ENTERPRISE SOC DEPLOYMENT & THREAT DETECTION LAB

Security Operations Portfolio Project

Author: Joshua Blankenship

Date: December 1, 2025

Environment: VMware Workstation / Wazuh SIEM / Windows 11 / Kali Linux

1. Project Scope & Topology

Overview

This project involved the design, deployment, and validation of a virtualized Security Operations Center (SOC). The objective was to emulate an enterprise network environment to generate real-world attack telemetry and configure a SIEM (Wazuh) for threat detection.

Network Configuration

The lab operates on a **NAT Network** topology hosted on VMware Workstation, isolating malicious traffic from the host LAN while allowing internal communication between the attacker and victim nodes.

Infrastructure Components

- **Security Information & Event Management (SIEM):**
  - **OS:** Amazon Linux 2023 (Wazuh OVA)
  - **Software:** Wazuh Manager v4.14.1
  - **IP Address:** 192.168.245.129
- **Victim Endpoint:**
  - **OS:** Windows 11 Enterprise (Evaluation Build)
  - **IP Address:** 192.168.245.130
  - **Defensive Tools:** Windows Defender, Wazuh Agent, Windows Audit Policies
- **Adversary Node:**
  - **OS:** Kali Linux 2025.3
  - **IP Address:** DHCP Assigned
  - **Offensive Tools:** Hydra, Nmap, Smbclient

2. Executive Summary

Objective

To validate the detection capabilities of the Wazuh SIEM against common adversarial tactics, including Credential Access (T1110), Persistence (T1136), and Defense Evasion (T1562).

Key Achievements

- **Infrastructure:** Successfully deployed a functional SIEM pipeline ingesting logs from Windows Event Channels (Security, System, Application).
- **Detection Engineering:** Authored and verified detection logic for SMB Brute Force attacks (Event ID 4625) and Local Account Manipulation (Event ID 4720).
- **Malware Analysis:** Integrated Windows Defender operational logs into Wazuh to capture and alert on EICAR test file signatures.
- **Visibility:** Reduced logging blind spots by configuring advanced Audit Policies and disabling NLA (Network Level Authentication) to ensure authentication attempts are properly captured by Windows Security Event logs.
- **Defensive Hardening:** Validated security controls by configuring an Account Lockout Policy that successfully terminated the brute force attack after 5 failed attempts (Event ID 4740).

3. Infrastructure Deployment & Configuration

Virtualization Setup

The environment was hosted on **VMware Workstation**, utilizing a shared NAT network adapter to simulate a corporate intranet. This configuration allowed the Wazuh Manager (192.168.245.129) to communicate bidirectionally with the Windows 11 endpoint (192.168.245.130).

