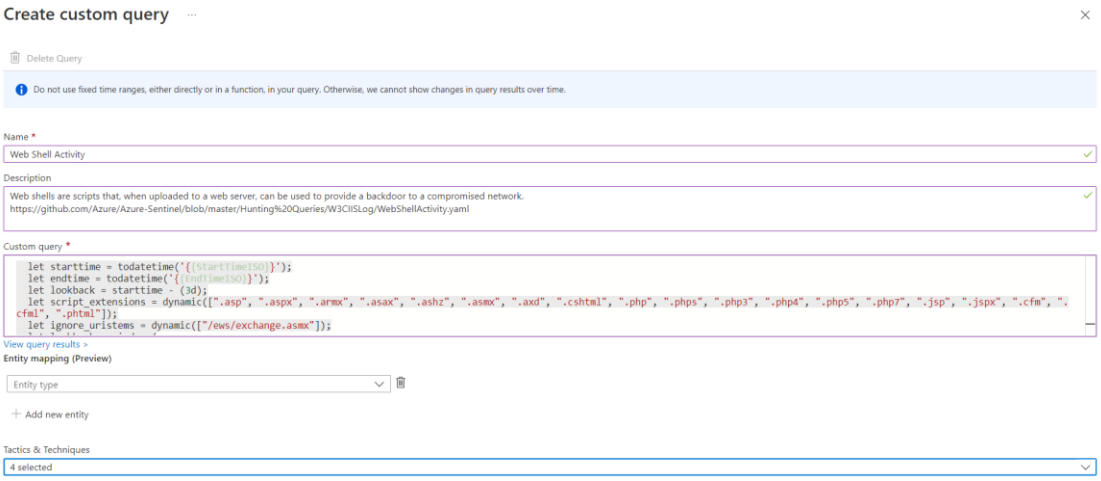

Figure 20. Custom hunting query for web shells.

Proper mitigations can also be done specially if no patch has been issued. Exchange server users can complete the URL rewrite rule for CVE-2022-41040(SSFR) and disable remote PowerShell to non-admins for CVE-2022-41082(RCE). URL rewrite rule change stops the attacker infecting the URL with malicious intent as explained in the second paragraph of this chapter and by disabling remote PowerShell access for normal users, we make attack surface non-existing, so even if the attacker gains access no further damages can be done (MSRC, 2022a).

3.7 Content management

To fully utilize Microsoft Sentinel, we want to get familiar with the official GitHub repository found at github.com/Azure/Azure-Sentinel. GitHub is a version control platform most notably used for open-source projects. The repository is unified with Microsoft Defender and contains out of the box detection queries for both. Also, for Sentinel we can find exploration queries, hunting queries, workbooks, playbooks and much more (Azure, 2022).

In Sentinel we can see the Content management section that includes Repositories, Content hub and Community pages. Repositories page allows us to form a connection to custom repository for example to the official Sentinel repository. Selecting “add new” we get the prompt shown in Figure 21 and we can input the right information. Users must name the connection and authorize

the chosen source control in our case GitHub. After selecting branch and content type we have a working connection that updates our Sentinel resources as they are created in the repository (McCollum, 2022).

