**Report**

Title:

Malware Download and Incident Response Plan



**Name: Saad Naveed**

**Position SOC interenee**

**Task No 03**

**Team EPSILON**

**Riphah International University Islamabad I-1**

**Github:**

Table of Contents

[Objective: 3](#_Toc207495805)

[Step 1: 3](#_Toc207495806)

[Lab Environment Setup: 3](#_Toc207495807)

[Components used in the Lab: 3](#_Toc207495808)

[Topology Used: 3](#_Toc207495809)

[Network Topology Diagram: 3](#_Toc207495810)

[Download Malware 4](#_Toc207495811)

[Downloading Malware Sample (TheZoo) 4](#_Toc207495812)

[5](#_Toc207495813)

[5](#_Toc207495814)

[5](#_Toc207495815)

[Step 2: 5](#_Toc207495816)

[Detection and Observation 5](#_Toc207495817)

[pfSense Monitoring 5](#_Toc207495818)

[Wazuh Dashboard: 12](#_Toc207495819)

[Step 3: Log and Malware Analysis 13](#_Toc207495820)

[Log Details Collection 13](#_Toc207495821)

[Potential IOCs 14](#_Toc207495822)

[IOCs (Indicators of Compromise) 16](#_Toc207495823)

[IOAs (Indicators of Attack) 16](#_Toc207495824)

[IOAs Mapped to MITRE ATT&CK 16](#_Toc207495825)

[Step 4 17](#_Toc207495826)

[Incident Response Plan 17](#_Toc207495827)

[Incident Response Plan (NIST-Based) 17](#_Toc207495828)

[. Detection 17](#_Toc207495829)

[Analysis 18](#_Toc207495830)

[Containment 18](#_Toc207495831)

[Eradication 19](#_Toc207495832)

[Recovery 19](#_Toc207495833)

[Lessons Learned 19](#_Toc207495834)

# Objective:

Download a freely available malware via a VM with an active pfsense firewall, observe detection and log activites, analyze logs and malware, and create and incident respose plan.

# Step 1:

## Lab Environment Setup:

To perform this experiment, I created a virtual lab environment. The purpose of the lab was to safely analyze malware, detect it using Wazuh, and test the incident response process.

## Components used in the Lab:

* Pfsense Firewall (VM): Used as a network security gateway.
* Wazuh Manger (VM): Installed on Linux to collect logs and alerts.
* Windows 10 VM: Configured as the endpoint machine with Wazuh Agent installed.

## Topology Used:

The topology was created using VMware. All machines were connected through a NAT Network + Internal Network to allow monitoring through the firewall.

## Network Topology Diagram:

Internet

pfsense

Firewall

Wazuh Manager (Kali)

Window 10 VM with Agent

This diagram show clearly show how traffic flows >Internet > Firewall > Endpoint > Wazuh Manager.

## Download Malware

Download a freely available malware sample from a reputable site (e.g., theZoo, VirusShare).

For safety, I executed the malware inside a Windows virtual machine with Host-Only networking and pfSense firewall rules applied, ensuring it did not affect the host or external system.

## Downloading Malware Sample (TheZoo)

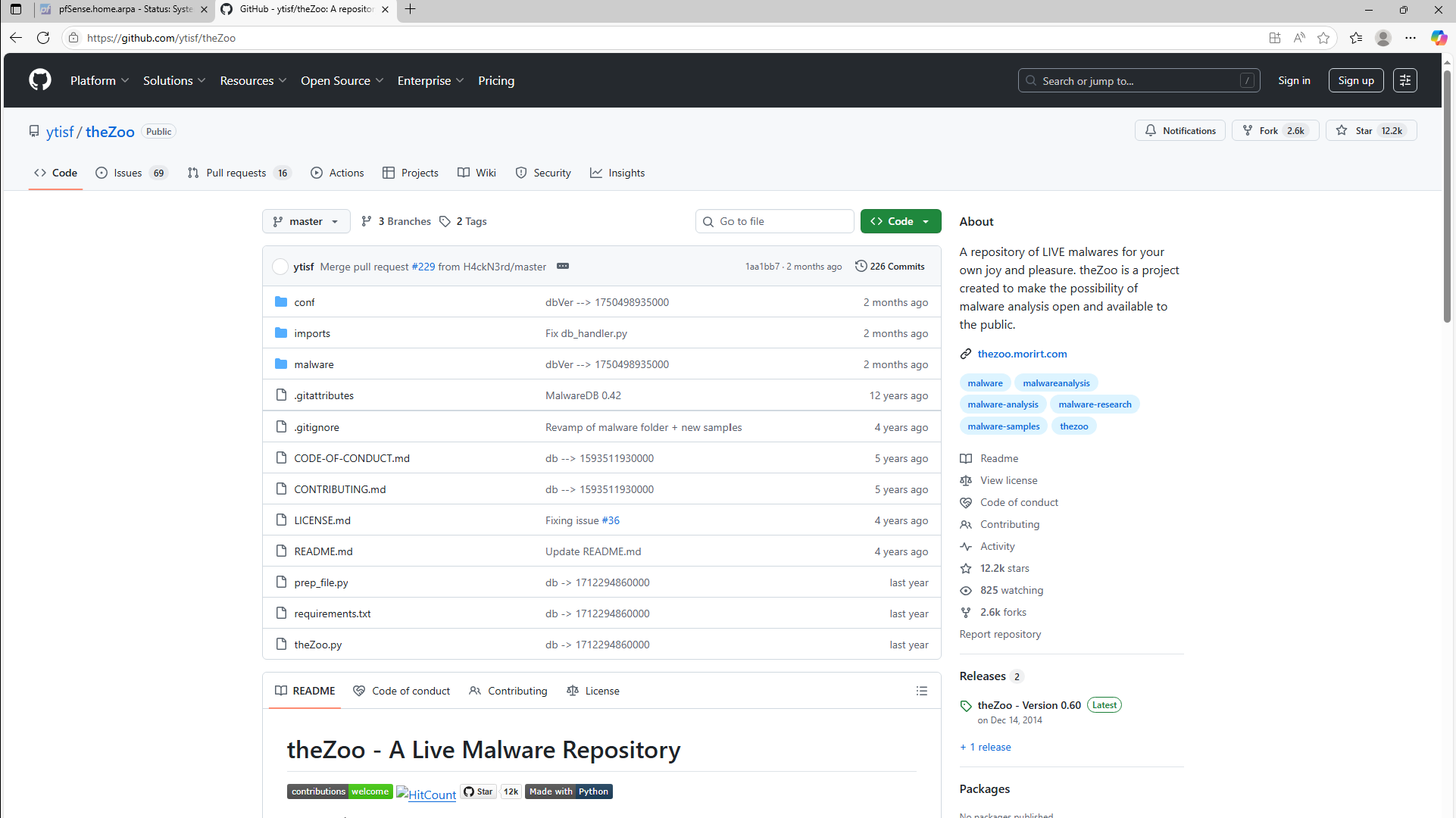
Defination

TheZoo is a project that provides live and source code samples of real-world malware (like viruses, worms, ransomware, Trojans, etc.) for researchers, penetration testers, and student to study how malware works.

**Step 1: Go to theZoo Github in Windows VM**

Open Brower Edge in my window machine.

Go to: <https://github.com/ytisf/theZoo>



**Step 2: Download ZIP**

On GitHub page > Click Code > Download ZIP.

Extract ZIP in Windows (Right click > Extract All)

# 

# 

# 

# Step 2:

## Detection and Observation

### pfSense Monitoring

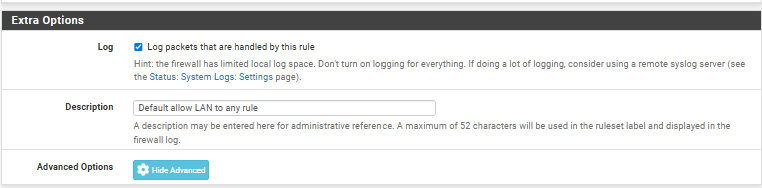
Enable logging.

