ECOLE NORMALE SUPÉRIEURE DE L'ENSEIGNEMENT
TECHNIQUE DE MOHAMMEDIA
UNIVERSITÉ HASSAN II DE CASABLANCA

École Normale Supérieure de
l'Enseignement Technique - Mohammedia

Department of Information and Mathematics

IT Engineering, Cybersecurity and Digital Trust engineering

Module : Cloud Computing

Wazuh SIEM/EDR Cloud Lab Implementation

Élèves :
Yasser NAMEZ

Enseignant :
Prof. Azeddine KHIAT

8 janvier 2026

Table des matières

1 Introduction

1.1 Project Context

In a context where cyber threats are becoming increasingly sophisticated, establishing a surveillance and security incident detection infrastructure has become essential for any organization. This project is part of the **Cloud Computing** module and aims to demonstrate the implementation of a SIEM (Security Information and Event Management) and EDR (Endpoint Detection and Response) solution in a cloud environment.

The **Wazuh** platform, a recognized open-source solution in the cybersecurity field, was chosen for its versatility, scalability, and ability to unify SIEM and EDR functionalities within a single platform.

1.2 Lab Objectives

This practical lab aims to :

1. **Design and deploy** a secure cloud architecture on AWS with network segmentation
2. **Install and configure** a Wazuh Manager server for centralized log collection
3. **Deploy agents** on Linux (Ubuntu) and Windows Server systems
4. **Generate and analyze** real-time security alerts
5. **Understand the differences** between SIEM and EDR approaches
6. **Apply proactive** Threat Hunting techniques
7. **Master IAM/PAM concepts** in an operational security context

1.3 Technologies Used

Category	Technology	Role
Cloud	AWS EC2 AWS VPC Security Groups	Virtual machine hosting Network isolation and segmentation Network access control (firewall)
SIEM/EDR	Wazuh Manager Wazuh Dashboard Wazuh Agents	Central collection and analysis server Visualization and reporting interface Event collection on endpoints
Endpoints	Ubuntu 22.04 LTS Windows Server 2022	Linux client for monitoring Windows client with Sysmon
Monitoring	Sysmon	Advanced Windows process telemetry

TABLE 1 – Lab Technology Stack

1.4 Lab Scope

This laboratory covers the following aspects :

— **Infrastructure :** Deployment of an AWS VPC with public subnets, EC2 instances, and security groups

— **Log Collection :** Configuration of Wazuh agents for system event forwarding

— **Attack Detection :** Simulation and analysis of SSH brute force attacks, privilege escalation
— **Windows Monitoring :** Sysmon integration for in-depth process visibility
— **Threat Hunting :** Creation of proactive threat search queries

Source Code

The source code and complete documentation for this project are available on GitHub :
https://github.com/yassernamez03/wazuh-siem-edr-cloud-lab

2 Architecture VPC + Security Groups + EC2 Instances

2.1 Overview

This section describes the cloud infrastructure deployed on AWS for the Wazuh SIEM/EDR lab environment. The architecture follows security best practices with network segmentation and least-privilege access controls.

