

SOC Monitoring and Brute-Force Attack Detection — Practical Lab Report

NAME : YALALA HEMANTH KUMAR

1. Introduction

The purpose of this project was to design and implement a mini-Security Operations Center (SOC) capable of detecting malicious activity on a Windows endpoint. The lab focused on security monitoring, log management, threat detection, and incident response using open-source tools.

The main key areas covered were:

- SOC fundamentals and operations
- Security monitoring basics
- Log management and event analysis
- SIEM-based alerting and threat detection

2. SOC Fundamentals & Operations (Theoretical Overview)

A SOC is responsible for proactive threat detection, continuous monitoring, alert triage, and incident response.

Core roles within SOC include:

- Tier-1 Analyst: monitor alerts and escalate incidents
- Tier-2 Analyst: investigate and validate threats
- Tier-3 Analyst / Threat Hunter: advanced threat analysis
- SOC Manager: oversee operations and reporting

Frameworks used:

- NIST Incident Response Framework
- MITRE ATT&CK for threat classification

3. Lab Architecture

The lab contained the following components:

Component	Technology	Purpose
Windows VM	Windows 10	Endpoint & attack simulation
Endpoint Telemetry	Sysmon	Detailed OS-level security events
Log Shipping	Wazuh Agent	Secure log forwarding
SIEM Platform	Wazuh Manager + Indexer + Dashboard	Log analysis & alerts
Host for SIEM	Ubuntu Linux	Runs the Wazuh stack

Data Flow

Windows System → Sysmon → Wazuh Agent → Wazuh Server → SIEM Dashboard → Analyst Review

4. Practical Tasks Performed

4.1 Log Collection & Forwarding

- Installed Sysmon to capture process, authentication, registry, DNS, and network events.
- Installed Wazuh Agent on Windows and connected it to Wazuh Manager.
- Successfully forwarded Windows native logs + Sysmon logs to SIEM.

4.2 Security Monitoring

Security events monitored include:

- Failed authentication attempts (Event ID 4625)
- New service creation (Event ID 7045)
- Process execution & system activity via Sysmon

Dashboards were developed to visualize:

- Frequency of failed logins over time
- Top usernames targeted by failed login attempts

4.4 Detection & Alerting

Wazuh triggered an alert based on its built-in correlation rule:

Field	Value
Alert Type	Brute-Force Authentication Attempt
Trigger Logic	Multiple failed login attempts in short timeframe
Source	Windows Agent
MITRE ATT&CK	T1110 — Brute Force

5. Incident Report

Field	Content
Incident Type	Brute-Force Login Attempt
Date & Time	(Detected via Wazuh alert timestamp)
Host	Windows VM
Event Code	4625
Severity	High
Status	Investigated
Detection Platform	Wazuh SIEM
MITRE ATT&CK Technique ID	T1110 — Brute Force
Description	Wazuh detected repeated failed authentication attempts on a Windows VM, indicating a possible brute-force attack.
Analyst Action	Validated failed logon events and reviewed authenticity of login source. No unauthorized access occurred.
Recommendations	Enable MFA, configure account lockout policy, and continuously monitor failed logon attempts.

6. Learning Outcomes

Through this lab, the following skills were gained:

- Understanding SOC role and workflow (detection → triage → investigation → response)
- Installation and configuration of SIEM platform
- Sysmon-based endpoint telemetry analysis
- Log correlation and alerting
- MITRE ATT&CK-based classification of threats
- Documentation and reporting of incidents

