

IJECBE

International Journal of Electrical, Computer and Biomedical Engineering

IJECBE (2024), 2, 2, 243–260
Received (4 June 2024) / Revised (5 June 2024)
Accepted (22 June 2024) / Published (30 June 2024)
<https://doi.org/10.62146/ijecbe.v2i2.49>
<https://ijecbe.ui.ac.id>
ISSN 3026-5258

RESEARCH ARTICLE

Performance Evaluation Elastic Security as Open Source Endpoint Detection and Response for Advanced Persistent Threat Cyberattack

Zegar Pradipta Putra,[†] Ruki Harwahyu,^{**†} and Evans Hebert[‡]

[†]Department of Electrical Engineering, Faculty of Engineering, Universitas Indonesia, Depok, Indonesia

[‡]National Taiwan University of Science and Technology

^{*}Corresponding author. Email: ruki.h@ui.ac.id

Abstract

Detecting APT using conventional information protection systems poses significant challenges. For instance, signature-based detection tools like antivirus primarily rely on predefined signature rules to identify malware. However, in scenarios like zero-day attacks where malware signatures are unknown, detection becomes unreliable. While EDR traditionally hinges on signature-based rules, recent advancements integrate machine learning techniques for enhanced detection capabilities. In this study, we conducted an evaluation of open-source EDR, specifically Elastic Security, for APT detection. APT attack vectors were simulated utilizing the Caldera Platform. The evaluation involved validating each attack vector sent by Caldera against detection alerts generated by Elastic Security. The detection outcomes revealed three categories: detected alerts conforming to predefined rules, undetected alerts despite predefined rules, and undetected alerts due to undefined rules. Some attack vectors lacked rule definitions, potentially resulting in elevated false positives. Additionally, certain attack vectors failed to trigger alerts despite rule definitions.

Keywords: evaluation, elastic security, advanced persistent threat, endpoint detection and response, opensource

1. Introduction

Since the invention of the Internet, the Internet has become a daily necessity for every citizen. Undeniably, everyone is connected to the Internet to support their daily needs. Based on a report issued by International Telecommunication Union (ITU) as of January 2022, it is known that as many as 175 million people, around

64% of the 272 million population in Indonesia, have internet penetration) [1]. This is also confirmed through a survey report conducted by APJII, where in 2022, the penetration of internet users reached 77.02% of the total population of Indonesia [2]. In this case, there was an increase when compared to previous years.

The increasing use of the Internet increases the danger that threatens users through cyberattacks. In the Cyber Security Monitoring Results Report published by the National Cyber and Crypto Agency (BSSN) in 2022, there were 976,429,996 traffic anomalies [3]. This figure is an increase compared to the Cyber Security Monitoring Results 2021, where the number of traffic anomalies was 495,337,202 [4]. This shows that there is an increase in cyberattacks in Indonesia. One type of attack detected as a traffic anomaly, APT, was detected at 4,421,992 during 2022, consisting of the Winnti, Lazarus, APT 40, Magecart, and Kimsuky groups. An Advanced Persistence Threat (APT) is an attack campaign carried out by a threat actor, a statesponsored or non-state-sponsored actor. This threat actor uses various sophisticated methods/techniques designed to carry out persistent, sophisticated, and clandestine cyberattacks to gain access to the system and stay in the system for an extended period. APTs have impacts, such as data theft, gaining access to the system, damaging the system, or espionage [3].

Detecting APTs using conventional information protection systems with the latest techniques is challenging [5]. For example, signature-based detection tools such as antivirus (AV) detect malware with previously defined signature rules; if the analysis process of the malware is by the defined rules, then the malware will be detected as malicious. However, if the AV device does not define the rules against malware, such as in a zero-day attack, then it is possible that the malware will not be detected as malicious [6].

Endpoint Detection and Response (EDR) traditionally relies on signature-based detection rules [7], but recent advancements have incorporated machine learning techniques for data analysis and correlation in identifying malicious activities [8]. The term EDR, also known as endpoint threat detection and response (ETDR), was coined by Antonio Chuvakin in 2013 [9]. EDR is an addition to the capabilities of antivirus as a security perimeter because EDR will notify alerts once it detects an anomaly. Therefore, EDR can detect unknown threats (zero-day) and pre-empt the system before the activity is executed on a behavioral basis rather than just a signature-based [5].

However, some existing paid EDRs are limited by the operating system (OS) and developed as a closed platform, making it difficult to customize the user environment. To overcome these limitations, open-source EDR is needed. Open-source EDR is a cost-effective cybersecurity tool with high expected value in flexibility, utilization, and scalability [10]. One of EDR tools are commonly used, namely Elastic Security. Elastic Security utilize signature-based detection rules and machine learning to detect attacks [11]. However, there is a challenge in the detection process carried out by EDR, that is the high rate of false positives in detection [12].

Several recent studies related to Endpoint Detection Response are used as initial references in this research. The research by [10] discusses the empirical assessment conducted on the 11 best-paid Endpoint Detection and Response devices in 2021

based on Gartner. The eleven EDR devices were assessed for capabilities in several attack vectors commonly used by APTs in attacks, such as shellcode execution into Windows child processes and DLL Side loading. Whereas in the research conducted by [5], the implementation of open source EDR using Google Rapid Response is an open-source device in remote forensics tools and OSQuery to detect USB attack scenarios inserted by malware. In [12], an additional mechanism was developed in EDR, namely Tactical Graph Provenance, which claimed that the mechanism could overcome the high number of false positive alerts on EDR devices. However, the research did not implicitly attach data about the high number of false positive alerts on EDR. While in the research conducted by Subramanian et al., researchers evaluated Elastic Stack to detect several attack scenarios such as brute force attack, dictionary attack, DDoS attack, social engineering scenario, and payload injection. The attack scenarios were then analyzed using conventional software such as audit logs and webserver logs. In this research, Elastic Stack is utilized as a System Information and Event Management (SIEM), so it has not utilized Elastic Security as EDR [13].

