



Data Security Controls

Lab 5: Logging and SIEM

Michael Herman

Toni Peltola

Karri Päivärinta

Project report

Instructor: Jarmo Viinikanoja

Return date: 6.9.2023

Group: TIC21S1

Contents

1	Introduction	6
2	Theoretical background	7
2.1	SIEM systems.....	7
2.2	Elastic.....	7
2.2.1	Agents	8
2.2.2	Logging.....	8
2.2.3	Alerts.....	9
2.2.4	Cases	9
3	Methodology.....	10
3.1	Frameworks.....	10
3.2	MITRE ATT&CK	11
3.2.1	ATT&CK matrix.....	11
3.3	Atomic Red Team	11
4	Methods.....	12
4.1	Atomic Red Team / MITRE integration	12
4.2	Attacks.....	12
5	Configuration.....	13
5.1	Elastic SIEM setup	13
5.2	Fleet Server	16
5.3	Agents.....	18
5.3.1	Agent installation on NS01 and WWW.....	21
5.3.2	Viewing results.....	21
5.4	Logging	22
5.4.1	Enabling firewall logging.....	22
5.4.2	Sending firewall logs to the SIEM	26
5.4.3	Data collection integrations.....	26
5.5	Windows integrations	30
6	Testing.....	34
6.1	Attack 1: T1087.001 Account Discovery Local Account	34
6.2	Attack 2: T1087.002 Account Discovery Domain Account	35
6.3	Attack 3: T1140 Deobfuscate/Decode Files or Information	35
6.4	Attack 4: T1113 Screen capture	36
6.5	Attack 5: T1036.005 Masquerade Match Legitimate Name or Location	37

6.6	Attack 6: T1012 Query Registry.....	38
6.7	Attack 7: T1547.001 Boot or Logon AutoStart Execution Registry Run Keys / Startup Folder 39	
6.8	Attack 8: T1574.001 Hijack Execution Flow DLL Search Order Hijacking.....	40
6.9	Attack 9: T1070.001 Indicator Removal on Host Clear Windows Event Logs	40
6.10	Attack 10: T1112 Modify Registry	41
6.11	Uncaught attacks.....	41
6.11.1	Legitimate usage	42
6.11.2	Risk thresholds.....	42
6.11.3	Third party software	42
6.11.4	Privilege escalation	42
6.12	Attack analysis.....	43
7	Cases	43
7.1	Timelines	43
8	Analytics.....	44
9	Dashboard	45
10	Conclusion	48
11	Sources.....	49

Figures

Figure 1: New security policy rules	13
Figure 2: Elastic SIEM login screen.....	14
Figure 3: Welcome to Elastic.....	14
Figure 4: Choose Security.....	15
Figure 5: Select prebuilt rules and timeline templates.....	15
Figure 6: SIEM rules.....	16
Figure 7: Error enabling rules.....	16
Figure 8: Fleet server installation.....	17
Figure 9: SSH connection to SIEM	17
Figure 10: Fleet server installation on SIEM	18
Figure 11: Installation successful	18
Figure 12: Add agent screen	19
Figure 13: Installing agent to the host	19
Figure 14: WS01 agent installation in Windows	20
Figure 15: WS01 agent installation continued.....	20

Figure 16: Agent installation confirmed	20
Figure 17: Setting PasswordAuthentication to yes	21
Figure 18: Agent installation for NS01	21
Figure 19: systemctl restart sshd.service	21
Figure 20: All agents installed	22
Figure 21: Syslog profile creation.....	22
Figure 22: Log forwarding profile and log forwarding profile match list.....	23
Figure 23: Log forwarding profile object	24
Figure 24: Policy forwarding logs	24
Figure 25: Active log forwarding	24
Figure 26: GlobalProtect logs activated	25
Figure 27: Service route configuration	25
Figure 28: Opening UDP port 514 on the SIEM firewall	26
Figure 29: Data coming from Palo Alto to SIEM	26
Figure 30: Palo Alto Next-Gen Firewall integration	27
Figure 31: Beats logging integration	27
Figure 32: Palo Alto Networks PAN-OS Logs module	28
Figure 33: Installing Filebeat on the SIEM	28
Figure 34: filebeat.yml configuration.....	29
Figure 35: Filebeat setup.....	29
Figure 36: Configurations in panw.yml	30
Figure 37: Data received from the <i>panw</i> module.....	30
Figure 38: Windows integration	31
Figure 39: Adding the Elastic agent to Windows	31
Figure 40: Agent configuration	32
Figure 41: Agent deployment confirmation	32
Figure 42: Endpoint and Cloud Security integration.....	33
Figure 43: Windows integration policies	33
Figure 44: Endpoint and Cloud Security integration policies.....	34
Figure 45: T1087.001 - Account Discovery	34
Figure 46: Attack alert 1.....	35
Figure 47: T1087.002 - Account Discovery: Domain account.....	35
Figure 48: Attack alert 2.....	35
Figure 49: T1140 - Deobfuscate/Decode Files or Information	35

Figure 50: Attack alert 3	36
Figure 51: T1113: Screen capture	36
Figure 52: Attack alert 4.....	36
Figure 53: T1036.005 - Masquerade.....	37
Figure 54: Attack alert 5.....	37
Figure 55: T1012 - Query Registry.....	38
Figure 56: Attack alert 6.....	38
Figure 57: T1547.001 - Boot or Logon Autostart Execution	39
Figure 58: Attack alert 7.....	39
Figure 59: T1574.001 - Hijack Execution Flow	40
Figure 60: Attack alert 8.....	40
Figure 61: 1070.001 - Indicator Removal on Host	40
Figure 62: Attack alert 9.....	41
Figure 63: T1112 - Modify Registry	41
Figure 64: Attack alert 10.....	41
Figure 65: Attack missed by the SIEM.....	42
Figure 66: Cases main view	43
Figure 67: Attacks case.....	44
Figure 68: Analytics overview	44
Figure 69: Donut graph	46
Figure 70: Horizontal bar graph	46
Figure 71: Custom dashboard	47

1 Introduction

This report examines the process of configuring logging in the Elastic Security Information and Event Management (SIEM) system. It begins with a theoretical discussion. The general aims of this discussion are twofold: to assess standard SIEM functionalities and discuss how they are implemented in the Elastic SIEM. Core features and their roles in information and event management are evaluated. These include agents, logging, alerts and cases.

The report then proceeds to a methodological discussion. The section assesses the suitability of various frameworks available for testing SIEM alert capabilities. Discussion focuses on the MITRE ATT&CK framework. It examines how the ATT&CK matrix can be operationalized using Red Canary's Atomic Red Team resources. The methods section outlines the general approach to testing and explains its underlying logic.

The technical discussion begins with a presentation of the configuration process. The discussion covers core elements of the Elastic SIEM system. It begins with a presentation of the steps involved in the initial setup. Agent and logging configuration processes are then described. This sets the stage for the alert system tests. The testing section presents the outcomes of ten attacks performed on the WS01 machine. The purpose of these attacks is to gain a better understanding of the types of commands required to produce alerts, the threshold for notification and the process of forensic analysis writ large.

Section 7 examines how Elastic's *Cases* feature can be used to organize logging and event-related data. It discusses how it can be used to streamline the incident-management process using event timelines. This folds into a discussion in section 8 of the *Analytics* feature. Section 9 discusses the range of dashboard customization options available. An example of a customized dashboard is then presented using data gleaned from the attacks performed in section 6. The report concludes by highlighting the challenges faced and insights generated in the completion of the task.

2 Theoretical background

2.1 SIEM systems

There are a number of advantages associated with SIEM-based security management. They serve as centralized hubs for monitoring, analyzing and responding to security events (Kotenko & Chechulin, 2012). SIEM systems collect and normalize data from an array of sources. This can include network devices, servers and applications. They provide real-time monitoring capabilities to detect suspicious or anomalous activities.

SIEMs are designed to identify complex attack patterns and potential security threats which may go unnoticed when examining individual events (Berdibayev et al., 2021). Data can be correlated from a wide range of sources. The system will generate alerts when predefined rules or patterns are detected. SIEM-based investigation, tracking and automated response tools are frequently used in attack scenarios. Alerts and advanced incident response functionalities are typical elements of SIEM management systems (Montesino, Fenze & Baluja, 2012). They are also capable of real-time monitoring.

SIEM systems can be used to ensure regulatory and compliance requirements are met. Reporting and documentation features are designed to comply with security policies and industry-specific regulations. SIEM rules and policies can be adapted to meet specific security requirements. SIEM systems are designed to provide as holistic a view of the threat landscape as possible (Mokalled et al., 2019).

2.2 Elastic

The Elastic SIEM operates within the Elastic Stack ecosystem. It offers a range of capabilities for security monitoring and management. The SIEM uses real-time monitoring and alerts to track suspicious activities and respond to security threats. Monitoring and alerts can operate according to prebuilt or custom rulesets. The system is capable of ingesting data from an array of sources. This includes logs and network traffic. Elasticsearch is used to standardize data for analysis (Kotenko, Kuleshov & Ushakov, 2017).

The system provides robust incident response tools. Elastic supports integrations with threat intelligence feeds and endpoint security solutions. Incidents can be organized into and analyzed through *cases*. It is possible to generate a timeline view of security events. Custom dashboards facilitate more efficient forensic analysis (Vazao et al., 2021). Report generation features streamline the process of meeting compliance and reporting obligations.

2.2.1 Agents

Agents in Elastic SIEMs are lightweight, self-updating components. They facilitate data collection from a range of sources (Mulyadi et al., 2020). This includes logs, event streams and endpoints. Agents are installed on host machines. They process and enrich locally-collected data before it is forwarded to a central Elastic SIEM instance. Agents are equipped with security features which ensure data integrity during transmission. Data centralization enables efficient analysis, visualization, threat detection and reporting (Elastic, n.d.-a). This makes it easier to detect and investigate security incidents.

2.2.2 Logging

Elastic is capable of ingesting, storing and enriching a wide array of logging data (El Arass & Souissi, 2019). These can be leveraged to create a comprehensive security information and event management solution. Data ingestion involves collecting information from various sources. These include logs and security events. This is typically performed using Logstash. Logstash is an open-source data collection and transformation engine used to forward log and event information to Elasticsearch (Elastic, n.d.-a). Elasticsearch then stores and indexes the data for future reference and analysis.

Data enrichment adds context and metadata to the ingested data. This ensures its usefulness for security monitoring. Elastic SIEM also offers inbuilt and custom data analysis capabilities. These include threat and anomaly detection. The Kibana interface serves as Elastic's visualization and reporting platform. It is possible to create custom interactive dashboards. These ensure relevant security data is immediately accessible for analysis whenever required (Elastic, n.d.-b).

Elastic has robust alerting capabilities. It is possible to configure rules and detection algorithms which trigger alerts upon the identification of potential threats or anomalies. These alerts are central in initiating incident response workflows. They can be used to facilitate a more rapid response to and mitigation of security incidents (Subramian & Meng, 2021). Alert capabilities are discussed in more detail below.

2.2.3 Alerts

Alerts play a crucial role in enhancing operational security. They allow analysts to proactively identify and respond to specific security events and incidents (Tariq et al., 2022). The process begins with the ingestion of data from various sources. This includes logs and security events. These are then analyzed using predefined rules and detection algorithms. Alerting rules and thresholds are defined to trigger alerts when specific criteria or conditions are met.

An alert is generated when a security event matches these criteria. They can be communicated through various channels. This includes email and third-party integrations. Alerts initiate the incident response workflow. They facilitate prompt investigation and remediation of threats (Mancini, 2019). Alerts can be triaged efficiently using the Elastic's Kibana interface. The interface provides critical contextual information and monitors the status and actions taken during investigations (Elastic, n.d.-c).

2.2.4 Cases

Cases and timelines are essential features in the Elastic stack. They are the primary tools used to manage and investigate security incidents. Cases can be created as containers for incident-related information and tasks. These cases can be associated with alerts and observables. This provides context and a central hub for investigation. (Elastic, n.d.-d). It is also possible to add comments, notes, and tasks to the case timeline. This makes it easier to keep track of key events.

The investigation workbench in Elastic provides the possibility to visualize timelines. This streamlines the process of reconstructing the sequence of events and correlating event notifications and alerts. This in turn makes it easier to identify patterns and trends (Nabil et al., 2017). Integration

with SIEM alerting and reporting features ensures a seamless and efficient incident response process.

3 Methodology

3.1 Frameworks

Validating SIEM capabilities through rigorous testing ensures system resilience and improves the overall security posture (Avison & Fitzgerald, 2006). A variety of testing frameworks are available for this purpose. Testing according to preexisting frameworks has a range of practical advantages. They remove much of guesswork associated with the testing process. They are standardized and based on real-world threat-intelligence. Standardization facilitates efficient communication and collaboration across teams and organizations (Johnstone, 2009). Extant frameworks align closely with industry standards and regulatory requirements. They provide a range of tactics, techniques and best practices.

The most widely used frameworks are the Open Web Application Security Project's (OWASP) Risk Assessment Framework, the National Institute of Standards (NIST) Cybersecurity Framework and the MITRE ATT&CK Framework (Shah & Mehtre, 2015). The OWASP framework evaluates risk in web applications. It also provides a Risk Rating Methodology (RRM) to identify, estimate and mitigate risks (OWASP, 2013). Determining a suitable testing framework depends on operational requirements and organizational focus. NIST's Cybersecurity Framework provides a broad set of guidelines and best practices. The framework is organized primarily around risk management and compliance (NIST, 2023).

The framework providing the most utility is in this case MITRE ATT&CK. It provides an overview of the tactics, techniques and procedures (TTPs) used in cyberattacks (MITRE, n.d.). Information is presented in a detailed yet accessible matrix. This can be used to assess operational readiness to a comprehensive array of cyber threats (Valli et al., 2014). The framework is of particular relevance when testing SIEM capabilities.

3.2 MITRE ATT&CK

The ATT&CK framework provides an extensive catalog of adversary tactics and techniques. These are especially useful because they are taken from real-world attacks. This enables testers to assess threat detection and response abilities using a diverse set of known attack vectors (Geogiadou, Mouzakitis & Askounis, 2021). MITRE ATT&CK's mappings to detection rules and its risk assessment capabilities allow testers to create precise detection scenarios.

The framework is also useful for penetration testing. Penetration testing is commonly used to gauge incident response and threat detection capabilities. MITRE ATT&CK is updated frequently and provides a collaborative and comprehensive approach to testing SIEM capabilities. The matrix enables organizations to adapt easily to the evolving cyber threat landscape (Tang, 2014). Refinements can be prioritized based on attack vectors judged the highest risk.

3.2.1 ATT&CK matrix

The tool most associated with MITRE is the ATT&CK matrix. The matrix organizes cyberattacks into a structured framework with columns and rows. The columns represent high-level tactics used by adversaries. They cover various stages of an attack. Tactics are provided for a wide range of attack vectors. These include *Initial Access*, *Execution*, *Privilege Escalation*, *Exfiltration* and others. Multiple rows representing specific techniques employed by threat actors appear in each column (MITRE, n.d.).

Each technique is assigned a unique identifier. The identifier is accompanied by references and documentation. These offer insights and real-world examples. The matrix includes mappings to Advanced Persistent Threat (APT) groups. Information concerning specific tactics and techniques associated with these groups is also provided. Standardized, comprehensive and up-to-date views of cyber threats are widely considered essential elements in understanding, defending against and responding to cyber threats (Frankland, 2009; Midian, 2003; Yeo, 2013).

3.3 Atomic Red Team

Atomic Red Team leverages the MITRE ATT&CK framework to create practical and relevant tests for evaluating the detection and response capabilities of cybersecurity systems (Red Canary, 2023). This

includes SIEM solutions. Testing scenarios are mapped to specific tactics and techniques provided the MITRE ATT&CK matrix. This ensures tests are aligned with real-world adversary behavior. A list of commands capable of performing the attack in question is provided. These are sourced directly from the Red Canary GitHub repository (Red Canary, n.d.). A detailed description sourced from MITRE ATT&CK is also available.

Red-teams have considerable flexibility in how attacks can be performed using this method (Shah & Mehtre, 2015). Maximum effectiveness across a range of network configurations is assured. These scenarios enable the creation of use-cases and detection rules. They are expected to trigger alerts or actions when specific attack techniques are detected. These can then be used to validate and fine-tune security systems, identify weaknesses and make improvements. It is a tangible and actionable method to test systematically in a controlled environment (Tang, 2014).