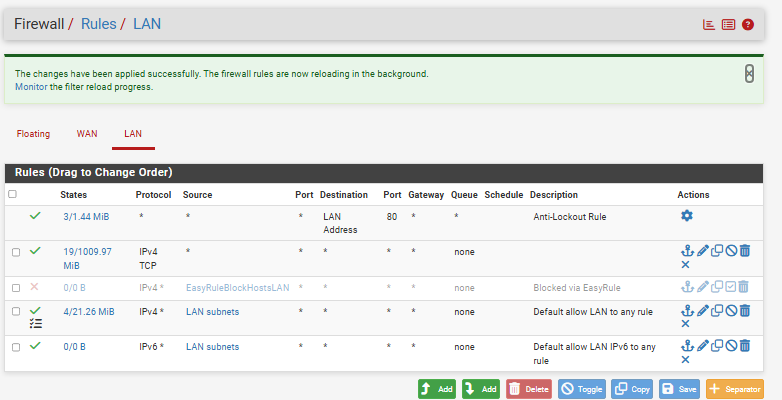
Go to firewall > Rules> LAN

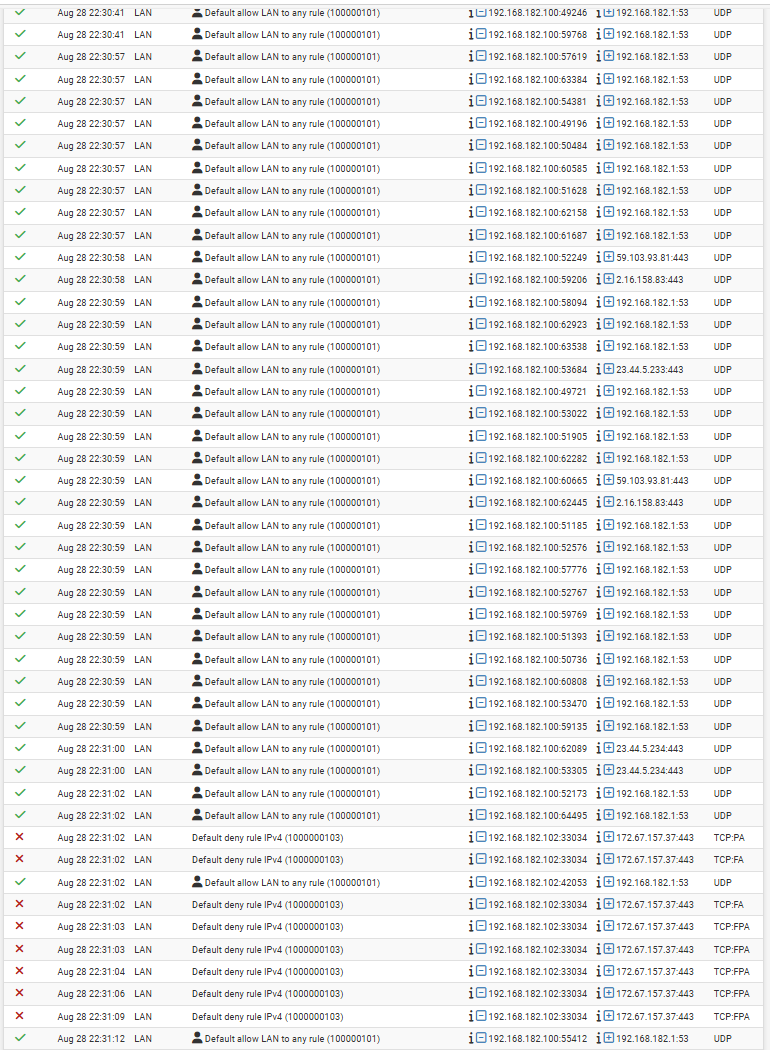
Edit ”default allow LAN to any rule”.

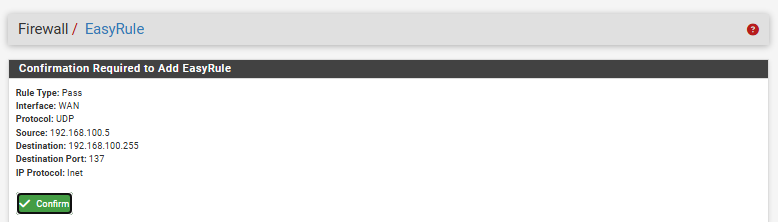
Scroll down > under Advanced Options > Log packets that are handle by this rule > Enable logging.

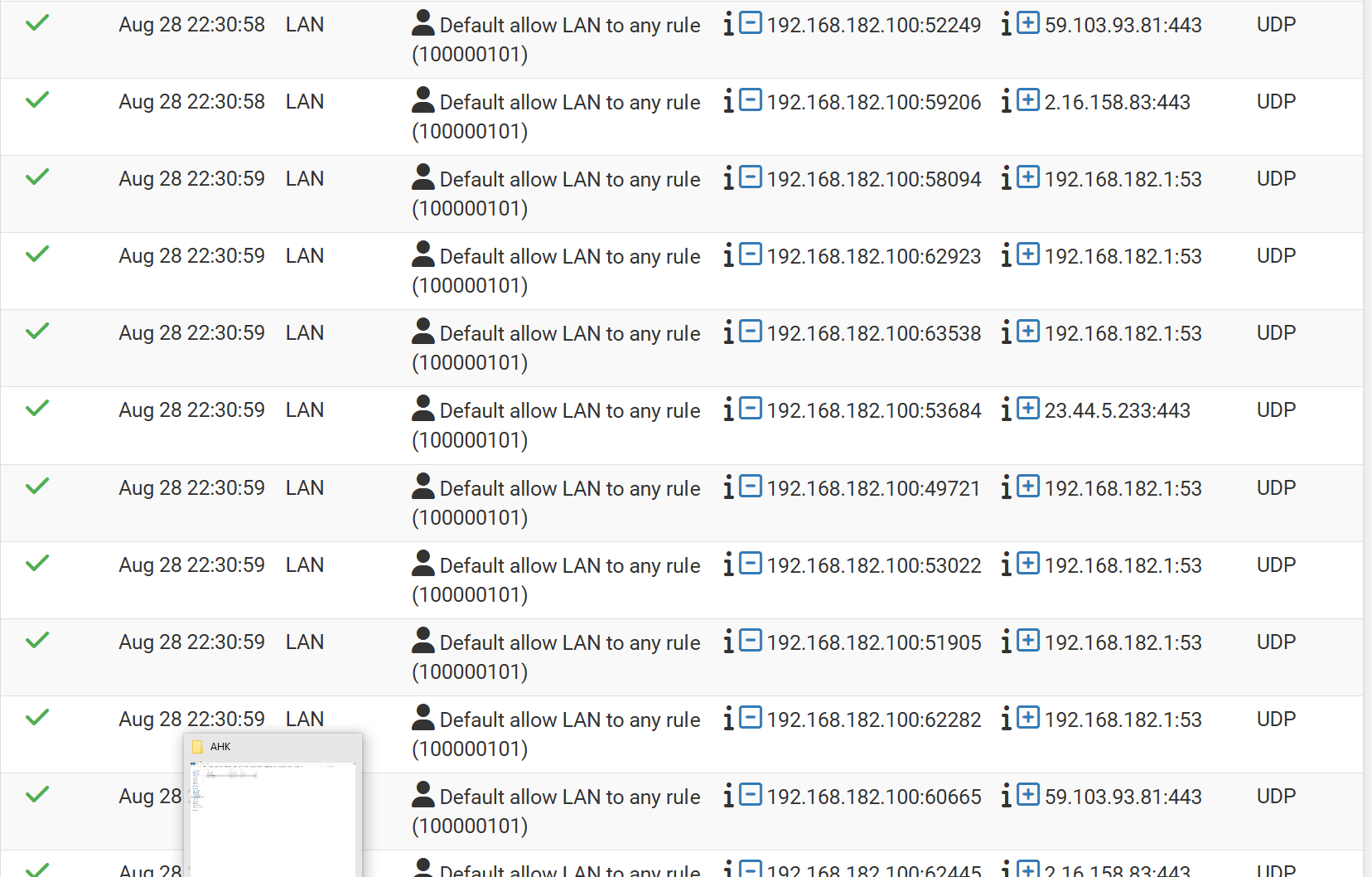
Save & Apply.

