



MALWARE DETECTION AND RESPONSE

Submitted in 10/24/2024

ABSTRACT

This Report Summarizes
the journey of
Discovering the logs and
Configuring SIEM
solution into an
Environment

Contents

Introduction.....	3
Malware Types	4
Correlating Malware Types with MITRE ATT&CK.....	7
What are SIEM Solutions?	10
SIEM Solution Selection	11
Elk Configuration	12
1. Cloud Deployment Strategy	13
2. Endpoint Integration.....	13
Windows Environment Configuration	13
Linux Environment Configuration	15
3. Filebeat Implementation and Troubleshooting.....	15
4. Integration Validation.....	16
Setting Detection Rules and Malware Testing.....	17
Setting Detection Rules and Malware Testing.....	17
Detection Rule Configuration.....	17
Accessing the Rule Creation Interface.....	17
Critical Rule Components.....	17
Malware Detection Testing.....	18
Test Procedure	18
Test Results.....	20
Recommended Rule Configurations.....	20
User Awareness Training: Bridging the Technical Gap	21
Training Objectives	21
Key Training Components.....	21
1. Understanding Cyber Threats.....	21

2. Phishing Attack Awareness.....	22
3. Malware Prevention for Non-Technical Users.....	22
Training Delivery Methods.....	22
Practical Guidelines Provided	23
Key Takeaways for Participants.....	23
Security Best Practices:	23
Response Procedures:.....	23
Training Impact Assessment	24
 Figure 1:Malware Types	4
Figure 2:Splunk SIEM.....	11
Figure 3 ELK stack.....	11
Figure 4 IBM Qradar SIEM	11
Figure 5 SIEM cloud instance	13
Figure 6 windows user agent installation	13
Figure 7 fleet managment after endpoint added.....	14
Figure 8 Windows User Agent Installation	14
Figure 9 Critical Integrations in the agent policy.....	15
Figure 10 Linux user agent installation.....	15
Figure 11 Malware bazaar website.....	18
Figure 12 VM network settings	19
Figure 13 EDR detection and response.....	20
Figure 14 process logs	20

Introduction

Picture this: You're tasked with defending a digital fortress, but you don't know what the invaders look like or how they operate. Sounds like a recipe for disaster, right? That's exactly the challenge we faced when we embarked on our four-week journey with DEPI to tackle the ever-evolving threat of malware.

This report documents our adventure from wide-eyed novices to seasoned malware hunters. We started with a simple yet crucial realization: you can't detect and prevent something you aren't aware of. It's like trying to catch a thief without knowing what they look like or how they break in. So, we rolled up our sleeves and dove headfirst into the murky waters of malware research.

Our first stop? Identifying the various breeds of digital nasties out there. From sneaky trojans to ransomware that holds your data hostage, we left no stone unturned. But knowing your enemy is only half the battle. We needed a map to make sense of this chaotic landscape, and that's where MITRE ATT&CK came in - a framework so well-respected in the cybersecurity world, it's practically the Rosetta Stone of digital threats.

Armed with knowledge and a battle plan, we set our sights on building a formidable defense. Enter the ELK stack - our secret weapon for correlating data from various endpoints. It was like setting up a network of digital security cameras, each keeping a vigilant eye out for any suspicious activity.

But here's the thing about cybersecurity - it's not just about fancy tools and tech jargon. The strongest firewall in the world is useless if someone unwittingly leaves the back door open. That's why we took on the challenge of creating user training materials for our non-technical colleagues. Because let's face it, in this digital age, we're all on the front lines.

So, buckle up and join us on this whirlwind tour through the world of malware analysis, detection, and prevention. It's a tale of teamwork, technology, and tenacity - proving that with the right tools and knowledge, even the most formidable digital threats can be tamed.

Malware Types

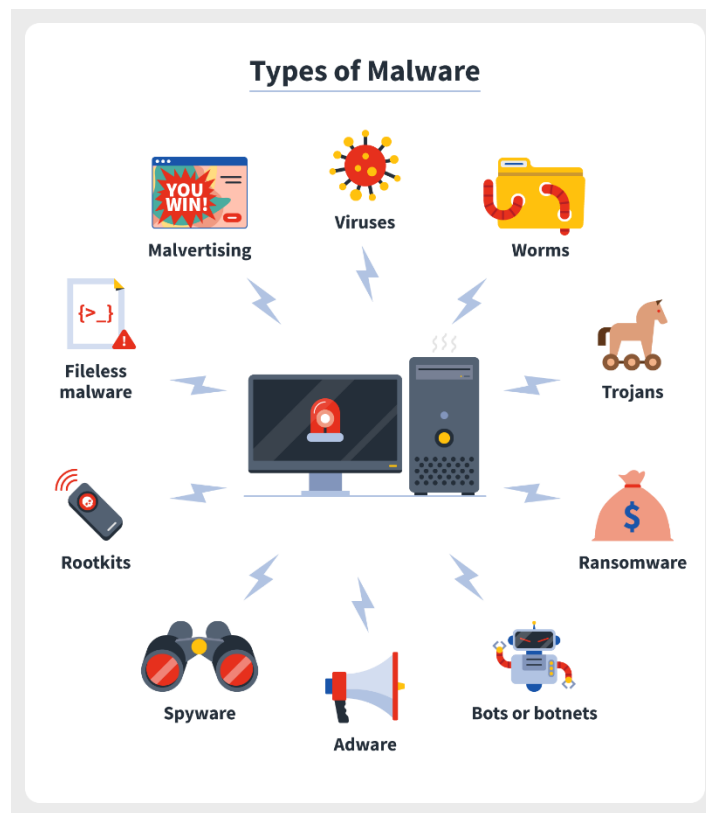


FIGURE 1: MALWARE TYPES

In the dynamic field of cybersecurity, a thorough understanding of various malware types is essential for developing robust defense strategies. This section provides a detailed examination of primary malware categories, their characteristics, and potential impacts on systems and networks.