In the few studies conducted, research has yet to specifically discuss the open-source EDR tools Elastic Security in the detection and prevention of APT attacks, as mentioned in the background of this research. In addition, the accuracy problem of EDR open-source tools has yet to be discussed in the research. Therefore, this research will evaluate open-source EDR tools Elastic Security, in detecting APT attacks through the Caldera attack emulation tool. The evaluation will look at the capabilities of EDR open-source tools in detecting APT attacks in terms of accuracy and effectiveness.

2. Method

The research was conducted using the Elastic Security as EDR opensource, which is available as open source on the Elastic site [14]. The object of this research is the implementation of Elastic Security, which is expected to provide notification in the form of alerts in the event of an attack generated by Caldera Emulation Attack Platform. The data processed in this research is the accuracy of information sent by Elastic Security in the event of an attack. The addition of Elastic Security is expected to improve the security aspects by providing notifications or alerts when an attack occurs aimed.

This research uses an experimental method, which the first stage is implementing Elastic Security as an endpoint security on Windows Workstation. Elastic Security consists of Elasticsearch and Elastic Agent. Elasticsearch acts as a manager and Elastic Agent as a slave. Elasticsearch serves for storing, managing, and searching data, paired with Kibana, an opensource platform for analytics and visualization tailored for Elasticsearch [11]. Elastic Agent offers a consolidated approach to incorporate monitoring for logs, metrics, and diverse data types into a host [15]. Endpoint Detection and Response (EDR) agents are pivotal in cybersecurity, offering real-time monitoring and response to potential security threats across networks. Employing agent-based frameworks, as examined by Kendrick et al., facilitates analyzing cyber events across different network scales, thereby improving detection capabilities for complex multi-stage attacks [16].

Third, the testing stage, the testing stage, testing and evaluation of Elastic Security against APT attack scenarios have been made to see the level of effectiveness and accuracy of detection.

2.1 Experimental Environment

The system built in this research is in a virtual environment. It is intended that the attack vector built in Caldera has no impact on operational assets. The following are the specifications used to run the virtual experimental environment.

Table 1. Virtual Environment Specification

| | |
|-------------------------|------------------------------|
| Operating System | Sonoma 14.2.1 |
| RAM | 16384 Mb |
| Storage | 512000 Mb |
| Processor | 2,6 GHz 6-Core Intel Core i7 |

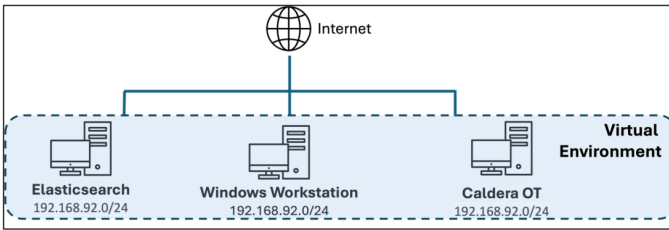


Figure 1. Environment Developed

2.1.1 Elastic Security

Elastic Security consists of two components: Elasticsearch, which acts as a manager, and Elastic Agent, which acts as a slave. For Elastic Security to act as an EDR, several components in Elasticsearch need to be considered, such as Integrations and Detection Rules. Integrations are a collection of assets that define how to observe certain products or services with Elastic Stack. In this research we use three integrations, there are Windows, Elastic Defend and System. Each of these integrations needs to be log and event collet from the Windows Workstation. In the Elastic Defend Integration, there are additional feature that only available in subscription version of Elastic Security, like ransomware protection, memory threat, detection malicious behavior, and attack surface reduction.

| Name | Integration | Namespace | Actions |
|----------------|------------------------|-----------|---------|
| elastic-defend | Elastic Defend v8.13.0 | default | ... |
| system-2 | System v1.54.0 | default | ... |
| windows-1 | Windows v1.44.4 | default | ... |

Figure 2. Enabled Integration Elastic Security

Detection Rules help users set up and get their detections and security monitoring going as soon as possible. Detection Rules consist of 5 domains: Endpoint, Cloud, Container, Network, and LLM. The following research will focus on the Endpoint domain because Elastic Agent will be installed on the Windows Workstation as an endpoint. Meanwhile, based on the type of rules, it consists of machine learning, building block rules, High Order Rules, and Indicator Match with 1080 rules. In the open-source Elastic Security, the rules that can be utilized are 1008, while the other 72 rules require a subscription.

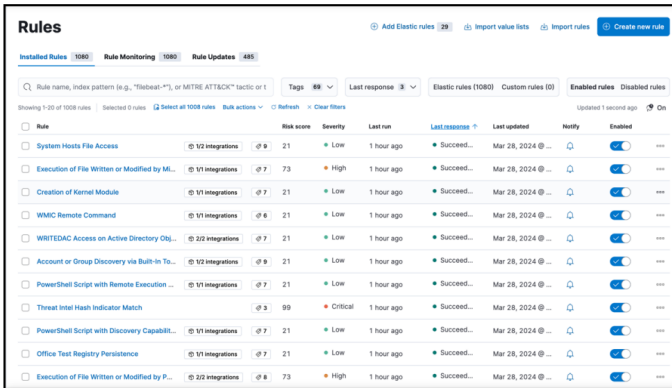


Figure 3. Enabled Rules on Elastic Security

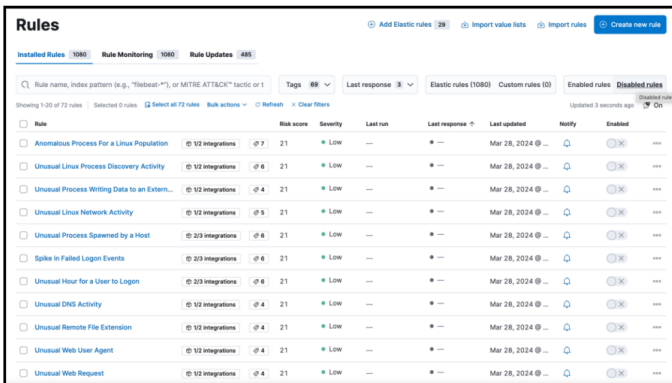


Figure 4. Disabled Rules on Elastic Security

According to the Elastic Rule Documentation, Elastic Security can cover three types of operating systems: Windows, Linux, and macOS.