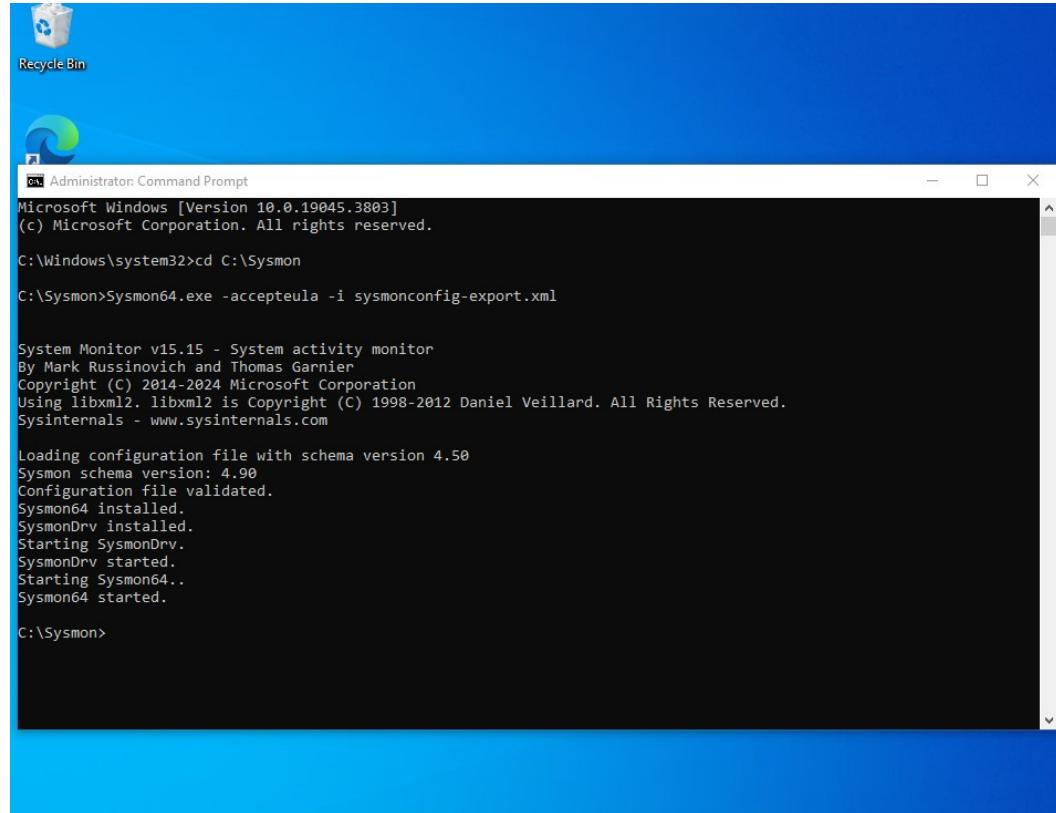
7. Conclusion

This project successfully demonstrated the deployment of a mini-SOC environment focused on Windows security monitoring and brute-force attack detection. Logs from the Windows endpoint were ingested into the SIEM where they were analyzed and correlated. A brute-force attack was detected automatically, and the incident was investigated and documented according to SOC procedures.

The implementation provides a strong foundation for future advanced SOC capabilities, including:

- File integrity monitoring
- PowerShell attack detection
- Malware behavior analytics
- Threat hunting and EDR integration

OUTPUT:



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.19045.3803]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd C:\Sysmon

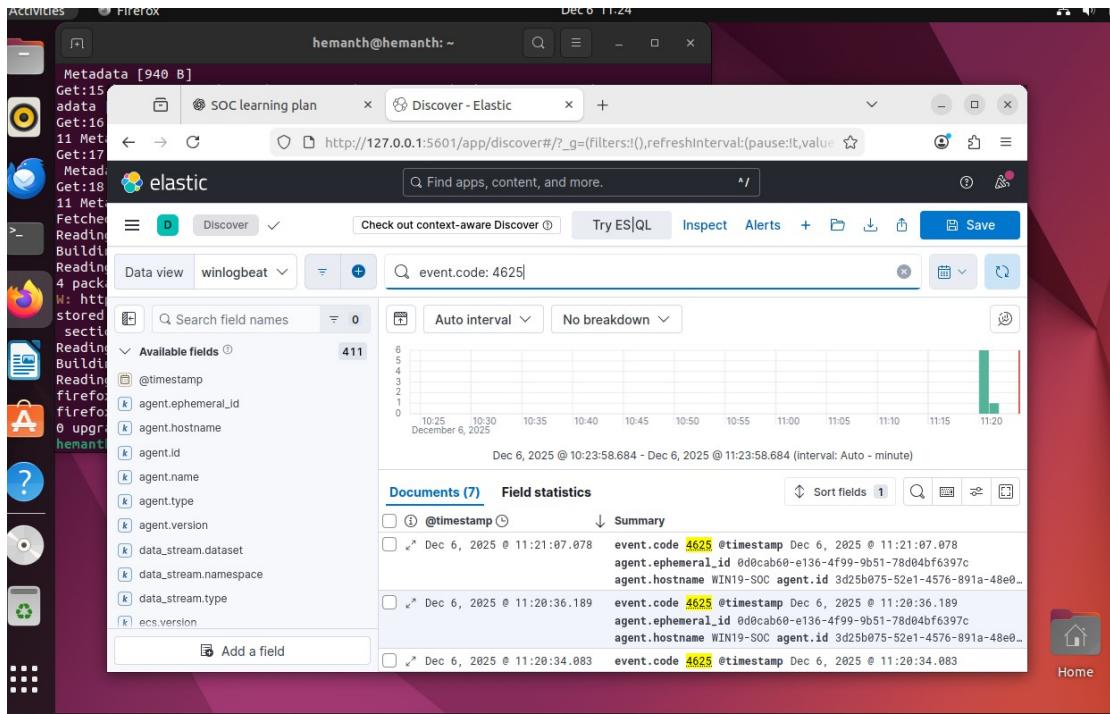
C:\Sysmon>Sysmon64.exe -accepteula -i sysmonconfig-export.xml