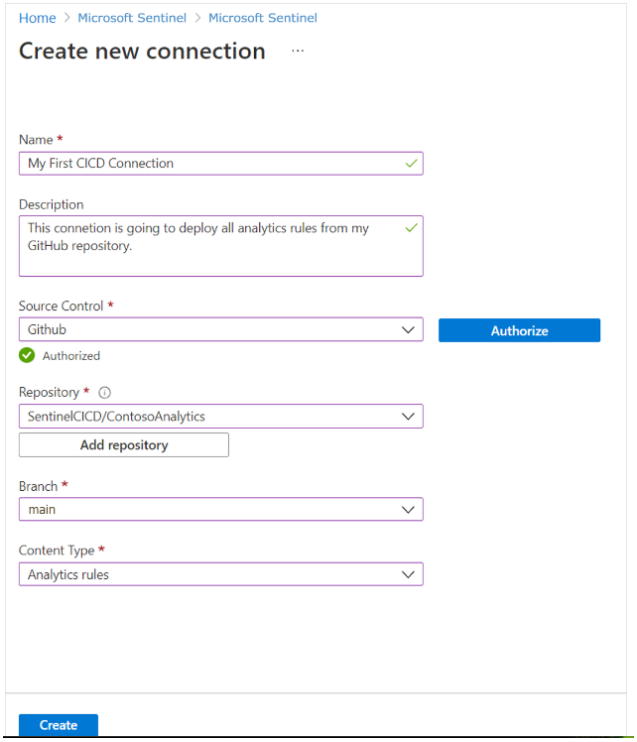

Figure 21. Creating a new connection to a custom repository.

Content hub page is the Microsoft Sentinel's own out of the box content and solution distribution service. Content is mostly maintained by Microsoft staff. With a single click users can install solution packs for vulnerabilities or problems as shown in Figure 22 the Log4j vulnerability detection solution. These solutions contain multiple types of Sentinel resources like playbooks, analytics rules, and workbooks. Or they can be custom data connectors like the Abnormal Security Events shown at the bottom right.

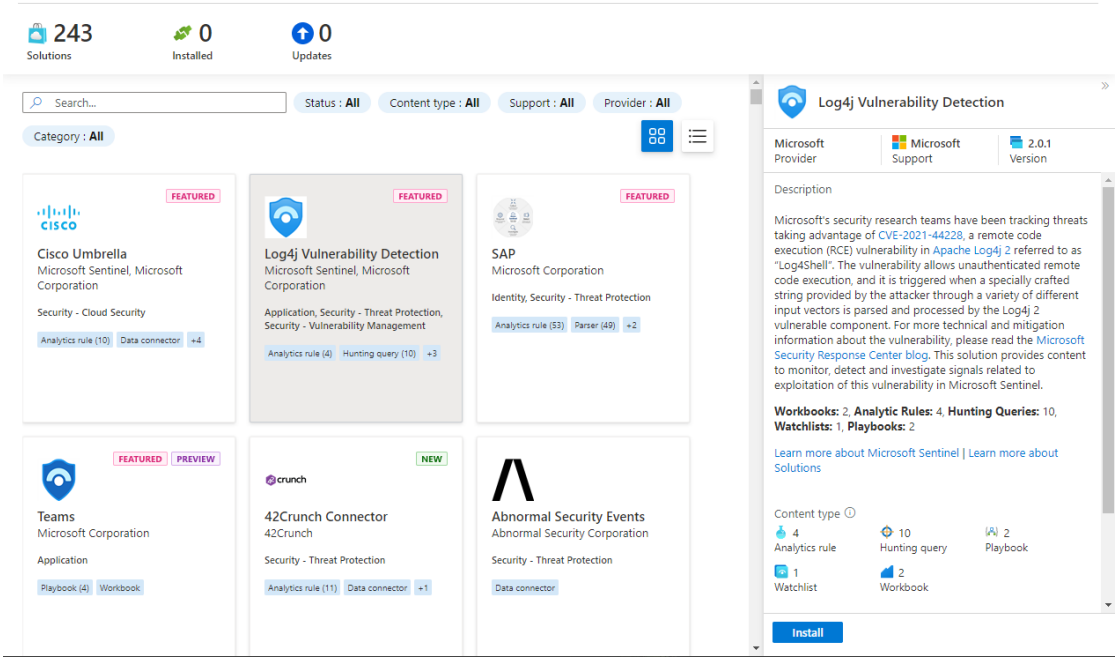

Figure 22. Content hub, Log4j Vulnerability Detection and Abnormal Security Events example.

Community page contains awareness and news for cyber-security threats. The latest awareness campaigns from Microsoft include DEV-0537 aka LAPSUS$ attack and cyber threat activity in Ukraine. LAPSUS has been identified as a large-scale social engineering and extortion group, which has been attacking many organizations including Microsoft and their partners. For the situation in Ukraine Microsoft has published reports and analysis to help organizations respond and proactively protect against the possible threats. For both the awareness campaigns we can discover Microsoft Sentinel solutions, for example hunting queries to find known attacking tactics.