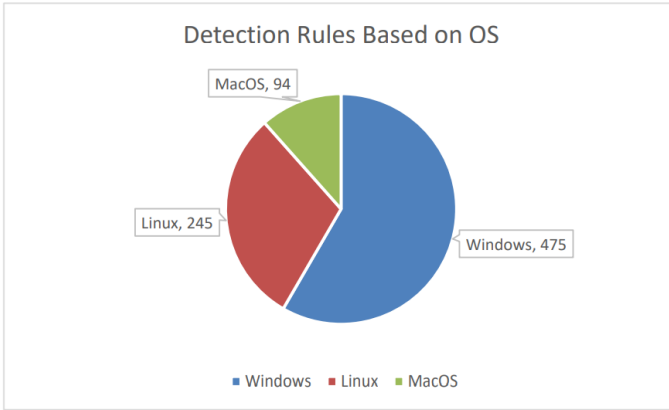


Figure 5. Detection Rules Based on OS

Elastic Agent is installed on Windows Workstation. The following are the specifications of the Elastic Security that will be used.

Table 2. Windows Workstation Specification

| | |
|------------------|----------------------------------|
| Operating System | Ubuntu 22.04.3 LTS |
| Version | Elasticsearch 8.13 |
| RAM | 4096 Mb |
| Network Adapter | Adapter 1: NAT (192.168.92.0/24) |

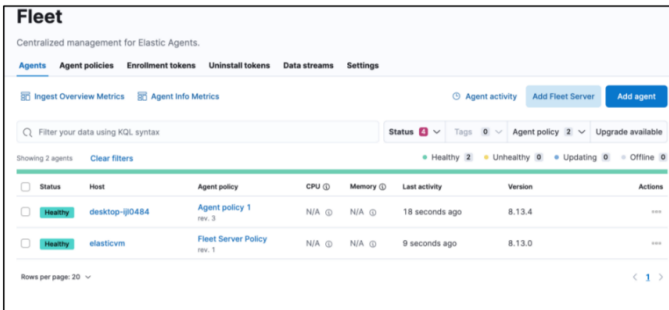


Figure 6. Agent Installed on Elastic Security

2.1.2 Caldera Attack Emulation

Caldera is a platform for adversary emulation, crafted to facilitate effortless execution of autonomous hacking and attack simulation exercises. It offers the capability to conduct manual red team engagements or automated incident responses. Built upon the MITRE ATT&CK™ framework, Caldera serves as an active research project

at MITRE. In the following scenario, Caldera acting as an attacker machine, will simulate an APT attack on a Windows Workstation equipped with an EDR agent.

Agents are payload processes installed on compromised Windows Workstation, which establish periodic connections with the Caldera Attack Emulation Platform as Command and Control (C2) server to receive instructions. Each agent connects to the server through a designated point called "contact," which serves as a specific connection point facilitating communication between the agent and Caldera Attack Emulation Platform server [17].

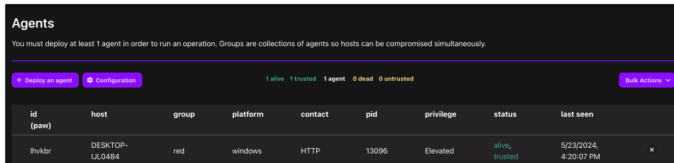


Figure 7. Agent Installed on Caldera Platform

Table 3. Caldera Platform Specification

| | |
|-------------------------|----------------------------------|
| Operating System | Ubuntu 22.04.4 LTS |
| Version | V5.0.0 |
| RAM | 4096 Mb |
| Network Adapter | Adapter 1: NAT (192.168.92.0/24) |

2.1.3 Windows Workstation

Windows Workstation will simulate as an attack target. To evaluate Elastic Security EDR on a standalone basis, perimeter defenses from Microsoft were disabled, such as Microsoft Defender and Microsoft Antivirus. So that the defense mechanism on Windows Workstation depends on Elastic Security. The following are the specifications of the Windows Workstation virtual machine used.

Table 4. Windows Workstation Specification

| | |
|-------------------------|----------------------------------|
| Operating System | Windows 10 |
| Hostname | DESKTOP-IJL0484 |
| Version | Enterprise LTSC 64bit |
| RAM | 4096 Mb |
| Network Adapter | Adapter 1: NAT (192.168.92.0/24) |

2.2 Attack Scenario

To create attack scenario in Caldera, Caldera consists of several component, like Abilities, Adversaries, and Operations. An ability is a specific implementation of an ATT&CK tactic or technique that can be executed on active agents. It consists of the commands to execute, the platforms or executors the commands can run on Windows/PowerShell, payloads to include, and a reference to a module for parsing the output on the Caldera server. Adversary profiles are collections of abilities, representing the tactics, techniques, and procedures (TTPs) available to a threat actor. These profiles are utilized during operations to determine which abilities will be executed. Meanwhile, Operations execute abilities on groups of agents. Adversary profiles determine which abilities will be executed, and agent groups determine the agents on which these abilities will be executed [18].

In this research, we use the abilities provided by Caldera Attacker Machine. Then we create an adversary that consists of several abilities provided by Caldera Attacker Machine. This adversary will be the attack scenario that is run in the research.

Table 5. Attack Scenario Ability on Caldera

| No | Technique | Tactics |
|----|----------------------|--|
| 1. | Initial Access | Download Macro-Enabled Phishing Attachment |
| 2. | Discovery | Identify local users |
| | | Identify active users |
| | | Identify Firewalls |
| | | Discover antivirus programs |
| 3. | Defense Evasion | Disable Microsoft Defender Firewall |
| | | Disable Windows Defender All |
| 4. | Privelege Escalation | UAC bypass registry |
| 5. | Lateral Movement | Disable NLA for RDP via Command Prompt |

3. Result

Based on the attack scenario compiled on the Caldera Platform, the test results will be validated with alerts that appear on Elastic Security. The validation is done by seeing whether the attack vector is detected by the Elastic Security alert in the kibana alert rule name field.