1. Viruses: Self-replicating malicious programs that attach to clean files and spread throughout computer systems, often causing widespread damage. Viruses can be further categorized into: a)
 1. Monomorphic Viruses: These maintain a constant structure and code across infections, making them easier to detect once identified.
 2. Polymorphic Viruses: More sophisticated variants that can change their code or encryption techniques with each infection, significantly complicating detection efforts.
2. Worms: Standalone malware that replicates itself to spread to other computers, often through network connections, without requiring human interaction.
3. Trojans: Deceptive programs that appear legitimate but contain malicious code, often used to create backdoors in security systems for other malware or unauthorized access.
4. Ransomware: Malicious software designed to block access to a computer system or data until a sum of money (ransom) is paid.
5. Spyware: Software that covertly gathers user information through the user's internet connection without their knowledge, usually for advertising purposes or to steal sensitive data.
6. Adware: Often bundled with free software, adware displays unwanted advertisements and can sometimes contain more malicious payloads.

7. Bots or Botnets: Networks of infected computers controlled remotely by attackers, often used for distributed denial-of-service (DDoS) attacks or spam distribution.
8. Rootkits: Malware designed to provide privileged access to a computer while actively hiding its presence, making detection and removal particularly challenging.
9. Fileless Malware: A sophisticated threat that operates entirely in a system's RAM, leaving no files on the hard drive and thus evading traditional signature-based detection methods.
10. Malvertising: The use of online advertising to spread malware, often through legitimate advertising networks and websites, making it particularly insidious.

Each of these malware types presents unique challenges to cybersecurity professionals. Their diverse methods of propagation, concealment, and system compromise necessitate a multifaceted approach to detection, prevention, and mitigation. The evolution from monomorphic to polymorphic viruses exemplifies the ongoing arms race between malware creators and security experts, highlighting the need for continually updated defense mechanisms.

In the subsequent section, we will explore how these various malware types correlate with the MITRE ATT&CK framework, providing a structured approach to understanding their tactics, techniques, and procedures. This analysis will form the foundation for developing robust, targeted cybersecurity measures tailored to address specific threat vectors and their evolving nature.

Correlating Malware Types with MITRE ATT&CK

1. Viruses (Monomorphic and Polymorphic):

- User Execution (T1204)
- Obfuscated Files or Information (T1027)
- Masquerading (T1036)

2. Worms:

- Exploitation of Remote Services (T1210)
- Network Service Scanning (T1046)
- Remote System Discovery (T1018)

3. Trojans:

- Registry Run Keys / Startup Folder (T1547.001)
- Exploitation for Privilege Escalation (T1068)
- Credentials from Password Stores (T1555)

4. Ransomware:

- Data Encrypted for Impact (T1486)
- Data Destruction (T1485)
- Exfiltration Over C2 Channel (T1041)

5. Spyware:

- Input Capture (T1056)
- Screen Capture (T1113)

- Data from Local System (T1005)

6. Adware:

- Browser Extensions (T1176)
- Modify Registry (T1112)
- Code Signing (T1553.002)

7. Bots/Botnets:

- Application Layer Protocol (T1071)
- Network Denial of Service (T1498)
- Remote Access Software (T1219)

8. Rootkits:

- Bootkit (T1542.003)
- Rootkit (T1014)
- System Binary Proxy Execution (T1218)

9. Fileless Malware:

- PowerShell (T1059.001)
- Windows Management Instrumentation (T1047)
- Regsvr32 (T1218.010)

10. Malvertising:

- Drive-by Compromise (T1189)

- Malicious File (T1204.002)
- Exploit Public-Facing Application (T1190)

By associating these specific MITRE ATT&CK technique IDs with each malware type, we create a more precise mapping between the threats and the framework. This detailed correlation serves several purposes:

1. It provides a common language for discussing threat behaviors across different security teams and tools.
2. It allows for more targeted threat hunting and incident response strategies.
3. It helps in prioritizing security controls and mitigation strategies based on the most relevant techniques for each malware type.
4. It facilitates the integration of threat intelligence into existing security operations and tools that leverage the MITRE ATT&CK framework.

When configuring our ELK stack and other security tools, we can use these technique IDs to create more specific detection rules and alerts. For instance, we might prioritize monitoring for PowerShell execution (T1059.001) when defending against fileless malware, or focus on detecting unusual registry modifications (T1112) when concerned about adware infections.