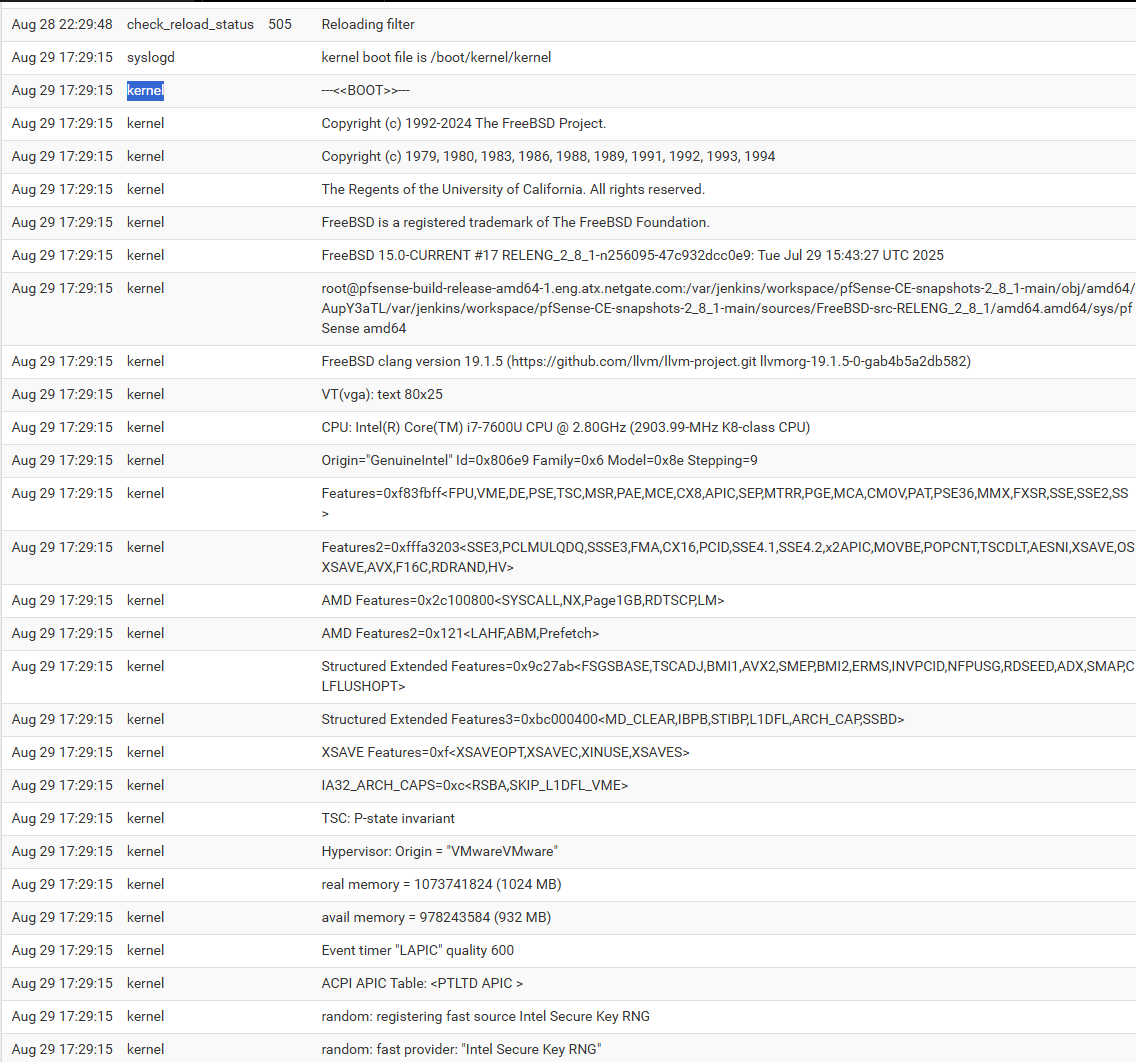


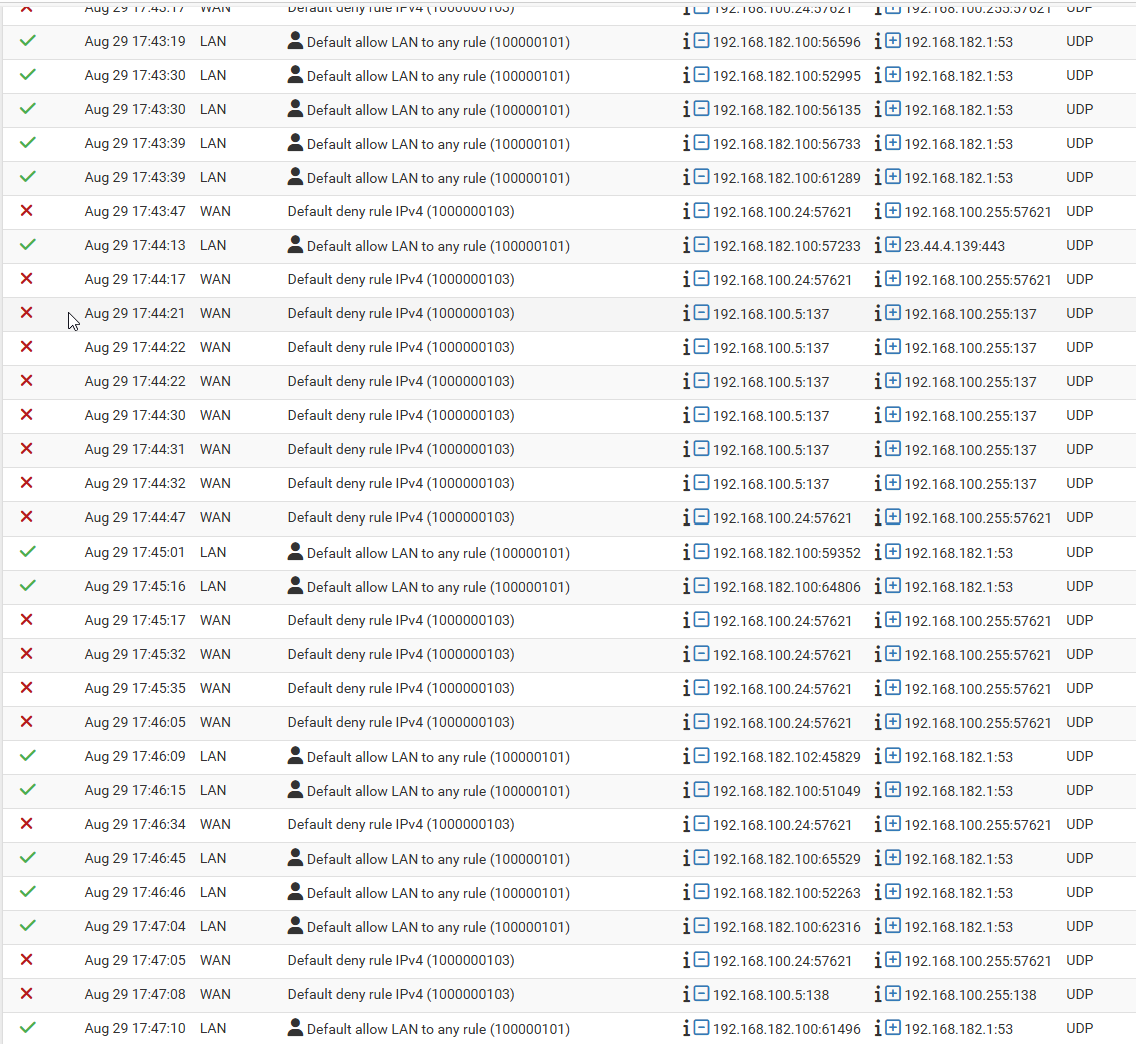


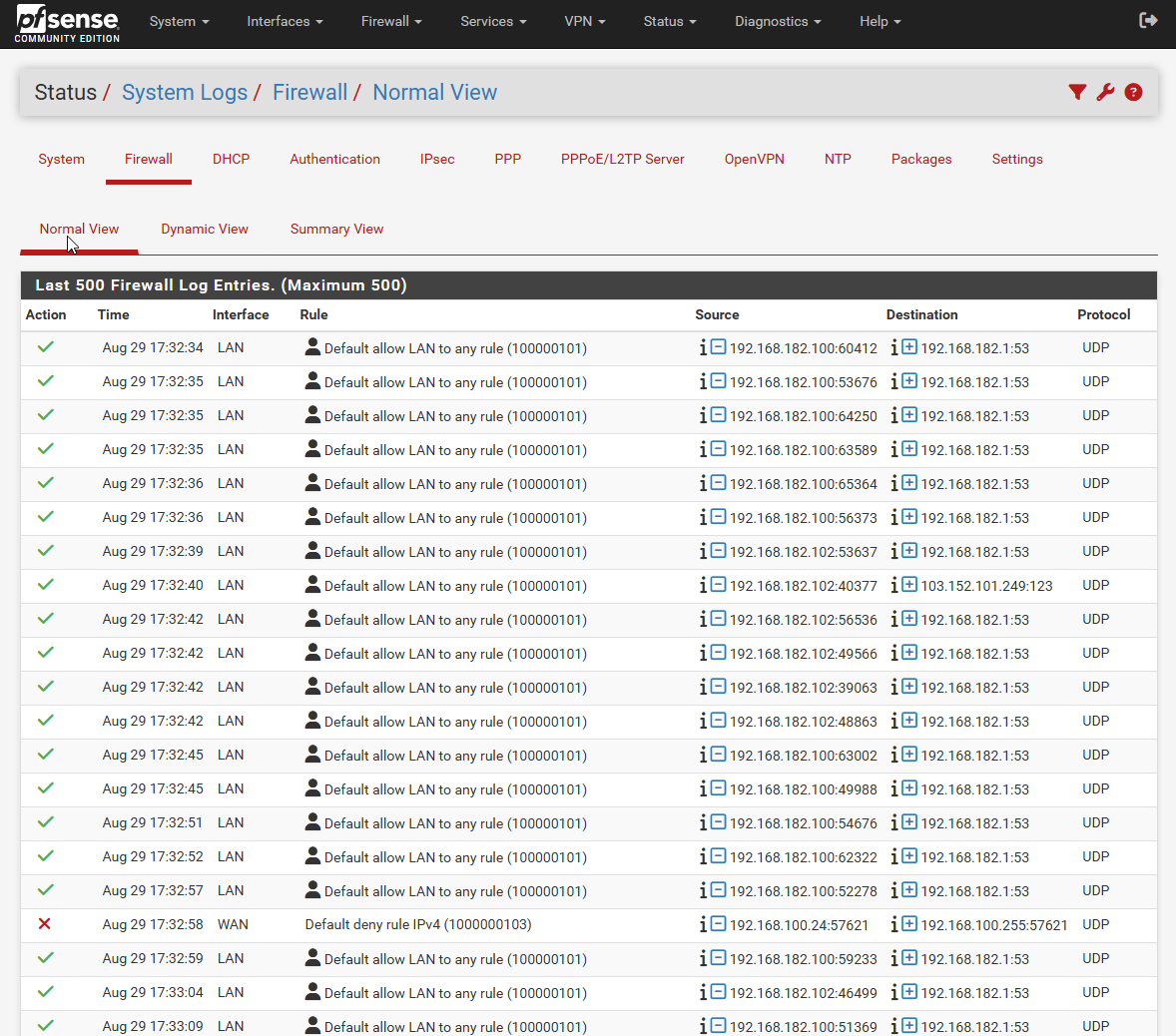