2.2 AWS VPC Configuration

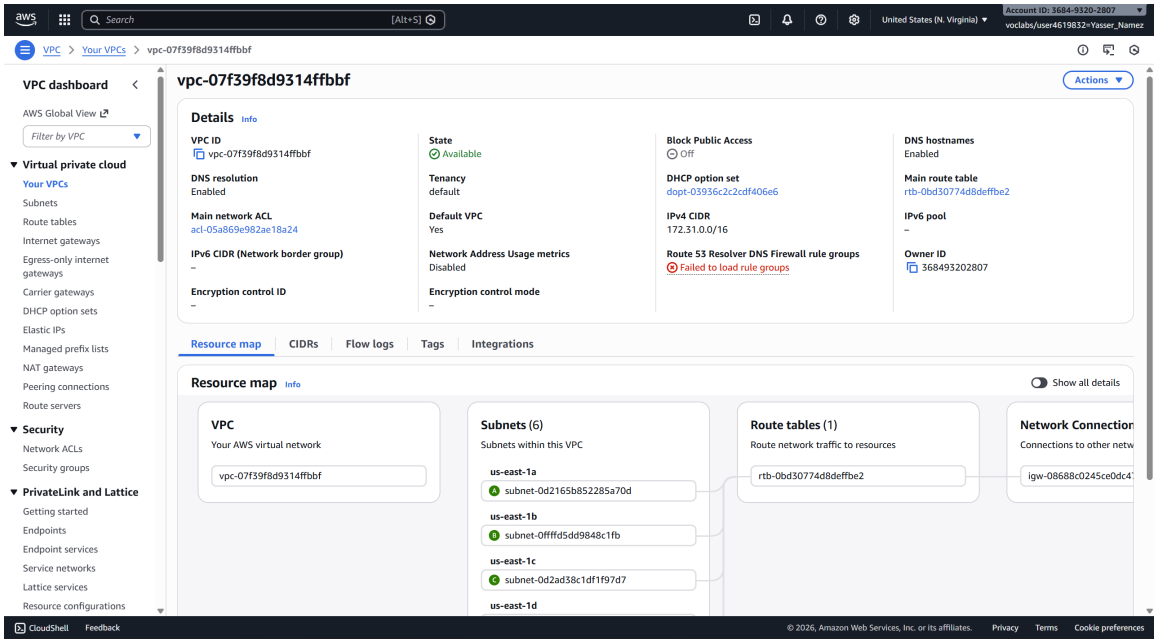

FIGURE 1 – AWS VPC Configuration - 10.0.0.0/16

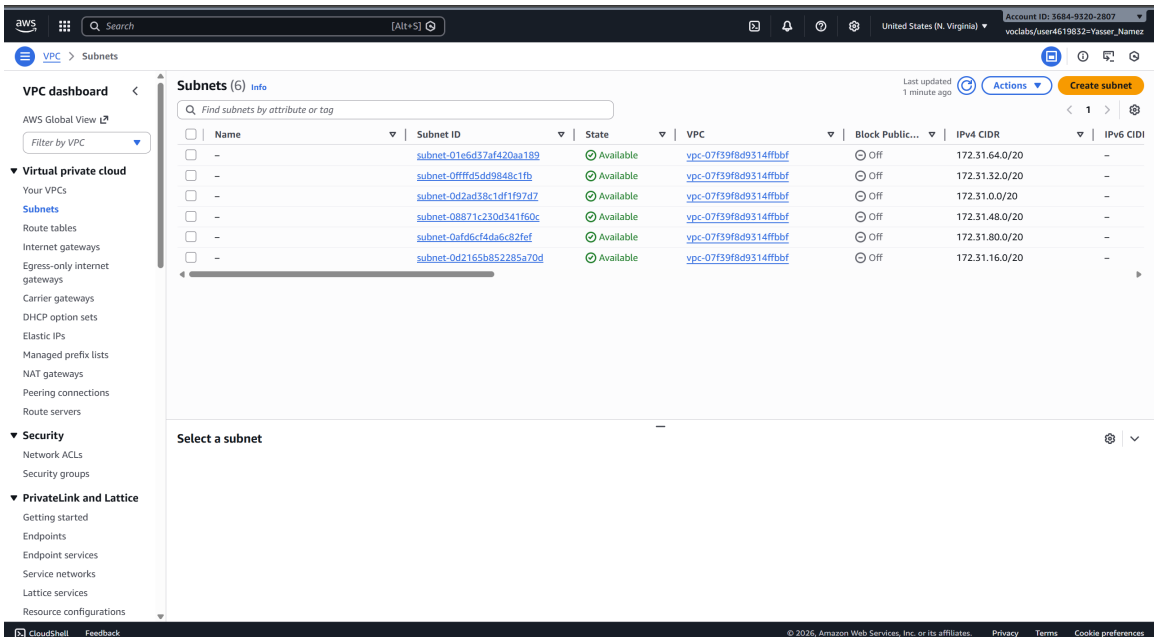

FIGURE 2 – VPC Subnets Configuration

2.3 EC2 Instances

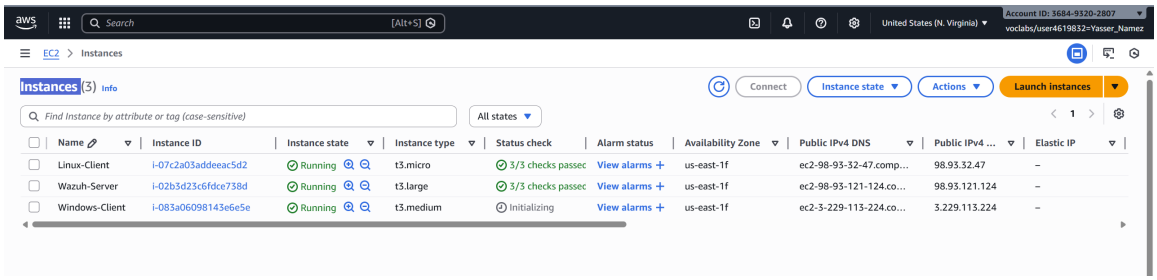

FIGURE 3 – All EC2 Instances Running

2.3.1 Wazuh Server Instance

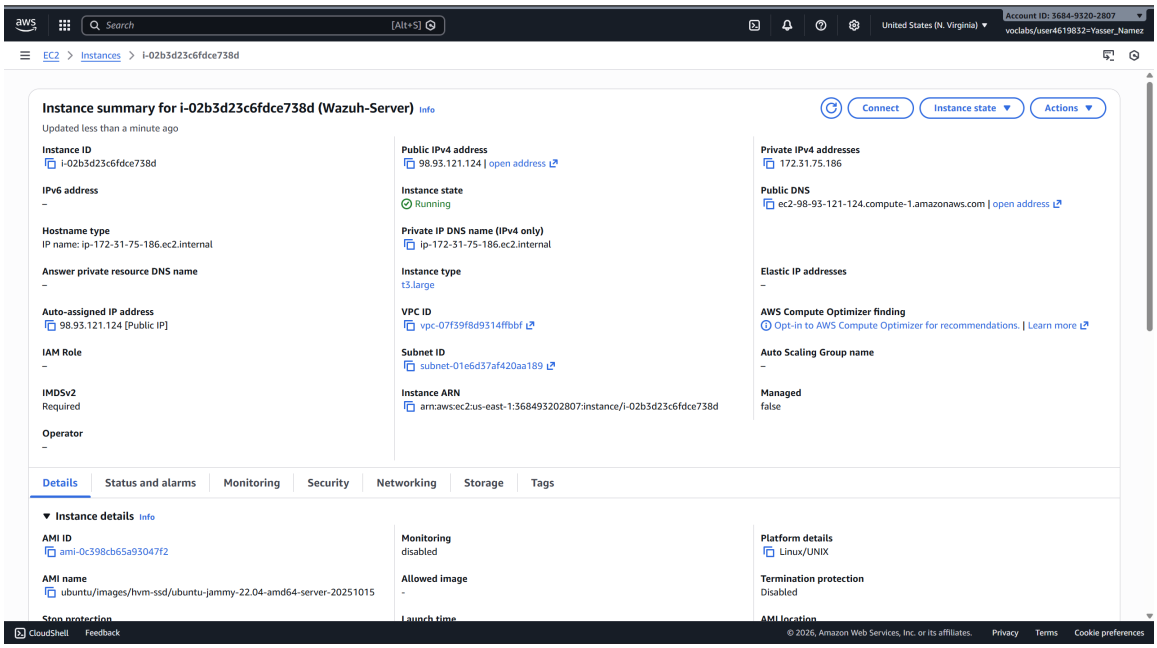

FIGURE 4 – Wazuh-Server Instance Details (Ubuntu 22.04, t3.large)

2.3.2 Linux Client Instance

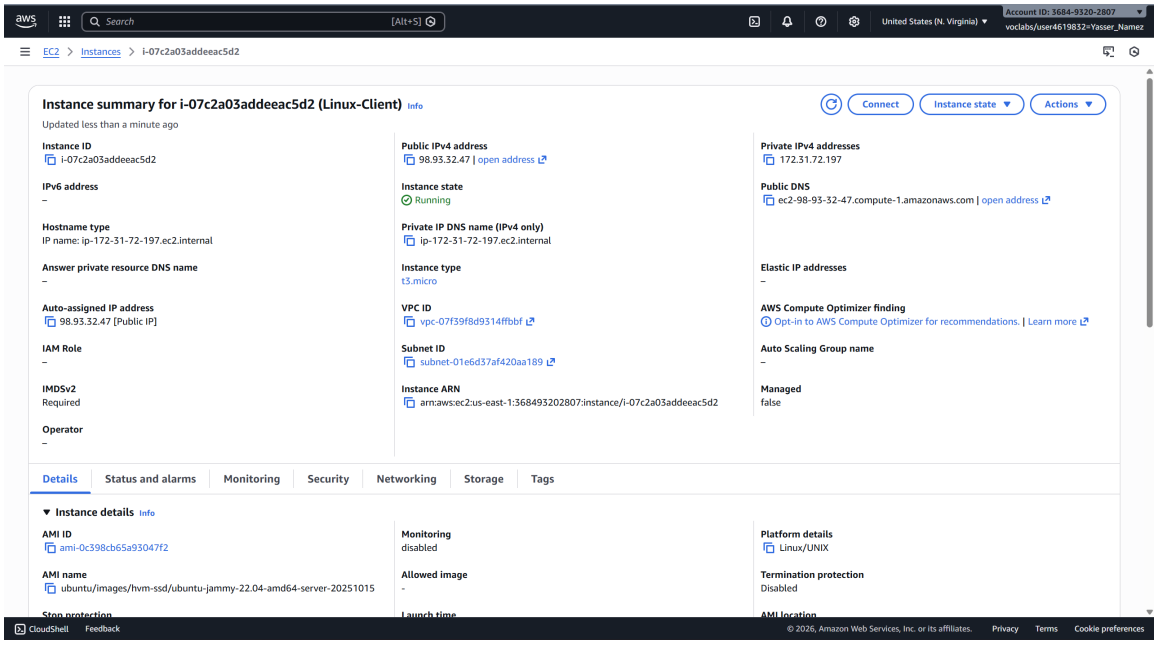

FIGURE 5 – Linux-Client Instance Details (Ubuntu 22.04, t2.micro)