3.1 Initial Access

Initial Access consists of techniques that adversaries may use as entry vectors to gain an initial foothold. These techniques include compromising operational technology assets, IT resources in the OT network, and external remote services and websites [19]. At the Initial Access stage, Caldera Attacker Machine sends the Windows Workstation a payload that downloads a macro-enabled document from Atomic Red

Team's GitHub repository, simulating the end user clicking on the phishing link to download the file. The **"PhishingAttachment.xlsm"** file is downloaded to the **%temp%** directory. Below is the command send from Caldera Attacker Machine to the Windows Workstation.

```

$url = 'https://github.com/redcanaryco/atomic-red-team/raw/master/atomics/T1566.001/bin/PhishingAttachment.xlsm';
[Net.ServicePointManager]::SecurityProtocol =
[Net.SecurityProtocolType]::Tls12; Invoke-WebRequest -Uri $url -OutFile
$env:TEMP\PhishingAttachment.xlsm
  
```

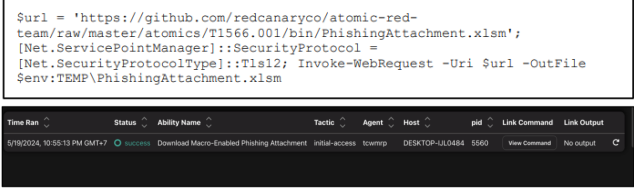


Figure 8. Emulation Successful on Caldera

| @timestamp | host.hostname | agent.name | message | libre.alert.category.name |
|-----------------------------|-----------------|------------|--|--|
| May 19, 2024 9:22:08.935194 | desktop-1120484 | - | DNS query is completed for the name raw.githubusercontent.com, type 28, query options 02090000100000 with status 0 success | Connection to Commonly Abused Web Services |
| May 19, 2024 9:22:08.935197 | desktop-1120484 | - | DNS query is completed for the name raw.githubusercontent.com, type 7, query options 02090000100000 with status 0 success | Connection to Commonly Abused Web Services |

Figure 9. Detection Result on Elastic Security

Figure 8 shows that the “Download Macro-Enable Phishing Attachment” attack scenario was successfully executed. However, the alert shown on Elastic Security only detected “Connection to Commonly Abused Web Services”. The alert does not include the fact that a potentially malicious file was downloaded into the **TEMP** directory.

3.2 Discovery

Discovery involves methods employed by an adversary to acquire information regarding the system and internal network. These methods enable adversaries to assess the environment and position themselves before determining their course of action [20].

3.2.1 Identify local users

At this stage, the command is run to get information about local users on Windows Workstations. The command line that is executed on Caldera Attacker Machine is below.

```

Get-WmiObject -Class Win32_UserAccount
  
```

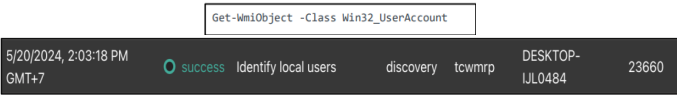


Figure 10. Emulation Successful on Caldera



Figure 11. Detection Result on Elastic Security

Figure 10 shows that Elastic Security successfully detected the attempt to obtain information about the local user with the “Powershell Script with Discovery Capabilities” alert. In the Elastic rules documentation, the “Powershell Get-WmiObject” command with the Win32_UserAccount object is included in Discovery efforts such as enumerating users, shares, sessions, domain trusts, and groups.

3.2.2 Identify active users

This stage is used to get information about active local users used on Windows Workstation. The command line that is executed is below

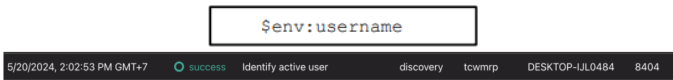


Figure 12. Emulation Successful on Caldera



Figure 13. Detection Result on Elastic Security

Figure 12 shows that the command executed by Caldera to get information about active local users was not detected by the Elastic alert.

3.2.3 Identify Firewalls

This stage is used to obtain information about Firewalls security products used on Windows Workstations. The command line that run on Caldera is below

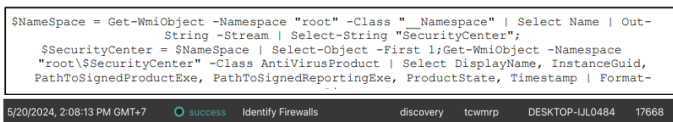


Figure 14. Emulation Successful on Caldera

| | | |
|-----------------------------|--|--|
| May 29, 2024 @ 14:08:17.858 | powershell.exe ExecutionPolicy Bypass -C ... | CommandInvocation(Get-WebObject): 'Get-WebObject' ParameterBinding(Get-WebObject): name='Namespace', value='root\SecurityCenter2' ParameterBinding(Get-WebObject): name='Class', value='AntiVirusProduct'... |
| May 29, 2024 @ 14:08:17.855 | powershell.exe ExecutionPolicy Bypass -C ... | Pipeline execution details for command line: \$Namespace - Get-WebObject -Namespace 'root' -Class '_Namespace' Select-Name Out-String -Stream Select-String 'SecurityCenter' SecurityCenter - \$Namespace Select-Object - First Get-WebObject -Namespace 'root\SecurityCenter' -Class AntiVirusProduct Select DisplayName, InstanceId... |
| May 29, 2024 @ 14:08:17.771 | powershell.exe ExecutionPolicy Bypass -C ... | CommandInvocation(Select-Object): 'Select-Object' ParameterBinding(Select-Object): name='First', value='1' ParameterBinding(Select-Object): name='InputObject', value='SecurityCenter'... |
| May 29, 2024 @ 14:08:17.765 | powershell.exe ExecutionPolicy Bypass -C ... | Pipeline execution details for command line: \$Namespace - Get-WebObject -Namespace 'root' -Class '_Namespace' Select-Name Out-String -Stream Select-String 'SecurityCenter' SecurityCenter - \$Namespace Select-Object - First Get-WebObject -Namespace 'root\SecurityCenter' -Class AntiVirusProduct Select DisplayName, InstanceId... |
| May 29, 2024 @ 14:08:17.756 | powershell.exe ExecutionPolicy Bypass -C ... | CommandInvocation(Get-WebObject): 'Get-WebObject' ParameterBinding(Get-WebObject): name='Namespace', value='root' ParameterBinding(Get-WebObject): name='Class', value='_Namespace'... |
| May 29, 2024 @ 14:08:17.749 | powershell.exe ExecutionPolicy Bypass -C ... | Pipeline execution details for command line: \$Namespace - Get-WebObject -Namespace 'root' -Class '_Namespace' Select-Name Out-String -Stream Select-String 'SecurityCenter' SecurityCenter - \$Namespace Select-Object - First Get-WebObject -Namespace 'root\SecurityCenter' -Class AntiVirusProduct Select DisplayName, InstanceId... |
| May 29, 2024 @ 14:08:16.573 | - | Creating scriptbook ees (1 of 1): \$Namespace - Get-WebObject -Namespace 'root' -Class '_Namespace' Select-Name Out-String -Stream Select-String 'SecurityCenter' SecurityCenter - \$Namespace Select-Object -First Get-WebObject -Namespace ... |