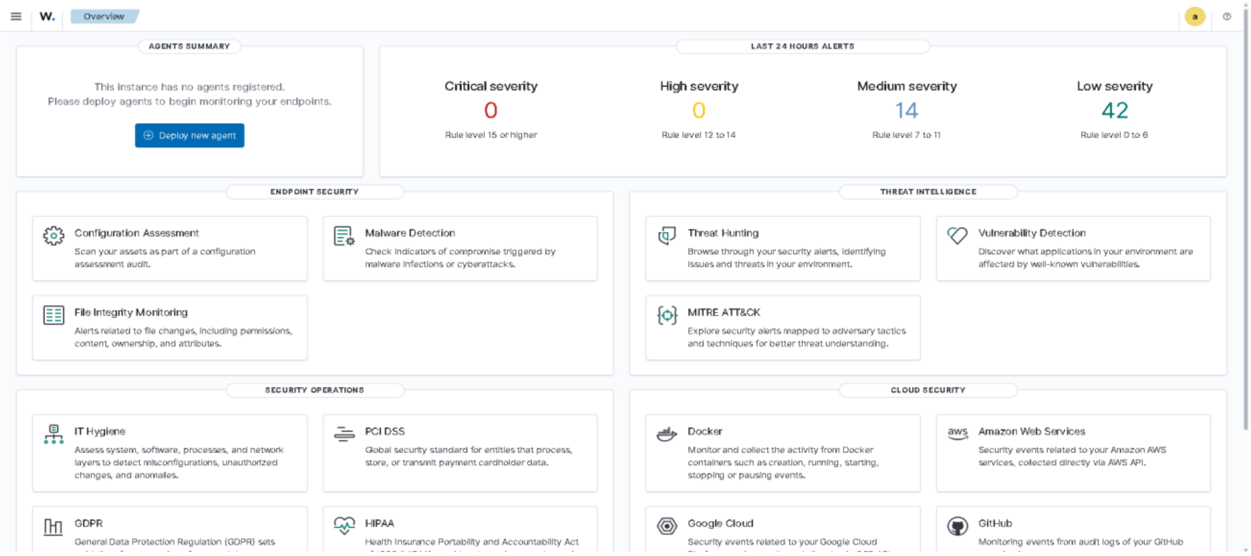
Agent Deployment

The **Wazuh Agent** was deployed on the Windows 11 victim machine using the MSI installer. The agent was configured to forward security telemetry (Event Logs) to the Wazuh Manager over port 1514/TCP.

Verification

Post-deployment verification confirmed the agent successfully registered with the Manager, reporting an "Active" status and providing baseline system inventory data.

Figure 1: Wazuh SIEM Dashboard Initial Setup



AGENTS SUMMARY

This instance has no agents registered.
Please deploy agents to begin monitoring your endpoints.

Deploy new agent

LAST 24 HOURS ALERTS

Critical severity	High severity	Medium severity	Low severity
0	0	14	42
Rule level 15 or higher	Rule level 12 to 14	Rule level 7 to 11	Rule level 0 to 6

ENDPOINT SECURITY

Configuration Assessment
Scan your assets as part of a configuration assessment audit.

Malware Detection
Check indicators of compromise triggered by malware infections or cyberattacks.

File Integrity Monitoring
Alerts related to file changes, including permissions, content, ownership, and attributes.

THREAT INTELLIGENCE

Threat Hunting
Browse through your security alerts, identifying issues and threats in your environment.

Vulnerability Detection
Discover what applications in your environment are affected by well-known vulnerabilities.

MITRE ATT&CK
Explore security alerts mapped to adversary tactics and techniques for better threat understanding.

SECURITY OPERATIONS

IT Hygiene
Assess system, software, processes, and network layers to detect misconfigurations, unauthorized changes, and anomalies.

PCI DSS
Global security standard for entities that process, store, or transmit payment cardholder data.

GDPR
General Data Protection Regulation (GDPR) sets

HIPAA
Health Insurance Portability and Accountability Act

CLOUD SECURITY

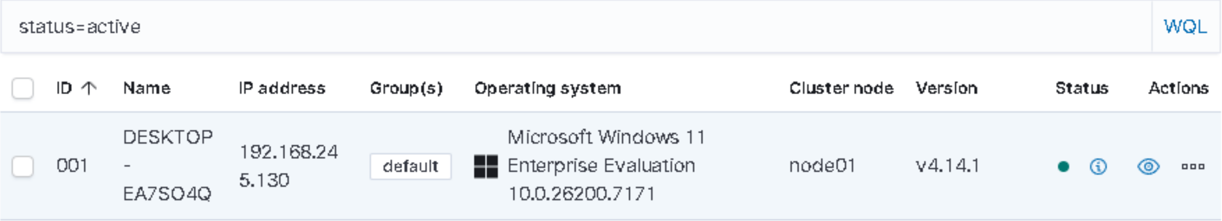
Docker
Monitor and collect the activity from Docker containers such as creation, running, starting, stopping or pausing events.

Amazon Web Services
Security events related to your Amazon AWS services, collected directly via AWS API.

Google Cloud
Security events related to your Google Cloud

GitHub
Monitoring events from audit logs of your GitHub

Figure 2: Windows Endpoint Successfully Onboarded



status=active

□	ID ↑	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
□	001	DESKTOP - EA7SO4Q	192.168.24 5.130	default	Microsoft Windows 11 Enterprise Evaluation 10.0.26200.7171	node01	v4.14.1	●	