This granular approach to mapping malware types to specific MITRE ATT&CK techniques provides a solid foundation for both proactive threat hunting and reactive incident response. It allows security

teams to focus their efforts on the most relevant areas based on their specific threat landscape and the types of malwares they're most likely to encounter.

What are SIEM Solutions?

Security Information and Event Management (SIEM) is a comprehensive approach to managing an organization's security posture. A SIEM solution combines two critical cybersecurity functions:

Security Information Management (SIM): Focuses on collecting, analyzing, and reporting on log data from various sources across an organization's IT infrastructure.

Security Event Management (SEM): Provides real-time monitoring, correlation of events, notifications, and console views for security incidents.

At its core, a SIEM solution acts as the central nervous system of an organization's cybersecurity operations. It collects data from multiple sources, including:

- Network devices

- Servers

- Applications

- Security tools (firewalls, antivirus software, intrusion detection systems)

- Cloud services

This data is then aggregated, normalized, and analyzed in real-time to detect potential security threats, policy violations, or other anomalies. Key features of modern SIEM solutions include:

Log Management: Centralized collection and storage of log data from various sources.

Event Correlation: Analyzing disparate events to identify patterns indicative of security incidents.

Automated Alerting: Generating notifications for security teams when potential threats are detected.

Compliance Reporting: Assisting with regulatory compliance by providing audit trails and reports.

Threat Intelligence Integration: Incorporating external threat data to enhance detection capabilities.

By providing a holistic view of an organization's security landscape, SIEM solutions enable security teams to detect, investigate, and respond to threats more efficiently. They serve as a crucial tool in maintaining a robust security posture in today's complex and evolving threat environment.

SIEM Solution Selection



FIGURE 3 ELK STACK



FIGURE 2: SPLUNK SIEM



FIGURE 4 IBM QRADAR SIEM

With numerous options available, selecting the right SIEM solution was crucial for us. The decision to adopt the ELK Stack was a game-changer, as it allowed us to strike the optimal balance between resource efficiency and reliability. Factoring in time constraints, ELK emerged as the most viable solution among the alternatives.

We chose Elastic SIEM primarily for its cloud-based infrastructure, which eliminates the need for local storage and high-performance hardware—requirements typically associated with solutions like IBM Qradar. Furthermore, Elastic SIEM comes with a pre-configured architecture, sparing us the complexity of setting up clusters and indices, as would be necessary with Splunk SIEM. This streamlined approach made Elastic SIEM the ideal solution for our specific needs.

Elk Configuration

After identifying various malware types and mapping them to the MITRE ATT&CK framework, the next crucial step was implementing a robust monitoring solution. We chose the ELK (Elasticsearch, Logstash, Kibana) stack as our SIEM solution, configuring it to effectively monitor and detect potential malware activities across our infrastructure.

1. Cloud Deployment Strategy

We opted for a cloud-based deployment on Google Cloud Platform (GCP), specifically selecting the Tokyo region to optimize latency and comply with data residency requirements. This decision provided us with the scalability and reliability necessary for enterprise-wide security monitoring.

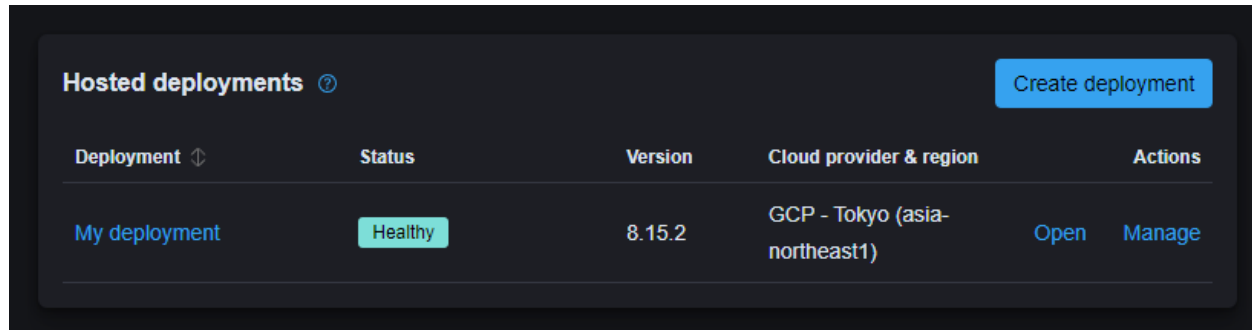


FIGURE 5 SIEM CLOUD INSTANCE

2. Endpoint Integration

The integration of endpoints with our SIEM solution involved a systematic approach across different operating systems:

Windows Environment Configuration

1. Fleet Management Setup:

- Deployed Elastic agents via Fleet management interface
- Executed deployment commands through PowerShell with administrative privileges
- Implemented Sysmon for enhanced system monitoring capabilities