3.8 Evaluating information security value

When planning your organization's cyber-security infrastructure, one would want all the protection that can be installed and is available. It is not possible to buy everything, because organizations usually have limited resources and money. One must consider how useful and valuable the product or service is going to be compared to what is it going to cost.

SIEMs are powerful and effective information security tools but are not for every network and organization. They are relatively expensive and more likely are difficult to use. This is generally the case about SIEMs, but Sentinel turned out to be more user friendly at the surface level but still complex when doing

more specific operations. Sentinel or SIEMs in general don’t replace the existing firewalls and anti-viruses, they are used to add more security value to your information security environment and to do more specific and complex threat hunting operations. Thus, if organizations information security is protected well enough just with firewalls and anti-viruses and is relatively small it is safe to say Sentinel would not give much security value.

When should organizations use Sentinel then? The first thing to consider is the case when organizations are responsible for the security of outside networks. Throughout the making this thesis Sentinel has shown great response and detection of new and emerging threats, especially when no easy fix or patch has been released yet. This gives an opportunity to hunt and fix threats as they are discovered and not to just wait for a patch. These hunting and fixing operations would naturally be billed work which would hopefully create a profit for the organization handling the networks. I can conclude with confidence that Sentinel is a good choice when doing business with other organizations and dealing with their information security.

Considering Sentinel as an internal security tool is bit different in my opinion. As said before Sentinel is another tool on top of the existing tools and thus another payment on top of the existing payments. My opinion is that there are two scenarios when organizations should implement Sentinel. The first is when an organization is large, talking about hundreds of people, and if they have their own cyber-security team, Sentinel would be a good choice for even just a birds-eye-view of all the security events. Naturally the bigger a company size, the bigger the risk of breach. People and social engineering are the number one weak points of any organization’s information security.

Second scenario would be when an organization is expecting more threats that is normal or they know a targeted attack is or could be coming. Sentinel offers much more sophisticated and specific detection than firewalls and anti-viruses usually. You could think Sentinel is the tool to detect the attackers that can evade your firewalls and anti-viruses.

To conclude this evaluation, the usefulness of Sentinel depends on the organization size and their threat environment. Also, as an extra mention if an organization is already heavily invested in Microsoft products Sentinel should at least be considered and looked at. The free connectors should no matter what be taken advantage of.

4 CONCLUSION

Microsoft Sentinel is initially easy to install and deploy, but hard to master information security tool. The installation and adding connectors is a smooth process and doesn't require any extra skills. Utilizing Sentinel's hunting and searching capabilities require good knowledge of cyber-security as a whole and an ability to understand KQL coding language. Microsoft Sentinel does not replace existing security measurements in place, it only adds more. Sentinels' best quality in my opinion is to find and investigate new threats that does not have a patch or fix released yet. Sentinel and SIEMs in general are great and broad information security tools, thus they also require a broad knowledge and interest in information security.

Weather to deploy Sentinel to an organization's network or not depends on the scenarios discussed in the previous chapter and there are downsides if used when not needed. Sentinel requires someone's time and money to be fully operational, which are resources not be wasted. When used in suitable organization and in right hands, you have a top of the class information security tool to watch over an any network.

Further research and investigation could be done with Jupyter notebooks and threat hunting. My own skills and expertise are not that high level right now that I could start developing notebooks myself. A good future project would be to penetrate a company network with out of the box methods using anti-virus and firewall evasion tactics. Then with Sentinel investigate and develop a notebook or analytics rule to counter that. When doing the attacking myself I can fully investigate and see what is detected and what is not. Thus, possibly develop new hypothesis and fix security holes. Threat hunting and a hypothesis in general were barely scratched and could also have project of their own.

5 REFERENCES

Azure (2022). Microsoft Sentinel and Microsoft 365 Defender. [online] GitHub. Available at: https://github.com/Azure/Azure-Sentinel [Accessed 16 Nov. 2022].

Buck, A (2021). Resource naming and tagging decision guide - Cloud Adoption Framework. [online] docs.microsoft.com. Available at: https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/decision-guides/resource-tagging/?toc=%2Fazure%2Fazure-resource-manager%2Fmanagement%2Ftoc.json [Accessed 12.8.2022].