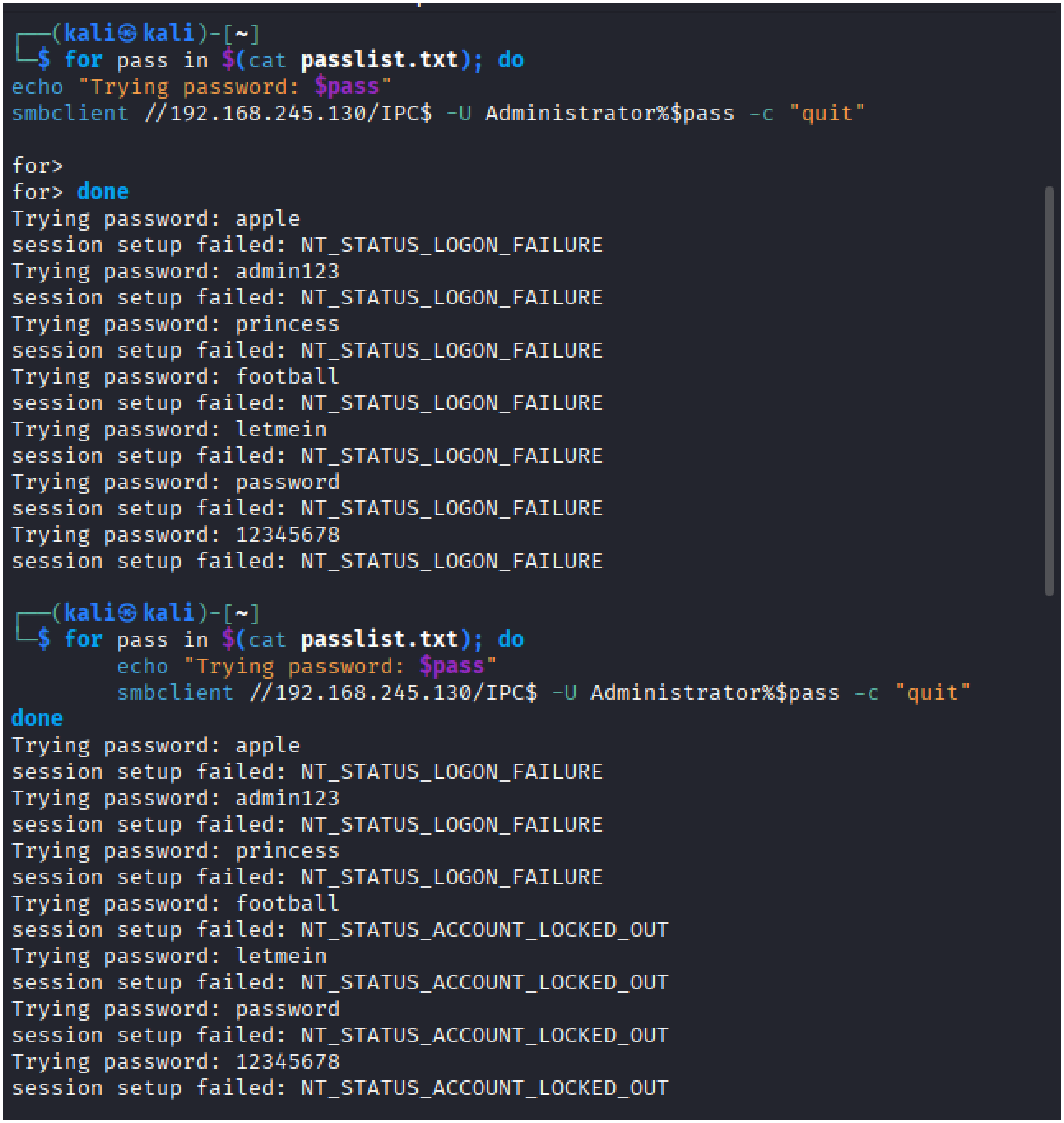
4. Threat Emulation & Adversary Tactics

Scenario A: Network Propagation via SMB Brute Force

To simulate an attacker attempting lateral movement, we executed a dictionary attack against the SMB (Server Message Block) protocol on Port 445.

- **Technique:** MITRE ATT&CK T1110.001 (Password Guessing)
- **Tool:** smbclient (Kali Linux)
- **Command:** Bash script iteration of passlist.txt against the IPC$ share.
- **Outcome:** The attack initially generated "Logon Failure" events (Event ID 4625). After the 5th failed attempt, the configured Audit Policy successfully triggered, locking the "Administrator" account and halting the attack (Event ID 4740). This is visible in **Figure 3** where the error message shifts to NT_STATUS_ACCOUNT_LOCKED_OUT.