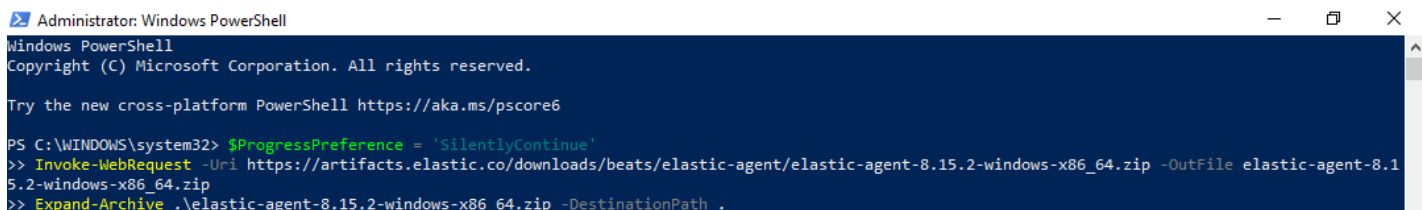


FIGURE 6 WINDOWS USER AGENT INSTALLATION

```

Elastic Agent will be installed at C:\Program Files\Elastic\Agent and will run as a service. Do you want to continue? [Y/n]:
[ === ] Service Started [7s] Elastic Agent successfully installed, starting enrollment.
[ == ] Waiting For Enroll... [8s] {"log.level":"info","@timestamp":"2024-10-08T10:03:17.605+0200","log.origin":{"function":"github.com/elastic/elastic-agent/internal/pkg/agent/cmd.(*enrollCmd).enrollWithBackoff","file.name":"cmd/enroll_cmd.go","file.line":518},"message":"Starting enrollment to URL: https://6fc8f71acac849af98f987124fdf5426.fleet.asia-northeast1.gcp.cloud.es.io:443/", "ecs.version":"1.6.0"}
[====] Waiting For Enroll... [16s] {"log.level":"info","@timestamp":"2024-10-08T10:03:25.913+0200","log.origin":{"function":"github.com/elastic/elastic-agent/internal/pkg/agent/cmd.(*enrollCmd).daemonReloadWithBackoff","file.name":"cmd/enroll_cmd.go","file.line":481},"message":"Restarting agent daemon, attempt 0","ecs.version":"1.6.0"}
[====] Waiting For Enroll... [16s] {"log.level":"info","@timestamp":"2024-10-08T10:03:25.936+0200","log.origin":{"function":"github.com/elastic/elastic-agent/internal/pkg/agent/cmd.(*enrollCmd).Execute","file.name":"cmd/enroll_cmd.go","file.line":299},"message":"Successfully triggered restart on running Elastic Agent.","ecs.version":"1.6.0"}
Successfully enrolled the Elastic Agent.
[=== ] Done [16s]
Elastic Agent has been successfully installed.
PS C:\WINDOWS\system32\elastic-agent-8.15.2-windows-x86_64>
PS C:\WINDOWS\system32\elastic-agent-8.15.2-windows-x86_64>
PS C:\WINDOWS\system32\elastic-agent-8.15.2-windows-x86_64> $ProgressPreference = 'SilentlyContinue'
PS C:\WINDOWS\system32\elastic-agent-8.15.2-windows-x86_64> Invoke-WebRequest -Uri https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.15.2-windows-x86_64.zip -OutFile elastic-agent-8.15.2-windows-x86_64.zip

```

FIGURE 8 WINDOWS USER AGENT INSTALLATION

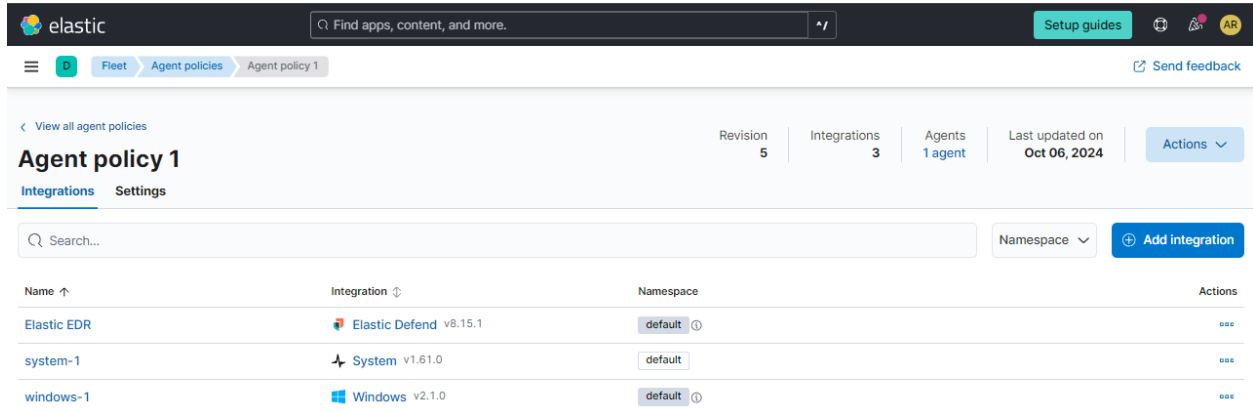
Status	Host	Agent policy	CPU	Memory	Last activity	Version	Actions
Healthy	DESKTOP-I07LO42	Agent policy 1 rev. 5	N/A	N/A	24 seconds ago	8.15.2	...
Healthy	8b1938ae2356	Elastic Cloud agent policy rev. 5	N/A	N/A	18 seconds ago	8.15.2	...