Figure 15. Detection Result on Elastic Security

Figure 14 shows that kibana.alert.rule.name does not trigger an alert on Elastic Security for the attack vector. Caldera Attacker Machine runs to get information about Firewalls on Windows Workstations. According to the rules documentation, this is because the rules do not cover the Security Center string.

3.2.4 Discover antivirus Programs

This stage is used to obtain information about Antivirus security products used on Windows Workstations. The command line that run on Caldera Attacker Machine is below.

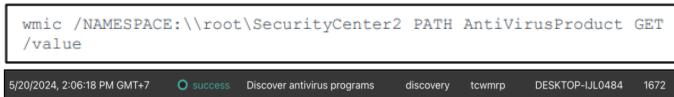


Figure 16. Emulation Successful on Caldera

| @timestamp | kibana.alert.rule.name | process.args | message | kibana.alert.severity |
|-----------------------------|--|---|------------------------|-----------------------|
| May 29, 2024 @ 14:18:18.888 | Unusual Discovery Activity by User | ["C:\Windows\System32\Wbem\WMIEXEC.exe", "/NAMESPACE:\\root\SecurityCenter2\PATH: AntiVirusProduct.GET /value"] | Endpoint process event | low |
| May 29, 2024 @ 14:18:01.166 | Unusual Discovery Signal Alert with Unusual Process Command Line | ["C:\Windows\System32\Wbem\WMIEXEC.exe", "/NAMESPACE:\\root\SecurityCenter2\PATH: AntiVirusProduct.GET /value"] | Endpoint process event | low |
| May 29, 2024 @ 14:09:52.198 | Security Software Discovery using WMI | ["C:\Windows\System32\Wbem\WMIEXEC.exe", "/NAMESPACE:\\root\SecurityCenter2\PATH: AntiVirusProduct.GET /value"] | Endpoint process event | medium |

Figure 17. Detection Result on Elastic Security

The discover antivirus program attack vector is detected with several alerts. In the Security Software Discovery using WMIC alert, based on the Elastic rules documentation, it is detected based on the process name run by Caldera Platform, namely wmic.exe and process arguments `/namespace : \\ \ root \ SecurityCenter2`. Meanwhile, the “Unusual Discovery Signal Alert with Unusual Process Command Line” and “Unusual Discovery Activity by User” alerts are detected due to the trigger of the ID Security Software Discovery using WMIC alert [21], [22].

3.3 Defense Evasion

Defense evasion refers to the tactics adversaries employ to circumvent detection during their compromise. Strategies utilized for defense evasion encompass uninstalling or disabling security software, as well as obfuscating or encrypting data and scripts [23].

3.3.1 Disable Windows Defender All

This stage is to disable all Windows Defender features. In the commands run by *Caldera Attacker Machine*, such as “DisableIntrusionPreventionSystem” is used to remove the cmdlet whether to configure network protection against exploitation of known vulnerabilities. “DisableIOAVProtection” cmdlet removes whether Windows Defender scans all downloaded files and attachments. “DisableRealtimeMonitoring” cmdlet removes whether to use real-time protection. “DisableScriptScanning” cmdlet removes whether to disable script scanning during malware scans. “EnableControlledFolderAccess” cmdlet clears the status for the controlled folder access feature.