4 Methods

4.1 Atomic Red Team / MITRE integration

The exercise examines what kinds of attacks generate alerts in the Elastic SIEM. The default settings are used. Attacks are designed to be as systematic as possible. They evaluate a specific detection or response capability. Attacks are performed using the Atomic Red Team framework. The framework is mapped to the MITRE ATT&CK classification system. Testing begins with an initial assessment to identify relevant attack vectors and techniques.

Attacks corresponding to these vectors are then selected. Publicly reported APT attack techniques are mapped to the ATT&CK matrix. The scope of available attack vectors is vast. A major challenge for neophytes is deciding on which attacks to focus. The most logical path through this morass is simply using attacks associated with specific APT groups. This was deemed the most efficient way to address decision paralysis.

4.2 Attacks

Attacks requiring non-standard software are excluded. Only commands using inbuilt services and software are used. This ensures relevance across a wide range of networked Windows



environments. It has the additional benefit of streamlining the attack process. A significant result is that not all attacks generate alerts. This is because some of the commands executed are not strictly associated with malicious activity. Others may only be considered potentially malicious when executed with basic user privileges. These cases are noted in the technical discussion.

5 Configuration

5.1 Elastic SIEM setup

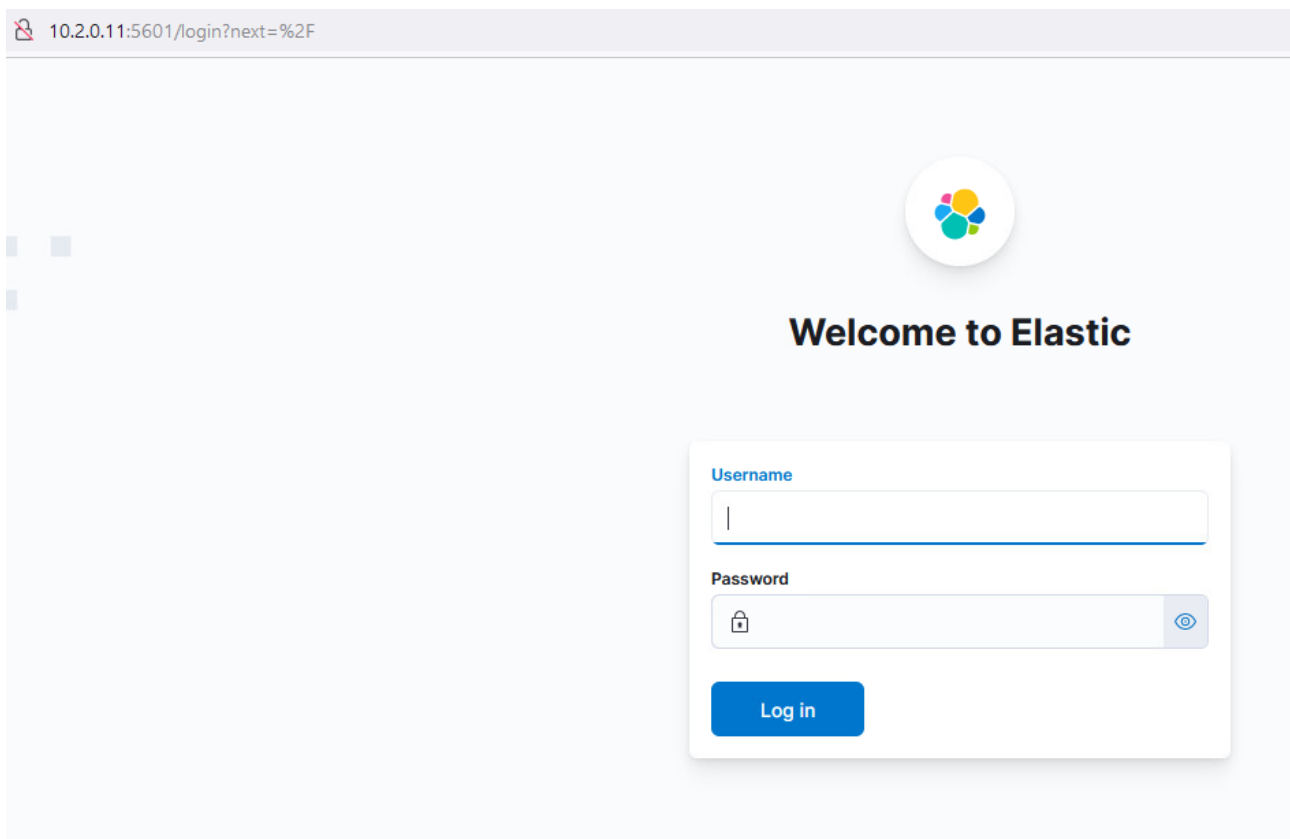
New rules need to be applied on the Palo Alto Firewall for the Elastic SIEM to function correctly. The first new rule defines the traffic between Admin-net and Servers-net, workstations and the DMZ. This ensures connectivity between the SIEM system in Admin-net and the other machines in the environment. The second rule is defined for SSH connectivity between WS01 and the machines in the DMZ. These are WWW and NS01. This rule allows agent installations in the Linux machines in the DMZ. Agent installation is covered in more detail in section 5.3. All installations are performed on WS01.

Figure 1: New security policy rules

12	G3_SIEM	none	universal	 DMZ  SERVERS-NET  WS-NET	any	any	any	 ADMIN-NET	any	any	any	any	 Allow
13	G3_nameserver_ssh	none	universal	 WS-NET	any	any	any	 DMZ	any	any	 ssh	any	 Allow

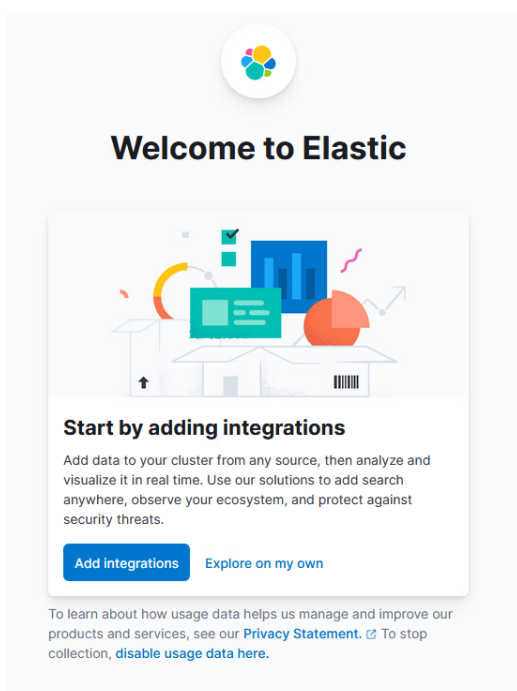
The SIEM is accessible via the browser on WS01 once the above rules have been defined. The address for the SIEM is <http://10.2.0.11:5601>. The initial login credentials are elastic / elastic.

Figure 2: Elastic SIEM login screen



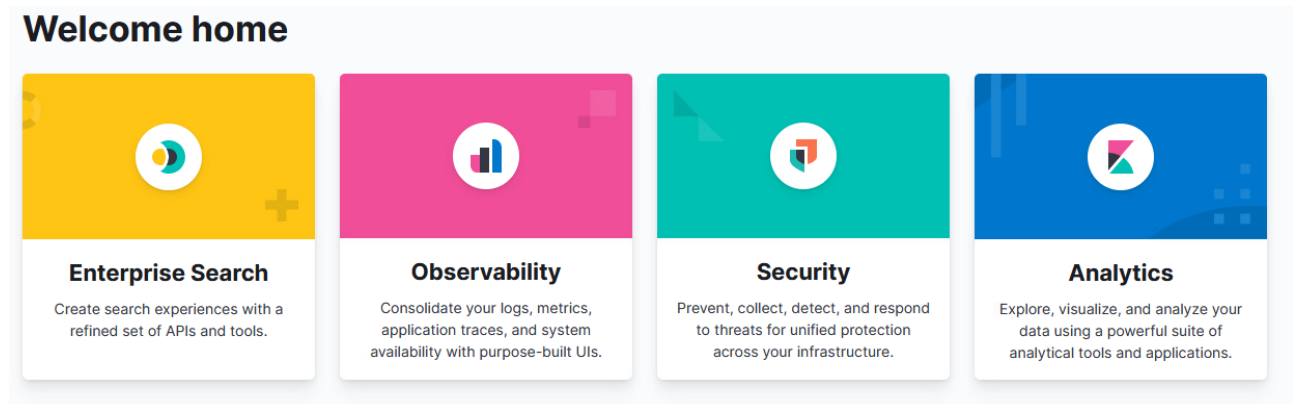
The user is greeted with a *Welcome to Elastic* message and a suggestion to begin by adding integrations. The *Explore on my own* option is selected.

Figure 3: Welcome to Elastic



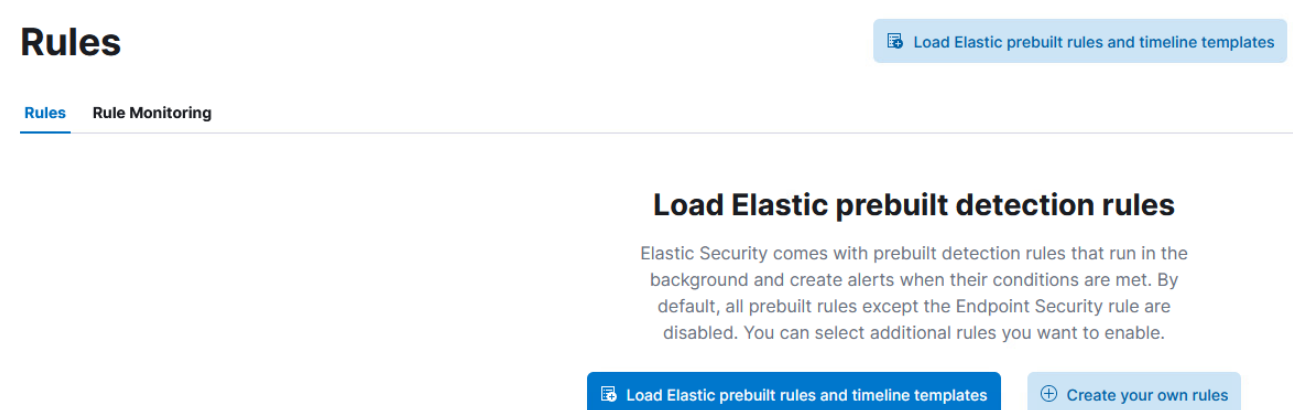
Security is selected from the options available below.

Figure 4: Choose Security



Within the Security menu the Rules tab is chosen. Premade rules and timeline templates can then be loaded.

Figure 5: Select prebuilt rules and timeline templates



All rules should be selected. They can be installed in bulk.

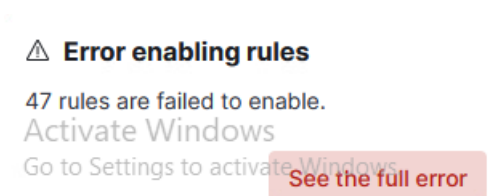
Figure 6: SIEM rules

Showing 734 rules | Selected 734 rules [× Clear selection](#) Bulk actions [v](#) [Refresh](#) [Refresh settings v](#)

<input checked="" type="checkbox"/> Rule			Risk score
<input checked="" type="checkbox"/> Endpoint Security	0/1 integrations	2	47
<input checked="" type="checkbox"/> Potential Admin Group Account Addition	0/1 integrations	5	47
<input checked="" type="checkbox"/> Potential Hidden Local User Account Creation	0/1 integrations	5	47
<input checked="" type="checkbox"/> SystemKey Access via Command Line	0/1 integrations	5	73
<input checked="" type="checkbox"/> TCC Bypass via Mounted APFS Snapshot Access	0/1 integrations	6	73
<input checked="" type="checkbox"/> RDP (Remote Desktop Protocol) from the Internet		6	47
<input checked="" type="checkbox"/> SMTP on Port 26/TCP		6	21
<input checked="" type="checkbox"/> MsBuild Making Network Connections	0/2 integrations	5	47
<input checked="" type="checkbox"/> Exploit - Detected - Elastic Endgame		5	73
<input checked="" type="checkbox"/> Suspicious Hidden Child Process of Launchd	0/1 integrations	6	47
<input checked="" type="checkbox"/> Web Application Suspicious Activity: POST Request Declin...	0/1 integrations	2	47

Not all rules are expected to be enabled successfully. The task description indicates failures during this process can safely be ignored.

Figure 7: Error enabling rules



5.2 Fleet Server

A Fleet Server can be created after the basic settings are established. Fleet Servers are centralized hubs for agent installation and configuration (Elastic, n.d.-e). Agents are installed on target

machines. They rely on information regarding actions performed on targets. This takes the form of logs and security events. These are then relayed back to the SIEM. The logging and security event examination process is described in detail in section 5.2.

Figure 8: Fleet server installation

Add a Fleet Server

A Fleet Server is required before you can enroll agents with Fleet. Follow the instructions below to set up a Fleet Server. For more information, see the [Fleet and Elastic Agent Guide](#).

Quick Start

Advanced

1 Get started with Fleet Server

First, set the public IP or host name and port that agents will use to reach Fleet Server. It uses port **8220** by default. We'll then generate a policy for you automatically.

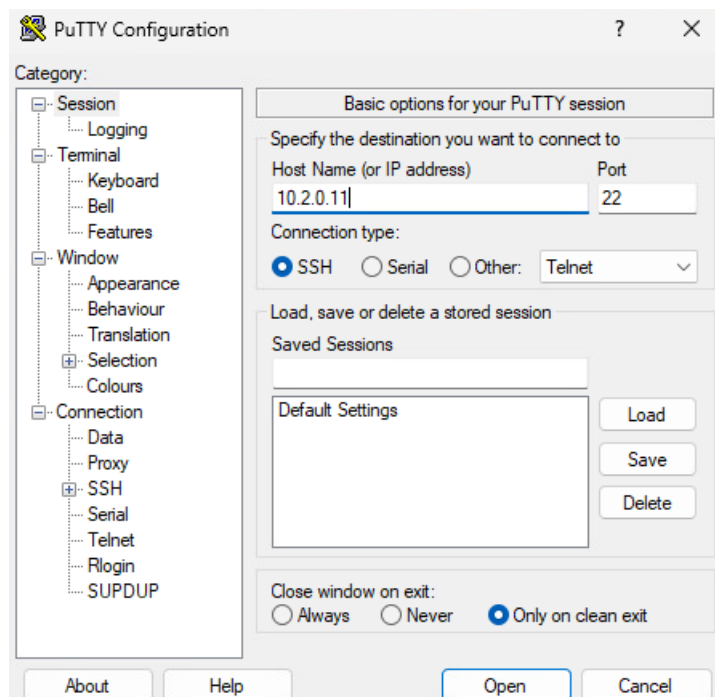
Fleet Server host

https://10.2.0.11:8220

Generate Fleet Server policy

The Fleet Server host IP address is associated with port 8220 for the. The IP address in this case is <https://10.2.0.11>. An SSH connection from WS01 to the SIEM is required for the policy to be defined.

Figure 9: SSH connection to SIEM



The instructions provide a set of Linux terminal commands used in the installation.

Figure 10: Fleet server installation on SIEM

Install Fleet Server to a centralized host

Install Fleet Server agent on a centralized host so that other hosts you wish to monitor can connect to it. In production, we recommend using one or more dedicated hosts. For additional guidance, see our [installation docs](#).

Linux Tar Mac Windows RPM DEB

```
curl -L -O https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.3.3-linux-x86_64.tar.gz
tar xzvf elastic-agent-8.3.3-linux-x86_64.tar.gz
cd elastic-agent-8.3.3-linux-x86_64
sudo ./elastic-agent install \
  --fleet-server-es=https://10.2.0.11:9200 \
  --fleet-server-service-token=AAEAAWVsYXN0aWVZmx1ZXQtc2VydMvYl3Rva2VuLTE2OTY1ODY1Mjc4Nzc6MUDHNG5xVzNUUXVqRWt5dVRpYz1SUQ \
  --fleet-server-policy=fleet-server-policy \
  --fleet-server-es-ca-trusted-fingerprint=e18a3dbf38c9dbc62fee265f0a414feb1fae084e2d6ec77f04ea6e1bddd4effa
```

The terminal session indicates the installation is successful.