FIGURE 7 FLEET MANAGEMENT AFTER ENDPOINT ADDED

2. Critical Integrations:

- Elastic Defend (EDR):
 - Implemented comprehensive endpoint protection
 - Enabled malware and ransomware prevention capabilities
 - Established behavioral monitoring across Windows, macOS, and Linux
 - Configured credential hardening for Windows environments
- System Integration:
 - Deployed for comprehensive metrics collection
 - Established baseline performance monitoring
 - Enabled anomaly detection capabilities

- Windows-Specific Integration:
 - Configured specialized Windows event collection
 - Established custom alert criteria
 - Implemented Windows-specific security policies



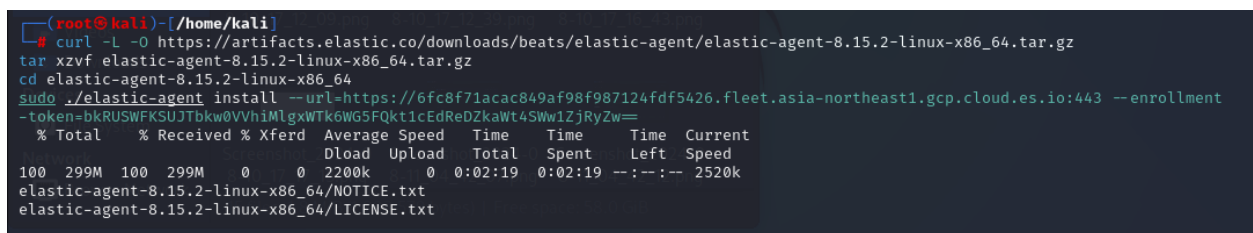
The screenshot shows the Elastic Agent Policy interface. At the top, there's a search bar and navigation links for Fleet, Agent policies, and Agent policy 1. Below this, a summary bar shows Revision 5, Integrations 3, Agents 1 agent, and Last updated on Oct 06, 2024. The main section is titled 'Agent policy 1' and has tabs for Integrations and Settings. A search bar is present above a table of integrations. The table has columns for Name, Integration, Namespace, and Actions.

Name	Integration	Namespace	Actions
Elastic EDR	Elastic Defend v8.15.1	default	...
system-1	System v1.61.0	default	...
windows-1	Windows v2.1.0	default	...

FIGURE 9 CRITICAL INTEGRATIONS IN THE AGENT POLICY

Linux Environment Configuration

- Deployed Elastic agents via terminal commands
- Implemented Auditd logs integration for system audit capabilities
- Configured Journalctl for comprehensive system logging



```
(root@kali)~# curl -L -O https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.15.2-linux-x86_64.tar.gz
tar xzvf elastic-agent-8.15.2-linux-x86_64.tar.gz
cd elastic-agent-8.15.2-linux-x86_64
sudo ./elastic-agent install --url=https://6fc8f71acac849af98f987124fdf5426.fleet.asia-northeast1.gcp.cloud.es.io:443 --enrollment-token=bkRUSWFKSUJTbkW0VVhIMlgxWTk6WG5FQkt1cEdReDZkaWt4SWw1ZjRyZw==
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           Dload  Upload   Total   Spent    Left   Speed
100 299M  100 299M    0     0  2200k      0  0:02:19  0:02:19 --:--:-- 2520k
elastic-agent-8.15.2-linux-x86_64/NOTICE.txt
elastic-agent-8.15.2-linux-x86_64/LICENSE.txt
```

FIGURE 10 LINUX USER AGENT INSTALLATION

3. Filebeat Implementation and Troubleshooting

During our deployment, we encountered significant challenges with log collection from endpoints. The initial configuration failed to properly

forward logs to our cloud-based SIEM solution. To resolve this, we implemented Filebeat as an additional component:

```
filebeat.inputs:
- type: log
  enabled: true
  paths:
    - /var/log/*.log      # Linux logs
    - C:\Windows\System32\winevt\Logs\*.evtx    # Windows logs

output.elasticsearch:
  hosts: ["cloud-instance:9200"]
  protocol: "https"
  ssl.certificate_authorities: ["path/to/ca.crt"]
```

The Filebeat implementation resolved our log forwarding issues by:

- Providing reliable log shipping capabilities
- Ensuring consistent log formatting
- Maintaining log integrity during transmission
- Enabling efficient log parsing and indexing

This configuration proved crucial in establishing a robust log collection pipeline from our endpoints to the cloud-based SIEM, enabling comprehensive security monitoring and malware detection capabilities.

4. Integration Validation

After completing the configuration, we validated our setup by:

1. Confirming log receipt in Elasticsearch
2. Verifying proper log parsing and indexing
3. Testing alert configurations
4. Ensuring real-time monitoring capabilities

This comprehensive setup provides us with the foundation necessary for implementing advanced malware detection and prevention strategies, which we'll explore in subsequent sections of this report.