2.3.3 Windows Client Instance

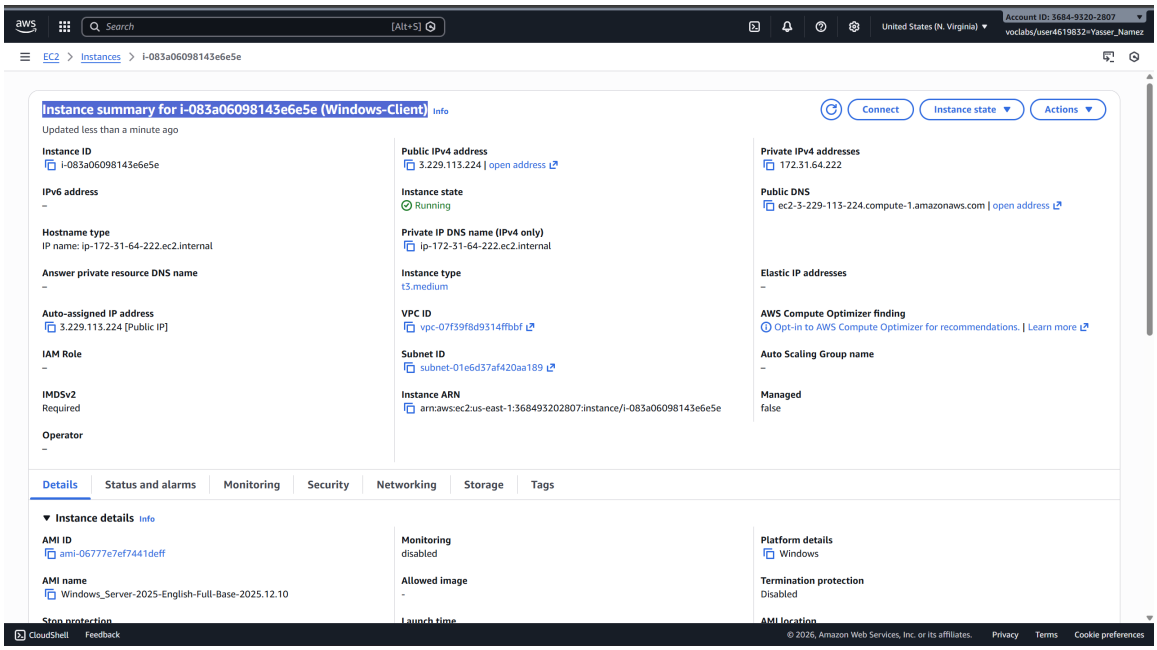

FIGURE 6 – Windows-Client Instance Details (Windows Server 2022, t2.medium)

2.4 Security Groups Configuration

2.4.1 Wazuh Server Security Group

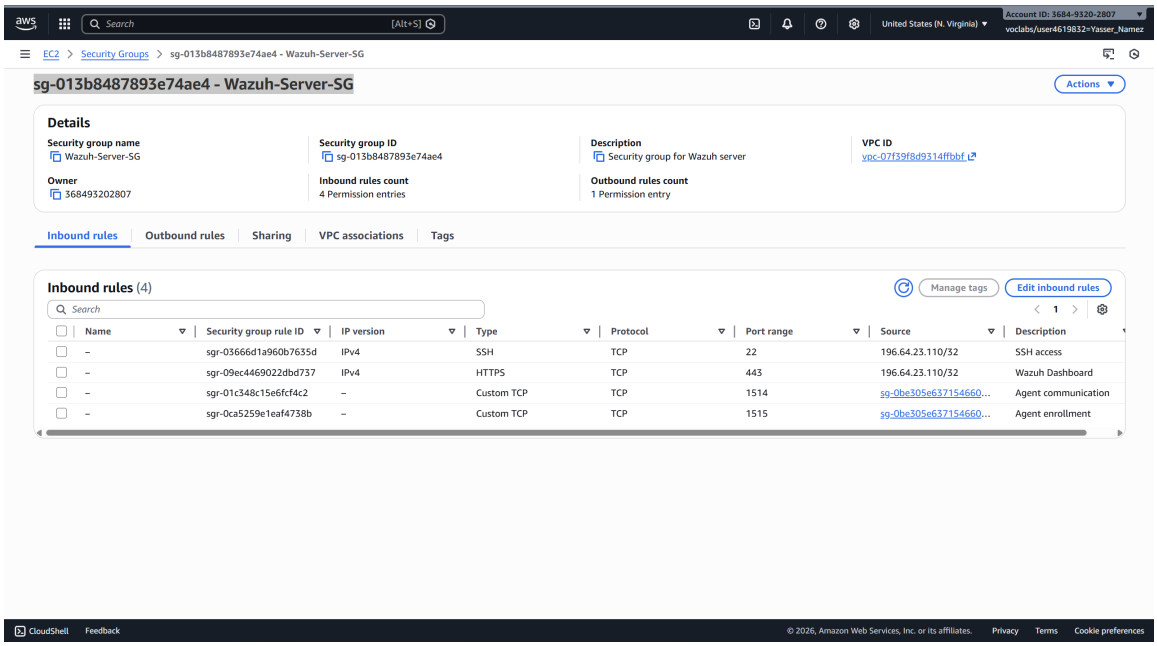

FIGURE 7 – Wazuh-Server-SG : Inbound Rules (Ports 22, 443, 1514, 1515)

2.4.2 Wazuh Clients Security Group

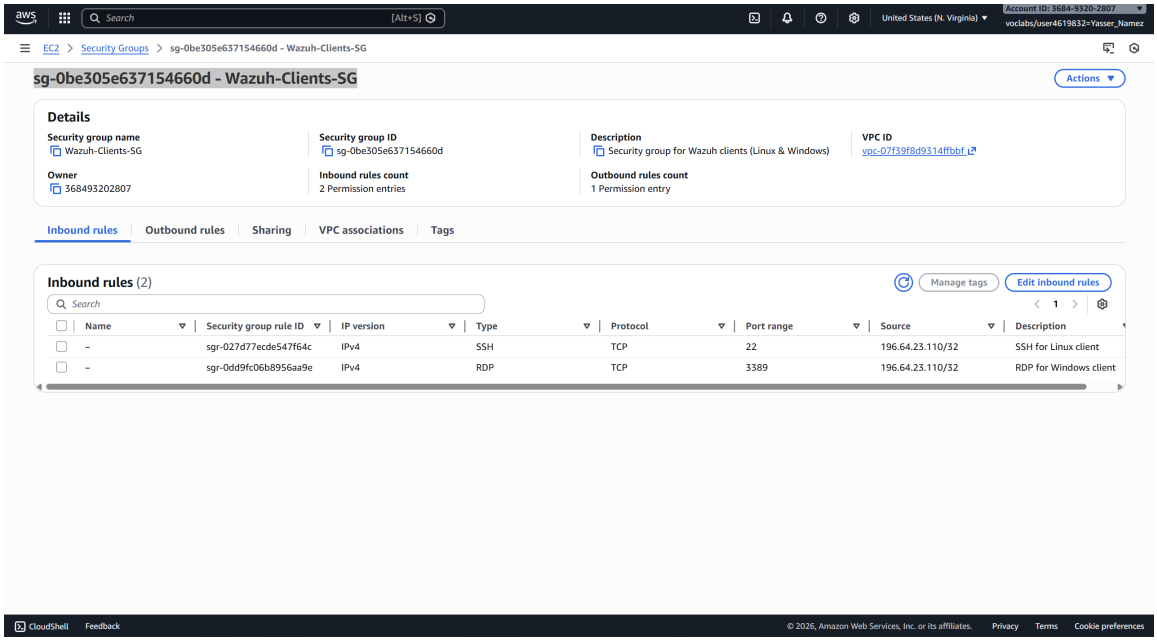

FIGURE 8 – Wazuh-Clients-SG : Inbound Rules (SSH 22, RDP 3389)