Figure 11: Installation successful

```
Elastic Agent will be installed at /opt/Elastic/Agent and will run as a service. Do you want to continue? [Y/n]:y
{"log.level":"info","@timestamp":"2023-10-06T13:07:50.864+0300","log.origin":{"file.name":"cmd/enroll_cmd.go","file.line":403},"message":"Generating self-signed certificate for Fleet Server","ecs.version":"1.6.0"}
{"log.level":"info","@timestamp":"2023-10-06T13:07:52.128+0300","log.origin":{"file.name":"cmd/enroll_cmd.go","file.line":759},"message":"Waiting for Elastic Agent to start Fleet Server","ecs.version":"1.6.0"}
{"log.level":"info","@timestamp":"2023-10-06T13:07:54.130+0300","log.origin":{"file.name":"cmd/enroll_cmd.go","file.line":792},"message":"Fleet Server - Starting","ecs.version":"1.6.0"}
{"log.level":"info","@timestamp":"2023-10-06T13:07:58.133+0300","log.origin":{"file.name":"cmd/enroll_cmd.go","file.line":773},"message":"Fleet Server - Running on policy with Fleet Server integration: fleet-server-policy; missing config fleet.agent.id (expected during bootstrap process)","ecs.version":"1.6.0"}
{"log.level":"info","@timestamp":"2023-10-06T13:07:58.636+0300","log.origin":{"file.name":"cmd/enroll_cmd.go","file.line":471},"message":"Starting enrollment to URL: https://siem:8220/", "ecs.version":"1.6.0"}
{"log.level":"info","@timestamp":"2023-10-06T13:07:59.642+0300","log.origin":{"file.name":"cmd/enroll_cmd.go","file.line":273},"message":"Successfully triggered restart on running Elastic Agent.", "ecs.version":"1.6.0"}
Successfully enrolled the Elastic Agent.
Elastic Agent has been successfully installed.
[root@siem elastic-agent-8.3.3-linux-x86_64]#
```

5.3 Agents

The agent installation process is similar for all machines. Only the installation process for WS01 is described here for the sake of brevity. Examples of differences between agent installations in Linux and Windows environments are also provided. A different approach for agent setup is necessary on the NS01 and WWW machines. This is also documented.

A new policy first needs to be defined in order for the agent installation to proceed. The policies themselves are similar. Individual policies for Workstations, Servers, the nameserver and the WWW machine were defined for the sake of clarity. Tightly defined policies will be also easier to adjust in the future if necessary.

Figure 12: Add agent screen

Add agent

Add Elastic Agents to your hosts to collect data and send it to the Elastic Stack.

[Enroll in Fleet](#) [Run standalone](#)

Enroll an Elastic Agent in Fleet to automatically deploy updates and centrally manage the agent.

1 What type of host are you adding?

Type of hosts are controlled by an [agent policy](#). Create a new agent policy to get started.

[Create policy](#)

☒ Collect system logs and metrics ⓘ

> [Advanced options](#)

2 Install Elastic Agent on your host

Elastic provides the terminal commands necessary to install, enrol and initialise agents on Windows machines.

Figure 13: Agent installation on host

2 Install Elastic Agent on your host

Select the appropriate platform and run commands to install, enroll, and start Elastic Agent. Reuse commands to set up agents on more than one host. For aarch64, see our [downloads page](#). For additional guidance, see our [installation docs](#).

Linux Tar Mac **Windows** RPM DEB

```
$ProgressPreference = 'SilentlyContinue'
Invoke-WebRequest -Uri https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.3.3-windows-x86_64.zip -DestinationPath .
Expand-Archive .\elastic-agent-8.3.3-windows-x86_64.zip -DestinationPath .
cd elastic-agent-8.3.3-windows-x86_64
.\elastic-agent.exe install --url=https://10.2.0.11:8220 --enrollment-token=bGt0M0JJc0JqazdGTV
```

These are then copied in the terminal. Commands are run as administrator. The suffix `--insecure` is added to the end of the command line as instructed.

Figure 14: WS01 agent installation in Windows

```

Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\g3_domadmin> $ProgressPreference = 'SilentlyContinue'
PS C:\Users\g3_domadmin> Invoke-WebRequest -Uri https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.3.3-windows-x86_64.zip -OutFile elastic-agent-8.3.3-windows-x86_64.zip
PS C:\Users\g3_domadmin> Expand-Archive .\elastic-agent-8.3.3-windows-x86_64.zip -DestinationPath .
PS C:\Users\g3_domadmin> cd elastic-agent-8.3.3-windows-x86_64
PS C:\Users\g3_domadmin\elastic-agent-8.3.3-windows-x86_64> .\elastic-agent.exe install --url=https://10.2.0.11:8220 --enrollment-token=bGt0M0Jjc0JqazdGTVFHMnlxYW06S3gzM0lKNWRTQzJZS1hHWFF1U1c4Zw== --insecure

```

Figure 15: WS01 agent installation continued

```

Elastic Agent will be installed at C:\Program Files\Elastic\Agent and will run as a service. Do you want to continue? [Y/n]:Y
{"log.level":"warn","@timestamp":"2023-10-06T13:15:19.654+0300","log.logger":"tls","log.origin":{"file.name":"tlscommon/tls_config.go","file.line":104},"message":"SSL/TLS verifications disabled.","ecs.version":"1.6.0"}
{"log.level":"info","@timestamp":"2023-10-06T13:15:20.641+0300","log.origin":{"file.name":"cmd/enroll_cmd.go","file.line":471},"message":"Starting enrollment to URL: https://10.2.0.11:8220/","ecs.version":"1.6.0"}
{"log.level":"warn","@timestamp":"2023-10-06T13:15:20.762+0300","log.logger":"tls","log.origin":{"file.name":"tlscommon/tls_config.go","file.line":104},"message":"SSL/TLS verifications disabled.","ecs.version":"1.6.0"}
{"log.level":"info","@timestamp":"2023-10-06T13:15:21.511+0300","log.origin":{"file.name":"cmd/enroll_cmd.go","file.line":273},"message":"Successfully triggered restart on running Elastic Agent."}
Successfully enrolled the Elastic Agent.
Elastic Agent has been successfully installed.
PS C:\Users\g3_domadmin\elastic-agent-8.3.3-windows-x86_64>

```

The process is confirmed in the dashboard once the installation is complete.

Figure 16: Agent installation confirmed



Agent enrollment confirmed

✓ 1 agent has been enrolled.

[View enrolled agents](#)



Incoming data confirmed

✓ Incoming data received from 1 of 1 recently enrolled agent.

5.3.1 Agent installation on NS01 and WWW

Some settings need to be adjusted on the NS01 and WWW machines. SSH connections are prohibited on these machines in the DMZ by default. This requires updating the PA-VM settings presented in section 5. The *SSHD_config* files on NS01 and WWW should also be updated. The *PasswordAuthentication* option in both cases should to be changed from *no* to *yes*.

Figure 17: Setting PasswordAuthentication to yes

```
# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication yes
#PermitEmptyPasswords no
#PasswordAuthentication no
```

An SSH connection from WS01 can be established once these changes are implemented. The same procedure is followed on WS01.

Figure 18: Agent installation for NS01

```
[root@ns1 elastic-agent-8.3.3-linux-x86_64]# sudo ./elastic-agent install --url=https://10.2.0.11:8220 --enrollment-token=TFpaaEU0c0JqazdGTVFHMkdObWo6Y0hPRHBDTudTd2VEX1Y1SWVUM3UzUQ== --insecure
Elastic Agent will be installed at /opt/Elastic/Agent and will run as a service. Do you want to continue? [Y/n]:Y
{"log.level":"warn","@timestamp":"2023-10-09T12:16:47.144+0300","log.logger":"tls","log.origin":{"file.name":"tlscommon/tls_config.go","file.line":104},"message":"SSL/TLS verifications disabled.","ecs.version":"1.6.0"}
{"log.level":"info","@timestamp":"2023-10-09T12:16:47.915+0300","log.origin":{"file.name":"cmd/enroll_cmd.go","file.line":471},"message":"Starting enrollment to URL: https://10.2.0.11:8220/","ecs.version":"1.6.0"}
{"log.level":"warn","@timestamp":"2023-10-09T12:16:48.030+0300","log.logger":"tls","log.origin":{"file.name":"tlscommon/tls_config.go","file.line":104},"message":"SSL/TLS verifications disabled.","ecs.version":"1.6.0"}
{"log.level":"info","@timestamp":"2023-10-09T12:16:48.795+0300","log.origin":{"file.name":"cmd/enroll_cmd.go","file.line":273},"message":"Successfully triggered restart on running Elastic Agent.","ecs.version":"1.6.0"}
Successfully enrolled the Elastic Agent.
Elastic Agent has been successfully installed.
[root@ns1 elastic-agent-8.3.3-linux-x86_64]#
```

The *sshd.service* systemctl service must be restarted before the changes will take effect.

Figure 19: systemctl restart sshd.service

```
[root@ns1 ssh]# systemctl restart sshd.service
[root@ns1 ssh]# _
```

5.3.2 Viewing results

Agents can be viewed from the Fler Server's main menu once they are installed.

Figure 20: All agents installed

Fleet
Centralized management for Elastic Agents.

[Agents](#) [Agent policies](#) [Enrollment tokens](#) [Data streams](#) [Settings](#)

Filter your data using KQL syntax Status ▾ Tags 0 ▾ Agent policy 5 ▾ Upgrade available Add Fleet Server Add agent

Showing 7 agents ● Healthy 7 ● Unhealthy 0 ● Updating 0 ● Offline 0

<input type="checkbox"/>	Host	Status	Tags	Agent policy	Version	Last activity	Actions
<input type="checkbox"/>	www.group3.ttc60z.vle.f i	Healthy		G3_WWW rev. 1	8.3.3	22 seconds ago	...
<input type="checkbox"/>	ns1.group3.ttc60z.vle.fi	Healthy		G3_nameserver rev. 1	8.3.3	22 seconds ago	...
<input type="checkbox"/>	WSUS	Healthy		G3_servers rev. 1	8.3.3	29 seconds ago	...
<input type="checkbox"/>	SRV01	Healthy		G3_servers rev. 1	8.3.3	26 seconds ago	...
<input type="checkbox"/>	DC01	Healthy		G3_servers rev. 1	8.3.3	16 seconds ago	...
<input type="checkbox"/>	WS01	Healthy		G3_workstations rev. 1	8.3.3	24 seconds ago	...
<input type="checkbox"/>	siem	Healthy		Fleet Server Policy rev. 1	8.3.3	1 second ago	...

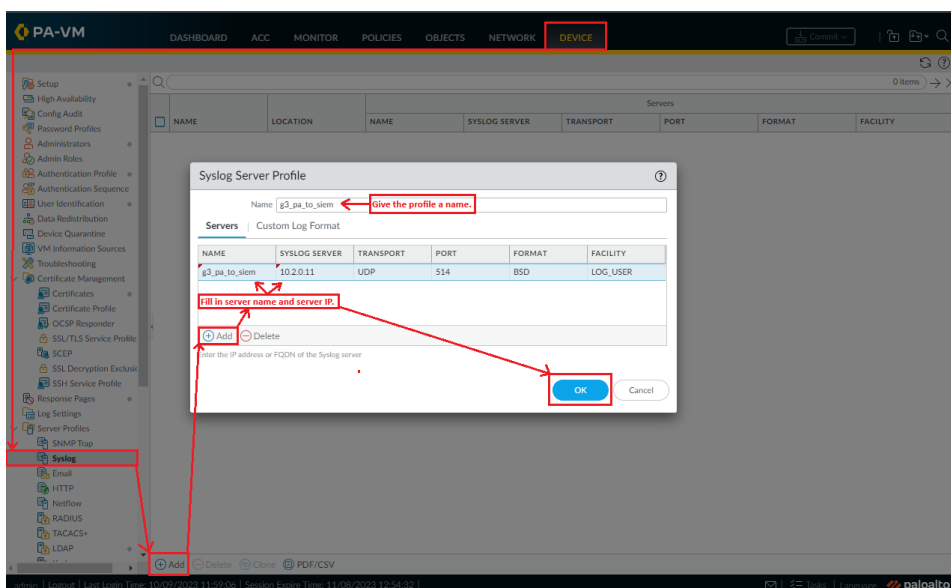
Rows per page: 20 ▾ < 1 >

5.4 Logging

5.4.1 Enabling firewall logging

This section describes how to enable firewall logging in the SIEM. First a syslog profile should be created.

Figure 21: Syslog profile creation



A log forwarding profile should then be created. This will be used to generate a log forwarding match list. The list is comprised of objects used to forward the required log types through the syslog service. There are two necessary log types in the VLE environment: traffic and threats. Figure 22 illustrates the log forwarding profile and log forwarding match list creation processes. The completed log forwarding profile object is shown in figure 23.

Figure 22: Log forwarding profile and log forwarding profile match list

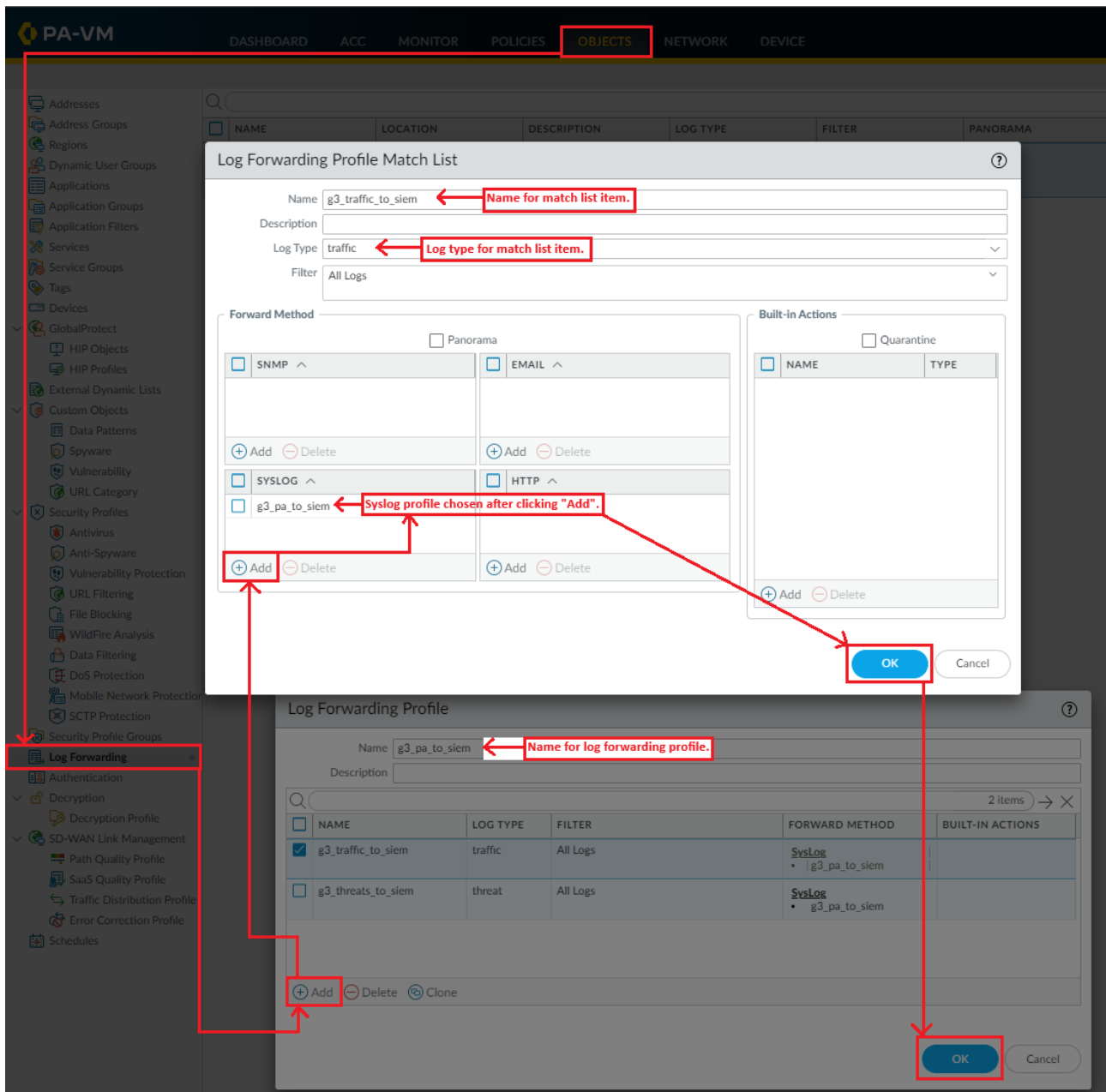
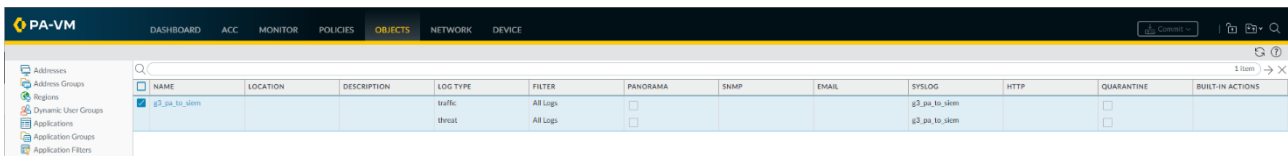


Figure 23: Log forwarding profile object



NAME	LOCATION	DESCRIPTION	LOG TYPE	FILTER	PANORAMA	SNMP	EMAIL	SYSLOG	HTTP	QUARANTINE	BUILT-IN ACTIONS
g3_pa_to_siem			traffic	All Logs	<input type="checkbox"/>			g3_pa_to_siem		<input type="checkbox"/>	
			threat	All Logs	<input type="checkbox"/>			g3_pa_to_siem		<input type="checkbox"/>	

The log forwarding profile is then applied to security policies. The policies in question are *intrazone-default* and *interzone-default*. This is sufficient to cover traffic monitoring and alerts. Figure 24 demonstrates how the policy forward logs upon clicking. Figure 25 shows the selected policy icons when log forwarding is set to *active*.