Setting Detection Rules and Malware Testing

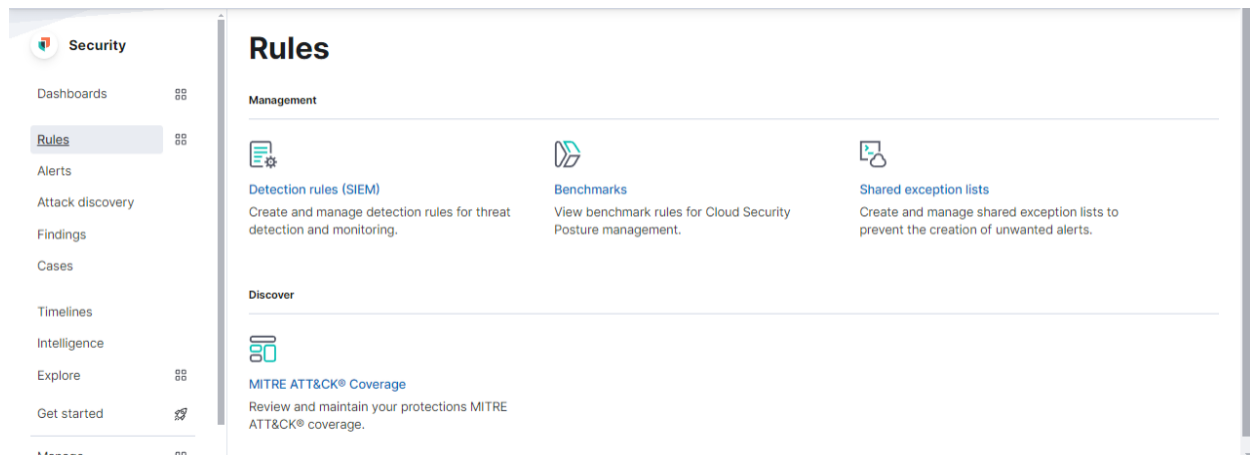
Setting Detection Rules and Malware Testing

After configuring our ELK stack, the next crucial phase was establishing effective detection rules and validating them through controlled malware testing. This section details our approach to rule creation and practical validation.

Detection Rule Configuration

Accessing the Rule Creation Interface

1. Navigate to the Security page in Kibana
2. Access the "Rules" section
3. Select "Detection Rules"
4. Choose "Create new rule"



Critical Rule Components

We configured several detection rules focusing on:

- Process creation anomalies
- Suspicious file modifications
- Network connection patterns

- Registry modifications
- PowerShell command execution
- Unusual system behaviors

Malware Detection Testing

To validate our detection capabilities, we conducted controlled testing using known malware samples. This approach allowed us to:

1. Verify rule effectiveness
2. Fine-tune detection parameters
3. Validate EDR response
4. Confirm proper alert generation

Test Procedure

1. Sample Acquisition

- Source: Malware Bazaar (controlled environment)
- Strict adherence to security protocols during sample handling

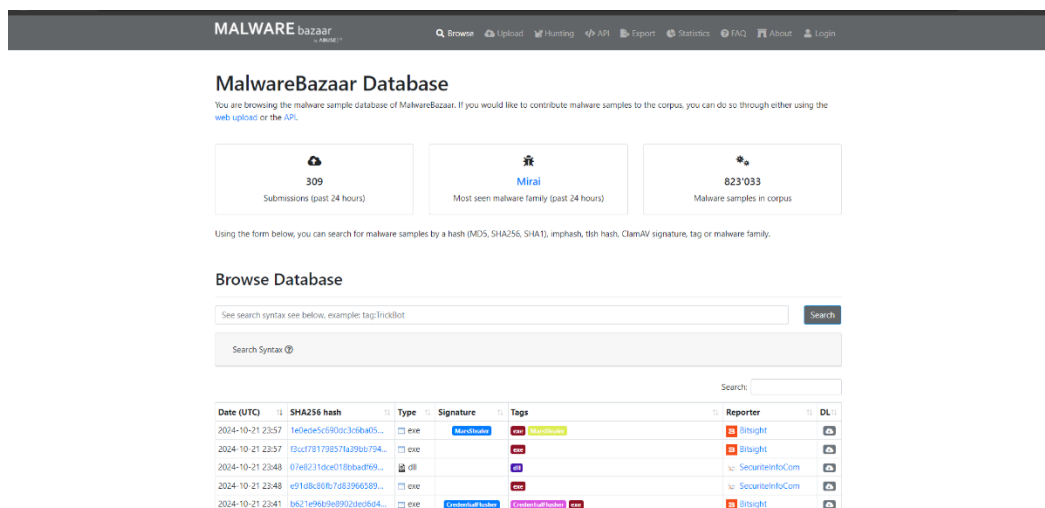


FIGURE 11 MALWARE BAZAAR WEBSITE

2. Testing Environment Setup

- Isolated virtual environment
- Network monitoring enabled
- Full logging capabilities activated
- EDR monitoring active