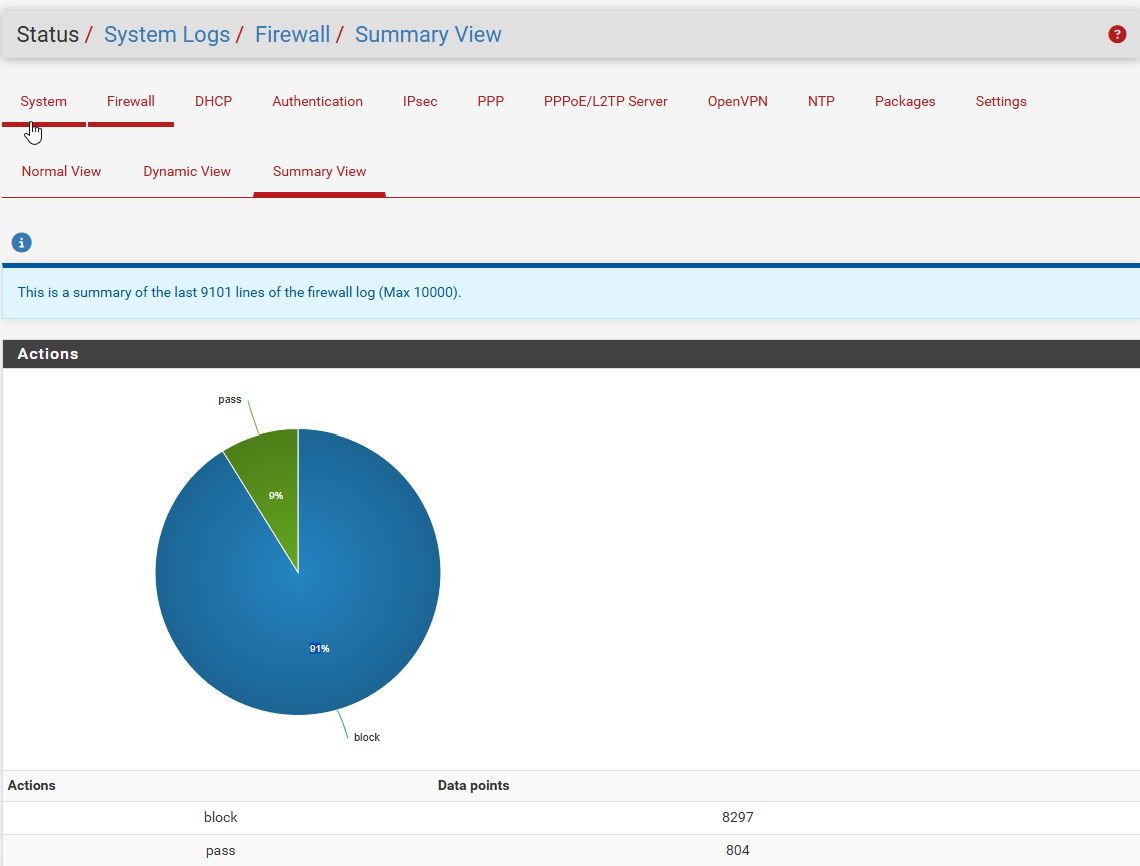


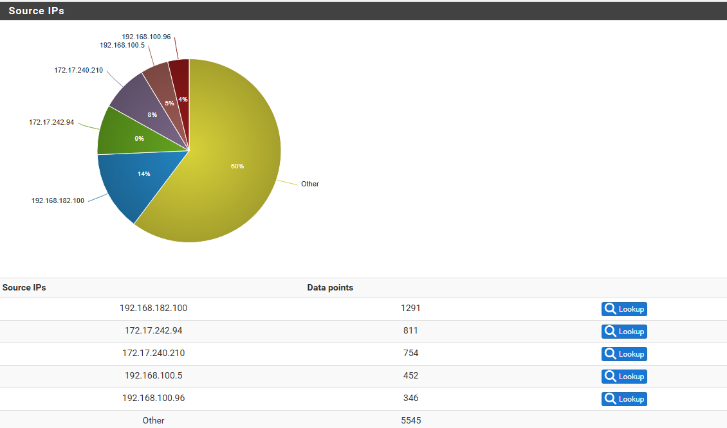
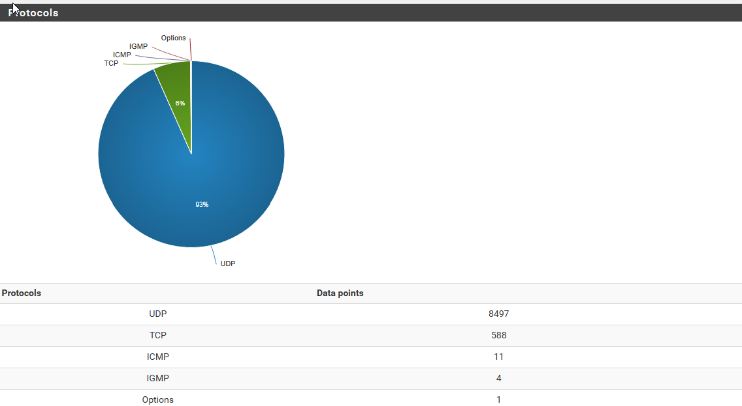