Figure 24: Policy forwarding logs

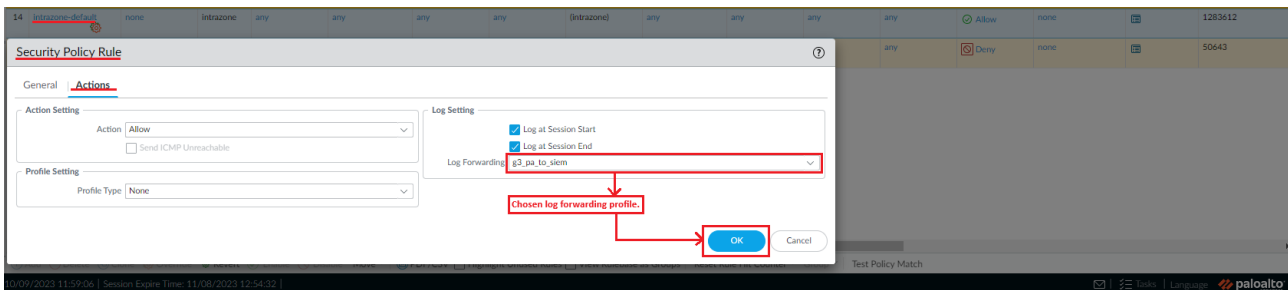
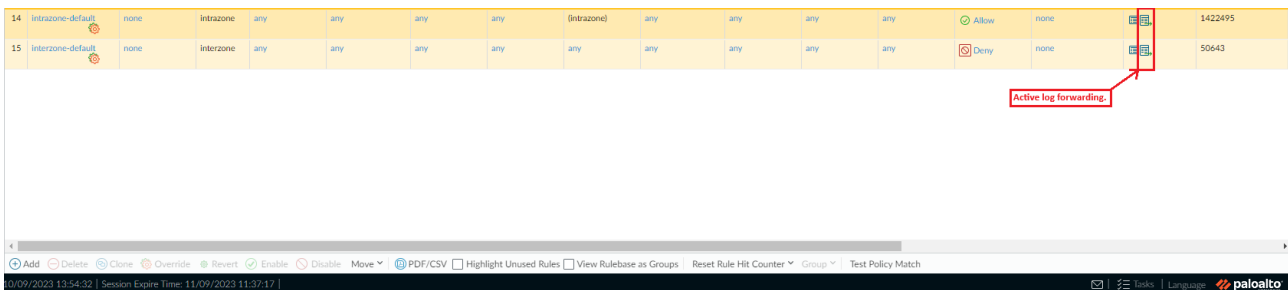


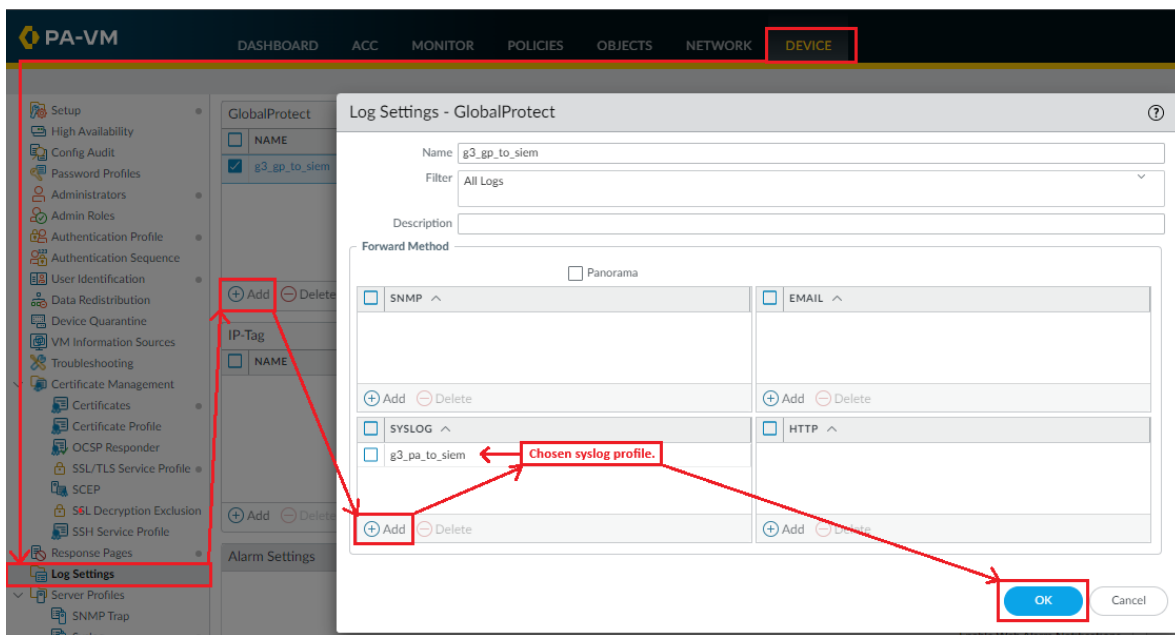
Figure 25: Active log forwarding



ID	Name	Location	Description	Log Type	Filter	Panorama	SNMP	Email	Syslog	HTTP	Quarantine	Built-in Actions	Log Forwarding	Log Forwarding Profile	Log Forwarding Status	Log Forwarding Description
14	Intrazone-default	none	intrazone	any	any	any	any	(Intrazone)	any	any	any	any	Allow	none	<input checked="" type="checkbox"/>	Active log forwarding.
15	Interzone-default	none	interzone	any	any	any	any	any	any	any	any	any	Deny	none	<input checked="" type="checkbox"/>	Active log forwarding.

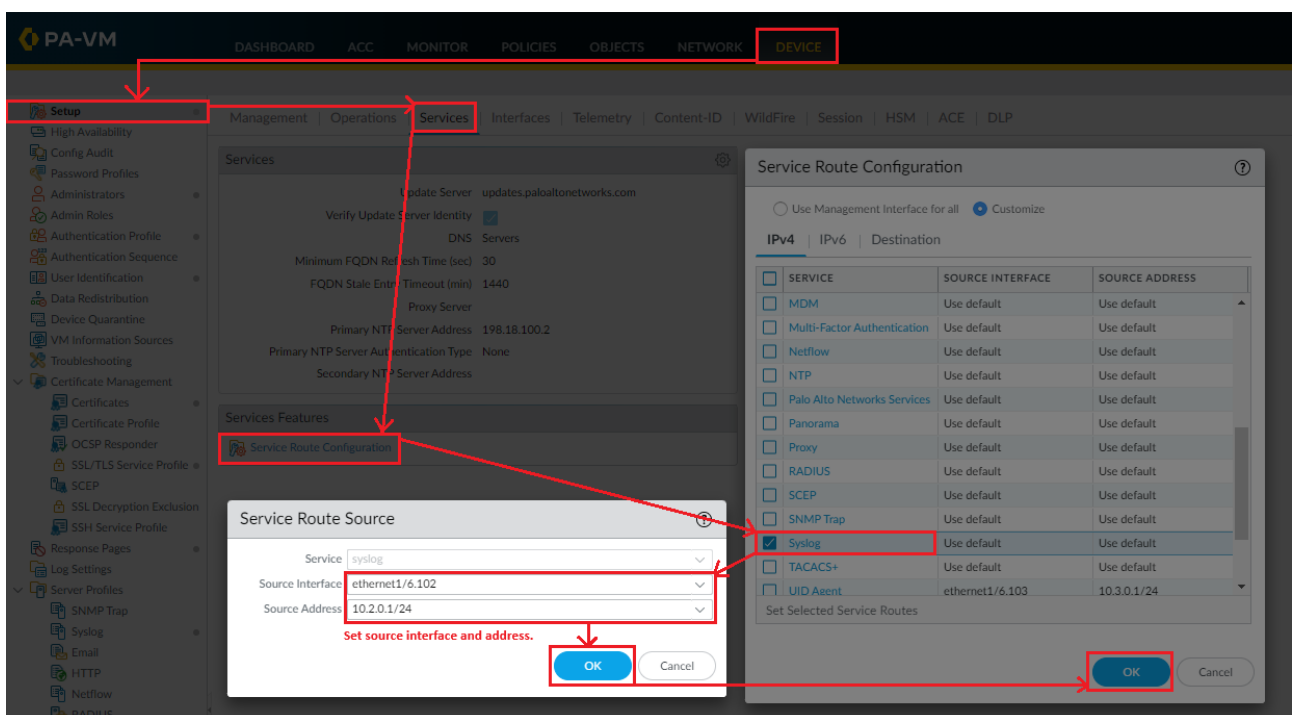
GlobalProtect logs are required in addition to traffic and threat logs. Figure 26 demonstrates how logging settings for GlobalProtect can be defined.

Figure 26: GlobalProtect logs activated



The next step is to configure a service route. This involves customizing and enabling syslog. Changes should be committed after all configuration modifications have been implemented.

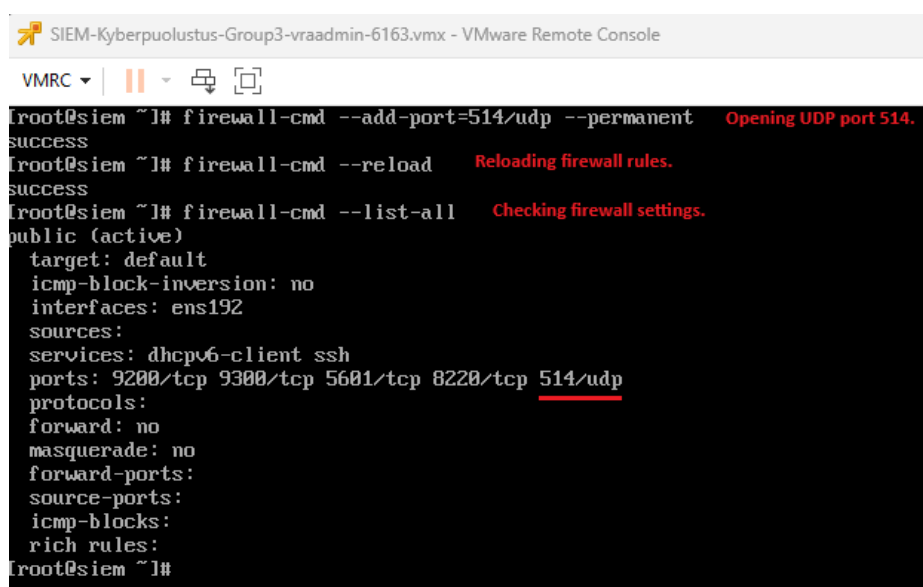
Figure 27: Service route configuration



5.4.2 Sending firewall logs to the SIEM

Changes to the SIEM configuration are required for firewall logs to be available for analysis. The first step is to open UDP port 514 on the SIEM's internal firewall. Firewall rules should then be refreshed. Settings should be checked to confirm the port has been added correctly. The PuTTY SSH client can be used to connect to the SIEM from WS01.

Figure 28: Opening UDP port 514 on the SIEM firewall



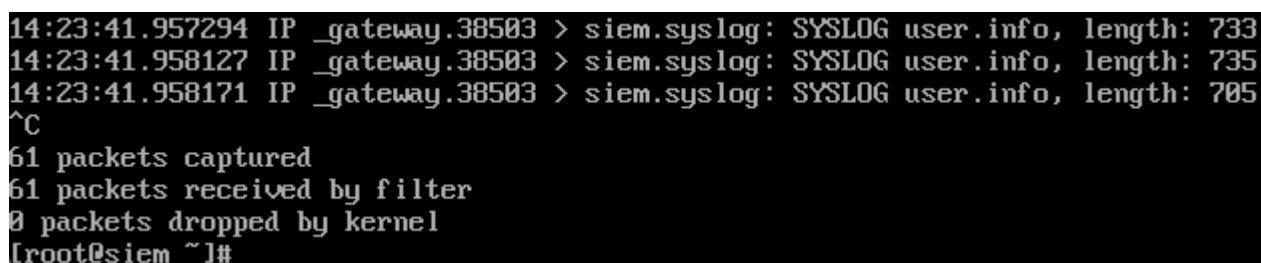
```

SIEM-Kyberpuolustus-Group3-vraadmin-6163.vmx - VMware Remote Console
VMRC | [Icons]
[root@siem ~]# firewall-cmd --add-port=514/udp --permanent  Opening UDP port 514.
success
[root@siem ~]# firewall-cmd --reload  Reloading firewall rules.
success
[root@siem ~]# firewall-cmd --list-all  Checking firewall settings.
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: ens192
  sources:
  services: dhcpv6-client ssh
  ports: 9200/tcp 9300/tcp 5601/tcp 8220/tcp 514/udp
  protocols:
  forward: no
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
[root@siem ~]#

```

The *tcpdump port 514* command tests if data originates from the firewall. Captured packets should confirm the connection and data flow.