System Monitor v15.15 - System activity monitor
By Mark Russinovich and Thomas Garnier
Copyright (C) 2014-2024 Microsoft Corporation
Using libxml2. libxml2 is Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.
Sysinternals - www.sysinternals.com

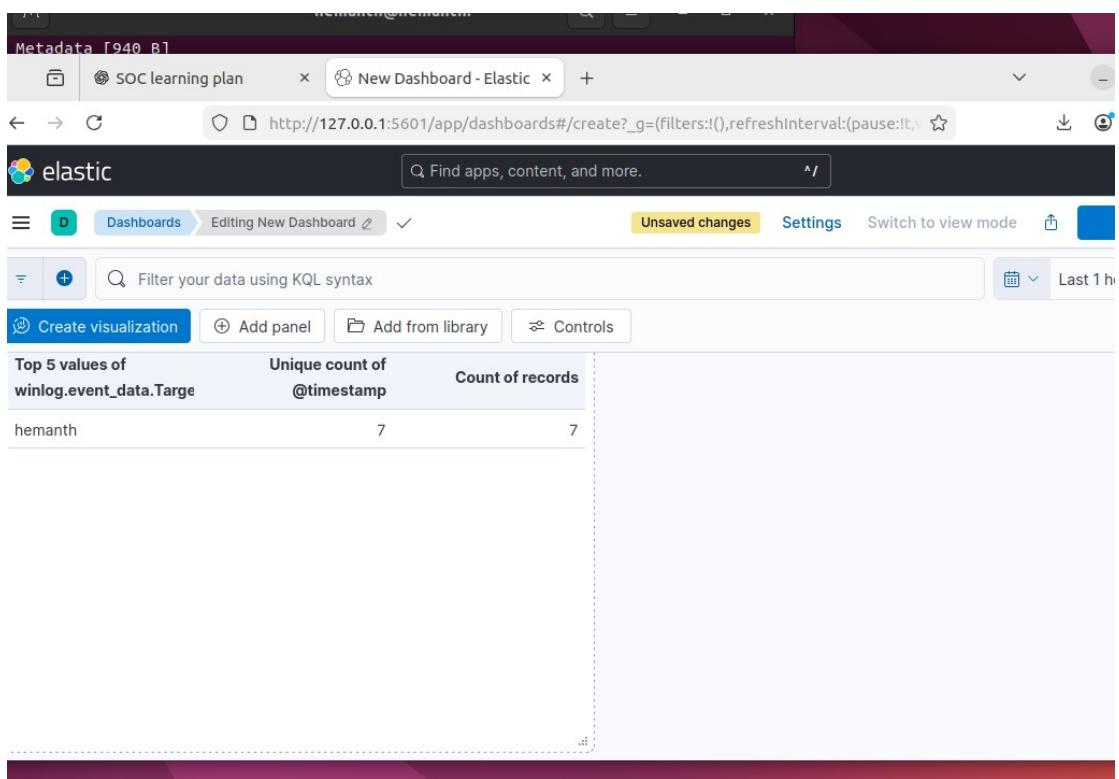
Loading configuration file with schema version 4.50
Sysmon schema version: 4.90
Configuration file validated.
Sysmon64 installed.
SysmonDrv installed.
Starting SysmonDrv.
SysmonDrv started.
Starting Sysmon64..
Sysmon64 started.