2.5 Network Architecture Diagram

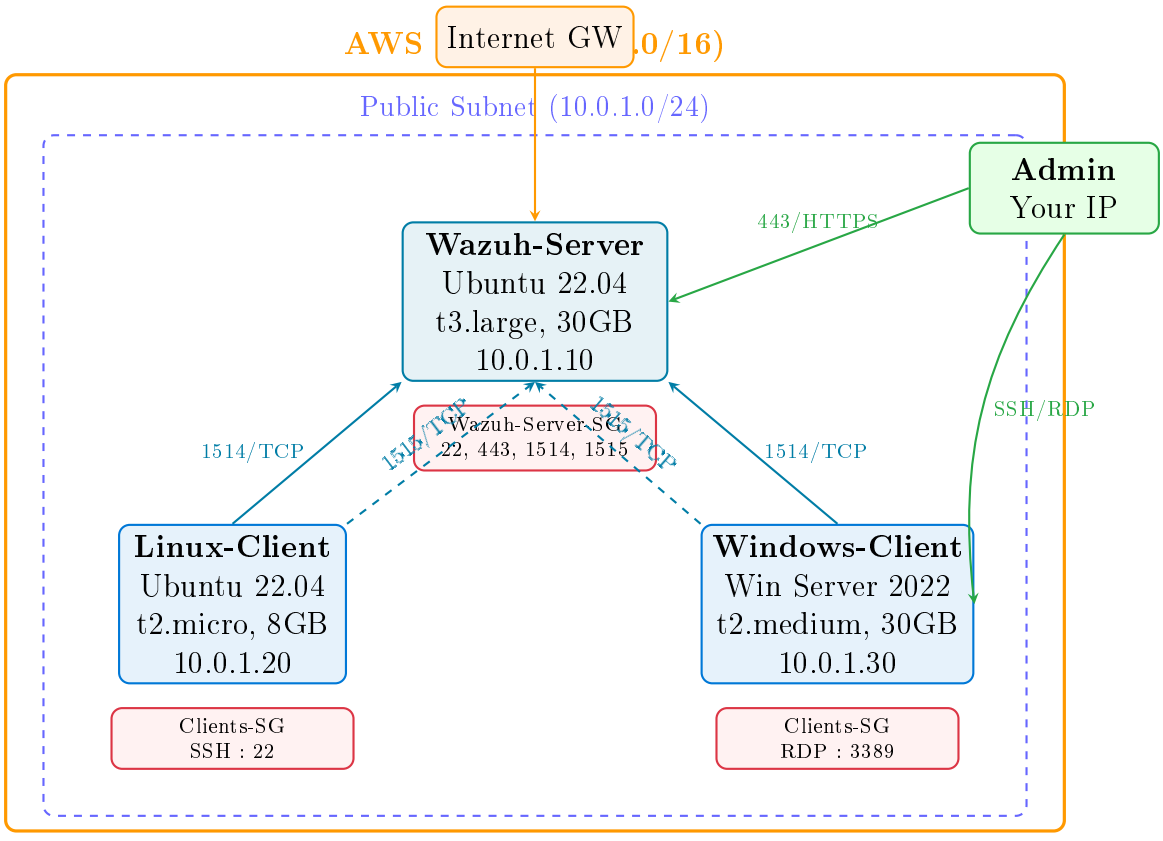

FIGURE 9 – Wazuh SIEM/EDR Lab Architecture Diagram

2.6 Connectivity Testing

2.6.1 SSH to Wazuh Server

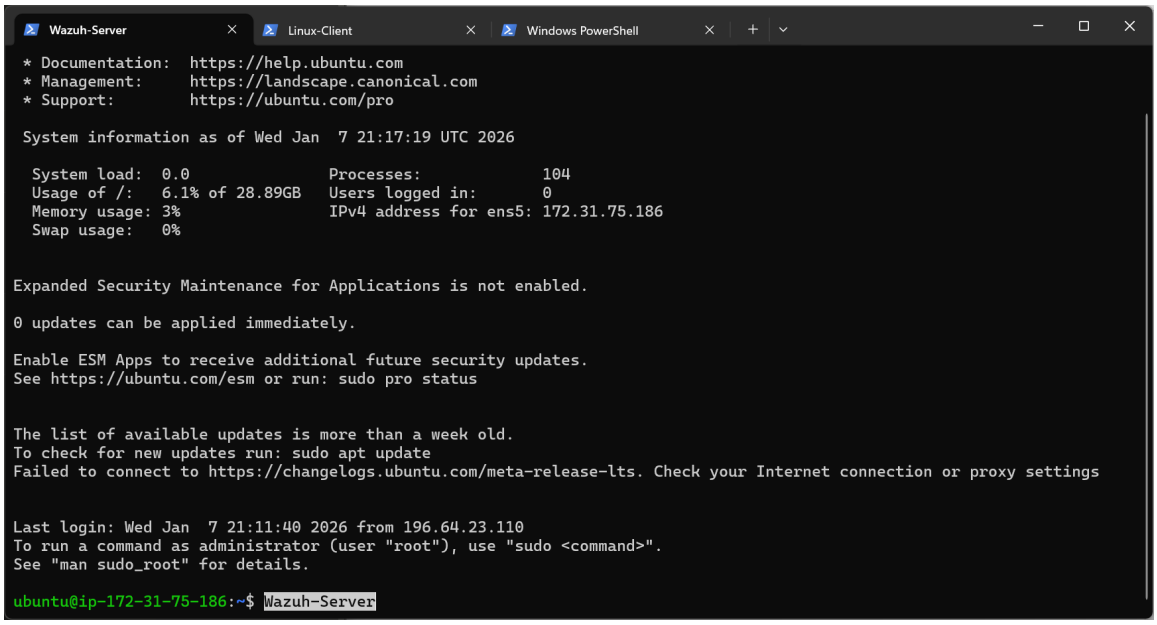

FIGURE 10 – SSH Connection Test to Wazuh-Server

2.6.2 SSH to Linux Client

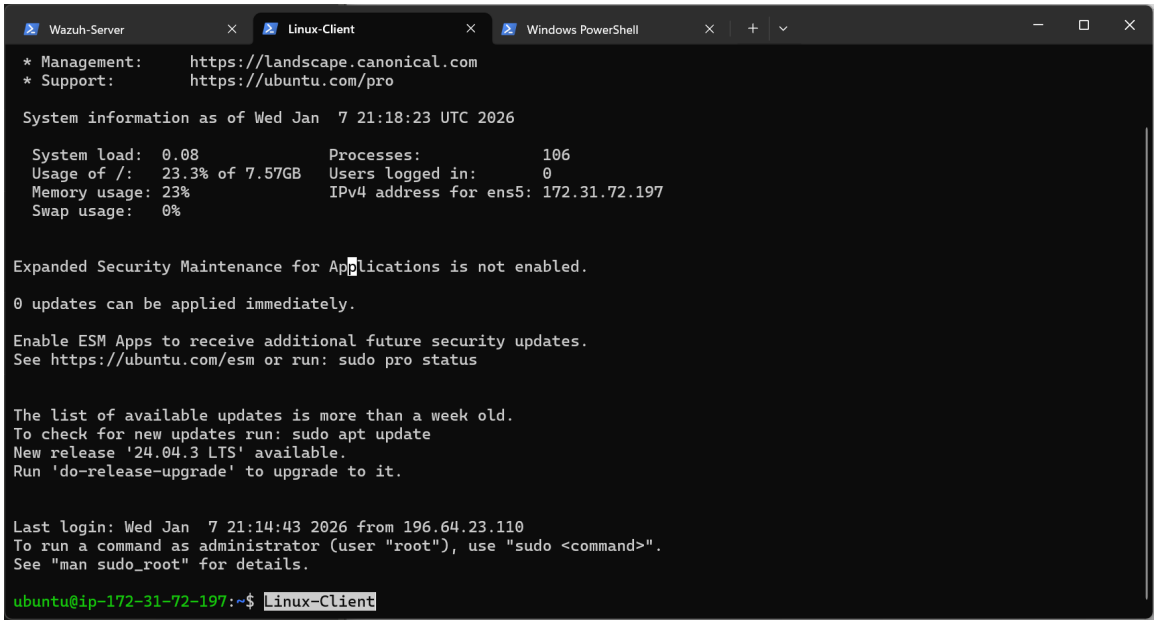

FIGURE 11 – SSH Connection Test to Linux-Client

2.6.3 RDP to Windows Client

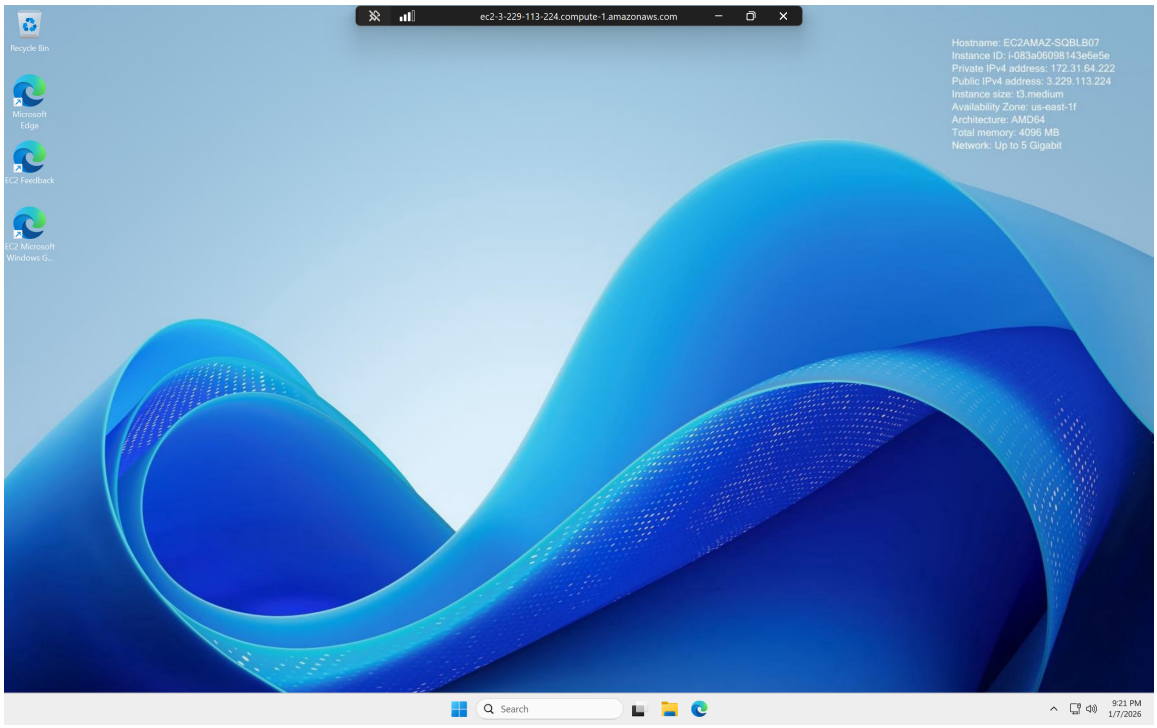

FIGURE 12 – RDP Connection Test to Windows-Client

2.7 Infrastructure Summary

Instance	Operating System	Type	Storage	Private IP
Wazuh-Server	Ubuntu 22.04 LTS	t3.large	30 GB	10.0.1.10
Linux-Client	Ubuntu 22.04 LTS	t2.micro	8 GB	10.0.1.20
Windows-Client	Windows Server 2022/2025	t2.medium	30 GB	10.0.1.30

TABLE 2 – EC2 Instance Specifications

Security Best Practices Implemented

- All agent-to-server communication uses private IP addresses within the VPC
- Management ports are restricted to specific administrator IP addresses
- Security groups follow the principle of least privilege
- Encrypted communication channels for all sensitive traffic
- Network segmentation isolates the monitoring infrastructure