Figure 29: Data coming from Palo Alto to SIEM



```

14:23:41.957294 IP _gateway.38503 > siem.syslog: SYSLOG user.info, length: 733
14:23:41.958127 IP _gateway.38503 > siem.syslog: SYSLOG user.info, length: 735
14:23:41.958171 IP _gateway.38503 > siem.syslog: SYSLOG user.info, length: 705
^C
61 packets captured
61 packets received by filter
0 packets dropped by kernel
[root@siem ~]#

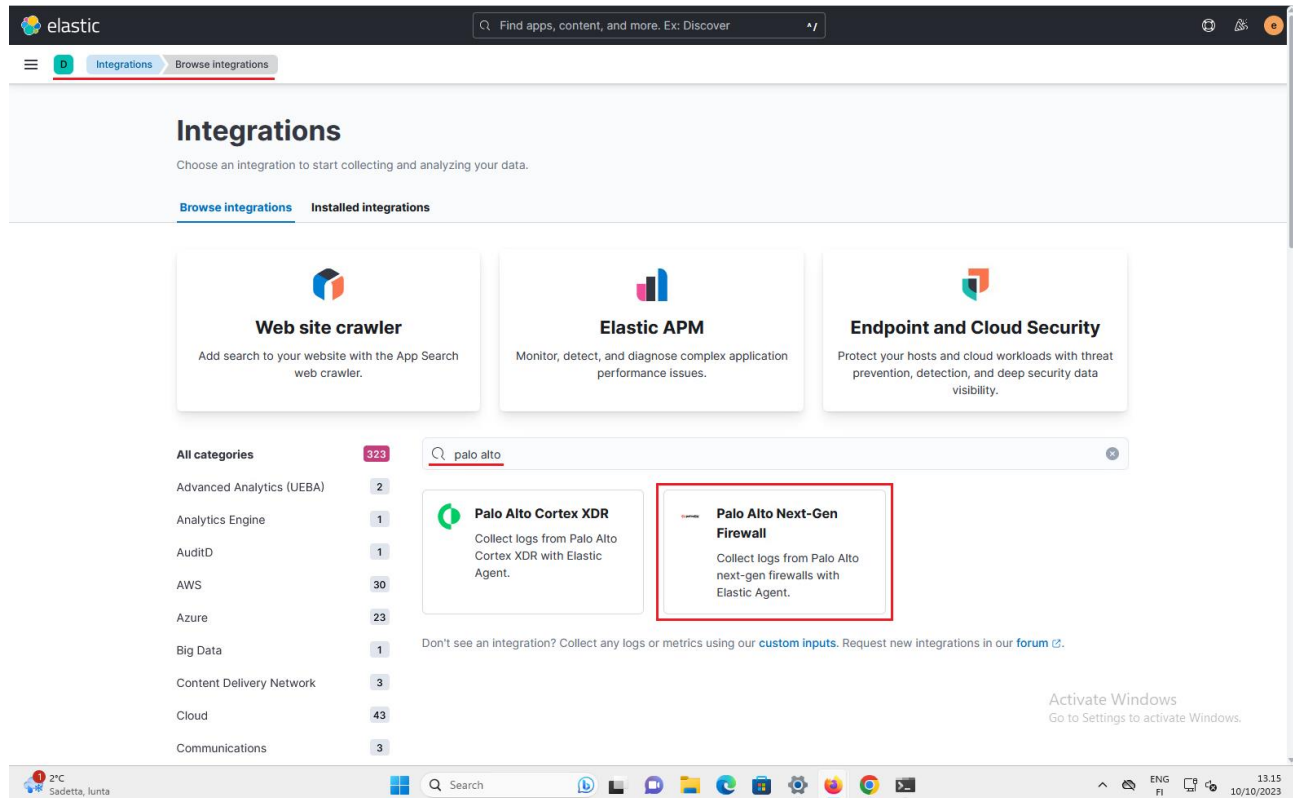
```

5.4.3 Data collection integrations

The next step is to add the necessary integrations to collect and utilize the data. Integrations are added through the Elastic GUI. The connection is established via the browser on WS01. This requires

navigating to the SIEM IP address and inputting the elastic user-credentials. The first integration added is for the Palo Alto Next-Gen Firewall.

Figure 30: Palo Alto Next-Gen Firewall integration



Beats integration is next. Figure 32 shows the *Palo Alto Networks PAN-OS Logs* module page after the link in Figure 31 is clicked. The page contains instructions on how to install Filebeat on the SIEM machine. Filebeat is a log shipper which monitors, collects and forwards log files (Elastic, n.d.-f). The installation process is presented in Figures 33 to 37.

Figure 31: Beats logging integration

Also available in Beats

Elastic Agent Integrations are recommended, but you can also use Beats. For more details, check out our [comparison page](#).

[Palo Alto Networks PAN-OS Logs](#)

Figure 32: Palo Alto Networks PAN-OS Logs module

[Browse all integrations](#)

Palo Alto Networks PAN-OS Logs

This is a module for Palo Alto Networks PAN-OS firewall monitoring logs received over Syslog or read from a file. It currently supports messages of Traffic and Threat types. [Learn more](#).

[View exported fields](#)

③ A newer version of this module is [available as an Elastic Agent integration](#). To learn more about integrations and the new Elastic Agent, read our [announcement blog post](#).

Self managed Elastic Cloud

macOS Linux DEB **Linux RPM** Windows

Getting Started

- Download and install Filebeat**

First time using Filebeat? See the [Quick Start](#).

```
curl -L -O https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-8.3.3-x86_64.rpm
sudo rpm -vi filebeat-8.3.3-x86_64.rpm
```

Looking for the 32-bit packages? See the [Download page](#).

Figure 33: Installing Filebeat on the SIEM

```
root@siem:~
[root@siem ~]# curl -L -O https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-8.3.3-x86_64.rpm
% Total    % Received % Xferd Average Speed   Time    Time     Time  Current
           Dload  Upload   Total   Spent    Left   Speed
100 57.1M  100 57.1M    0     0  15.5M    0  0:00:03  0:00:03 --:--:-- 15.5M
[root@siem ~]# sudo rpm -vi filebeat-8.3.3-x86_64.rpm
Verifying packages...
Preparing packages...
filebeat-8.3.3-1.x86_64
[root@siem ~]#
```

Some minor configuration changes to the filebeat.yml in /etc/filebeat/ are necessary. The relevant fingerprint can be found and copied through the Elastic GUI. This is executed on the Fleet tab. The path is as follows: *Fleet -> Settings -> Outputs -> Actions -> Modify*.

Figure 34: filebeat.yml configuration

```

root@siem:/etc/filebeat/modules.d
GNU nano 2.9.8 /etc/filebeat/filebeat.yml

# ===== Kibana =====
# Starting with Beats version 6.0.0, the dashboards are loaded via the Kibana API.
# This requires a Kibana endpoint configuration.
setup.kibana:

# Kibana Host
# Scheme and port can be left out and will be set to the default (http and 5601)
# In case you specify an additional path, the scheme is required: http://localhost:5601/path
# IPv6 addresses should always be defined as: https://[2001:db8::1]:5601
host: "localhost:5601"

# Kibana Space ID
# ID of the Kibana Space into which the dashboards should be loaded. By default,
# the Default Space will be used.
#space.id:

# ===== Elastic Cloud =====
# These settings simplify using Filebeat with the Elastic Cloud (https://cloud.elastic.co/).

# The cloud.id setting overwrites the 'output.elasticsearch.hosts' and
# 'setup.kibana.host' options.
# You can find the 'cloud.id' in the Elastic Cloud web UI.
#cloud.id:

# The cloud.auth setting overwrites the 'output.elasticsearch.username' and
# 'output.elasticsearch.password' settings. The format is 'user:password'.
#cloud.auth:

# ===== Outputs =====
# Configure what output to use when sending the data collected by the beat.

# ----- Elasticsearch Output -----
output.elasticsearch:
  # Array of hosts to connect to.
  hosts: ["https://localhost:9200"]

  # Protocol - either 'http' (default) or 'https'.
  #protocol: "https"

  # Authentication credentials - either API key or username/password.
  #api_key: "id:api key"
  username: "" Elastic credentials.
  password: ""
  ssl.ca_trusted_fingerprint: "" Fingerprint.

# ----- Logstash Output -----

```

The *panw* Filebeat module should be enabled before the Filebeat service can be initialized. This process is shown in Figure 35. Figure 36 displays the changes made to the *panw.yml* file located in */etc/filebeat/modules.d/*.

Figure 35: Filebeat setup

```

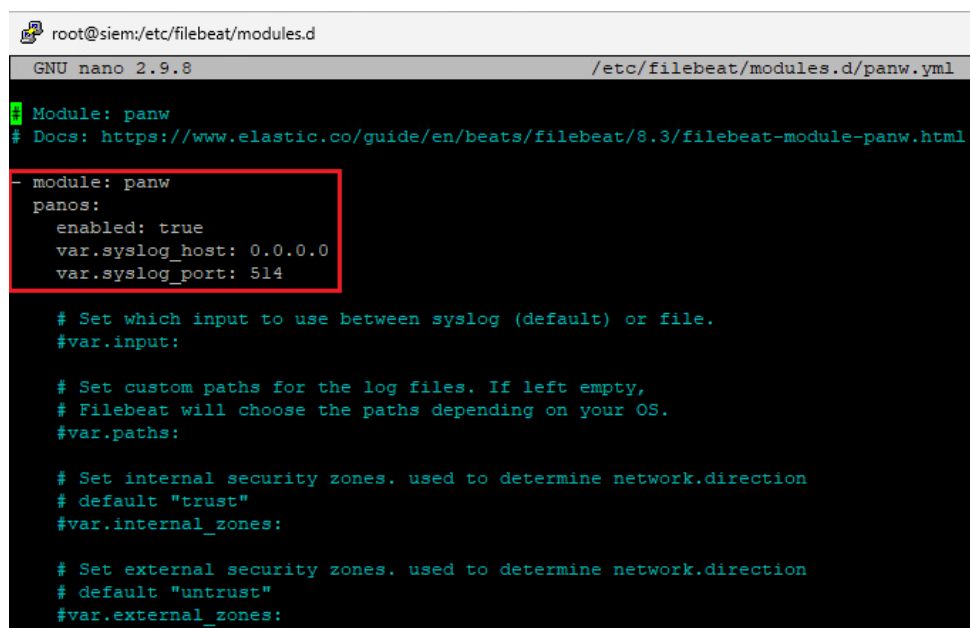
root@siem:/etc/filebeat/modules.d

[root@siem modules.d]# sudo filebeat modules enable panw
Enabled panw
[root@siem modules.d]# nano /etc/filebeat/modules.d/panw.yml
[root@siem modules.d]# sudo filebeat setup
Overwriting ILM policy is disabled. Set `setup.ilm.overwrite: true` for enabling.

Index setup finished.
Loading dashboards (Kibana must be running and reachable)
Loaded dashboards
Loaded Ingest pipelines
[root@siem modules.d]# sudo service filebeat start
Starting filebeat (via systemctl): [ OK ]
[root@siem modules.d]#

```

Figure 36: Configurations in panw.yml



```

root@siem:/etc/filebeat/modules.d
GNU nano 2.9.8 /etc/filebeat/modules.d/panw.yml
Module: panw
# Docs: https://www.elastic.co/guide/en/beats/filebeat/8.3/filebeat-module-panw.html

- module: panw
  panos:
    enabled: true
    var.syslog_host: 0.0.0.0
    var.syslog_port: 514

# Set which input to use between syslog (default) or file.
#var.input:

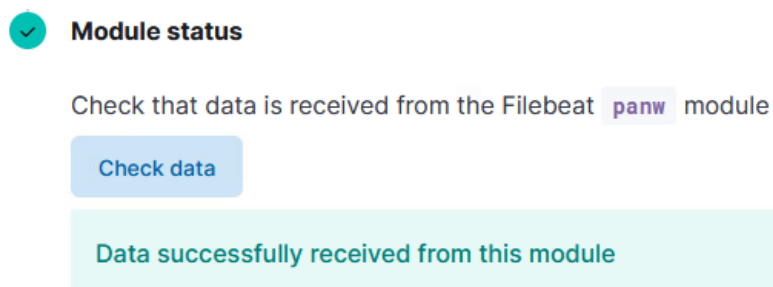
# Set custom paths for the log files. If left empty,
# Filebeat will choose the paths depending on your OS.
#var.paths:

# Set internal security zones. used to determine network.direction
# default "trust"
#var.internal_zones:

# Set external security zones. used to determine network.direction
# default "untrust"
#var.external_zones:

```

Module connectivity can be tested in the Elastic GUI. Data flow will be viewable in the GUI if the *panw* file is configured correctly.

Figure 37: Data received from the *panw* module

5.5 Windows integrations

There are four Windows machines in the VLE environment. Logs from these machines must be viewable in the SIEM. WS01 is located in the WS-net subnet. DC01, WSUS and SRV01 are located in the Server-net subnet. The Windows integration process for the WS01 machine is shown below. The steps taken have been replicated on all other Windows machines. Figure 38 illustrates the initial phase of the integration process.

Figure 38: Windows integration

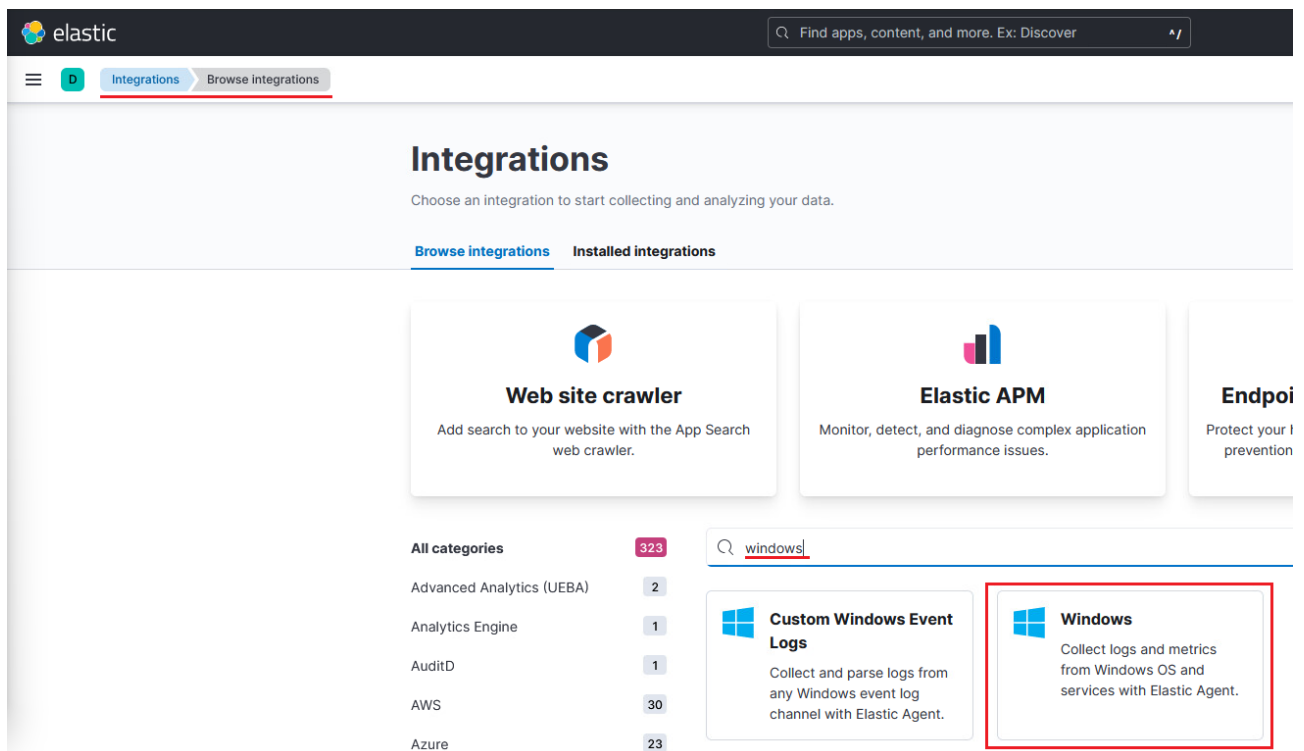


Figure 39: Adding the Elastic agent to Windows

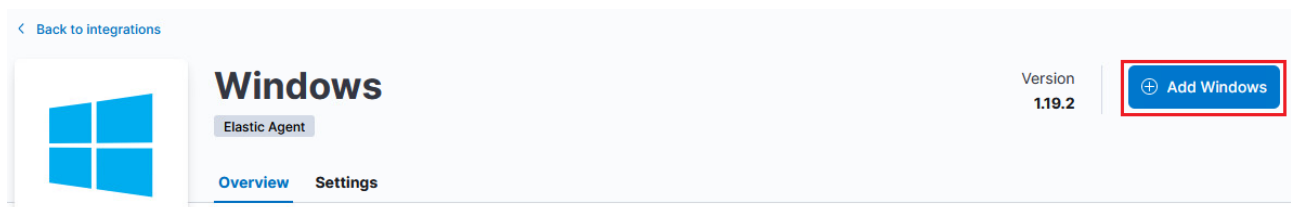


Figure 40 presents the agent configurations for WS01. A name for the integration is required. A description can also be provided but is not required. Log collection options can be left at the default values. Integration should be added to the existing host. A policy can then be selected. The agent policy for WS01 is in this case *G3_workstations*. There is one agent on the workstation.

The *G3_servers* policy provides integration for servers in the environment. It covers three machines. Agents for each machine can be added simultaneously. After clicking *Save and continue* a confirmation window for agent deployment (or updating) will appear. Clicking *Save and deploy changes* deploys the agent on WS01.

Figure 40: Agent configuration

Add Windows integration Agent policy: **G3_workstations**

Configure an integration for the selected agent policy.

1 Configure integration

Integration settings
Choose a name and description to help identify how this integration will be used.