C:\Sysmon>
```

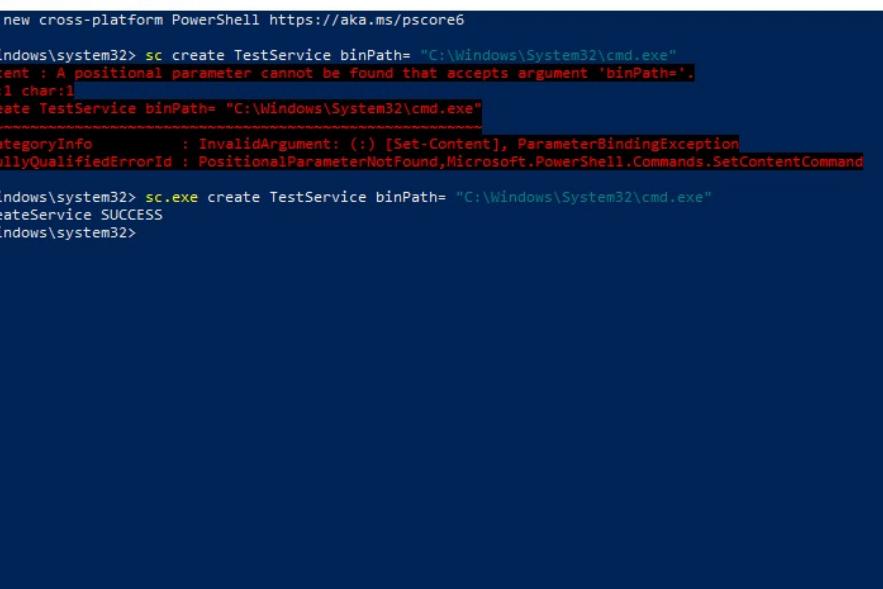
SYSMON INSTALLED AND CONFIGURED



SUCCESSFUL BRUTE FORCE ATTACK HAS ATTEMPTED



TABLES CREATED SUCESSFULLY FOR 4525 EVENT ID



The screenshot shows a Windows PowerShell window titled "Administrator: Windows PowerShell". The URL in the address bar is <https://chatgpt.com/c/692e7588...>. The PowerShell command being run is:

```
PS C:\Windows\system32> sc create TestService binPath= "C:\Windows\System32\cmd.exe"
```

An error message is displayed:

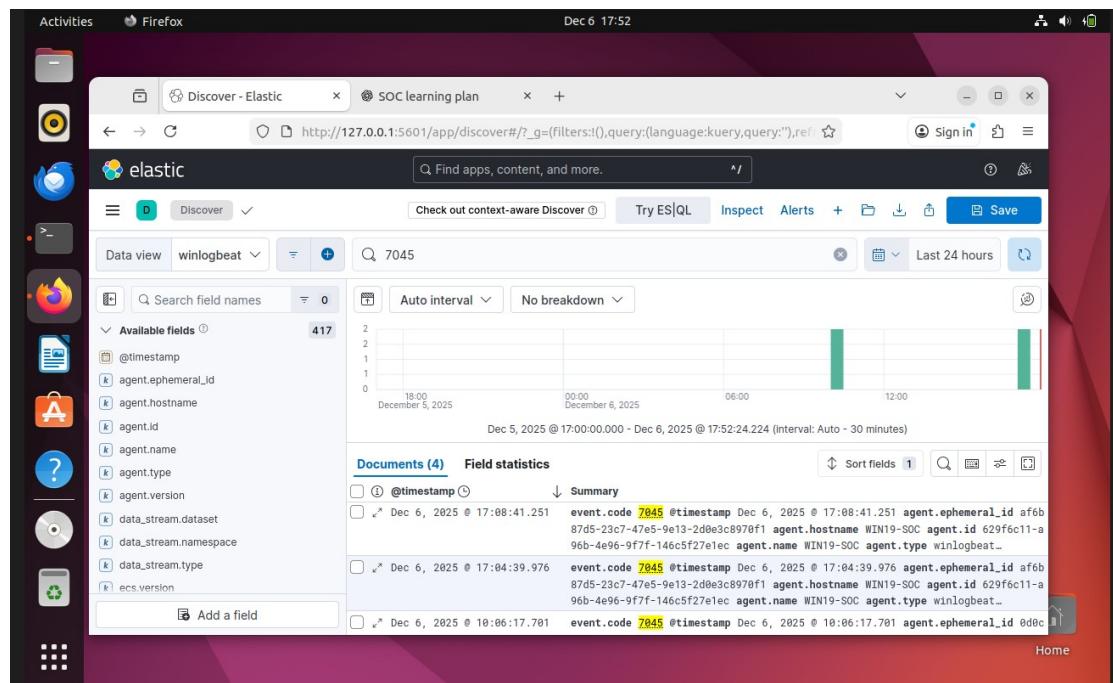
```
Set-Content : A positional parameter cannot be found that accepts argument 'binPath='.
```

Details of the error are shown:

```
At line:1 char:1
+ sc create TestService binPath= "C:\Windows\System32\cmd.exe"
+
+ CategoryInfo          : InvalidArgument: (:) [Set-Content], ParameterBindingException
+ FullyQualifiedErrorId : PositionalParameterNotFound,Microsoft.PowerShell.Commands.SetContentCommand
```

After the error, the command is run again using sc.exe:

```
PS C:\Windows\system32> sc.exe create TestService binPath= "C:\Windows\System32\cmd.exe"
[SC] CreateService SUCCESS
PS C:\Windows\system32>
```



SERVICE CREATED EVENT ID 7045

The screenshot shows the Wazuh Security Events interface in a Firefox browser window. The URL is 192.168.56.101/app/wazuh#/overview/?_g=(filters:(),refreshInterval:(pause:0,value:0)). The page displays two log entries:

Date	User	Host	Action	Details	Severity	ID	
Dec 6, 2025 @ 19:48:46.191	001	WIN10	T1078	Defense Evasion, Persistence, Privilege Escalation, Initial Access	Windows logon success.	3	60106
Dec 6, 2025 @ 19:48:32.421	001	WIN10			License activation (slui.exe) failed.	5	60646

A modal window is open, showing the details for the first log entry (ID 60106). The modal content includes:

Table	JSON	Rule
@timestamp	2025-12-06T14:18:32.421Z	
_id	hzUH9JoB23nEPT87W29D	
agent.id	001	
agent.ip	10.0.2.15	
agent.name	WIN10	
data.win.eventdata.data	hr=0x803F7001,RuleId=31e71c49-8da7-4a2f-ad92-45d98a1c79ba;Action=AutoActivate/AppId=55c92734-d682-4d71-983e-d6ec3f16059f;Skuid=2b1f36bb-c1cd-4306-bf5c-a0367c2d97d8;NotificationInterval=1440;Trigger=UserLogon;SessionId=2	
data.win.system.channel	Application	
data.win.system.computer	WIN19-SOC	

WAZUH INSTALLED

The screenshot shows the Wazuh Dashboard interface in a Firefox browser window. The URL is 192.168.56.101/app/wazuh#/overview/?_g=(filters:(),refreshInterval:(pause:0,value:0)). The dashboard displays the following information:

- Total Alerts:** 725
- Level 12 or above alerts:** 0
- Authentication failure:** 15
- Authentication success:** 30

A search bar at the top contains the query: https://192.168.56.101/app/wazuh#/overview/?_g=(filters:(),refreshInterval:(pause:0,value:0),time:(from:now-24h,to:now)), a_(columns:(_source),filters:(("\$state":("isImplicit",store:AppState),meta:(alias:in,disabled:!f,index:wazuh-alerts-*,"key:manager.name,negate:if,params:(query:hemanth),removable:f,type:phrase),query:(match:(manager.name:(query:hemanth,type:phrase))))),index:wazuh-alerts-*',interval:auto,query:(language:kury,query:""),sort:(),tab:general&tabView=panels)

Below the stats, there are two visualizations:

- Alert level evolution:** A line chart showing the count of alerts over time. The x-axis shows hours from 21:00 to 18:00. The y-axis shows the count from 0 to 500. A sharp peak is visible around 18:00, with values ranging from 7 to 10.
- Top MITRE ATT&CKs:** A donut chart showing the distribution of MITRE ATT&CK techniques. The categories and counts are:
 - Valid Accounts: 7
 - Account Access Re...: 3
 - Brute Force: 8
 - Create Account: 5
 - Disable or Modify T...: 10

AGENT IS INSTALLED IN WINDOWS(VM)

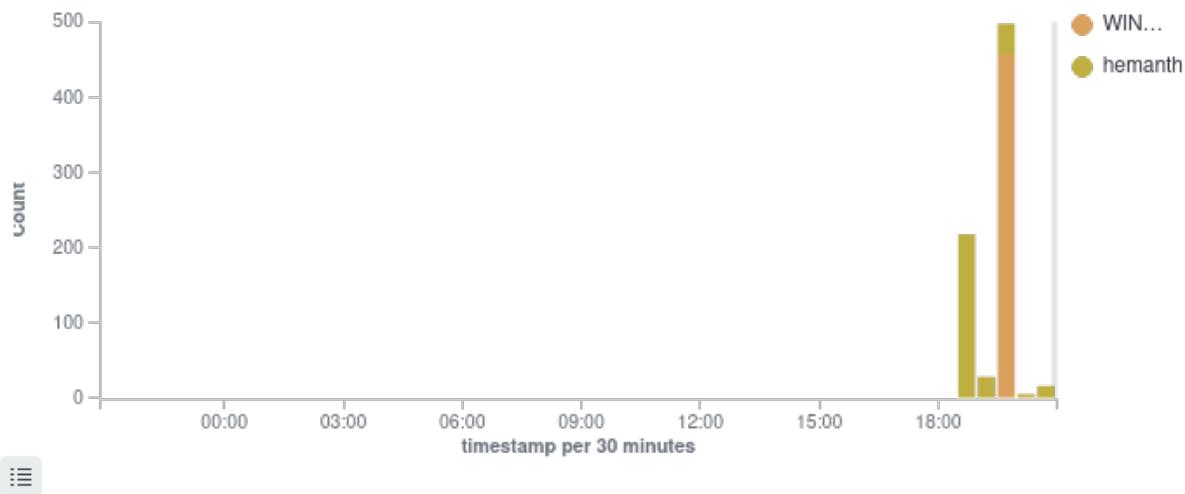
Security events report

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

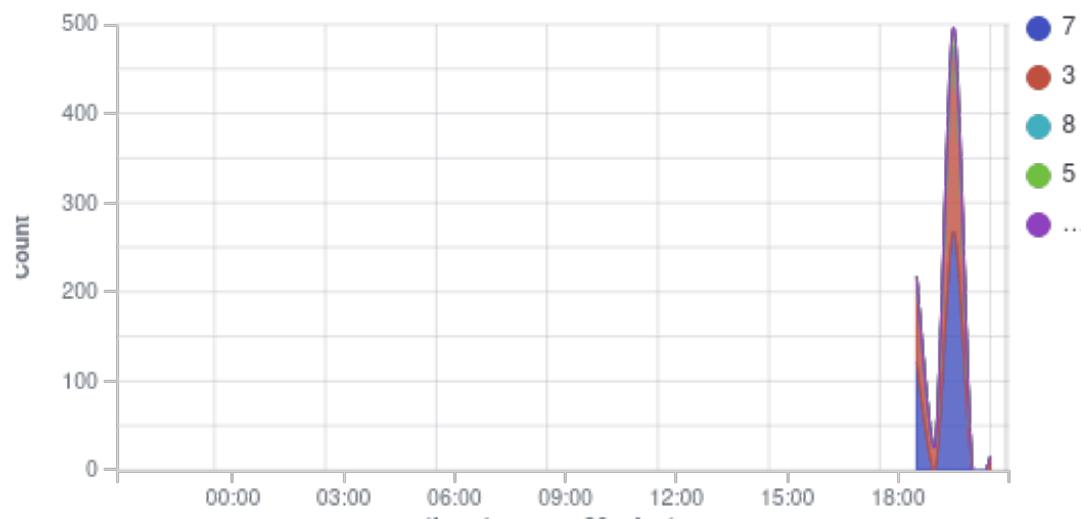
⌚ 2025-12-05T20:51:00 to 2025-12-06T20:51:00

🔍 manager.name: hemanth

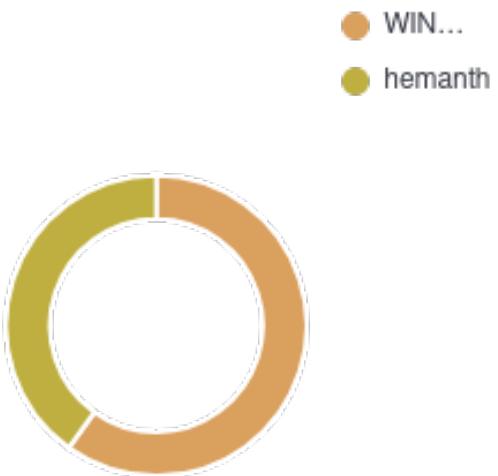
Alerts evolution Top 5 agents



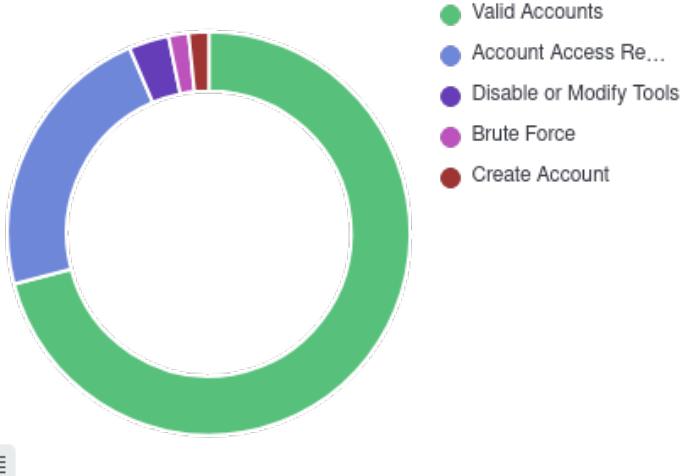
Alert level evolution



Top 5 agents



Alerts



Alerts summary

Rule ID	Description	Level	Count
52002	Apparmor DENIED	3	96
60106	Windows logon success.	3	21
60122	Logon failure - Unknown user or bad password.	5	14
60137	Windows User Logoff.	3	9
5501	PAM: Login session opened.	3	5
60775	SessionEnv was unavailable to handle a notification event.	5	4
2902	New dpkg (Debian Package) installed.	7	4