3 Wazuh Server Setup and Dashboard

3.1 Wazuh Services Status

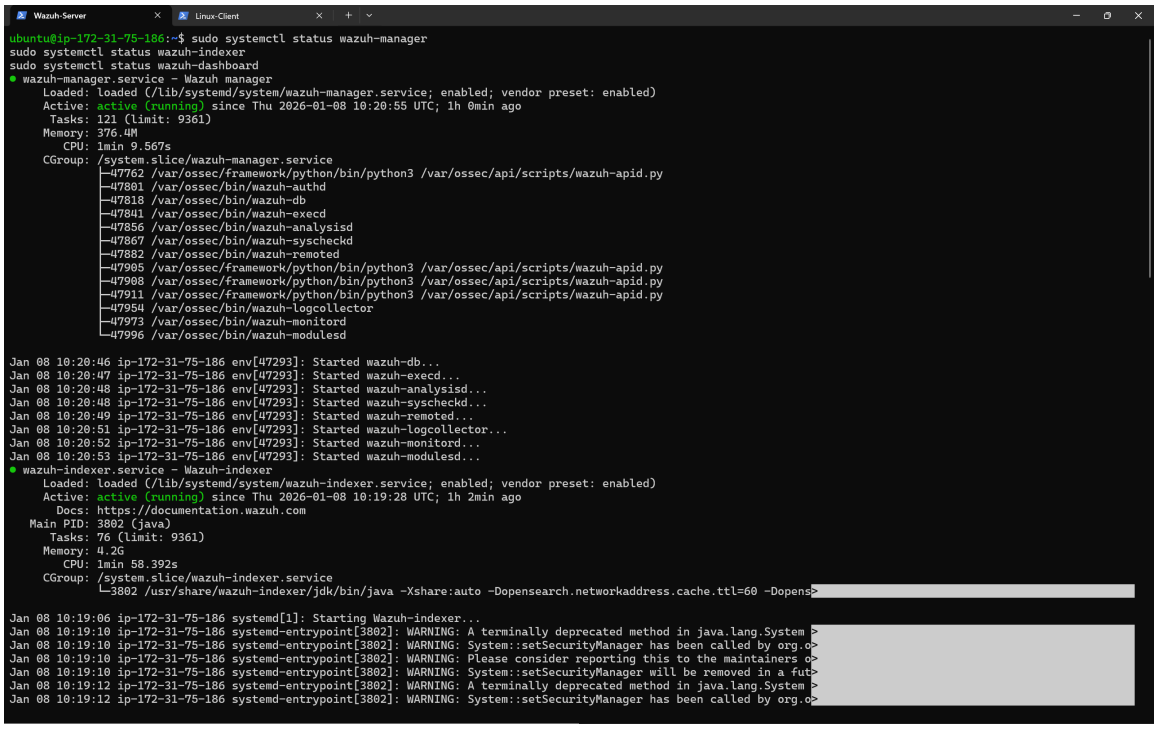

FIGURE 13 – Wazuh Services Running on Server

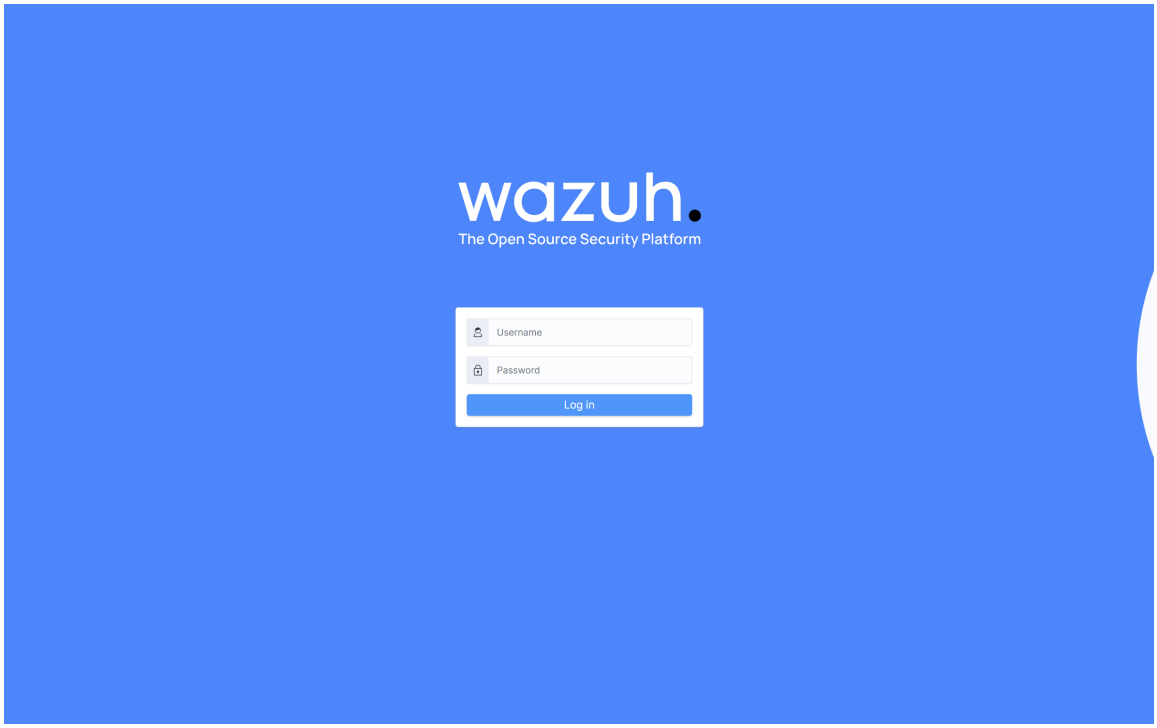

FIGURE 14 – Wazuh Services Status Verification

3.2 Wazuh Dashboard Access

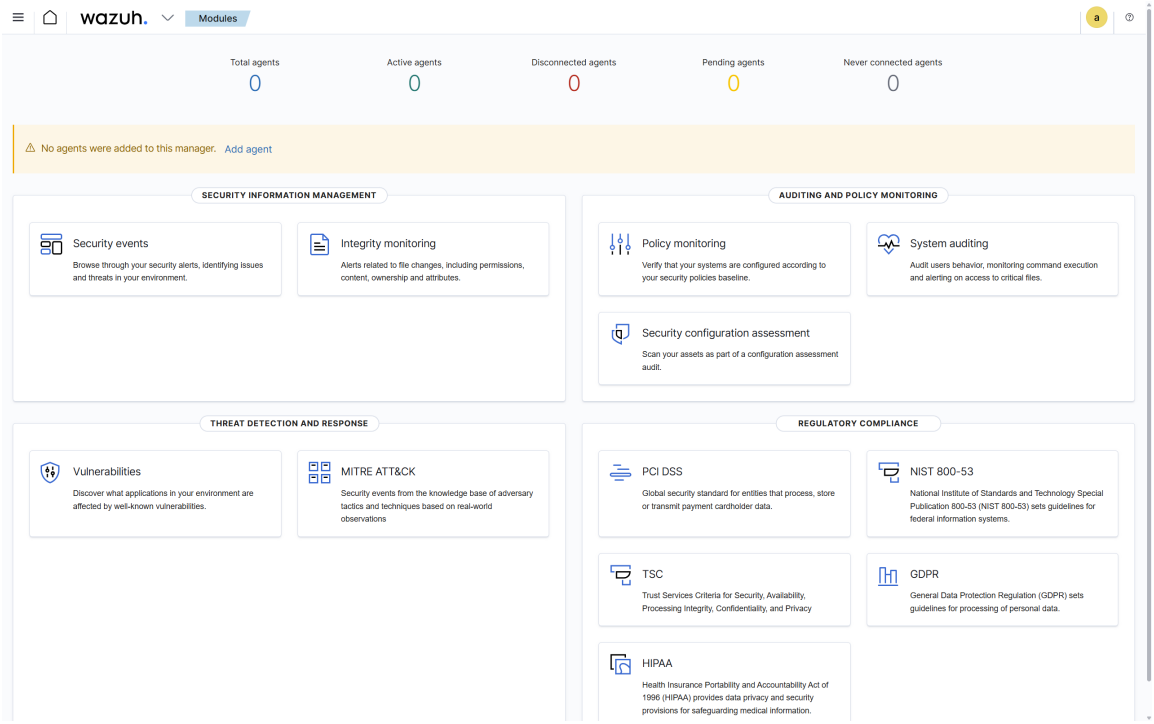

FIGURE 15 – Wazuh Dashboard Login Interface

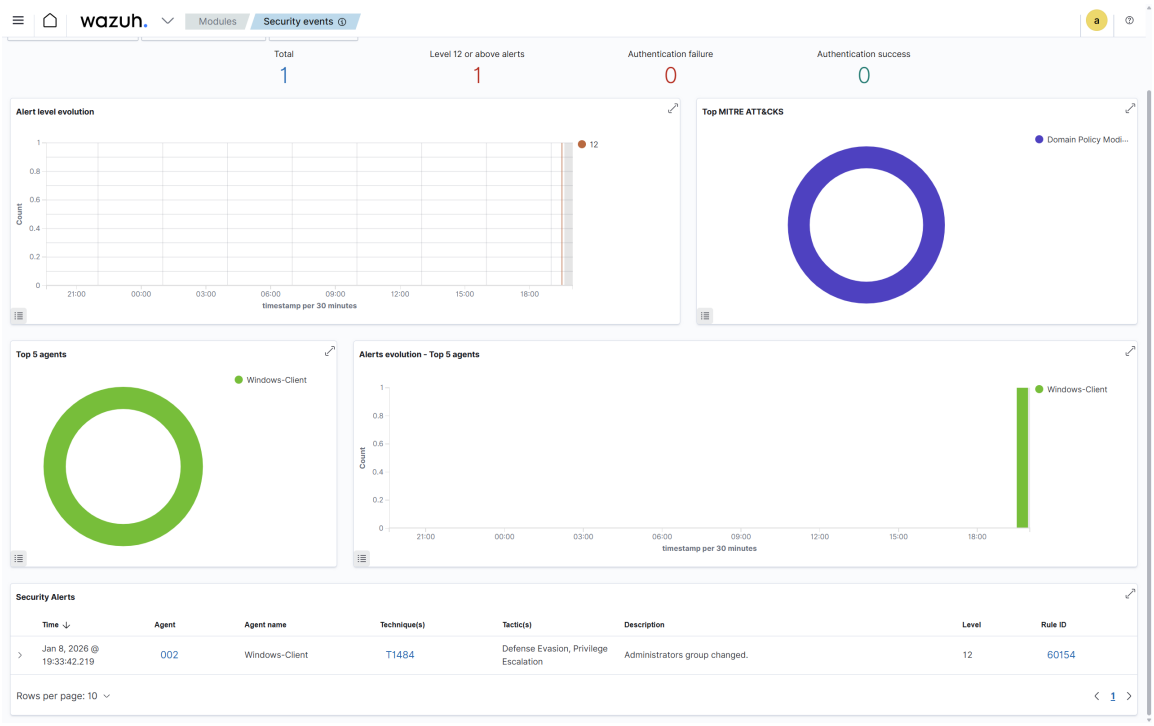

FIGURE 16 – Wazuh Dashboard Main Overview