Integration name:

Description: Optional

[Advanced options](#)

☒ Collect events from the following Windows event log channels: [Change defaults](#)

☒ Collect Windows perfmon and service metrics [Change defaults](#)

☐ Collect logs from third-party REST API (experimental) [Change defaults](#)

2 Where to add this integration?

New hosts: Existing hosts

Agent policy: G3_workstations
1 agent is enrolled with the selected agent policy.

Activate Windows
Go to Settings to activate Windows.

[Cancel](#) Save and continue

Figure 41: Agent deployment confirmation

Save and deploy changes

This action will update 1 agent

Fleet has detected that the selected agent policy, **G3_workstations**, is already in use by some of your agents. As a result of this action, Fleet will deploy updates to all agents that use this policy.

This action can not be undone. Are you sure you wish to continue?

[Cancel](#) Save and deploy changes

The second integration is for Endpoint and Cloud Security. The *Browse integrations* page is accessible via the *Integrations* tab. The process follows the same logic as above. The configuration in Figure 42 concerns WS01 endpoint policy. A similar process is required for servers. It is possible to enable the G3_servers policy on three agents simultaneously. Agents are updated when *Save and continue* is clicked and updates are accepted.

Figure 42: Endpoint and Cloud Security integration

Add Endpoint and Cloud Security integration

Agent policy
G3_workstations

Configure an integration for the selected agent policy.

1 Configure integration

Integration settings
Choose a name and description to help identify how this integration will be used.

Integration name
WS01-endpoint

Description
Optional

> Advanced options

We'll save your integration with our recommended defaults. You can change this later by editing the Endpoint and Cloud Security integration within your agent policy.

2 Where to add this integration?

New hosts
Existing hosts

Agent policy
Agent policies are used to manage a group of integrations across a set of agents.

Agent policy
G3_workstations

1 agent is enrolled with the selected agent policy.

Cancel Save and continue

Figures 43 and 44 show the integration policies tab in Elastic after agents have been successfully deployed and updated. The next step in the SIEM configuration process is to create and test alert functionality.

Figure 43: Windows integration policies

< Back to integrations

Windows

Elastic Agent

Version
1.19.2

Agent policies
2

+ Add Windows

Overview Integration policies Assets Settings

Integration policy	Version	Agent policy	Last updated by	Last updated	Agents	Actions
Servers-windows	v1.19.2	G3_servers rev. 5	elastic	2 seconds ago	3	...
WS01-windows	v1.19.2	G3_worksta... rev. 3	elastic	15 minutes ago	1	...

Rows per page: 20

< 1 >

Figure 44: Endpoint and Cloud Security integration policies

Back to integrations

Endpoint and Cloud Security

Elastic Agent

Version 8.3.0 Agent policies 2

+ Add Endpoint and Cloud Security

Overview Integration policies Assets Settings Advanced

Integration policy	Version	Agent policy	Last updated by	Last updated	Agents	Actions
Servers-endpoint	v8.3.0	G3_servers rev. 4	e elastic	2 minutes ago	3	...
WS01-endpoint	v8.3.0	G3_worksta... rev. 3	e elastic	10 minutes ago	1	...

Rows per page: 20

< 1 >

6 Testing

The alert system can be tested when the basic configuration is complete. Testing is performed using simulated attacks from Red Canary's Atomic Red Team library. The library is mapped to the MITRE ATT&CK framework. Attacks are executed locally on the target machine using Command Prompt and PowerShell. They are designed to test if malicious activity registers in Elastic's alert system. Attack-vectors associated with specific threat-actors (APT28 and APT 1) are used.

Attacks do not aim to replicate sophisticated APT attack-chains. They are strictly intended to test the alert system. Ten attacks are executed on WS01 for this purpose. They are presented according to their MITRE classifications. The specific commands executed and the alerts produced are presented. A brief analysis and summary of the attacks follows.

6.1 Attack 1: T1087.001 Account Discovery | Local Account

Figure 45: T1087.001 - Account Discovery

Atomic Test #9 - Enumerate all accounts via PowerShell (Local) [🔗](#)

Enumerate all accounts via PowerShell. Upon execution, lots of user account and group information will be displayed.







Supported Platforms: Windows

auto_generated_guid: ae4b6361-b5f8-46cb-a3f9-9cf108ccfe7b

Attack Commands: Run with powershell! [🔗](#)

```
net user
get-localuser
get-localgroupmember -group Users
cmdkey.exe /list
ls C:\Users
get-childitem C:\Users\
dir C:\Users\
get-localgroup
net localgroup
```

Figure 46: Attack alert 1

Actions	@timestamp	Rule	Severity	Risk Score	Reason	host.name	user.name	process.n...	file.name
  	Oct 12, 2023 @ 09:46:10.404	Enumeration of Privileged L...	medium	47	iam event by g3_domadmin on WS01.ad.ttc60z.vle.fi created medium alert...	WS01.ad.ttc...	g3_domadmin	—	—
  	Oct 12, 2023 @ 09:46:10.402	Enumeration of Privileged L...	medium	47	iam event by g3_domadmin on WS01.ad.ttc60z.vle.fi created medium alert...	WS01.ad.ttc...	g3_domadmin	—	—

6.2 Attack 2: T1087.002 Account Discovery | Domain Account

Figure 47: T1087.002 - Account Discovery: Domain account

Atomic Test #12 - Enumerate Active Directory Users with ADSISearcher [↗](#)

The following Atomic test will utilize ADSISearcher to enumerate users within Active Directory. Upon successful execution a listing of users will output with their paths in AD. Reference: <https://devblogs.microsoft.com/scripting/use-the-powershell-adsisearcher-type-accelerator-to-search-active-directory/>







Supported Platforms: Windows

auto_generated_guid: 02e8be5a-3065-4e54-8cc8-a14d138834d3

Attack Commands: Run with **powershell**! [↗](#)

```
([adsisearcher]"objectcategory=user").FindAll(); ([adsisearcher]"objectcategory=user").FindOne()
```

Figure 48: Attack alert 2

Actions	@timestamp	Rule	Severity	Risk Score	Reason	host.name	user.name	process.n...	file.name
  	Oct 12, 2023 @ 10:28:55.441	Connection to Commonly A...	low	21	network event with process powershell.exe;53, by g3_domadmin on WS01...	WS01	g3_domadmin	powershell.exe	—
  	Oct 12, 2023 @ 10:28:55.440	Connection to Commonly A...	low	21	network event with process powershell.exe;53, by g3_domadmin on WS01...	WS01	g3_domadmin	powershell.exe	—

6.3 Attack 3: T1140 Deobfuscate/Decode Files or Information

Figure 49: T1140 - Deobfuscate/Decode Files or Information

Atomic Test #1 - Deobfuscate/Decode Files Or Information [↗](#)

Encode/Decode executable Upon execution a file named T1140_calc_decoded.exe will be placed in the temp folder

Supported Platforms: Windows

auto_generated_guid: dc6fe391-69e6-4506-bd06-ea5eeb4082f8

Inputs: [↗](#)

Name	Description	Type	Default Value
executable	name of executable	path	C:\Windows\System32\calc.exe

Attack Commands: Run with **command_prompt**! [↗](#)

```
certutil -encode #{executable} %temp%\T1140_calc.txt
certutil -decode %temp%\T1140_calc.txt %temp%\T1140_calc_decoded.exe
```

Cleanup Commands: [↗](#)

```
del %temp%\T1140_calc.txt >nul 2>&1
del %temp%\T1140_calc_decoded.exe >nul 2>&1
```

Figure 50: Attack alert 3

Columns 1 field sorted 6 alerts Fields

Additional filters Grid view

Actions	@timestamp	Rule	Severity	Risk Score	Reason	host.name	user.name	process.n...	file.name
<input type="checkbox"/>	Oct 13, 2023 @ 12:05:12.518	Suspicious CertUtil Comma...	medium	47	process event with process certutil.exe, parent process powershell.exe, by ...	WS01	g3_domadmin	certutil.exe	—
<input type="checkbox"/>	Oct 13, 2023 @ 12:05:12.517	Suspicious CertUtil Comma...	medium	47	process event with process certutil.exe, parent process powershell.exe, by ...	WS01	g3_domadmin	certutil.exe	—
<input type="checkbox"/>	Oct 13, 2023 @ 12:05:12.516	Suspicious CertUtil Comma...	medium	47	process event with process certutil.exe, parent process powershell.exe, by ...	WS01	g3_domadmin	certutil.exe	—
<input type="checkbox"/>	Oct 13, 2023 @ 12:05:12.515	Suspicious CertUtil Comma...	medium	47	process event with process certutil.exe, parent process powershell.exe, by ...	WS01	g3_domadmin	certutil.exe	—

6.4 Attack 4: T1113 Screen capture

Figure 51: T1113: Screen capture

Atomic Test #6 - Windows Screen Capture (CopyFromScreen)

Take a screen capture of the desktop through a call to the [Graphics.CopyFromScreen](#) .NET API.

Supported Platforms: Windows

auto_generated_guid: e9313014-985a-48ef-80d9-cde604ffc187

Inputs:

Name	Description	Type	Default Value
output_file	Path where captured results will be placed	path	\$env:TEMP\T1113.png

Attack Commands: Run with powershell!

```
Add-Type -AssemblyName System.Windows.Forms
$screen = [Windows.Forms.SystemInformation]::VirtualScreen
$bitmap = New-Object Drawing.Bitmap $screen.Width, $screen.Height
$graphic = [Drawing.Graphics]::FromImage($bitmap)
$graphic.CopyFromScreen($screen.Left, $screen.Top, 0, 0, $bitmap.Size)
$bitmap.Save("#{output_file}")
```

Cleanup Commands:

```
Remove-Item #{output_file} -ErrorAction Ignore
```

Figure 52: Attack alert 4

Columns 1 field sorted 6 alerts Fields

Additional filters Grid view

Actions	@timestamp	Rule	Severity	Risk Score	Reason	host.name	user.name	process.n...	file.name
<input type="checkbox"/>	Oct 12, 2023 @ 11:26:08.510	Potential DLL SideLoading ...	high	73	process event with process not_an_scr.scr, parent process rundll32.exe, by...	WS01	g3_domadmin	not_an_scr.scr	—

6.5 Attack 5: T1036.005 Masquerade | Match Legitimate Name or Location

Figure 53: T1036.005 - Masquerade

Atomic Test #2 - Masquerade as a built-in system executable [↗](#)

Launch an executable that attempts to masquerade as a legitimate executable.

Supported Platforms: Windows

auto_generated_guid: 35eb8d16-9820-4423-a2a1-90c4f5edd9ca

Inputs: [↗](#)

Name	Description	Type	Default Value
executable_filepath	File path where the generated executable will be dropped and executed from. The filename should be the name of a built-in system utility.	string	\$Env:windir\Temp\svchost.exe

Attack Commands: Run with powershell! [↗](#)

```
Add-Type -TypeDefinition @"
public class Test {
    public static void Main(string[] args) {
        System.Console.WriteLine("tweet, tweet");
    }
}
"@ -OutputAssembly "#{executable_filepath}"

Start-Process -FilePath "#{executable_filepath}"
```

Cleanup Commands: [↗](#)

```
Remove-Item -Path "#{executable_filepath}" -ErrorAction Ignore
```

Figure 54: Attack alert 5

	@timestamp	Rule	Severity	Risk Score	Reason	host.name	user.name	process.n...	file.name	source.ip
...	Oct 12, 2023 @ 12:58:39.112	Mounting Hidden or WebDa...	medium	47	process event with process net.exe, parent process cmd.exe, by g3_doma...	WS01	g3_domadmin	net.exe	—	—
...	Oct 12, 2023 @ 12:58:39.111	Mounting Hidden or WebDa...	medium	47	process event with process net.exe, parent process cmd.exe, by g3_doma...	WS01	g3_domadmin	net.exe	—	—
...	Oct 12, 2023 @ 12:58:39.109	Mounting Hidden or WebDa...	medium	47	process event with process net.exe, parent process cmd.exe, by g3_doma...	WS01	g3_domadmin	net.exe	—	—
...	Oct 12, 2023 @ 12:58:39.108	Mounting Hidden or WebDa...	medium	47	process event with process net.exe, parent process cmd.exe, by g3_doma...	WS01	g3_domadmin	net.exe	—	—
...	Oct 12, 2023 @ 12:58:39.107	Mounting Hidden or WebDa...	medium	47	process event with process net.exe, parent process cmd.exe, by g3_doma...	WS01	g3_domadmin	net.exe	—	—

6.6 Attack 6: T1012 Query Registry


Figure 55: T1012 - Query Registry

Atomic Test #1 - Query Registry

Query Windows Registry. Upon successful execution, cmd.exe will perform multiple reg queries. Some will succeed and others will fail (dependent upon OS). References: <https://blog.cylance.com/windows-registry-persistence-part-2-the-run-keys-and-search-order> <https://blog.cylance.com/windows-registry-persistence-part-1-introduction-attack-phases-and-windows-services> <http://www.handgrep.se/repository/cheatsheets/postexploitation/WindowsPost-Exploitation.pdf> https://www.offensive-security.com/wp-content/uploads/2015/04/wp.Registry_Quick_Find_Chart.en_us.pdf

Supported Platforms: Windows

auto_generated_guid: 8f7578c4-9863-4d83-875c-a565573bbdf0

Attack Commands: Run with **command_prompt** ! Elevation Required (e.g. root or admin) 

```
reg query "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows"
reg query HKLM\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce
reg query HKCU\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce
reg query HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices
reg query HKCU\Software\Microsoft\Windows\CurrentVersion\RunServices
reg query "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify"
reg query "HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit"
reg query "HKCU\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell"
reg query "HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell"
reg query HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad
reg query HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce
reg query HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnceEx
reg query HKLM\Software\Microsoft\Windows\CurrentVersion\Run
reg query HKCU\Software\Microsoft\Windows\CurrentVersion\Run
reg query HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce
reg query HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run
reg query HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run
reg query HKLM\system\currentcontrolset\services /s | findstr ImagePath 2>nul | findstr /Ri ".*\sys$"
reg query HKLM\Software\Microsoft\Windows\CurrentVersion\Run
reg query HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot
reg query "HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components"
reg query "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\Scripts\Startup"
```

Figure 56: Attack alert 6

↓ @timestamp	↓ Rule	↓ Severity	↓ Risk Score	↓ Reason	↓ host.name	↓ user.name	↓ process.n...	↓ file.name	↓ source.ip
Oct 12, 2023 @ 13:21:09.057	Startup or Run Key Registry...	low	21	registry event with process reg.exe, by g3_domadmin on WS01 created lo...	WS01	g3_domadmin	reg.exe	—	—

6.7 Attack 7: T1547.001 Boot or Logon AutoStart Execution | Registry Run Keys / Startup Folder

Figure 57: T1547.001 - Boot or Logon Autostart Execution

Atomic Test #1 - Reg Key Run [↗](#)

Run Key Persistence

Upon successful execution, cmd.exe will modify the registry by adding "Atomic Red Team" to the Run key. Output will be via stdout.

Supported Platforms: Windows

auto_generated_guid: e55be3fd-3521-4610-9d1a-e210e42dcf05

Inputs: [↗](#)

Name	Description	Type	Default Value
command_to_execute	Thing to Run	path	C:\Path\AtomicRedTeam.exe

Attack Commands: Run with **command_prompt!** [↗](#)

REG ADD "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /V "Atomic Red Team" /t REG_SZ /F /D "#{command_to_execute" [↗](#)

Cleanup Commands: [↗](#)

REG DELETE "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /V "Atomic Red Team" /f >nul 2>&1 [↗](#)

Figure 58: Attack alert 7

<input type="checkbox"/>	Actions	<input type="checkbox"/>	@timestamp	<input type="checkbox"/>	Rule	<input type="checkbox"/>	Severity	<input type="checkbox"/>	Risk Score	<input type="checkbox"/>	Reason	<input type="checkbox"/>	host.name	<input type="checkbox"/>	user.name	<input type="checkbox"/>	process.n...	<input type="checkbox"/>	file.name
<input type="checkbox"/>	↗ 🔍 🔔 🔇		Oct 12, 2023 @ 13:29:21.868		Suspicious PowerShell Engl...		medium		47		library event with process updater.exe, by g3_domadmin on WS01 created...		WS01		g3_domadmin		updater.exe		—

6.8 Attack 8: T1574.001 Hijack Execution Flow | DLL Search Order Hijacking

Figure 59: T1574.001 - Hijack Execution Flow


Atomic Test #1 - DLL Search Order Hijacking - amsi.dll

Adversaries can take advantage of insecure library loading by PowerShell to load a vulnerable version of amsi.dll in order to bypass AMSI (Anti-Malware Scanning Interface) <https://enigma0x3.net/2017/07/19/bypassing-amsi-via-com-server-hijacking/>


Upon successful execution, powershell.exe will be copied and renamed to updater.exe and load amsi.dll from a non-standard path.