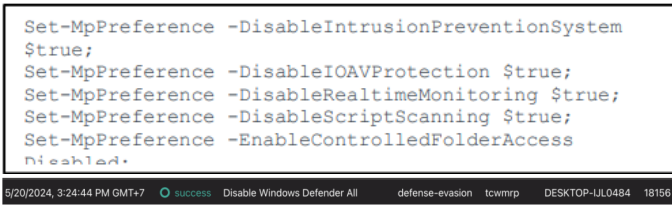


Figure 18. Emulation Successful on Caldera

| Timestamp | Alert Rule Name | Process Args |
|-----------------------------|-----------------|---|
| May 28, 2024 @ 15:25:41.535 | - | [powershell.exe -ExecutionPolicy Bypass -C Set-MpPreference -DisableIntrusionPreventionSystem \$true;Set-MpPreference -DisableIOAVProtection \$true;Set-MpPreference -DisableRealtimeMonitoring \$true;Set-MpPreference -DisableScriptScanning \$true;Set-MpPreference -... |
| May 28, 2024 @ 15:25:41.223 | - | [powershell.exe -ExecutionPolicy Bypass -C Set-MpPreference -DisableIntrusionPreventionSystem \$true;Set-MpPreference -DisableIOAVProtection \$true;Set-MpPreference -DisableRealtimeMonitoring \$true;Set-MpPreference -DisableScriptScanning \$true;Set-MpPreference -... |
| May 28, 2024 @ 15:25:41.222 | - | [powershell.exe -ExecutionPolicy Bypass -C Set-MpPreference -DisableIntrusionPreventionSystem \$true;Set-MpPreference -DisableIOAVProtection \$true;Set-MpPreference -DisableRealtimeMonitoring \$true;Set-MpPreference -DisableScriptScanning \$true;Set-MpPreference -... |
| May 28, 2024 @ 15:25:41.221 | - | [powershell.exe -ExecutionPolicy Bypass -C Set-MpPreference -DisableIntrusionPreventionSystem \$true;Set-MpPreference -DisableIOAVProtection \$true;Set-MpPreference -DisableRealtimeMonitoring \$true;Set-MpPreference -DisableScriptScanning \$true;Set-MpPreference -... |
| May 28, 2024 @ 15:25:41.220 | - | [powershell.exe -ExecutionPolicy Bypass -C Set-MpPreference -DisableIntrusionPreventionSystem \$true;Set-MpPreference -DisableIOAVProtection \$true;Set-MpPreference -DisableRealtimeMonitoring \$true;Set-MpPreference -DisableScriptScanning \$true;Set-MpPreference -... |
| May 28, 2024 @ 15:25:41.159 | - | [powershell.exe -ExecutionPolicy Bypass -C Set-MpPreference -DisableIntrusionPreventionSystem \$true;Set-MpPreference -DisableIOAVProtection \$true;Set-MpPreference -DisableRealtimeMonitoring \$true;Set-MpPreference -DisableScriptScanning \$true;Set-MpPreference -... |
| May 28, 2024 @ 15:25:41.158 | - | [powershell.exe -ExecutionPolicy Bypass -C Set-MpPreference -DisableIntrusionPreventionSystem \$true;Set-MpPreference -DisableIOAVProtection \$true;Set-MpPreference -DisableRealtimeMonitoring \$true;Set-MpPreference -DisableScriptScanning \$true;Set-MpPreference -... |
| May 28, 2024 @ 15:25:41.125 | - | [powershell.exe -ExecutionPolicy Bypass -C Set-MpPreference -DisableIntrusionPreventionSystem \$true;Set-MpPreference -DisableIOAVProtection \$true;Set-MpPreference -DisableRealtimeMonitoring \$true;Set-MpPreference -DisableScriptScanning \$true;Set-MpPreference -... |

Figure 19. Detection Result on Elastic Security

Figure 18 shows that the command executed by *Caldera Attacker Machine* was not detected by the Elastic Security. In the Elastic rules documentation, the rules defined and the command executed by Caldera are appropriate, but Elasticsearch has not been able to detect it [24].

3.3.2 Disable Microsoft Defender Firewall

This stage is to disable the Microsoft Defender Firewall by utilizing the netsh command in Powershell. When executed, this command disables the Windows Firewall, allowing all inbound and outbound network traffic without any filtering or blocking.

```
netsh advfirewall set currentprofile state off
```

5/20/2024, 3:25:44 PM GMT+7 ● success Disable Microsoft Defender Firewall defense-evasion tcwmp DESKTOP-IJ0484 21952

Figure 20. Emulation Successful on Caldera

The screenshot shows an alert in the Elastic Security interface. The alert title is "Disable Windows Firewall Rules via Netsh" with a risk score of 47. The alert is categorized as "Medium" and occurred on May 20, 2024, at 15:26:33.231. The status is "Open". Below the alert details, there are tabs for "Overview", "Table", and "JSON". The "Table" tab is selected, showing a table of highlighted fields. The fields include host.name (desktop-ij0484), user.name (Victim), rule.name (technique_id=T1518.001,technique_name=Security Software Discovery), process.executable (C:\Windows\System32\netsh.exe), kibana.alert.rule.type (eq), process.name (netsh.exe), process.parent.name (cmd.exe), and process.args (netsh advfirewall set currentprofile state off). There is also a "Visualizations" section at the bottom.

| Field | Value |
|------------------------|---|
| host.name | desktop-ij0484 |
| user.name | Victim |
| rule.name | technique_id=T1518.001,technique_name=Security Software Discovery |
| process.executable | C:\Windows\System32\netsh.exe |
| kibana.alert.rule.type | eq |
| process.name | netsh.exe |
| process.parent.name | cmd.exe |
| process.args | netsh advfirewall set currentprofile state off |

Figure 21. Detection Result on Elastic Security

Figure 20 shows that Caldera Attacker Machine action of disabling Microsoft Windows Firewall with netsh was detected by the Elastic alert "Disable Windows Firewall Rules via Netsh." In the Elastic rules documentation, the process name netsh.exe with process argument "advfirewall" and "off" triggers the alert [25].

3.4 Privilege Escalation

Privilege Escalation encompasses methods employed by adversaries to acquire high-level permissions within a system or network. While adversaries may initially infiltrate and navigate a network with lower-level access, they often require elevated permissions to fully execute their objectives [26].

One of the tactics used in Privilege Escalation is “User Access Control (UAC) Bypass”. UAC Bypass refers to a method that allows malicious software to elevate privileges and bypass security restrictions enforced by UAC in Windows operating systems. However, if malware can trick an elevated process into loading a malicious DLL, the code inside the DLL can gain administrator privileges. In Caldera, the UAC Bypass process is executed through the command line below.

```
New-ItemProperty -Path HKLM:\Software\Microsoft\Windows\CurrentVersion\Policies\System -
Name EnableLUA -PropertyType DWord -Value 0 -Force
```

The command line will bypass UAC by changing the “EnableLUA” registry value to 0 in the *HKLM : Software\Microsoft\Windows\CurrentVersion\Policies\System\registry*. Figure 22 shows that Elasticsearch is able to detect the change of UAC to 0. Based



Figure 22. Emulation Successfull on Caldera

| @timestamp | Rule | Severity | Risk Score | host.name | user.name | process.name |
|---------------------------|--|----------|------------|---------------|-----------|----------------|
| Jun 16, 2024 @ 15:30:4... | Disabling User Account Control via Registry Modification | medium | 47 | desktop-@0484 | Victim | powershell.exe |

Figure 23. Detection Result on Elastic Security

on Elasticsearch prebuilt rules, there are rules that have the capability to detect this, namely "Disabling User Account Control via Registry Modification" [27]. The rule checks activities with the Windows operating system, in the registry section with the change parameter, which indicates that there is a change in the registry value. The registry that is checked is *HKLM \ SOFTWARE \ Microsoft \ Windows \ CurrentVersion \ Policies \ System \ EnableLUA*

3.5 Lateral Movement

Lateral Movement involves tactics employed by adversaries to penetrate and control remote systems within a network. Achieving their primary objectives typically requires navigating the network to locate specific targets and subsequently gaining access to them [28].