2904	Dpkg (Debian Package) half configured.	7	4
5502	PAM: Login session closed.	3	4
60118	Windows workstation logon success.	3	4
19008	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Allow Basic authentication' is set to 'Disabled'.	3	2
19008	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Allow unencrypted traffic' is set to 'Disabled'.	3	2
19004	SCA summary: CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Score less than 50% (32)	7	2
19004	SCA summary: CIS Ubuntu Linux 22.04 LTS Benchmark v1.0.0: Score less than 50% (40)	7	2
2901	New dpkg (Debian Package) requested to install.	3	2
510	Host-based anomaly detection event (rootcheck).	7	2
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Configure 'Accounts: Rename administrator account'.	7	1
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Configure 'Accounts: Rename guest account'.	7	1
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Configure 'Interactive logon: Message text for users attempting to log on'.	7	1
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Configure 'Interactive logon: Message title for users attempting to log on'.	7	1
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Disable IPv6 (Ensure TCPIP6 Parameter 'DisabledComponents' is set to '0xff (255)').	7	1
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Account lockout duration' is set to '15 or more minute(s)'.	7	1
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Account lockout threshold' is set to '5 or fewer invalid logon attempt(s), but not 0'.	7	1
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Accounts: Block Microsoft accounts' is set to 'Users can't add or log on with Microsoft accounts'.	7	1
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Allow Clipboard synchronization across devices' is set to 'Disabled'.	7	1
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Allow Cloud Search' is set to 'Enabled: Disable Cloud Search'.	7	1
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Allow Cortana above lock screen' is set to 'Disabled'.	7	1
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Allow Cortana' is set to 'Disabled'.	7	1
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Allow Diagnostic Data' is set to 'Enabled: Diagnostic data off (not recommended)' or 'Enabled: Send required diagnostic data'.	7	1
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Allow Message Service Cloud Sync' is set to 'Disabled'.	7	1
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Allow Microsoft accounts to be optional' is set to 'Disabled'.	7	1

Rule ID	Description	Level	Count
'Enabled'.			
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Allow Online Tips' is set to 'Disabled'.	7	1
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Allow Print Spooler to accept client connections' is set to 'Disabled'.	7	1
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Allow Remote Shell Access' is set to 'Disabled'.	7	1
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Allow UI Automation redirection' is set to 'Disabled'.	7	1
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Allow Use of Camera' is set to 'Disabled'.	7	1
19008	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Accounts: Administrator account status' is set to 'Disabled'.	3	1
19008	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Accounts: Guest account status' is set to 'Disabled'.	3	1