Figure 3: Bash script iterating smbclient to execute SMB Brute Force attack



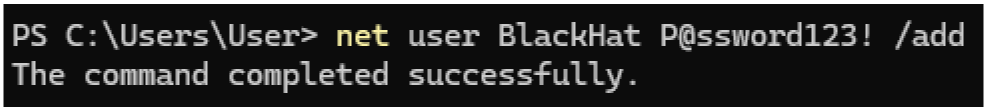
```
┌──(kali㉿kali)-[~]
└─$ for pass in $(cat passlist.txt); do
echo "Trying password: $pass"
smbclient //192.168.245.130/IPC$ -U Administrator%$pass -c "quit"

for>
for> done
Trying password: apple
session setup failed: NT_STATUS_LOGON_FAILURE
Trying password: admin123
session setup failed: NT_STATUS_LOGON_FAILURE
Trying password: princess
session setup failed: NT_STATUS_LOGON_FAILURE
Trying password: football
session setup failed: NT_STATUS_LOGON_FAILURE
Trying password: letmein
session setup failed: NT_STATUS_LOGON_FAILURE
Trying password: password
session setup failed: NT_STATUS_LOGON_FAILURE
Trying password: 12345678
session setup failed: NT_STATUS_LOGON_FAILURE

┌──(kali㉿kali)-[~]
└─$ for pass in $(cat passlist.txt); do
        echo "Trying password: $pass"
        smbclient //192.168.245.130/IPC$ -U Administrator%$pass -c "quit"
done
Trying password: apple
session setup failed: NT_STATUS_LOGON_FAILURE
Trying password: admin123
session setup failed: NT_STATUS_LOGON_FAILURE
Trying password: princess
session setup failed: NT_STATUS_LOGON_FAILURE
Trying password: football
session setup failed: NT_STATUS_ACCOUNT_LOCKED_OUT
Trying password: letmein
session setup failed: NT_STATUS_ACCOUNT_LOCKED_OUT
Trying password: password
session setup failed: NT_STATUS_ACCOUNT_LOCKED_OUT
Trying password: 12345678
session setup failed: NT_STATUS_ACCOUNT_LOCKED_OUT
```

Scenario B: Persistence via Local Account Creation

To simulate an attacker maintaining access after a reboot, we manually created a backdoor user account.

- **Technique:** MITRE ATT&CK T1136.001 (Create Account: Local Account)
- **Command:** net user BlackHat P@ssword123! /add
- **Outcome:** Triggered Windows Security Event ID 4720, providing high-fidelity evidence of unauthorized system modification.