3.5.1 Disable NLA for RDP via Command Prompt

Network Level Authentication (NLA) stands as a security measure within Remote Desktop Services (RDS), offering an additional authentication step prior to initiating a remote desktop session with either a server or a client. From an attacker’s perspective, disabling “NLA for RDS via Command Prompt” can provide them with easier access to target systems. With NLA disabled, the attacker doesn’t need to provide valid credentials before establishing an RDS session with the target system.

```
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\
WinStations\RDP-Tcp" /v UserAuthentication /d 0 /t REG_DWORD /f
```

5/21/2024, 10:57:22 PM GMT+7 ● success Disable NLA for RDP via Command Prompt lateral-movement *sjrjmy* DESKTOP-IJL0484 8352

Figure 24. Emulation Successful on Caldera

● Low

May 21, 2024 @ 22:59:09.117

Network-Level Authentication (NLA) Disabled

Status: Open Risk score: 21 Assignees: +

Overview Table JSON

Highlighted fields

| Field | Value |
|------------------------|--|
| host.name | desktop-ijl0484 |
| agent.status | Healthy |
| user.name | Victim |
| process.executable | C:\Windows\System32\reg.exe |
| kibana.alert.rule.type | eql |
| registry.key | SYSTEM\ControlSet001\Control\Terminal Server\WinStations\RDP-Tcp |
| registry.value | UserAuthentication |
| process.name | reg.exe |

Figure 25. Detection Result on Elastic Security

Figure 24 shows that *Caldera Attacker Machine* attempt to change the NLA value for RDS was detected. This is based on the Elastic rules documentation, which states that the alert is triggered based on the registry key and the value of the changed registry [29].

4. Discussion

Alerts are mapping into false positive, true positive, false negative, and false positive. A true positive alert occurs when Elasticsearch triggers an alert during an actual attack. False Positive alert is a situation where an alert is triggered by Elasticsearch, but upon validation, it is determined that no actual attack has occurred. Whereas, False Negative Alert refers to a scenario where an attack occur but Elasticsearch fails to generate an alert. Finally, True Negative Alert indicates that neither an alert was triggered nor did an attack occur.

Table 6. Detection Result based on Attack Vector

| No | Technique | Tactics | Detection Result |
|----|----------------------|---|------------------|
| 1 | Initial Access | Download Enabled Attachment Macro-Phishing | False Negative |
| 2 | Discovery | Identify local users | True Positive |
| | | Identify active users | False Negative |
| | | Identify Firewalls | False Negative |
| | | Discover antivirus programs | True Positive |
| 3 | Defense Evasion | Disable Defender Firewall Microsoft | True Positive |
| | | Disable Defender All Windows | False Negative |
| 4 | Privelege Escalation | UAC bypass registry | True Positive |
| 5 | Lateral Movement | Disable RDP via Command Prompt NLA for | True Positive |

False Negative alerts can arise due to two primary factors, undefined rules and alerts that do not appear even though rules are defined. As a result, the system fails to trigger alerts for certain types of attacks. In the Initial Access phase, the alerts only include attempts to connect to the targeted URL but do not include downloading files through that URL into the **TEMP** directory. This is because if rules are defined to detect the presence of files placed in the **TEMP** directory, it would increase the false positive detection rate. The **TEMP** directory does not indicate that files placed in it are malicious, as the **TEMP** folder is also used for legitimate actions. The "Identify Local Users" attack vector was not detected by Elastic Security due to the absence of a predefined rule for its detection. Meanwhile, in the "Identify Firewall" attack vector, alerts are not detected even though rules are defined for "Security Software Discovery using WMIC" due to the absence of some strings such as "*root \$ SecurityCenter*".

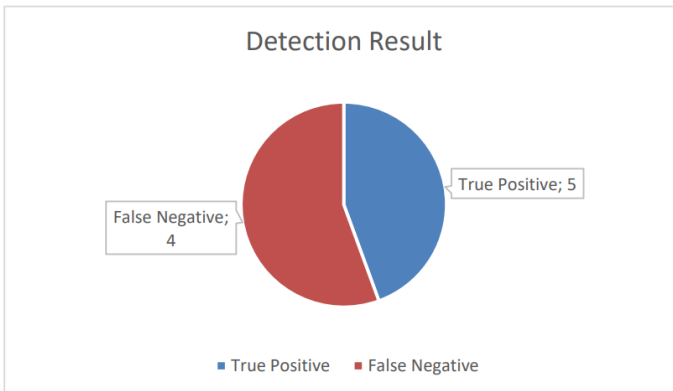


Figure 26. Detection Result

“Disabling Windows Defender Security Setting via PowerShell”, the process arguments disabled are not defined in detail [24]. Elasticsearch rules are open source, so some alerts that are not detected with predefined rules can be addressed by submitting them to the Elastic Detection Rules GitHub repository.

The APT attack detection by Elastic Security identified 5 True Positives and 4 False Negatives. These results stem from simulating 9 Tactics, Techniques, and Procedures (TTPs) using Caldera.

5. Conclusion

The research was conducted by evaluating open-source Elasticsearch Endpoint Detection and Response (EDR) to detect attack vector perform by Caldera Platform. Attack vector is construct using Ability feature in Caldera Platform started from Initial Access, Discovery, Defense Evasion, Privilege Escalation, Lateral Movement, Collection, and Impact. Attack simulations were conducted to assess Elasticsearch’s detection level based on the alerts generated for each attack vector. The detection results indicated the presence of detected alerts with predefined rules, undetected alerts with predefined rules, and undetected alerts with undefined rules. This was due to some attack vectors not being defined by the rules, potentially leading to high false positives. Additionally, there were attack vectors that did not trigger alerts even though rules had been defined. This is because the rules defined by Elastic do not cover some strings.