Bryan, P. (2021). Microsoft Sentinel and Microsoft 365 Defender. [online] GitHub. Available at: https://github.com/Azure/Azure-Sentinel/blob/08a8d2b9c5c9083e341be447773a34b56b205dee/Detections/W3CIISLog/ProxyShellPwn2Own.yaml [Accessed 7 Oct. 2022].

Bryan, P. (2022a). Microsoft Sentinel and Microsoft 365 Defender. [online] GitHub. Available at: https://github.com/Azure/Azure-Sentinel/blob/master/Detections/MultipleDataSources/ExchangeWorkerProcessMakingRemoteCall.yaml [Accessed 7 Oct. 2022].

Bryan, P. (2022b). Microsoft Sentinel and Microsoft 365 Defender. [online] GitHub. Available at: https://github.com/Azure/Azure-Sentinel/blob/master/Detections/http_proxy_oab_CL/ExchagngeSuspiciousFileDownloads.yaml [Accessed 7 Oct. 2022].

Gao, J. (2022). Manage resource groups - Azure portal - Azure Resource Manager. [online] docs.microsoft.com. Available at: https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/manage-resource-groups-portal [Accessed 29.8.2022].

Gegick, M. and Barnum, S. (2005). Least Privilege | CISA. [online] www.cisa.gov. Available at: https://www.cisa.gov/uscert/bsi/articles/knowledge/principles/least-privilege [Accessed 8.9.2022].

Kumar, N. (2022). Understanding Tenants and Subscriptions in Azure. [online] Azure Training Series. Available at: https://azure-training.com/2022/02/28/understanding-tenants-and-subscriptions-in-azure/ [Accessed 29.8.2022].

Levin, Y (2022a). Quickstart: Onboard in Microsoft Sentinel. [online] docs.microsoft.com. Available at: https://docs.microsoft.com/en-us/azure/sentinel/quickstart-onboard [Accessed 16.8.2022].

Levin, Y (2022b). What is Azure Sentinel? [online] docs.microsoft.com. Available at: https://docs.microsoft.com/en-us/azure/sentinel/overview [Accessed 24.8.2022].

Levin, Y. (2022c). Create custom analytics rules to detect threats with Microsoft Sentinel. [online] learn.microsoft.com. Available at: https://learn.microsoft.com/en-us/azure/sentinel/detect-threats-custom [Accessed 21.9.2022].

Levin, Y. (2022d). Use playbooks with automation rules in Microsoft Sentinel. [online] learn.microsoft.com. Available at: https://learn.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook?tabs=LAC [Accessed 26 Oct. 2022].

Lyon, R. (2022a). Azure portal overview - Azure portal. [online] docs.microsoft.com. Available at: https://docs.microsoft.com/en-us/azure/azure-portal/azure-portal-overview [Accessed 29.8.2022].

Lyon, R. (2019b). What is Azure Cloud Services. [online] Microsoft.com. Available at: https://docs.microsoft.com/en-us/azure/cloud-services/cloud-services-choose-me [Accessed 29.8.2022].

Lyon, R. (2021c). Assign Azure roles using the Azure portal - Azure RBAC. [online] docs.microsoft.com. Available at: https://docs.microsoft.com/en-us/azure/role-based-access-control/role-assignments-portal?tabs=current [Accessed 15 Aug. 2022].

McCafferty, K. (2022). Analyzing attacks using the Exchange vulnerabilities CVE-2022-41040 and CVE-2022-41082. [online] Microsoft Security Blog. Available at: https://www.microsoft.com/security/blog/2022/09/30/analyzing-attacks-using-the-exchange-vulnerabilities-cve-2022-41040-and-cve-2022-41082/ [Accessed 5 Oct. 2022].

McCollum, A. (2022). Deploy custom content from your repository - Microsoft Sentinel. [online] learn.microsoft.com. Available at: https://learn.microsoft.com/en-us/azure/sentinel/ci-cd?tabs=github [Accessed 16 Nov. 2022].