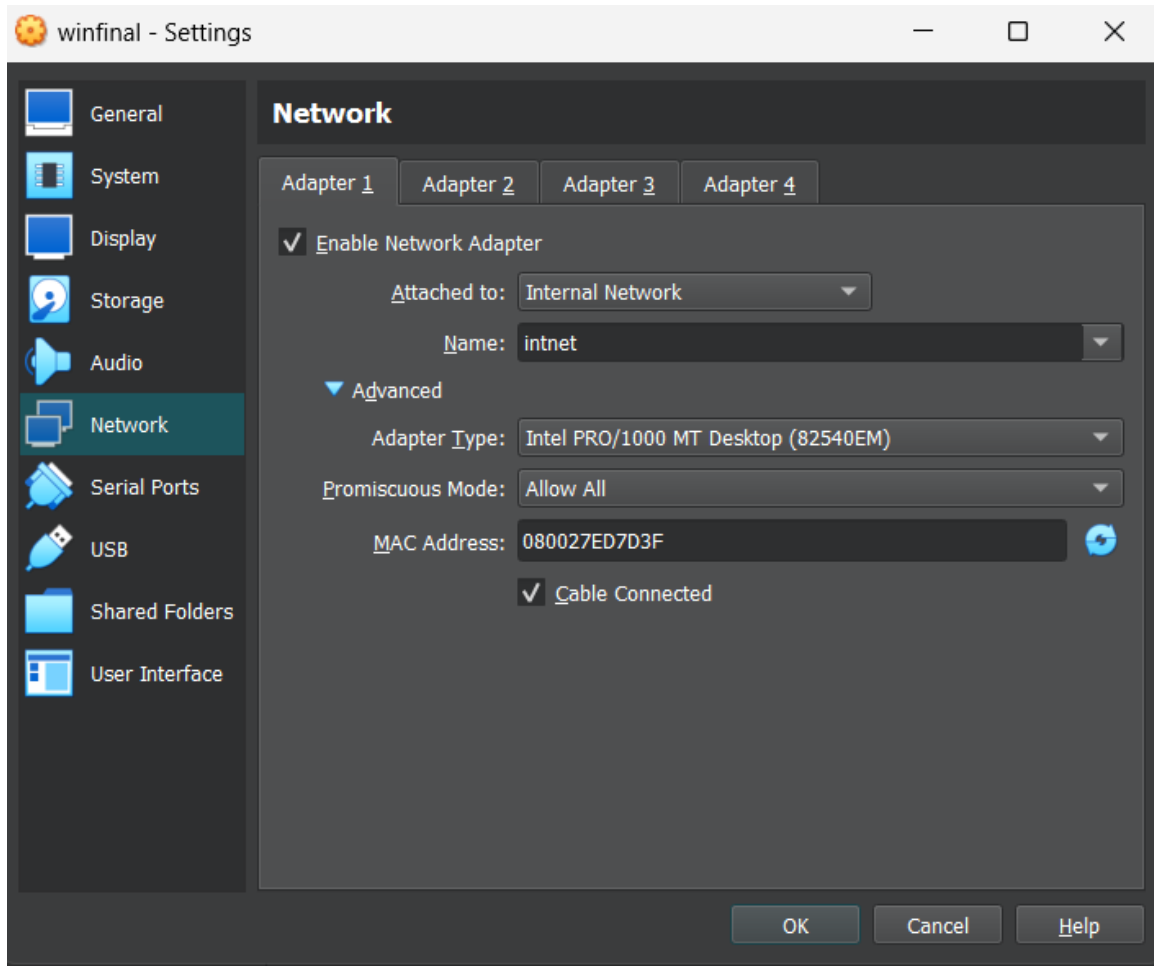


FIGURE 12 VM NETWORK SETTINGS

3. Execution and Monitoring

- Controlled malware execution
- Real-time monitoring of:
 - Process creation
 - File system changes
 - Network connections

Test Results

Our testing demonstrated successful:

- Immediate malware detection
- EDR prevention activation
- Real-time alert generation
- Accurate log forwarding
- Proper event correlation