References

- [1] International Telecommunication Union (ITU). *Individuals using the Internet (% of population) - Indonesia*. <https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=ID>. Accessed: 2024-05-22.
- [2] APJII. *Profil Internet Indonesia 2022*. 2022.
- [3] Badan Siber dan Sandi Negara. *LANSKAP KEAMANAN SIBER INDONESIA TAHUN 2023*. 2023.
- [4] Badan Siber dan Sandi Negara. *Laporan Tahunan Monitoring Keamanan Siber 2021 (compressed)*. 2022.
- [5] S. H. Park et al. “Performance Evaluation of Open-Source Endpoint Detection and Response Combining Google Rapid Response and Osquery for Threat Detection”. In: *IEEE Access* 10 (2022), pp. 20259–20269. doi: 10.1109/ACCESS.2022.3152574.
- [6] H. S. Galal, Y. B. Mahdy, and M. A. Atia. “Behavior-based features model for malware detection”. In: *Journal of Computer Virology and Hacking Techniques* 12.2 (May 2016), pp. 59–67. doi: 10.1007/s11416-015-0244-0.
- [7] F. Dong et al. “Are we there yet? An Industrial Viewpoint on Provenance-based Endpoint Detection and Response Tools”. In: *CCS 2023 - Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security*. Association for Computing Machinery, Inc, Nov. 2023, pp. 2396–2410. doi: 10.1145/3576915.3616580.
- [8] A. Kumar et al. “Endpoint Network Behavior Analysis and Anomaly Detection Using Unsupervised Machine Learning”. In: 2023, pp. 305–317. doi: 10.1007/978-981-19-4182-5_24.
- [9] A. Chuvakin. *Endpoint Threat Detection and Response Tools and Practices*. <https://www.gartner.com/en/documents/2596321>. Accessed: 2024-05-22.
- [10] G. Karantzas and C. Patsakis. “An Empirical Assessment of Endpoint Detection and Response Systems against Advanced Persistent Threats Attack Vectors”. In: *Journal of Cybersecurity and Privacy* 1.3 (July 2021), pp. 387–421. doi: 10.3390/jcp1030021.

- [11] Elastic. *Elastic Security overview* | *Elastic Security Solution [8.13]* | Elastic. <https://www.elastic.co/guide/en/security/current/es-overview.html>. Accessed: 2024-05-22.
- [12] W. U. Hassan, A. Bates, and D. Marino. "Tactical provenance analysis for endpoint detection and response systems". In: *Proceedings - IEEE Symposium on Security and Privacy*. Institute of Electrical and Electronics Engineers Inc., May 2020, pp. 1172–1189. DOI: 10.1109/SP40000.2020.00096.
- [13] K. Subramanian and W. Meng. "Threat Hunting Using Elastic Stack: An Evaluation". In: *2021 IEEE International Conference on Service Operations and Logistics, and Informatics, SOLI 2021*. Institute of Electrical and Electronics Engineers Inc., 2021. DOI: 10.1109/SOLI54607.2021.9672347.
- [14] Elastic Security. <https://www.elastic.co/guide/en/security/index.html>. Accessed: 2024-05-23.
- [15] Elastic. *Fleet and Elastic Agent overview* | *Fleet and Elastic Agent Guide [8.13]* | Elastic. <https://www.elastic.co/guide/en/fleet/current/fleetoverview.html>. Accessed: 2024-05-22.
- [16] P. Kendrick *et al.* "A self-organising multi-agent system for decentralised forensic investigations". In: *Expert Systems with Applications* 102 (July 2018), pp. 12–26. DOI: 10.1016/J.ESWA.2018.02.023.
- [17] caldera documentation. *How to Build Agents — caldera documentation*. <https://caldera.readthedocs.io/en/latest/How-to-Build-Agents.html>. Accessed: 2024-05-22.
- [18] caldera documentation. *Learning the terminology — caldera documentation*. <https://caldera.readthedocs.io/en/latest/Learning-the-terminology.html>. Accessed: 2024-05-23.
- [19] *Initial Access, Tactic TA0001 - Enterprise* | MITRE ATT&CK®. <https://attack.mitre.org/tactics/TA0001/>. Accessed: 2024-05-22.
- [20] *Discovery, Tactic TA0007 - Enterprise* | MITRE ATT&CK®. <https://attack.mitre.org/tactics/TA0007/>. Accessed: 2024-05-22.
- [21] Elastic. *Unusual Discovery Signal Alert with Unusual Process Command Line* | *Elastic Security Solution [8.13]* | Elastic. <https://www.elastic.co/guide/en/security/current/unusual-discovery-signal-alert-with-unusualprocess-command-line.html>. Accessed: 2024-05-22.
- [22] Elastic. *Unusual Discovery Activity by User* | *Elastic Security Solution [8.13]* | Elastic. <https://www.elastic.co/guide/en/security/current/unusuldiscovery-activity-by-user.html#unusual-discovery-activity-by-user>. Accessed: 2024-05-22.
- [23] *Defense Evasion, Tactic TA0005 - Enterprise* | MITRE ATT&CK®. <https://attack.mitre.org/tactics/TA0005/>. Accessed: 2024-05-22.
- [24] Elastic. *Disabling Windows Defender Security Settings via PowerShell* | *Elastic Security Solution [8.13]*. <https://www.elastic.co/guide/en/security/current/disabling-windows-defender-security-settingsvia-powershell.html>. Accessed: 2024-05-22.
- [25] Elastic. *Disable Windows Firewall Rules via Netsh* | *Elastic Security Solution [8.13]*. <https://www.elastic.co/guide/en/security/current/disable-windows-firewall-rules-via-netsh.html>. Accessed: 2024-05-22.
- [26] *Privilege Escalation, Tactic TA0004 - Enterprise* | MITRE ATT&CK®. <https://attack.mitre.org/tactics/TA0004/>. Accessed: 2024-05-22.
- [27] Elastic. *Disabling User Account Control via Registry Modification* | *Elastic Security Solution [7.17]*. <https://www.elastic.co/guide/en/security/7.17/prebuilt-rule-0-14-1-disabling-user-accountcontrol-via-registry-modification.html>. Accessed: 2024-05-22.
- [28] *Lateral Movement, Tactic TA0008 - Enterprise* | MITRE ATT&CK®. <https://attack.mitre.org/tactics/TA0008/>. Accessed: 2024-05-22.
- [29] Elastic. *Network-Level Authentication (NLA) Disabled* | *Elastic Security Solution [8.13]*. <https://www.elastic.co/guide/en/security/current/network-level-authentication-nla-disabled.html>. Accessed: 2024-05-22.