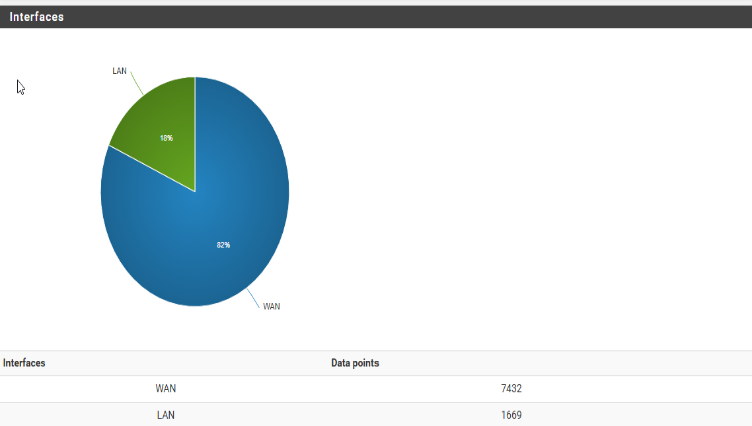


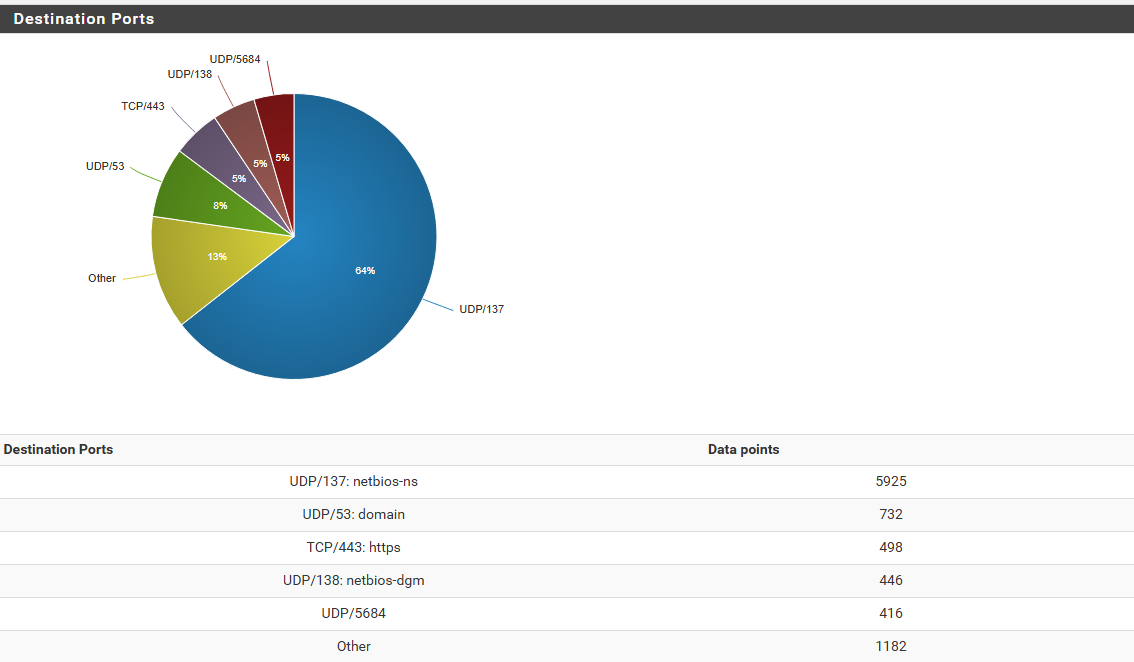








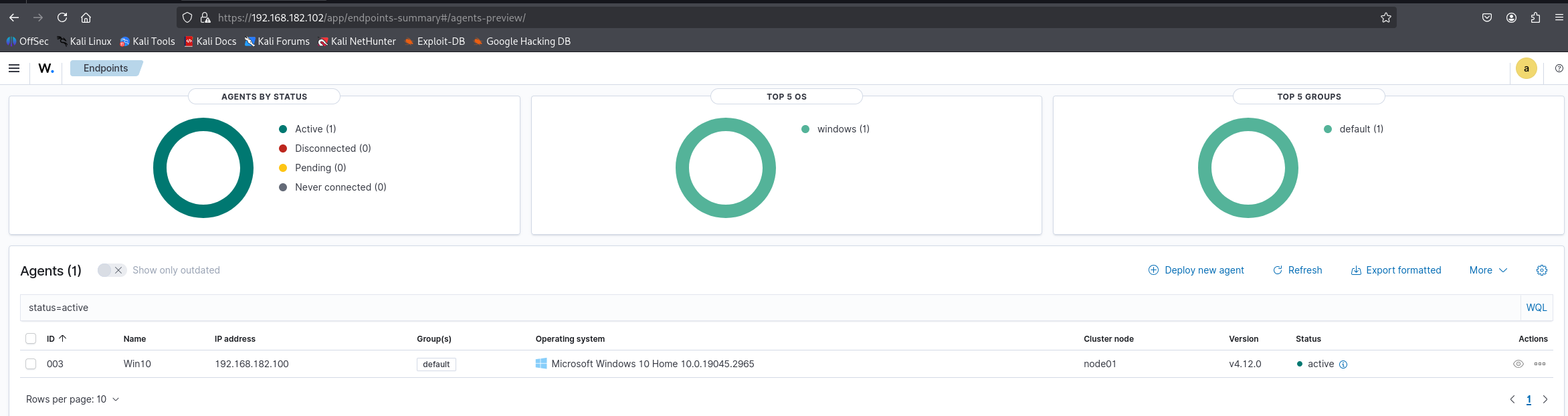


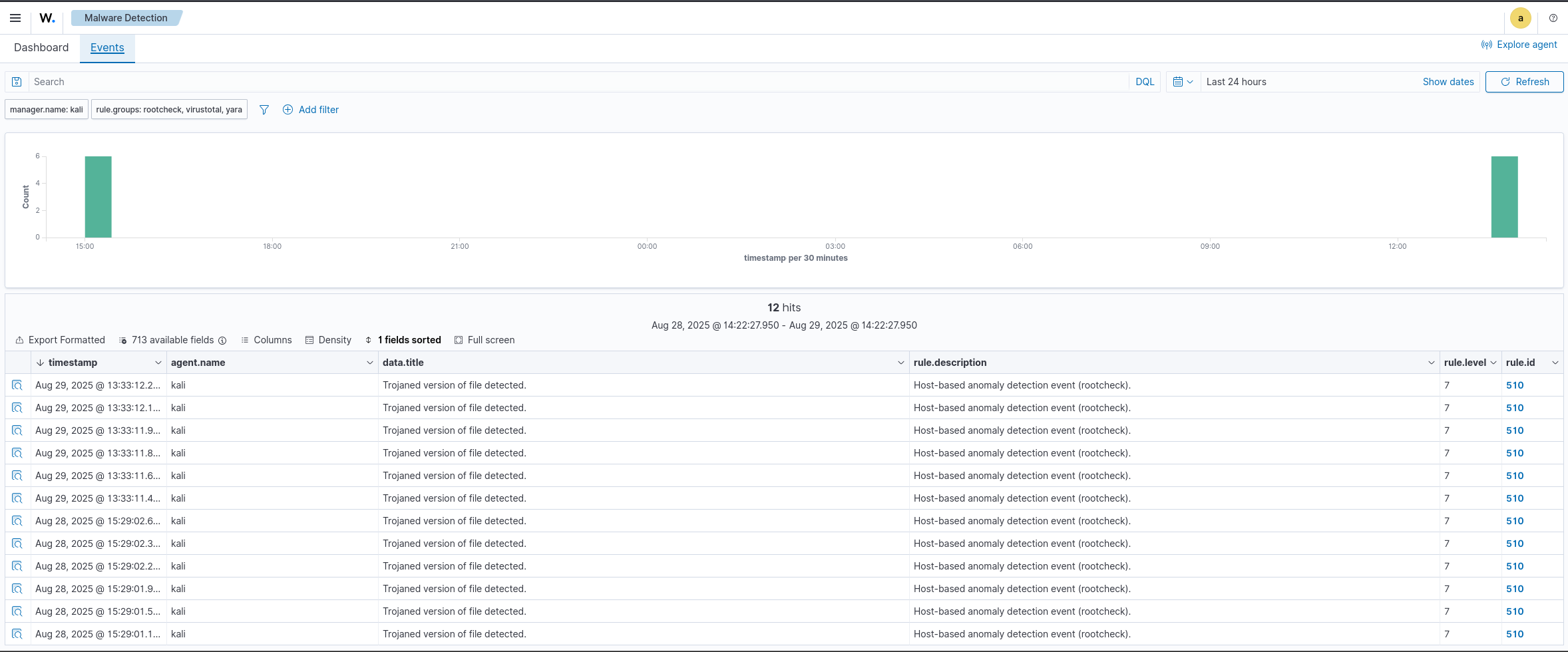


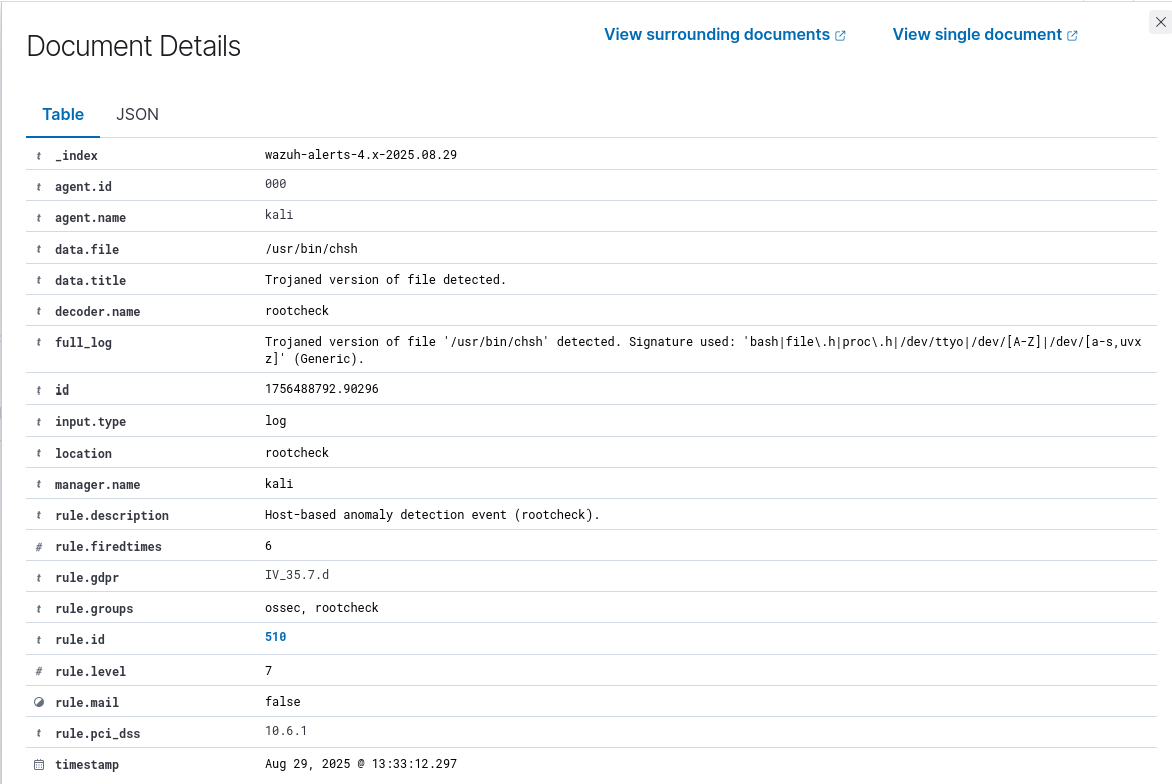
## Wazuh Dashboard:

Observe Wazuh for alerts/log entries related to the malware.

Gather detailed log entries.