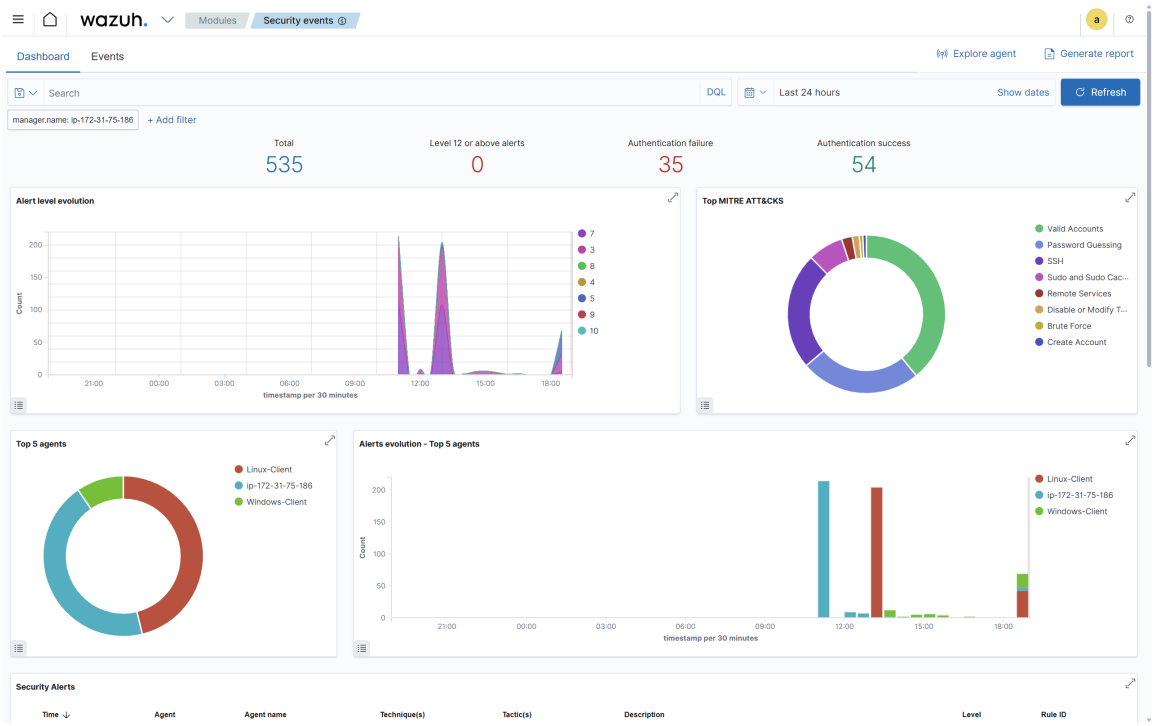

FIGURE 17 – Wazuh Security Events Dashboard

3.3 Agent Enrollment and Status

3.3.1 Linux Agent Connection

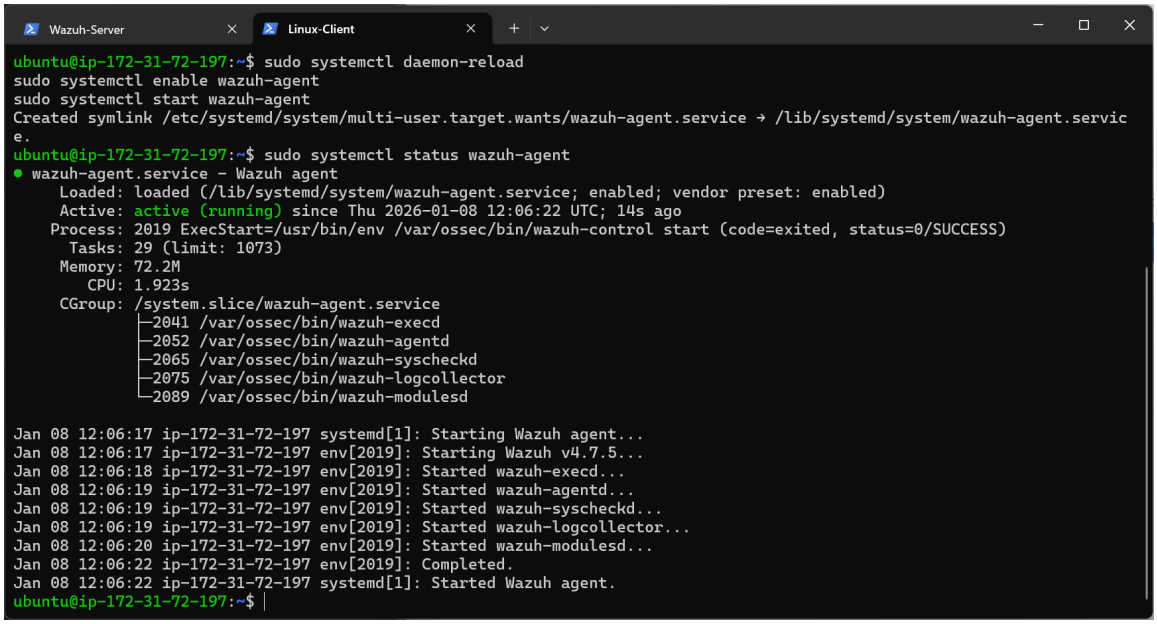

FIGURE 18 – Linux Agent Running and Connected

3.3.2 Windows Agent Connection

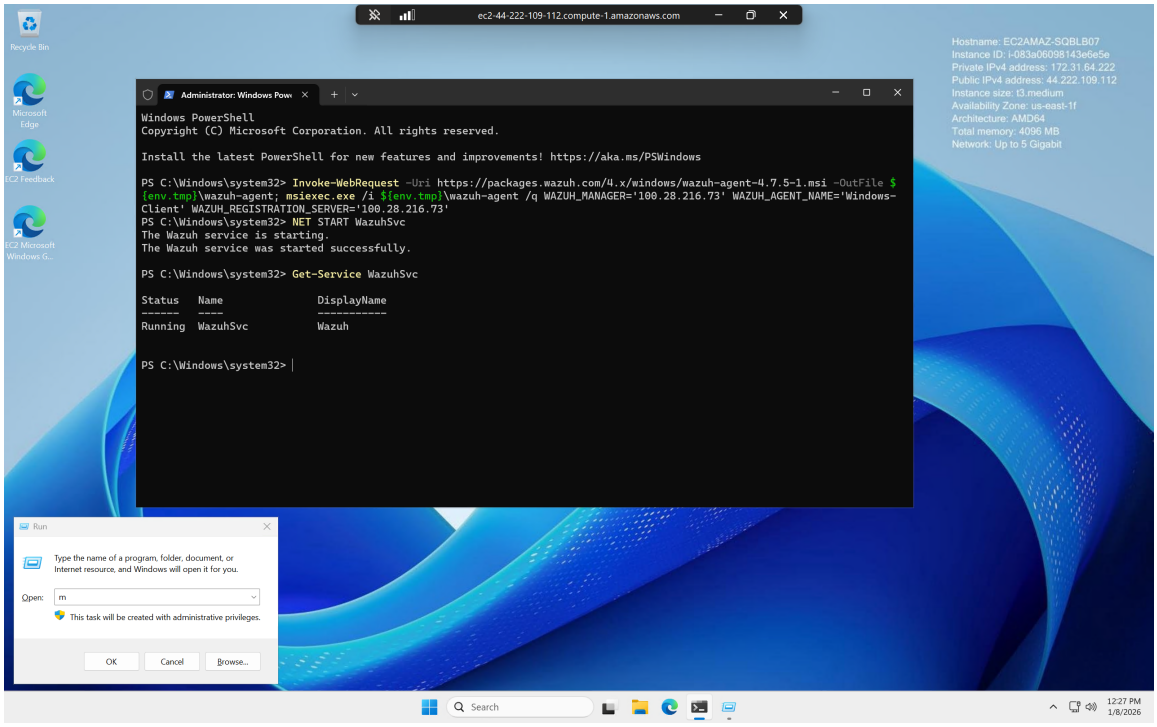

FIGURE 19 – Windows Agent Connecting to Wazuh Server

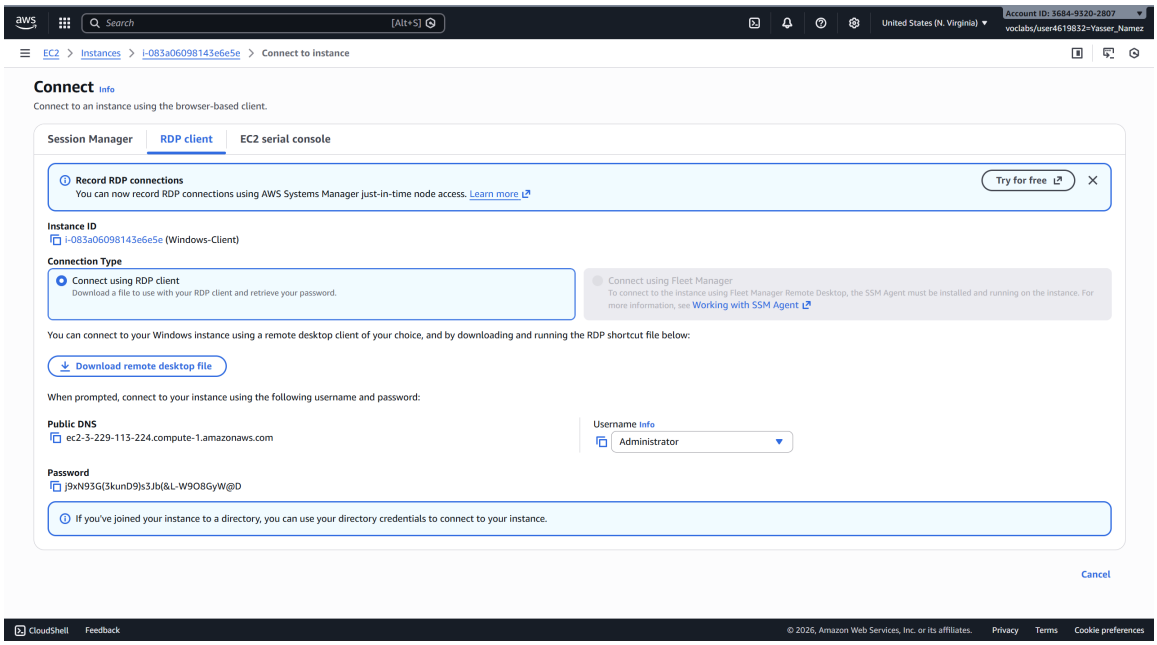

FIGURE 20 – Windows Client Agent Connection Status