Figure 4: Manual creation of unauthorized user account for persistence



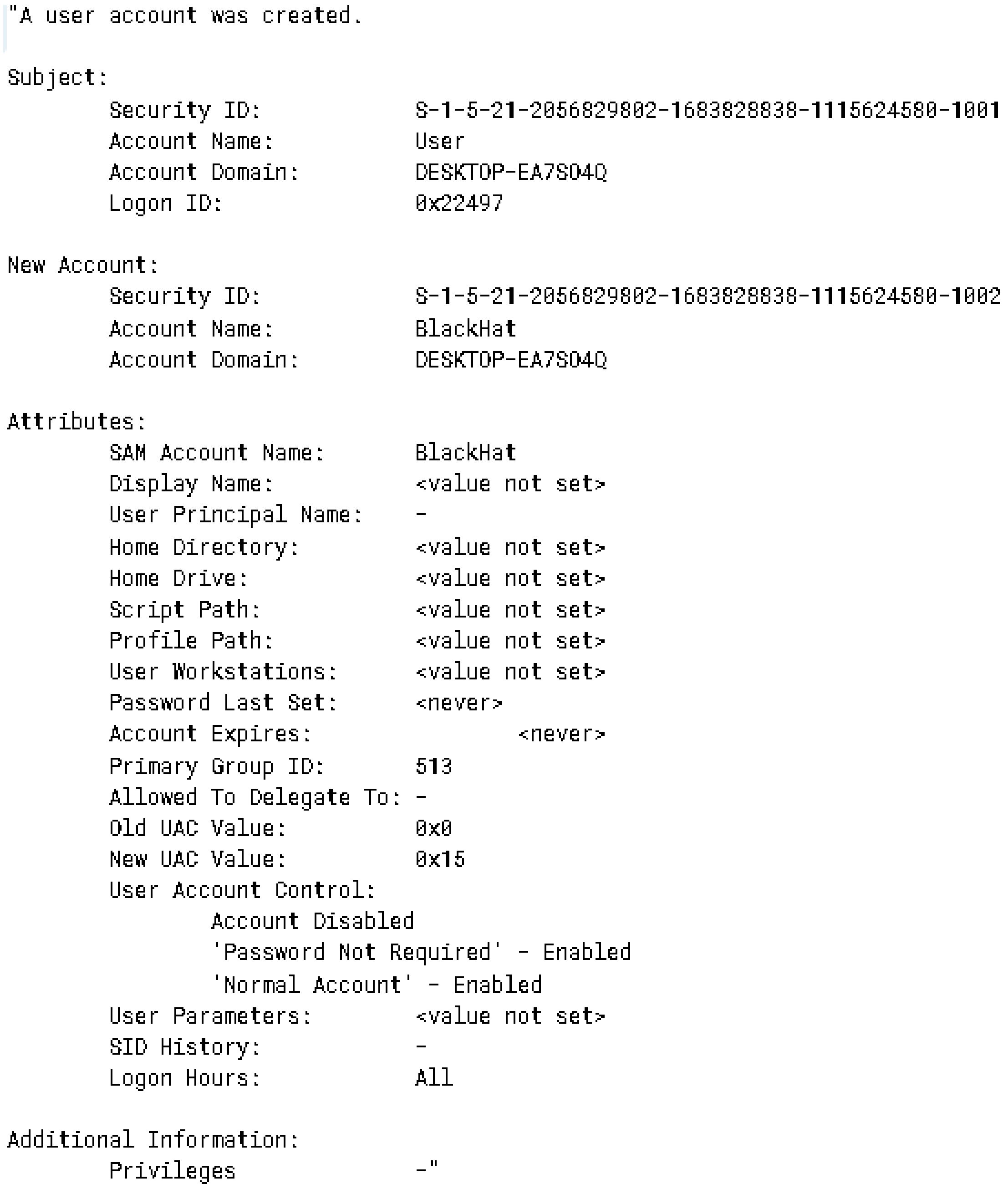
```
PS C:\Users\User> net user BlackHat P@ssword123! /add
The command completed successfully.
```

5. Detection & Analysis

The following evidence demonstrates Wazuh's ability to ingest, parse, and alert on the emulated threats.

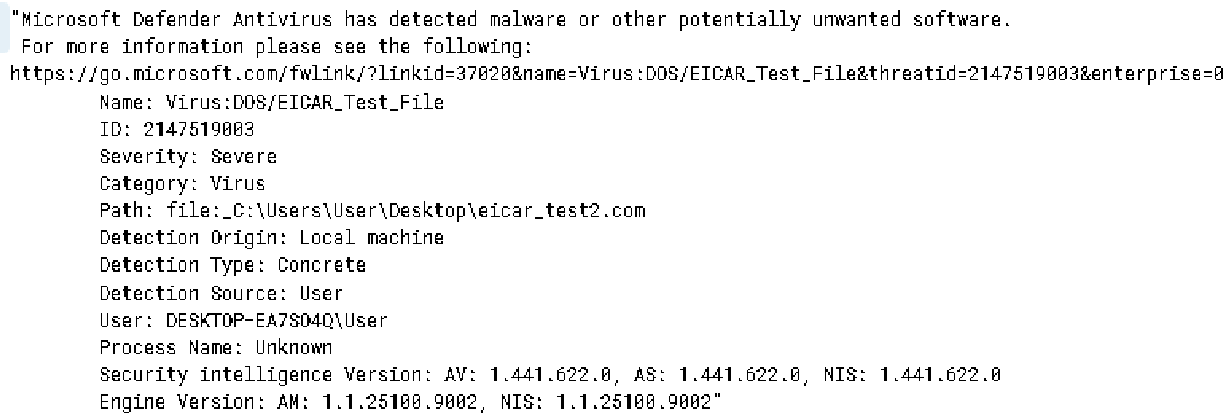
- **Figure 5:** Demonstrates detection of Persistence (User Creation) correlated with Rule ID 60109.
- **Figure 6:** Validates ingestion of Windows Defender logs detecting the EICAR malware sample.
- **Figure 7:** Confirms detection of the SMB Brute Force attack, identifying the source IP and the specific "Logon Failure" audit events.
- **Figure 8:** Confirms the active defense trigger, showing the "Account Lockout" alert (Event ID 4740) that halted the brute force attack.