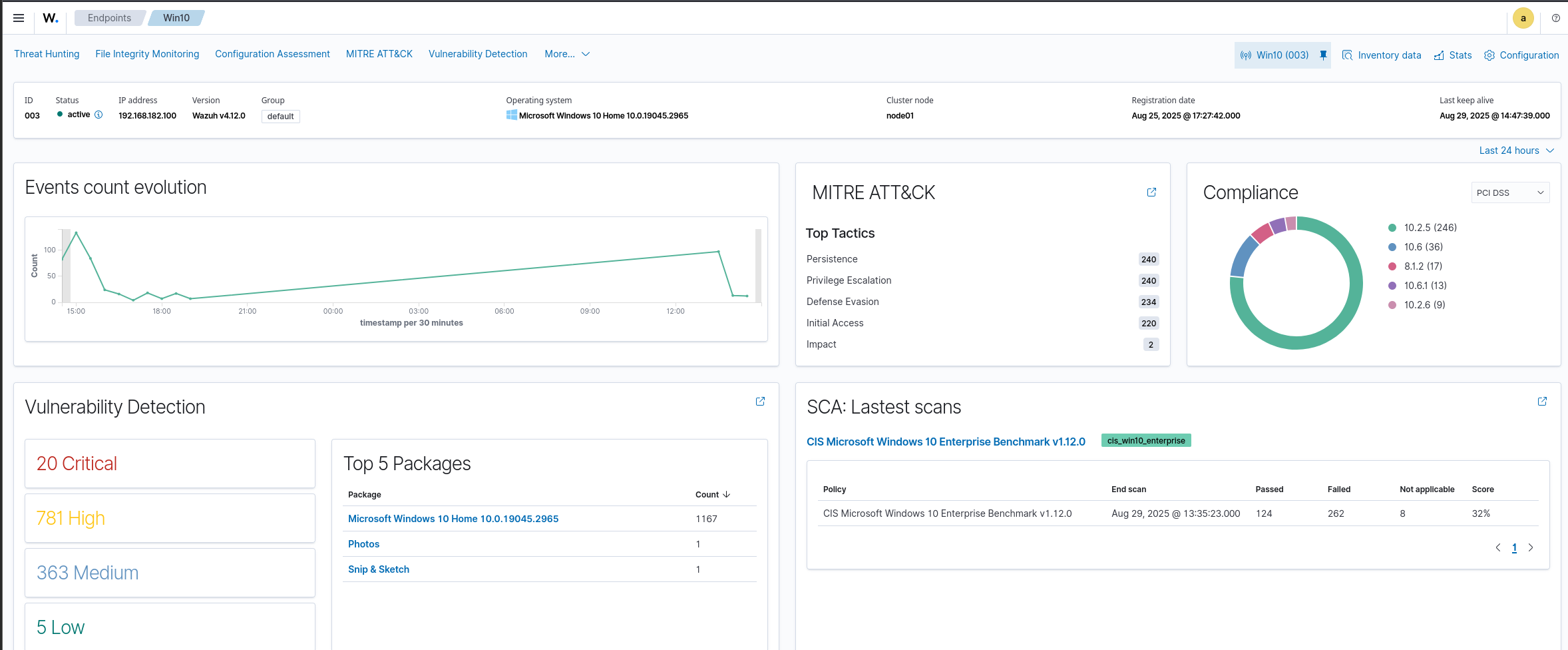


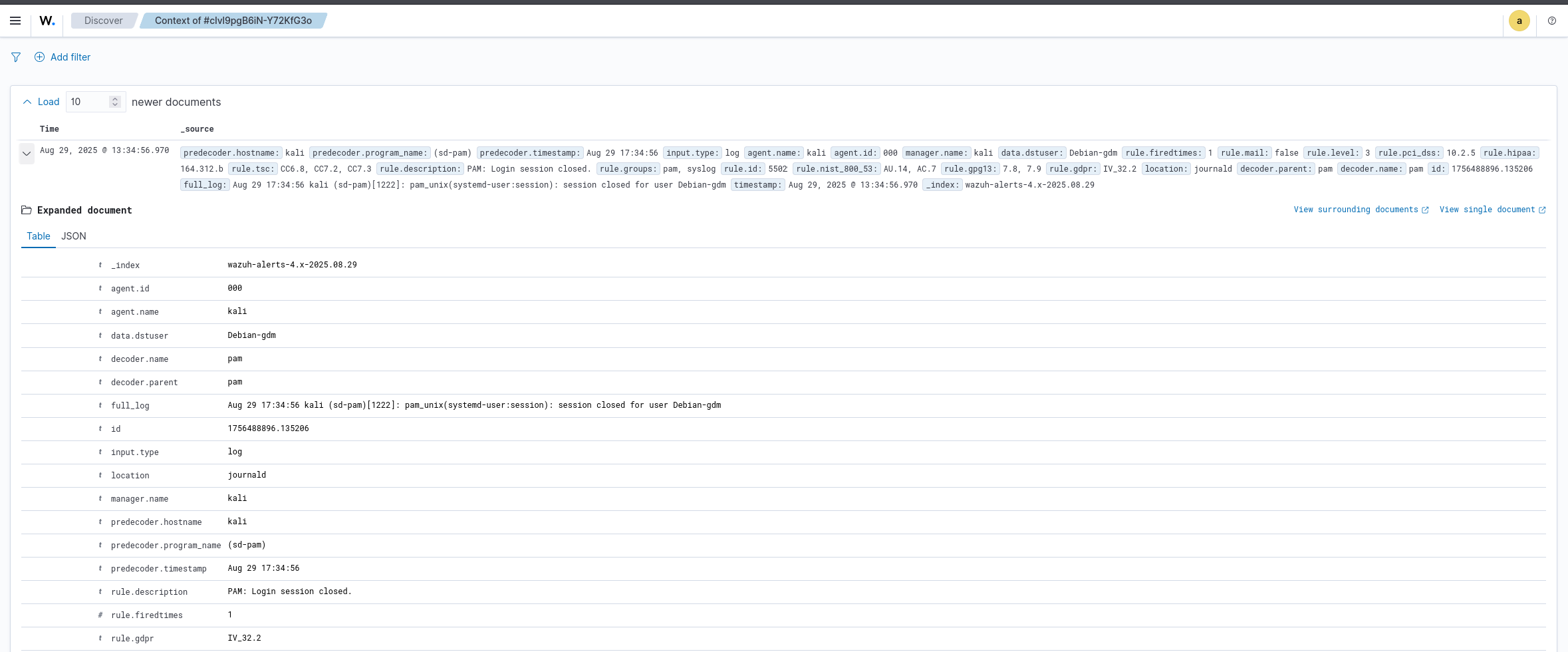
# Step 3: Log and Malware Analysis

## Log Details Collection

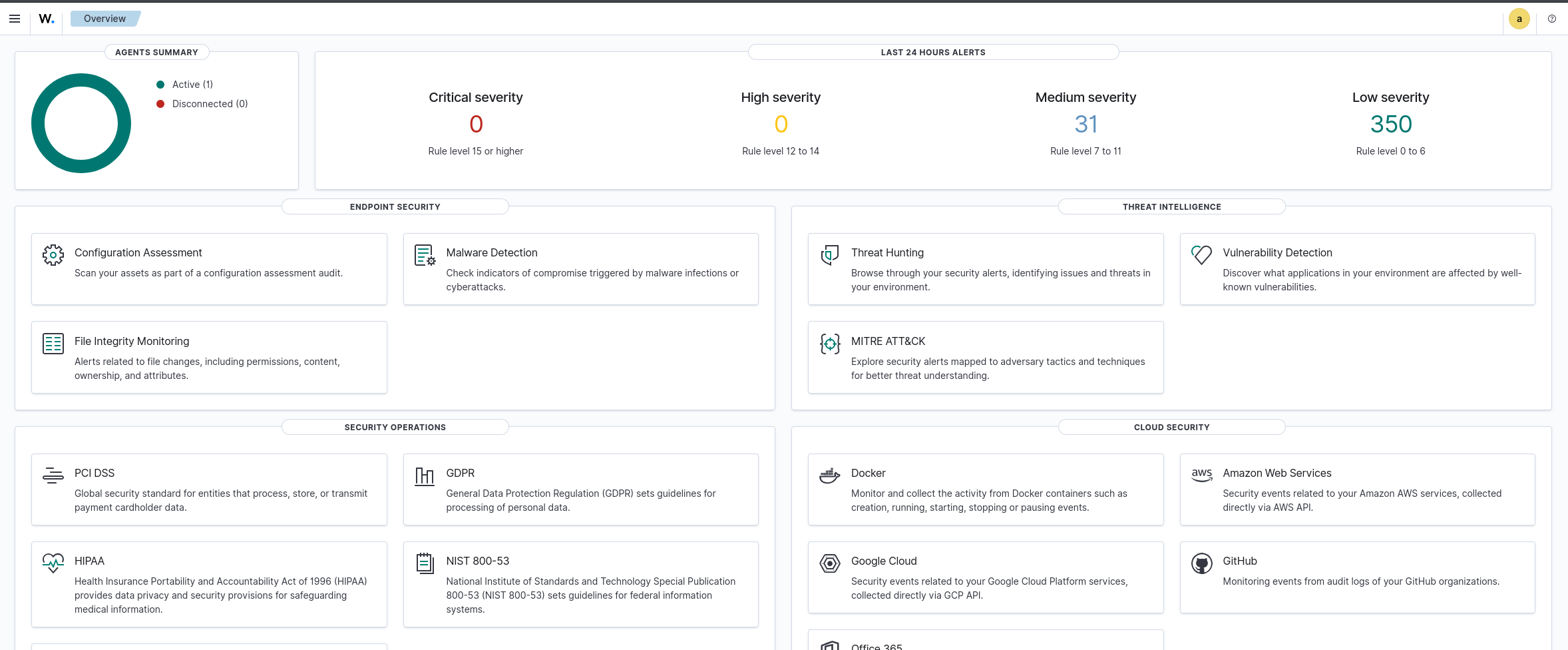