Microsoft Azure (2022). Azure Sentinel Pricing | Microsoft Azure. [online] azure.microsoft.com. Available at: https://azure.microsoft.com/en-gb/pricing/details/microsoft-sentinel/ [Accessed 23 Sep. 2022].

Microsoft Learn (2022). Explain threat hunting concepts in Microsoft Sentinel - Training. [online] learn.microsoft.com. Available at: https://learn.microsoft.com/fi-fi/training/modules/what-is-threat-hunting-azure-sentinel/ [Accessed 27 Sep. 2022].

Mitre Corporation (2017). cve-website. [online] www.cve.org. Available at: https://www.cve.org/About/Overview [Accessed 25.8.2022].

MSRC (2022a). Customer Guidance for Reported Zero-day Vulnerabilities in Microsoft Exchange Server – Microsoft Security Response Center. [online] msrc-blog.microsoft.com. Available at: https://msrc-blog.microsoft.com/2022/09/29/customer-guidance-for-reported-zero-day-vulnerabilities-in-microsoft-exchange-server/ [Accessed 19 Oct. 2022].

MSRC (2022b). Guidance for CVE-2022-30190 Microsoft Support Diagnostic Tool Vulnerability – Microsoft Security Response Center. [online] msrc-

blog.microsoft.com. Available at: https://msrc-blog.microsoft.com/2022/05/30/guidance-for-cve-2022-30190-microsoft-support-diagnostic-tool-vulnerability/ [Accessed 25.8.2022].

Palo Alto Networks (n.d.). What is SOAR? [online] Palo Alto Networks. Available at: https://www.paloaltonetworks.com/cyberpedia/what-is-soar [Accessed 9.9.2022].

Rosencrance, L. (2020). What is SIEM and Why is it Important? [online] SearchSecurity. Available at: https://www.techtarget.com/searchsecurity/definition/security-information-and-event-management-SIEM [Accessed 9.9.2022].

Sagir, S. (2022). Kusto Query Language (KQL) overview- Azure Data Explorer. [online] learn.microsoft.com. Available at: https://learn.microsoft.com/fi-fi/azure/data-explorer/kusto/query/ [Accessed 20.9.2022].

TRAFICOM (2022). Tunnistautumista vaativa etäkäytön mahdollistava haavoittuvuus Microsoft Exchangessa. [online] Kyberturvallisuuskeskus. Available at: https://www.kyberturvallisuuskeskus.fi/fi/haavoittuvuus_14/2022 [Accessed 5 Oct. 2022].

Trivedi, A. (2022). Azure-Sentinel/WebShellActivity.yaml at master · Azure/Azure-Sentinel. [online] GitHub. Available at: https://github.com/Azure/Azure-Sentinel/blob/master/Hunting%20Queries/W3CIISLog/WebShellActivity.yaml [Accessed 10 Oct. 2022].

Vice, K. (2022). Subscriptions, licenses, accounts, and tenants for Microsoft's cloud offerings - Microsoft 365 Enterprise. [online] docs.microsoft.com. Available at: https://docs.microsoft.com/en-us/microsoft-365/enterprise/subscriptions-licenses-accounts-and-tenants-for-microsoft-cloud-offerings?view=o365-worldwide [Accessed 29.8.2022].

Warner, T. (2022). Organize your resources with management groups - Azure Governance - Azure governance. [online] docs.microsoft.com. Available at: https://docs.microsoft.com/en-us/azure/governance/management-groups/overview [Accessed 29.8.2022].

Watson, C. (2022). Use notebooks with Microsoft Sentinel for security hunting. [online] learn.microsoft.com. Available at: https://learn.microsoft.com/en-us/azure/sentinel/notebooks [Accessed 28 Oct. 2022].

Wikipedia (2022). China Chopper. [online] Wikipedia. Available at: https://en.wikipedia.org/wiki/China_Chopper [Accessed 6 Oct. 2022].

Wild, G (2022). Design a Log Analytics workspace architecture - Azure Monitor. [online] docs.microsoft.com. Available at: https://docs.microsoft.com/en-us/azure/azure-monitor/logs/workspace-design [Accessed 12.8.2022].