Supported Platforms: Windows

auto_generated_guid: 8549ad4b-b5df-4a2d-a3d7-2aee9e7052a3

Attack Commands: Run with **command_prompt** ! Elevation Required (e.g. root or admin) 

```
copy %windir%\System32\windowspowershell\v1.0\powershell.exe %APPDATA%\updater.exe
copy %windir%\System32\amsi.dll %APPDATA%\amsi.dll
%APPDATA%\updater.exe -Command exit
```



Cleanup Commands: 

```
del %APPDATA%\updater.exe >nul 2>&1
del %APPDATA%\amsi.dll >nul 2>&1
```




Figure 60: Attack alert 8

@timestamp	Rule	Severity	Risk Score	Reason	host.name	user.name	process.n...	file.name	source.ip
Oct 12, 2023 @ 13:21:09.057	Startup or Run Key Registry...	low	21	registry event with process reg.exe, by g3_domadmin on WS01 created lo...	WS01	g3_domadmin	reg.exe	—	—

6.9 Attack 9: T1070.001 Indicator Removal on Host | Clear Windows Event Logs


Figure 61: 1070.001 - Indicator Removal on Host

Atomic Test #2 - Delete System Logs Using Clear-EventLog

Clear event logs using built-in PowerShell commands. Upon successful execution, you should see the list of deleted event logs Upon execution, open the Security.evtx logs at C:\Windows\System32\winevt\Logs and verify that it is now empty or has very few logs in it.

Supported Platforms: Windows

auto_generated_guid: b13e9306-3351-4b4b-a6e8-477358b0b498

Attack Commands: Run with **powershell** ! Elevation Required (e.g. root or admin) 

```
$logs = Get-EventLog -List | ForEach-Object {$_.Log}
$logs | ForEach-Object {Clear-EventLog -LogName $_}
Get-EventLog -list
```




Figure 62: Attack alert 9

	@timestamp	Rule	Severity	Risk Score	Reason	host.name	user.name	process.n...	file.name	source.ip
...	Oct 12, 2023 @ 13:39:12.745	Windows Event Logs Cleared	low	21	event on WS01.ad.ttc60z.vle.fi created low alert Windows Event Logs Clea...	WS01.ad.ttc...	—	—	—	—
...	Oct 12, 2023 @ 13:39:12.744	Windows Event Logs Cleared	low	21	event on WS01.ad.ttc60z.vle.fi created low alert Windows Event Logs Clea...	WS01.ad.ttc...	—	—	—	—
...	Oct 12, 2023 @ 13:39:12.743	Windows Event Logs Cleared	low	21	iam event by g3_domadmin on WS01.ad.ttc60z.vle.fi created low alert Win...	WS01.ad.ttc...	g3_domadmin	—	—	—

6.10 Attack 10: T1112 Modify Registry

Figure 63: T1112 - Modify Registry

Atomic Test #1 - Modify Registry of Current User Profile - cmd [↗](#)

Modify the registry of the currently logged in user using reg.exe via cmd console. Upon execution, the message "The operation completed successfully." will be displayed. Additionally, open Registry Editor to view the new entry in HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced.

Supported Platforms: Windows

auto_generated_guid: 1324796b-d0f6-455a-b4ae-21fee6aa6b9

Attack Commands: Run with **command_prompt!** [↗](#)

```
reg add HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced /t REG_DWORD /v HideFileExt /d 1
```

Cleanup Commands: [↗](#)

```
reg delete HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced /v HideFileExt /f >nul 2>&1
```

Figure 64: Attack alert 10

	@timestamp	Rule	Severity	Risk Score	Reason	host.name	user.name	process.n...	file.name	source.ip
...	Oct 12, 2023 @ 13:50:10.126	Service Control Spawned vi...	low	21	process event with process sc.exe, parent process powershell.exe, by g3_d...	WS01	g3_domadmin	sc.exe	—	—
...	Oct 12, 2023 @ 13:50:10.125	Service Control Spawned vi...	low	21	process event with process sc.exe, parent process powershell.exe, by g3_d...	WS01	g3_domadmin	sc.exe	—	—
...	Oct 12, 2023 @ 13:50:10.124	Service Control Spawned vi...	low	21	process event with process sc.exe, parent process powershell.exe, by g3_d...	WS01	g3_domadmin	sc.exe	—	—
...	Oct 12, 2023 @ 13:50:10.122	Service Control Spawned vi...	low	21	process event with process sc.exe, parent process powershell.exe, by g3_d...	WS01	g3_domadmin	sc.exe	—	—
...	Oct 12, 2023 @ 13:50:10.121	Service Control Spawned vi...	low	21	process event with process sc.exe, parent process powershell.exe, by g3_d...	WS01	g3_domadmin	sc.exe	—	—

6.11 Uncaught attacks

Library commands do not always produce alerts. There are several reasons for this. These are determined by the specific nature of the commands being executed and how they are understood by the system.

6.11.1 Legitimate usage

Attacks are in some cases associated with legitimate administrative tasks. Attacks executed with this type of command will not consistently be identified as malicious. This has obvious advantages from the attacker perspective.

6.11.2 Risk thresholds

The risk-threshold in other cases may simply be too low. The inclusion of such commands in the Atomic library stems from their *cumulative* effects. Attack-chains leveraging seemingly benign administrative tasks are less likely to be detected (Kalech, 2019). This is broadly reflective of how an APT group might operate when compromising a target system.

6.11.3 Third party software

Some commands required the installation of third-party software. These were methodologically excluded on the basis of limited applicability. The aim was for attacks to be as general as possible. The specific commands executed are expected to be effective against a wide range of system configurations and network-types.

6.11.4 Privilege escalation

Commands executed with administrative privileges are difficult to detect. Such commands typically require confirmation with administrative credentials before they are executed. They will be considered benign if the correct credentials are provided. In the case below a pop-up seemingly from Windows requests user credentials. The attacker will see the password *asdfvasd* entered by the user. None of this triggers SIEM alerts. This further emphasizes the importance of protecting admin-level users.

Figure 65: Attack missed by the SIEM

```
PS C:\WINDOWS\system32> # Creates GUI to prompt for password. Expect long pause before prompt is available.
PS C:\WINDOWS\system32> $cred = $host.UI.PromptForCredential('Windows Security Update', '', [Environment]::UserName, [Environment]::UserDomainName)
PS C:\WINDOWS\system32> # Using write-warning to allow message to show on console as echo and other similar commands are not visible from the Invoke-AtomicTest framework.
PS C:\WINDOWS\system32> write-warning $cred.GetNetworkCredential().Password
WARNING: asdfvasd
PS C:\WINDOWS\system32> _
```

6.12 Attack analysis

The Elastic SIEM environment can be confirmed to work as expected. But as an alerts tool it is not the most reliable. Several attacks did not show up on the data feed. Alerts which did appear did so with a considerable delay. This has serious implications in a time-critical attack scenario. It should be noted that the test environment was running on default settings. There are plenty of ways the alert system can be optimized. It is likely to be more responsive in a production environment.

7 Cases

A case has been built using the abovementioned attacks. Specific details can be investigated in the *Cases* section of the Security tab. Cases are streamlined mechanisms which allow analysts to determine forensically and understand attack patterns (Vazao, 2021). They act as a central repository for information associated with a given attack. This includes logs and alerts. This can be particularly useful when it is necessary to parse large volumes of information from multifarious sources.

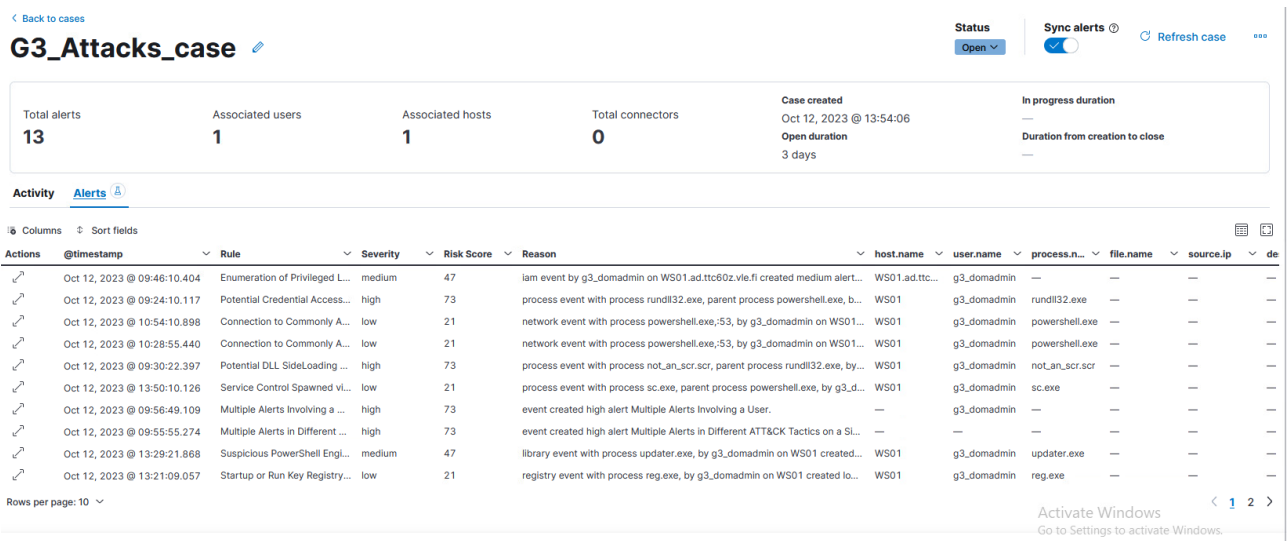
Figure 66: Cases main view

Cases									
Edit external connection Create case									
Open cases		In progress cases		Closed cases		Average time to close			
1		0		0		-			
<input type="text" value="e.g. case name"/> All severities All status Reporter 1 Tags 0									
Showing 1 case Selected 0 cases Bulk actions Refresh									
<input type="checkbox"/>	Name	Reporter	Tags	Alerts	Comments	Created on	External Incident	Status	Severity
<input type="checkbox"/>	G3_Attacks_case		—	13	0	Oct 12, 2023 @ 13:54:06	Not pushed	Open	Critical
Rows per page: 5 < 1 >									

7.1 Timelines

It is also possible to construct event timelines. Alert information associated with affected users and hosts can be examined using this method. Figure 67 presents the case built with alerts produced by the Atomic Red Team attacks.

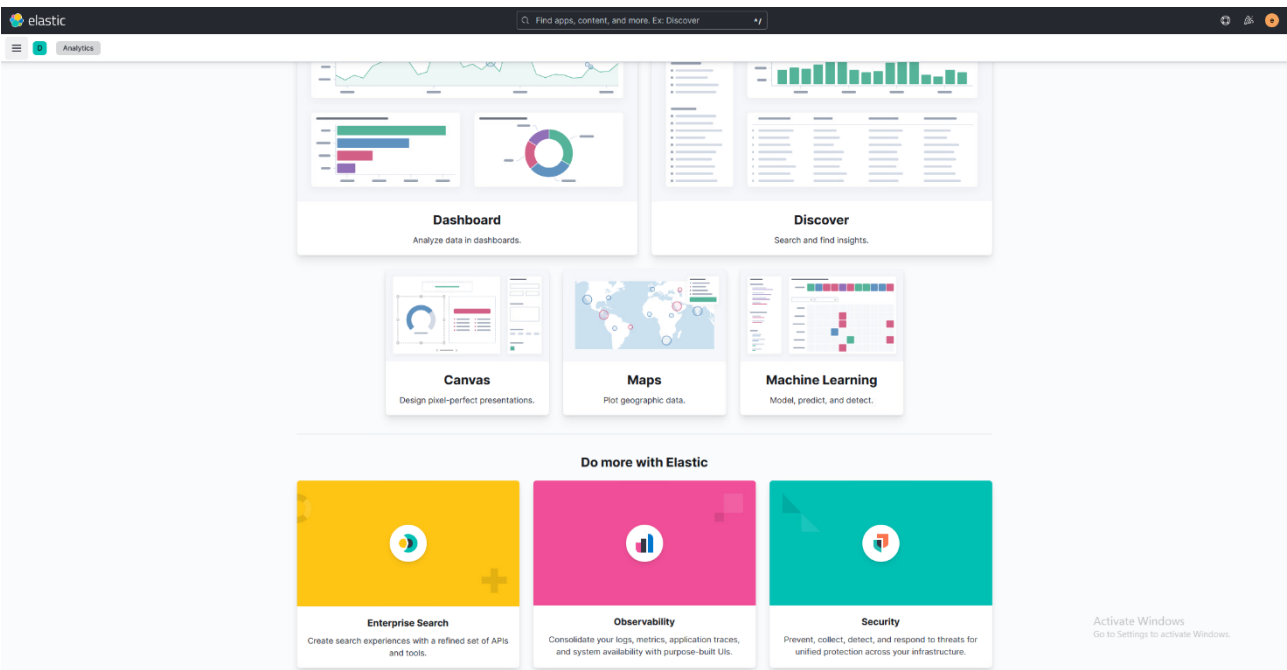
Figure 67: Attacks case



8 Analytics

This section discusses the different visualization options available in the Analytics view of the Elastic dashboard. Data are gathered via different agents. In the VLE environment data originates from the Filebeat module and its agents. A range of integrations can be used to filter and visualize data and deploy agents.

Figure 68: Analytics overview



Premade dashboards can be selected or custom ones created. Data streams can be queried via the Discover section. Data can be anything from IP addresses filtering identified and environment usage metrics. It is possible to filter for security-related alerts. These include incidents or incident-responses. Filtering is performed through data views.

A data view is essentially data sent to the SIEM. It can be log or metric data. Users can create custom data views for easier search. Dynamic data displays can be created with Elastic Canvas. Elastic Canvas is a data visualization and presentation tool with which live data can be pulled from Elasticsearch (Elastic, n.d.-g). Data can be combined with colors, images or text.¹

Maps creates and filter information on using a map format. Data can be anything from server connection locations to how much data is being transferred through specified paths. End-point security integrations have been added to workstations and servers. This process is described in detail in section 5.

9 Dashboard

Section 9 demonstrates how a custom dashboard can be created. Considerable time has been spent understanding different menu options and how data filtering works on basic level. Figure 68 illustrates how basic graphs can be created for the dashboard. The resulting dashboard visualizes a significant amount of information from the environment. Time restrictions limit the scope of what could reasonably be achieved for this part of the task, however. Figure 69 illustrates how a donut graph can be modified to display multiple alerts. The graph below displays SIEM alerts and alert severity levels.

¹ The feature has not been implemented in this particular dashboard because it is not required for the task.

Figure 69: Donut graph

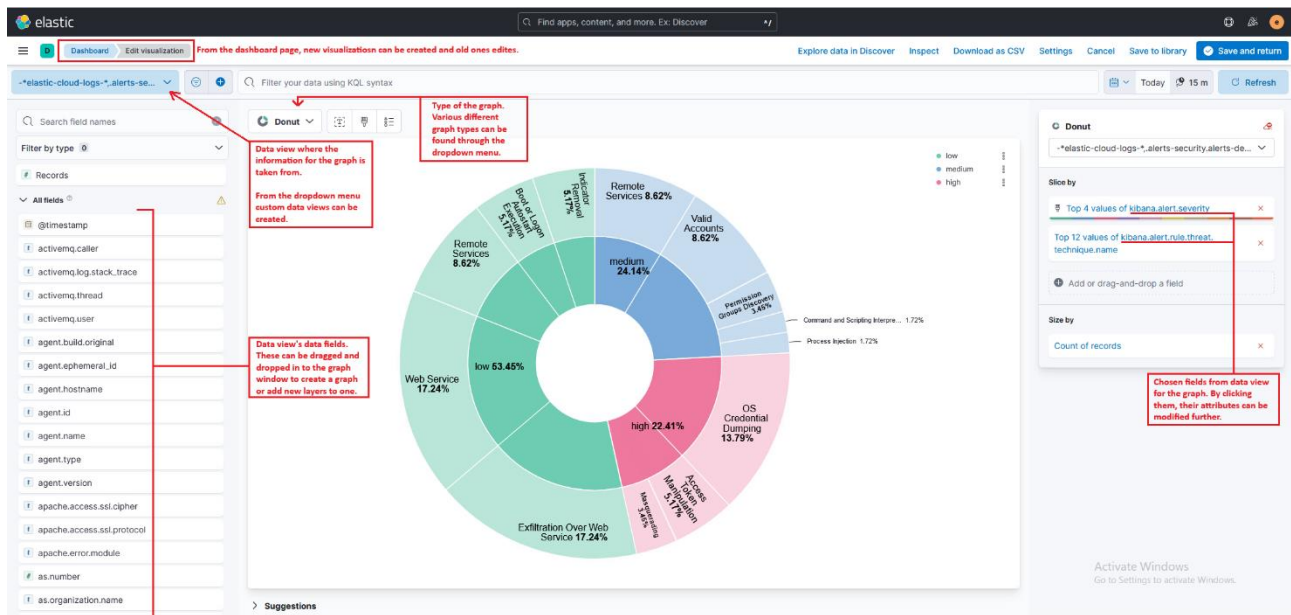


Figure 70 illustrates the process involved in generating horizontal bar graphs. It is similar to the aforementioned process.