Collect comprehensive logs from Wazuh.

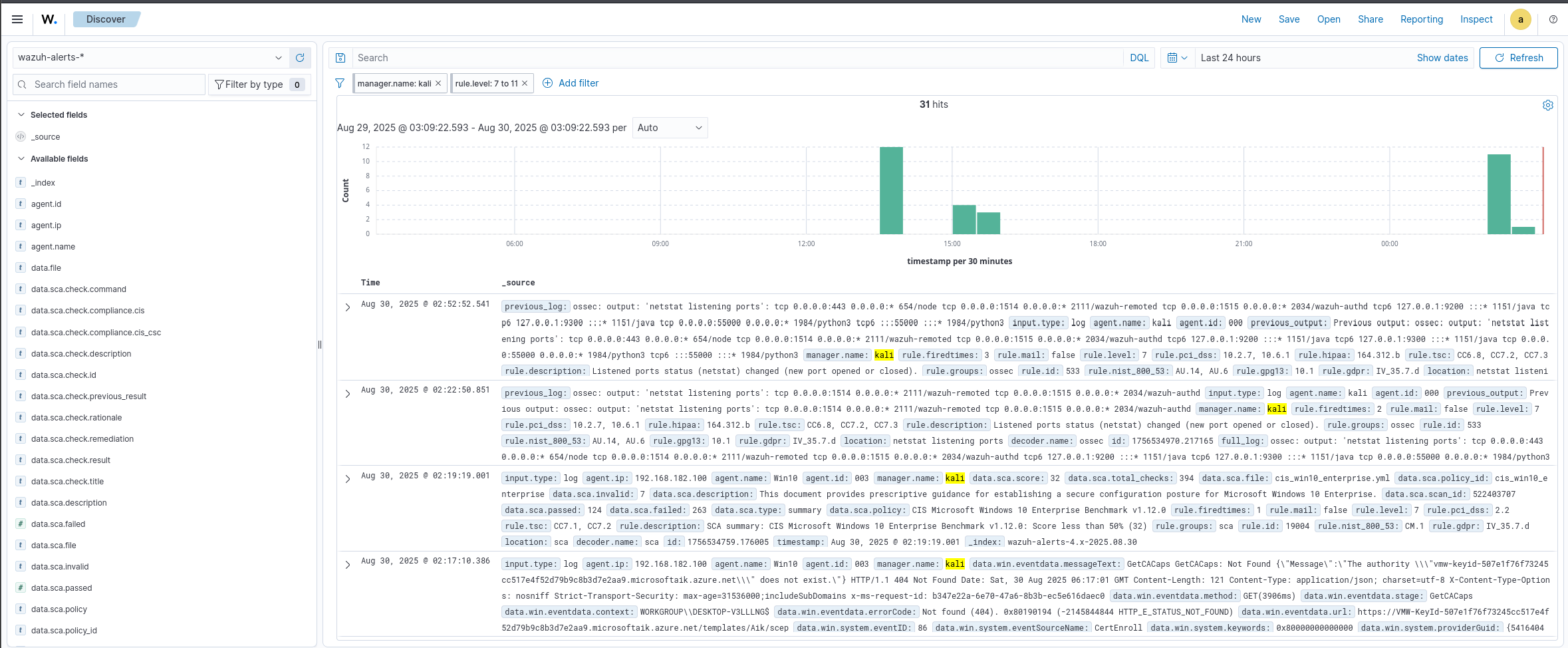
Identify Indicators of Compromise (IOCs) and Indicators of Attack (IOAs).