Figure 5: Wazuh SIEM detecting unauthorized user creation (ID 4720)

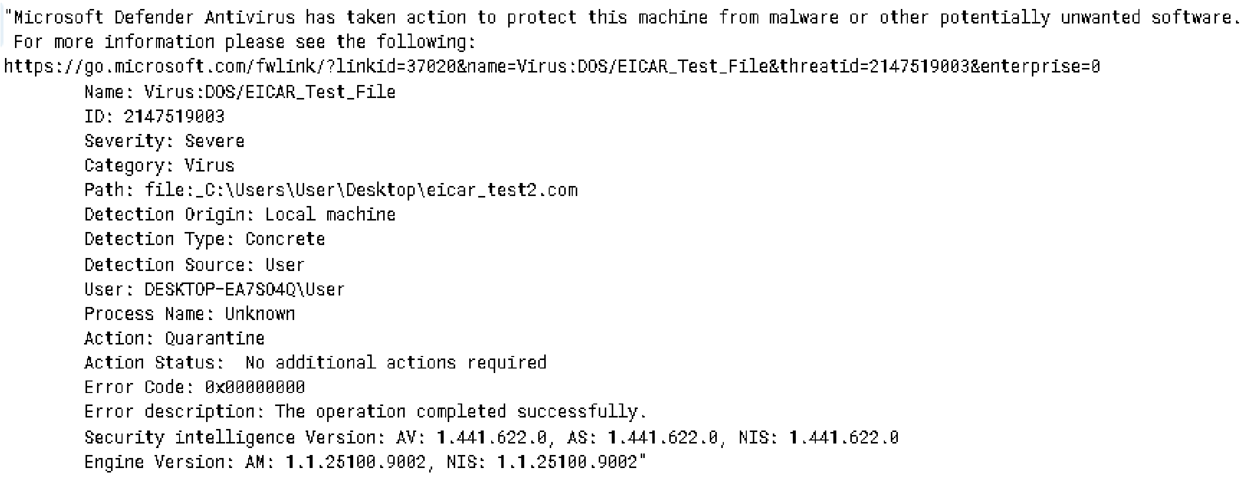


```
"A user account was created.

Subject:
        Security ID:            S-1-5-21-2056829802-1683828838-1115624580-1001
        Account Name:           User
        Account Domain:         DESKTOP-EA7SO4Q
        Logon ID:               0x22497

New Account:
        Security ID:            S-1-5-21-2056829802-1683828838-1115624580-1002
        Account Name:           BlackHat
        Account Domain:         DESKTOP-EA7SO4Q

Attributes:
        SAM Account Name:       BlackHat
        Display Name:           <value not set>
        User Principal Name:    -
        Home Directory:         <value not set>
        Home Drive:             <value not set>
        Script Path:            <value not set>
        Profile Path:           <value not set>
        User Workstations:      <value not set>
        Password Last Set:      <never>
        Account Expires:                <never>
        Primary Group ID:       513
        Allowed To Delegate To: -
        Old UAC Value:          0x0
        New UAC Value:          0x15
        User Account Control:
                Account Disabled
                'Password Not Required' - Enabled
                'Normal Account' - Enabled
        User Parameters:        <value not set>
        SID History:            -
        Logon Hours:            All

Additional Information:
        Privileges              -"
```

Figure 6: Wazuh SIEM successfully ingesting Windows Defender Malware Detection logs