Figure 70: Horizontal bar graph

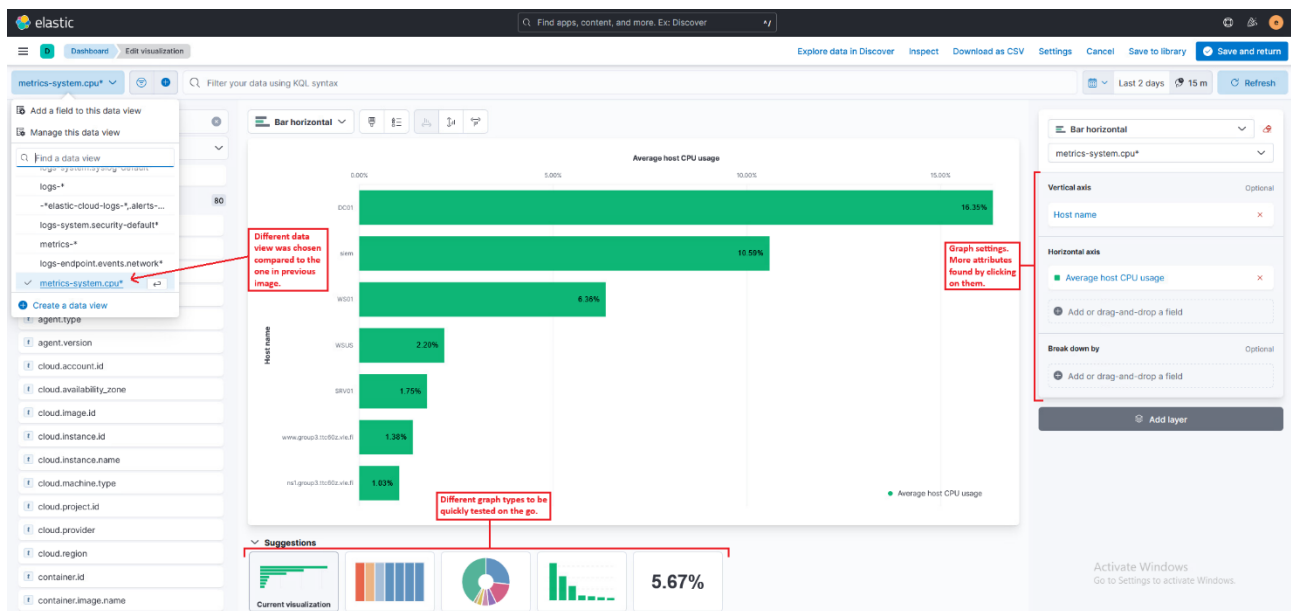
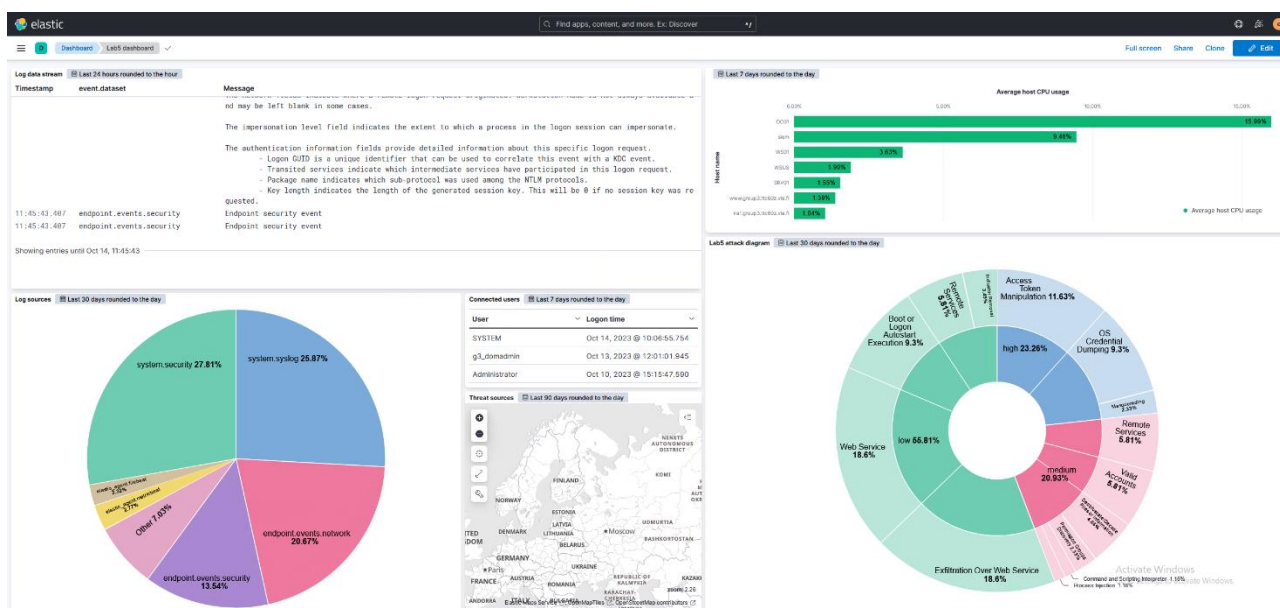


Figure 71 presents the completed dashboard. Other components have been added in the same manner as the examples above. Features have been selected according to the ease at which they can be observed. A brief rundown of dashboard components:

- Recent logs are shown in the Log data stream window. This is an easy way to check some of the most recent logs from the data stream if required.
- Average host CPU usage graph tracks CPU usage. This could prove valuable in the situation where usage fluctuates outside established parameters. CPU usage spikes suggest either malicious activity or system errors. In both cases further investigation would be necessary.
- Log sources are monitored. Increased log activity from unusual sources could suggest malicious activity or a system error. A spike in the number of log sources could indicate the same.
- An attack diagram has been generated using test attack data. This is valuable when determining what kind of attacks are most common and if more mitigation methods are required.
- It is useful to have the capability to view the number of connected users at a glance. Unusual login times by known users is typically worth following up.

The map visualizes where potential threats originate. The map appears inactive because the environment is well-insulated against external threats.

Figure 71: Custom dashboard



10 Conclusion

The technical aspect of SIEM logging and alert configuration is straightforward but extensive. There are many steps to complete before the system can be deployed. Considerable attention to detail is required. The process was time-consuming precisely because it was so hands-on. The benefits of this approach from an educational standpoint cannot be overstated. Our understanding of the Elastic SIEM has advanced measurably as a result.

The scope of the task was wider than previous labs. This meant the report would inevitably be more extensive. The writing process was also more demanding. It was clear a more sophisticated approach with an appropriate methodological scaffolding was necessary. Methodological factors added a new layer of complexity to the task. Considerable thought went into structuring the report. The result is a more systematic and refined document.

Understanding the limitations of SIEM alerts is a multifaceted challenge requiring a deep understanding of the diverse circumstances in which threats can manifest. The primary hurdle in this process is that not all attacks trigger alerts. There are several reasons for this. Legitimate administrative commands often share characteristics with those used for malicious intent. This makes their detection a complex task. Just as Melkor's corrupted elves of the Avári hid their true nature beneath a veneer of righteousness, malicious commands can be disguised within a sea of legitimate activity.

This leads to a situation where SIEM systems may fail to raise alerts promptly. This is especially problematic when the true nature of issued commands is not definitively understood. Commands executed with escalated privileges may also be wrongly perceived as benign. An important insight emerges from this complexity. Seemingly innocuous commands can produce outsized effects when woven together in a particular sequence. It is therefore imperative to understand which commands can be exploited in an attack scenario without triggering an alert. This is our task.

11 Sources

Tariq, A., Manzoor, J., Aziz, M. A., Tariq, Z. U. A., & Masood, A. (2022). Open source SIEM solutions for an enterprise. *Information & Computer Security*, 31(1), 88-107. <https://doi.org/10.1108/ICS-09-2021-0146>

Avison, D., & Fitzgerald, G. (2006). *Information Systems Development: Methodologies, Techniques and Tools*. London: McGraw-Hill.

Berdibayev, R., Gnatyuk, S., Yevchenko, Y., & Kishchenko, V. (2021). A concept of the architecture and creation for siem system in critical infrastructure. *Systems, Decision and Control in Energy II* (pp. 221-242). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-69189-9_13

El Arass, M., & Souissi, N. (2019). Smart SIEM: From big data logs and events to smart data alerts. *International Journal of Innovative Technology and Exploring Engineering*, 8(8), 3186-3191. Retrieved October 16, 2023, from https://www.researchgate.net/publication/333752299_Smart_SIEM_From_Big_Data_logs_and_events_to_Smart_Data_alerts

Elastic. (n.d.-a). Elastic Agent. Retrieved October 16, 2023, from <https://www.elastic.co/elastic-agent>

Elastic. (n.d.-b). LogStash: Collect, Parse, Transform Logs. Retrieved October 16, 2023, from <https://www.elastic.co/logstash>

Elastic. (n.d.-c). Kibana Alerting: Alerts & Actions for Elasticsearch data. Retrieved October 16, 2023, from <https://www.elastic.co/kibana/alerting>

Elastic. (n.d.-d). Cases | Elastic Security Solution [8.10]. Retrieved October 16, 2023, from <https://www.elastic.co/guide/en/security/current/cases-overview.html>

Elastic. (n.d.-e). Set up Fleet Server | Fleet and Elastic Agent Guide [8.10]. Retrieved October 16, 2023, from <https://www.elastic.co/guide/en/fleet/current/fleet-server.html>

Elastic. (n.d.-f). FileBeat: Lightweight log analysis & Elasticsearch. Retrieved October 16, 2023, from <https://www.elastic.co/beats/filebeat>

Elastic. (n.d.-g). Canvas | Kibana Guide [8.10]. Retrieved October 16, 2023, from <https://www.elastic.co/guide/en/kibana/current/canvas.html>

Frankland, J. (2009). The importance of standardizing methodology in penetration testing. *Database and Network Journal*, 39(3), 13. Retrieved 16 October, 2023, from <https://www.thefreelibrary.com/The+importance+of+standardising+methodology+in+penetration+testing.-a0202562264>

Johnstone, M.N. (2009). Security Requirements Engineering: The Reluctant Oxymoron. *Proceedings of the 7th Australian Information Security Management Conference*, Perth, Western Australia, 1st to 3rd December 2009. <https://doi.org/10.4225/75/57b4011e30de8>

Kalech, M. (2019). Cyber-attack detection in SCADA systems using temporal pattern recognition techniques. *Computers & Security*, 84, 225-238. <https://doi.org/10.1016/j.cose.2019.03.007>

Kotenko, I., & Chechulin, A. (2012, November). Common framework for attack modeling and security evaluation in SIEM systems. *2012 IEEE International Conference on Green Computing and Communications* (pp. 94-101). IEEE. <https://doi.org/10.1109/GreenCom.2012.24>

Kotenko, I., Kuleshov, A., & Ushakov, I. (2017, August). Aggregation of Elastic Stack instruments for collecting, storing and processing of security information and events. *2017 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation* (pp. 1-8). IEEE. <https://doi.org/10.1109/UIC-ATC.2017.8397627>

Mancini, M. (2019, December 31). *Security analytics with Elastic*. Retrieved October 16, 2023, from <https://openaccess.uoc.edu/handle/10609/113266>

Midian, P. (2003). Perspectives on Penetration Testing — Finding the Right Supplier. *Network Security*, 2003(2), 9-11. [https://10.1016/S1353-4858\(03\)00210-1](https://10.1016/S1353-4858(03)00210-1)

MITRE. (n.d.) *MITRE ATT&CK Matrix*. MITRE. Retrieved October 16, 2023, from <https://attack.mitre.org/>

Mokalled, H., Catelli, R., Casola, V., Debertol, D., Meda, E., & Zunino, R. (2019, June). The applicability of a siem solution: Requirements and evaluation. *2019 IEEE 28th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE)* (pp. 132-137). IEEE. <https://doi.org/10.1109/WETICE.2019.00036>

Montesino, R., Fenz, S., & Baluja, W. (2012). SIEM-based framework for security controls automation. *Information Management & Computer Security*, 20(4), 248-263. <https://doi.org/10.1108/09685221211267639>

Mulyadi, F., Annam, L. A., Promya, R., & Charnsripinyo, C. (2020, October). Implementing dockerized Elastic stack for security information and event management. *2020-5th International Conference on Information Technology (InCIT)* (pp. 243-248). IEEE. <https://doi.org/10.1109/InCIT50588.2020.9310950>

Nabil, M., Soukainat, S., Lakbabi, A., & Ghizlane, O. (2017, May). SIEM selection criteria for an efficient contextual security. In *2017 international symposium on networks, computers and communications (ISNCC)* (pp. 1-6). IEEE. <https://doi.org/10.1109/ISNCC.2017.8072035>

NIST. (2018, April 16). *Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1*. National Institute of Standards and Technology. Retrieved October 16, 2023, from <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>

OWASP. (2013, April 19). *OWASP Testing Guide 4.0*. Open Web Application Security Project. Retrieved October 11, 2023, from [https://http://www.owasp.org/index.php/OWASP Testing Guide v4 Table of Contents](https://http://www.owasp.org/index.php/OWASP_Testing_Guide_v4_Table_of_Contents)

Red Canary. (2023, August 29). *Incident Response and Readiness Guide*. Red Canary. Retrieved October 16, 2023, from <https://redcanary.com/resources/guides/incident-response-preparedness-guide/>

Red Canary. (n.d.). *Small and highly portable detection tests based on MITRE's ATT&CK*. GitHub. Retrieved October 16, 2023, from <https://github.com/redcanaryco/atomic-red-team>

Shah, S., & Mehtre, B. M. (2015). An overview of vulnerability assessment and penetration testing techniques. *Journal of Computer Virology and Hacking Techniques*, 11, 27-49. <https://doi.org/10.1007/s11416-014-0231-x>

Subramanian, K., & Meng, W. (2021, December). Threat hunting using elastic stack: An evaluation. 2021 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI) (pp. 1-6). IEEE. <https://doi.org/10.1109/SOLI54607.2021.9672347>

Tang, A. (2014). A guide to penetration testing. *Network Security*, 2014(8), 8. [http://10.1016/S1353-4858\(14\)70079-0](http://10.1016/S1353-4858(14)70079-0)

Valli, C., Woodward, A., Hannay, P., & Johnstone, M. (2014). Why Penetration Testing Is A Limited Use Choice For Sound Cyber Security Practice. *Proceedings of the Conference on Digital Forensics, Security and Law U6* 35. Retrieved from <http://ecu.summon.serialssolutions.com/>

Vazao, A., Santos, L., Oliveira, A., & Rabadao, C. (2021, June). A GDPR compliant SIEM solution. *European Conference on Cyber Warfare and Security* (pp. 440-XIV). Academic Conferences International Limited. <https://10.34190/EWS.21.081>

Yeo, J. (2013). Using penetration testing to enhance your company's security. *Computer Fraud & Security*, 2013(4), 17-20. [https://dx.doi.org/10.1016/S1361-3723\(13\)70039-3](https://dx.doi.org/10.1016/S1361-3723(13)70039-3)