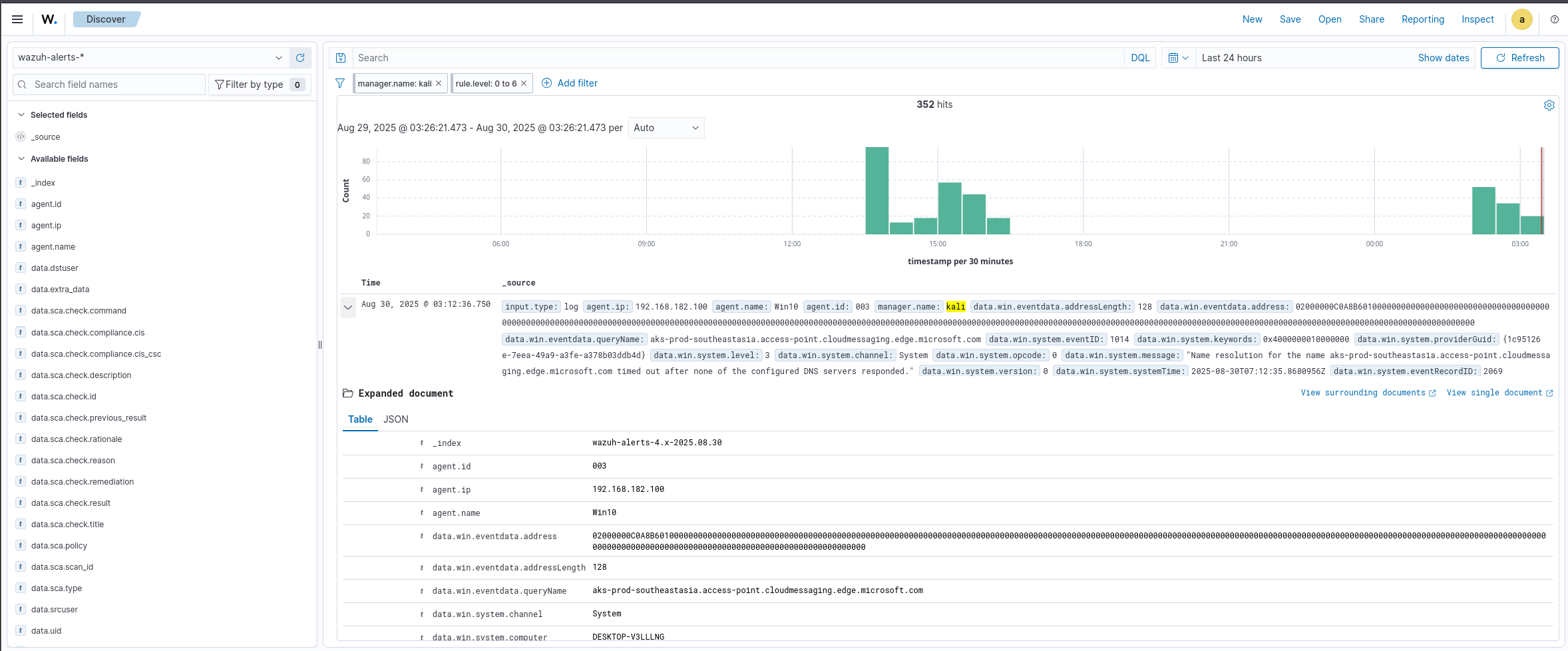




## Potential IOCs

****





## IOCs (Indicators of Compromise)

|  |  |
| --- | --- |
| Category | Value |
| Malware Source | https://github.com/ytisf/theZoo |
| Host IP | 192.168.182.100 (Windows 10 VM) |
| Outbound Ports | 52249, 59206, 58094, 62923, 63538, 53684, 49721, 53022, 51905, 62282 |
| Firewall RuleID | 100000101 (Default allow LAN to any rule) |
| Timestamps | Aug 28 22:30:58, Aug 28 22:30:59, Aug 29 17:29:15, Aug 29 17:44:13 |

## IOAs (Indicators of Attack)

|  |  |
| --- | --- |
| Attack Stage | Observed Activity |
| Initial Access | Malware downloaded from GitHub repo theZoo |
| Execution | Malware sample extracted & run inside Windows VM |
| Command & Control (C2) | Multiple outbound connections to random ports (possible beaconing) |
| Firewall Weakness | Outbound connections allowed due to default allow rule (100000101) |
| Persistence (Potential) | Expected file changes monitored by Syscheck/FIM |
| Lateral Movement Risk | VM connected outside the lab → chance of spreading to network |

## IOAs Mapped to MITRE ATT&CK

|  |  |  |  |
| --- | --- | --- | --- |
| IOA (Indicator of Attack) | MITRE Tactic | Technique (Name) | Technique ID |
| Execution of malicious PowerShell scripts | Execution | Command and Scripting Interpreter: PowerShell | **T1059.001** |
| Suspicious process creation (cmd.exe, rundll32) | Execution | Command and Scripting Interpreter | **T1059** |
| Persistence via registry run keys | Persistence | Boot or Logon Autostart Execution: Registry Run Keys | **T1547.001** |
| Scheduled task creation for persistence | Persistence | Scheduled Task/Job | **T1053** |
| Disabling security tools | Defense Evasion | Impair Defenses: Disable or Modify Tools | **T1562.001** |
| Clearing Windows event logs | Defense Evasion | Indicator Removal on Host: Clear Windows Event Logs | **T1070.001** |
| Suspicious network connection to C2 server | Command & Control (C2) | Application Layer Protocol (HTTP/HTTPS) | **T1071.001** |
| Exfiltration of data via encrypted channel | Exfiltration | Exfiltration Over C2 Channel | **T1041** |
| Privilege escalation using token manipulation | Privilege Escalation | Access Token Manipulation | **T1134** |
| Credential dumping via LSASS process | Credential Access | OS Credential Dumping: LSASS Memory | **T1003.001** |

# Step 4

# Incident Response Plan

Create incident response plan:

Develop an incident response plan based on industry standard.

Include steps for detection, analysis, containment, eradication, and recovery.

## Incident Response Plan (NIST-Based)

### . Detection

* **Tools Used:** Wazuh SIEM, pfSense firewall, Syscheck/FIM.
* **Indicators of Compromise (IOCs):**
  + Malware Source: [https://github.com/ytisf/theZoo](https://github.com/ytisf/theZoo?utm_source=chatgpt.com)
  + Host IP: 192.168.182.100 (Windows 10 VM)
  + Outbound Ports: 52249, 59206, 58094, 62923, 63538, 53684, 49721, 53022, 51905, 62282
  + Firewall RuleID: 100000101 (LAN to any)
  + Timestamps: Aug 28–29 (multiple events logged)
* **Indicators of Attack (IOAs):**
  + Malware download and execution from GitHub repo.
  + Multiple outbound C2 connections to random ports.
  + Suspicious process creation (cmd.exe, powershell.exe, rundll32.exe).
  + Registry persistence and scheduled tasks.
  + Security tools disabling and event log clearing.

## Analysis

* Malware attempted **C2 communication** (possible beaconing).
* Persistence confirmed via registry keys and scheduled tasks.
* Evidence of **defense evasion** and **credential dumping**.
* **Mapped to MITRE ATT&CK:**
  + Execution: PowerShell / cmd.exe (T1059)
  + Persistence: Registry Run Keys (T1547.001), Scheduled Tasks (T1053)
  + Defense Evasion: Disable Security Tools (T1562.001), Clear Logs (T1070.001)
  + C2: Encrypted traffic (T1071.001)
  + Credential Access: LSASS Dumping (T1003.001)
* **Risk Level:** High if VM connects outside lab (possible lateral movement & data exfiltration).

## Containment

* **Immediate:**
  + Isolate infected Windows VM from network.
  + Block outbound suspicious ports via pfSense.
  + Disable “allow any” firewall rule (100000101).
* **Short-Term:**
  + Kill malicious processes.
  + Restrict communication to external servers.
* **Long-Term:**
  + Harden firewall rules with least privilege.
  + Implement stricter application control.

## Eradication

* Remove malware binaries and persistence entries.
* Delete malicious scheduled tasks.
* Run antivirus/EDR scan.
* Reset firewall policies.
* Patch and update Windows VM.

## Recovery

* Restore VM from a clean snapshot.
* Validate system integrity using Wazuh and FIM.
* Reconnect to network after verification.
* Monitor for abnormal logs or re-infection attempts.

## Lessons Learned

* Replace weak firewall rules with strict controls.
* Train SOC staff to detect IOCs quickly.
* Regular phishing/malware awareness exercises (e.g., using GoPhish).
* Keep malware labs fully isolated to avoid spread.