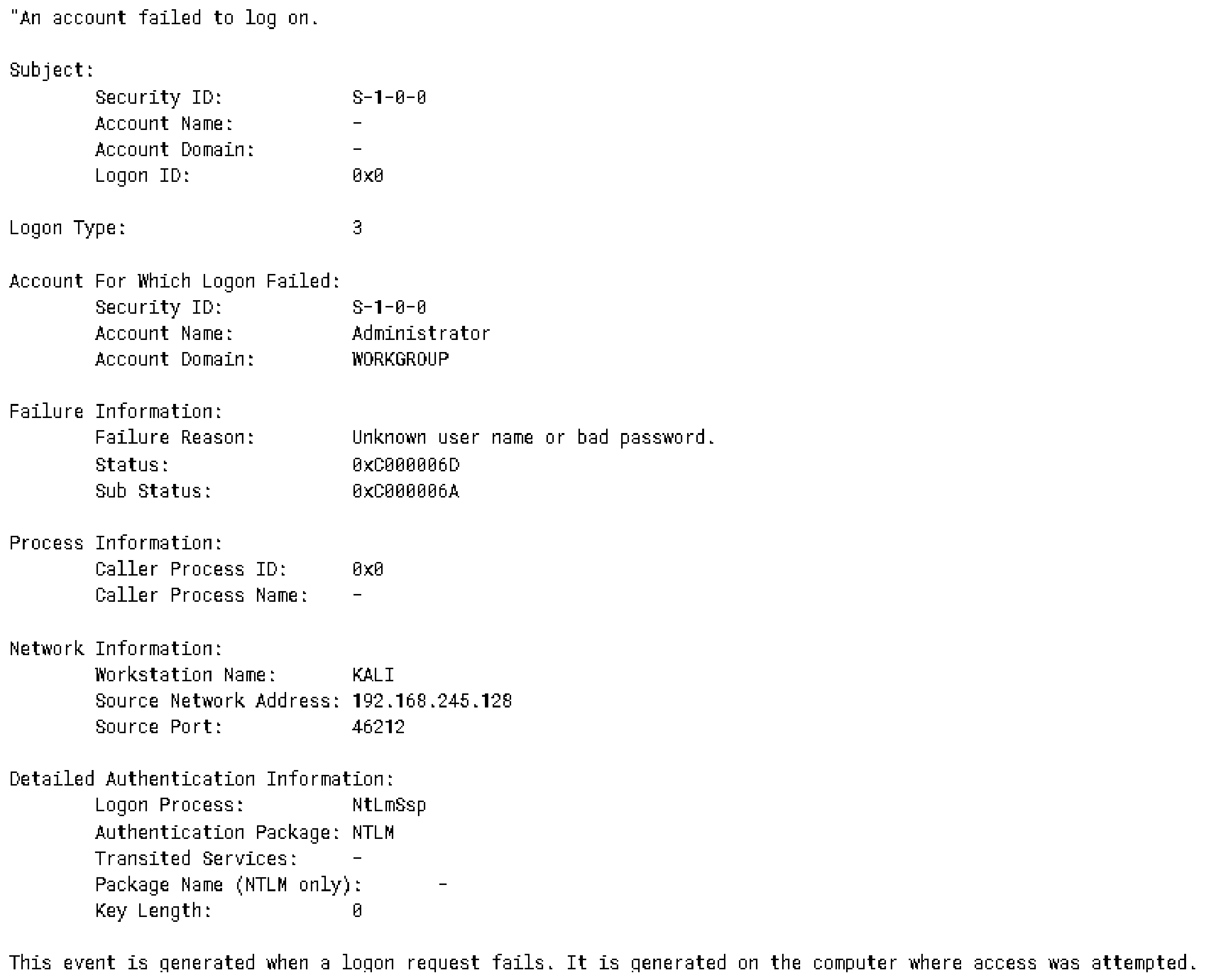


```
"Microsoft Defender Antivirus has detected malware or other potentially unwanted software.
 For more information please see the following:
https://go.microsoft.com/fwlink/?linkid=37020&name=Virus:DOS/EICAR_Test_File&threatid=2147519003&enterprise=0
 	Name: Virus:DOS/EICAR_Test_File
 	ID: 2147519003
 	Severity: Severe
 	Category: Virus
 	Path: file:_C:\Users\User\Desktop\eicar_test2.com
 	Detection Origin: Local machine
 	Detection Type: Concrete
 	Detection Source: User
 	User: DESKTOP-EA7SO4Q\User
 	Process Name: Unknown
 	Security intelligence Version: AV: 1.441.622.0, AS: 1.441.622.0, NIS: 1.441.622.0
 	Engine Version: AM: 1.1.25100.9002, NIS: 1.1.25100.9002"
```