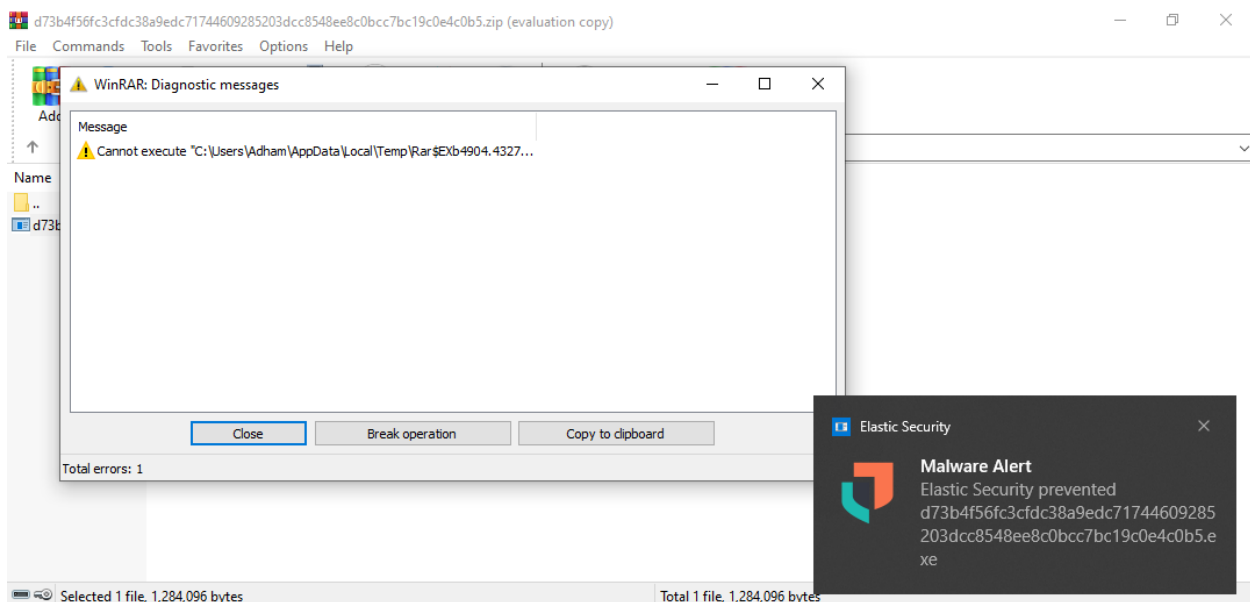


FIGURE 13 EDR DETECTION AND RESPONSE

<input checked="" type="checkbox"/>	Oct 8, 2024 @ 18:28:24.710	file.hash.sha256 d73b4f56fc3cfdc38a9edc71744609285203dcc8548ee8c0bcc7bc19c0e4c0b5 process.hash.sha256 d73b4f56fc3cfdc38a9edc71744609285203dcc8548ee8c0bcc7bc19c0e4c0b5 @timestamp Oct 8, 2024 @ 18:28:24.710 agent.build.original version: 8.15.2, compiled: Tue Sep 17 23:00:00 2024, branch: HEAD, commit: b4d81a7079c66492513f98f541621f2ec028a46d agent.id 9d57128e-764e-4132-b1ca-5f298af6079e agent.type endpoint agent.version 8.15.2 data_stream.dataset endpoint.alerts data_stream.namespace default data_stream.type logs ecs.version 8.10...
<input checked="" type="checkbox"/>	Oct 8, 2024 @ 18:28:24.784	file.hash.sha256 d73b4f56fc3cfdc38a9edc71744609285203dcc8548ee8c0bcc7bc19c0e4c0b5 @timestamp Oct 8, 2024 @ 18:28:24.784 agent.build.original version: 8.15.2, compiled: Tue Sep 17 23:00:00 2024, branch: HEAD, commit: b4d81a7079c66492513f98f541621f2ec028a46d agent.id 9d57128e-764e-4132-b1ca-5f298af6079e agent.type endpoint agent.version 8.15.2 data_stream.dataset endpoint.alerts data_stream.namespace default data_stream.type logs ecs.version 8.10 elastic.agent.id 9d57128e-764e-4132-b1ca-5f298af6079e...

FIGURE 14 PROCESS LOGS

Recommended Rule Configurations

Based on our testing, we developed a set of baseline rules that provide optimal detection capabilities while minimizing false positives:

```
rule_id: malware_detection_001
description: "Detect potential malware execution"
risk_score: 75
severity: "high"
type: "eq1"
query: '''
process where event.type == "creation" and
  (process.name : ("suspicious.exe", "*.tmp") or
   process.command_line : ("*powershell*encode*", "*certutil*decode*"))
'''
```

This comprehensive testing approach ensures our detection capabilities remain robust and effective against current malware threats while maintaining operational efficiency.

User Awareness Training: Bridging the Technical Gap

In the second part of our project, we shifted our focus from technical implementations to what is often considered the most vulnerable link in any security chain: the human element. Our user awareness training program was designed to empower non-technical staff with practical cybersecurity knowledge and skills.

Training Objectives

The primary goals of our awareness program were to:

- ease cybersecurity concepts for non-technical personnel
- Provide practical, actionable guidance for daily security practices
- Enable staff to recognize and respond to common cyber threats
- Foster a security-conscious organizational culture

Key Training Components

1. Understanding Cyber Threats

- Introduction to common cyber threats in plain language
- Real-world examples and case studies

- Impact of security breaches on organizations and individuals
- Cost implications of security incidents

2. Phishing Attack Awareness

- Identifying suspicious emails and messages
- Common phishing tactics and red flags
 1. Urgency in messaging
 2. Unusual sender addresses
 3. Grammar and spelling errors
 4. Suspicious attachments
 5. Unusual requests for personal information

3. Malware Prevention for Non-Technical Users

- Basic understanding of malware types and their impacts
- Safe browsing practices
- File download guidelines
- Importance of software updates

Training Delivery Methods

To ensure maximum engagement and retention, we employed a multi-faceted approach:

- Interactive presentations with real-world examples
- Hands-on workshops with simulated scenarios
- Q&A sessions addressing specific concerns
- Take-home reference materials
- Quick-reference guides for common security situations

Practical Guidelines Provided

We developed and distributed easy-to-follow guidelines for:

- Password management best practices
- Safe email handling procedures
- Secure remote work protocols
- Data protection measures
- Incident reporting procedures

Key Takeaways for Participants

Security Best Practices:

- Regular password updates using strong combinations
- Two-factor authentication importance
- Clean desk policy
- Screen locking when away

Response Procedures:

- Steps to take when encountering suspicious emails
- Protocol for potential malware incidents
- Proper channels for reporting security concerns
- Emergency contact information

Training Impact Assessment

To measure the effectiveness of our training program, we:

- Conducted pre- and post-training surveys
- Implemented simulated phishing tests
- Tracked security incident reporting rates
- Gathered feedback for future improvements

This comprehensive approach to user awareness training has significantly strengthened our organization's security posture by empowering non-technical staff with the knowledge and confidence to play their part in our collective cybersecurity efforts.