19008	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Accounts: Limit local account use of blank passwords to console logon only' is set to 'Enabled'.	3	1
19008	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Allow a Windows app to share application data between users' is set to 'Disabled'.	3	1
19008	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Allow indexing of encrypted files' is set to 'Disabled'.	3	1
19008	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Allow remote server management through WinRM' is set to 'Disabled'.	3	1
19008	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Allow user control over installs' is set to 'Disabled'.	3	1
19008	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Allow users to connect remotely by using Remote Desktop Services' is set to 'Disabled'.	3	1
19008	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Always install with elevated privileges' is set to 'Disabled'.	3	1
19008	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Application: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'.	3	1
19008	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Apply UAC restrictions to local accounts on network logons' is set to 'Enabled'.	3	1
19008	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Audit Audit Policy Change' is set to include 'Success'.	3	1
19008	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Audit Authentication Policy Change' is set to include 'Success'.	3	1
19008	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Audit Logoff' is set to include 'Success'.	3	1
19008	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Audit Logon' is set to 'Success and Failure'.	3	1
19008	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Audit Other System Events' is set to 'Success and Failure'.	3	1
19008	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Audit Security Group Management' is set to include 'Success'.	3	1
19008	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Audit Security State Change' is set to include 'Success'.	3	1
19009	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Configure Automatic Updates: Scheduled install day' is set to '0 - Every day'.	3	1
19009	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Download Mode' is NOT set to 'Enabled: Internet'.	3	1
19009	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Select when Quality Updates are received' is set to 'Enabled: 0 days'.	3	1
19009	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Support device authentication using certificate' is set to 'Enabled: Automatic'.	3	1

Rule ID	Description	Level	Count
19009	CIS Ubuntu Linux 22.04 LTS Benchmark v1.0.0: Ensure ntp access control is configured.	3	1
19009	CIS Ubuntu Linux 22.04 LTS Benchmark v1.0.0: Ensure only authorized groups are assigned ownership of audit log files.	3	1
60775	WSearch was unavailable to handle a notification event.	5	1
2501	syslog: User authentication failure.	5	1
501	New wazuh agent connected.	3	1
502	Wazuh server started.	3	1
503	Wazuh agent started.	3	1
504	Wazuh agent disconnected.	3	1
506	Wazuh agent stopped.	3	1
533	Listened ports status (netstat) changed (new port opened or closed).	7	1
5901	New group added to the system.	8	1
5902	New user added to the system.	8	1
60204	Multiple Windows logon failures.	10	1
60646	License activation (slui.exe) failed.	5	1
60776	SessionEnv was unavailable to handle a critical notification event.	7	1
61104	Service startup type was changed	3	1