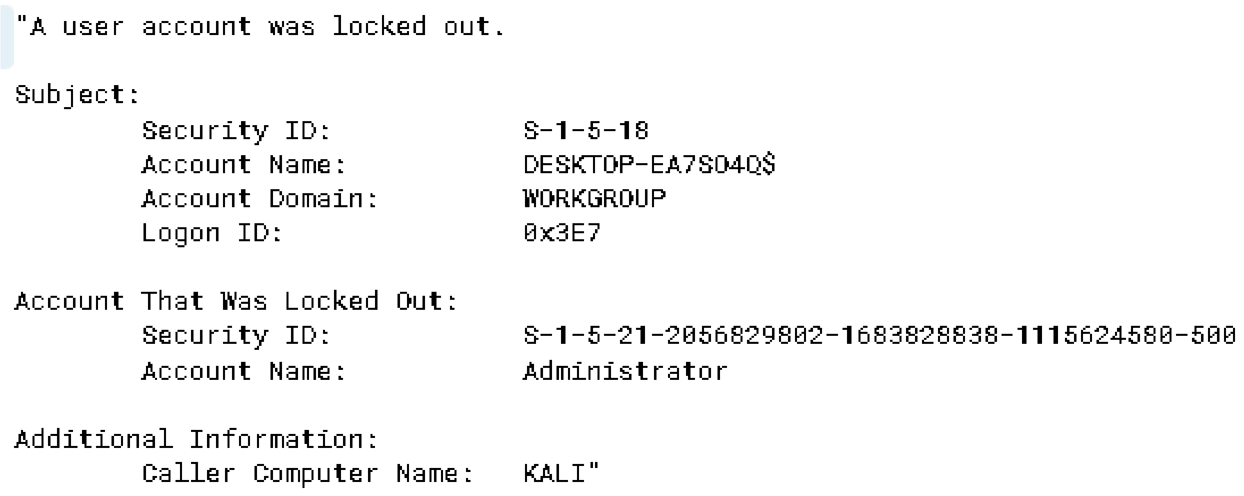
```
"Microsoft Defender Antivirus has taken action to protect this machine from malware or other potentially unwanted software.
 For more information please see the following:
https://go.microsoft.com/fwlink/?linkid=37020&name=Virus:DOS/EICAR_Test_File&threatid=2147519003&enterprise=0
 	Name: Virus:DOS/EICAR_Test_File
 	ID: 2147519003
 	Severity: Severe
 	Category: Virus
 	Path: file:_C:\Users\User\Desktop\eicar_test2.com
 	Detection Origin: Local machine
 	Detection Type: Concrete
 	Detection Source: User
 	User: DESKTOP-EA7SO4Q\User
 	Process Name: Unknown
 	Action: Quarantine
 	Action Status:  No additional actions required
 	Error Code: 0x00000000
 	Error description: The operation completed successfully.
 	Security intelligence Version: AV: 1.441.622.0, AS: 1.441.622.0, NIS: 1.441.622.0
 	Engine Version: AM: 1.1.25100.9002, NIS: 1.1.25100.9002"
```

Figure 7: Wazuh SIEM detecting SMB Brute Force attempts (Event ID 4625)



```
"An account failed to log on.

Subject:
        Security ID:            S-1-0-0
        Account Name:           -
        Account Domain:         -
        Logon ID:               0x0

Logon Type:                     3

Account For Which Logon Failed:
        Security ID:            S-1-0-0
        Account Name:           Administrator
        Account Domain:         WORKGROUP

Failure Information:
        Failure Reason:         Unknown user name or bad password.
        Status:                 0xC000006D
        Sub Status:             0xC000006A

Process Information:
        Caller Process ID:      0x0
        Caller Process Name:    -

Network Information:
        Workstation Name:       KALI
        Source Network Address: 192.168.245.128
        Source Port:            46212

Detailed Authentication Information:
        Logon Process:          NtLmSsp
        Authentication Package: NTLM
        Transited Services:     -
        Package Name (NTLM only):       -
        Key Length:             0

This event is generated when a logon request fails. It is generated on the computer where access was attempted.
```

Figure 8: Wazuh SIEM confirming the Account Lockout (Event ID 4740) defense trigger.



```
"A user account was locked out.

Subject:
        Security ID:            S-1-5-18
        Account Name:           DESKTOP-EA7SD4Q$
        Account Domain:         WORKGROUP
        Logon ID:               0x3E7

Account That Was Locked Out:
        Security ID:            S-1-5-21-2056829802-1683828838-1115624580-500
        Account Name:           Administrator

Additional Information:
        Caller Computer Name:   KALI"
```