3.4 Active Agents Overview

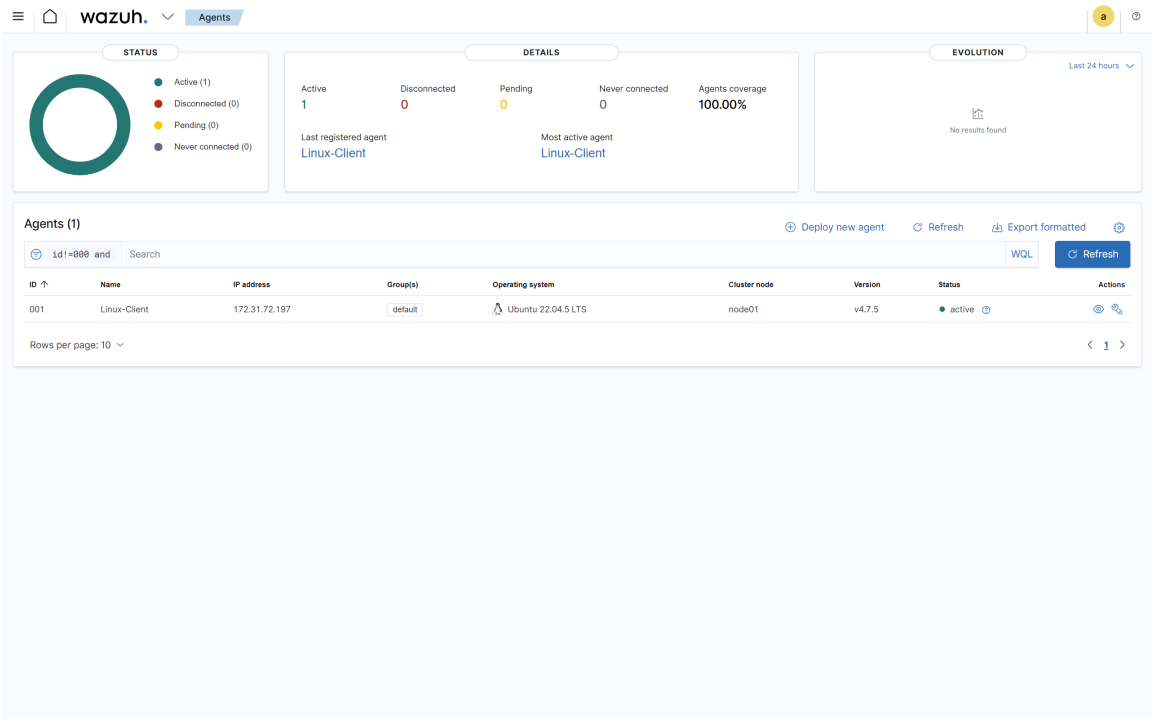

FIGURE 21 – Active Agents Dashboard View 1

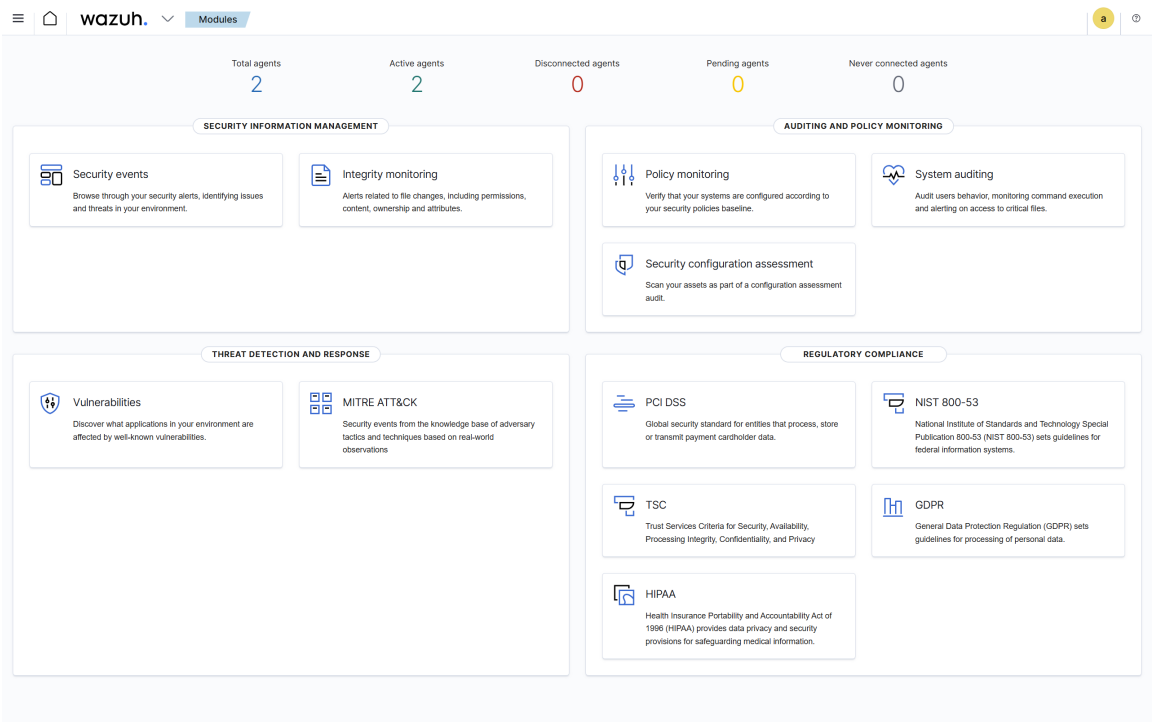

FIGURE 22 – Active Agents Dashboard View 2 - Both Agents Connected

Agent Name	IP Address	OS	Status	Version	
Linux-Client	10.0.1.20	Ubuntu 22.04	**Active**	4.x	
Windows-Client	10.0.1.30	Windows Server 2022	**Active**	4.x	

TABLE 3 – Connected Agents Summary

4 Security Events - Linux Client

This section documents the security alerts captured from the Linux client (Ubuntu 22.04) demonstrating Wazuh's detection capabilities for common attack patterns and security events.

4.1 Alert 1 : SSH Brute Force Attack

SSH Authentication Failure Detection

Rule IDs : 5710, 5712, 5720 (Progressive Severity)
Severity Level : 5-10 (Medium to High)
MITRE ATT&CK : T1110 - Brute Force

4.1.1 Attack Simulation

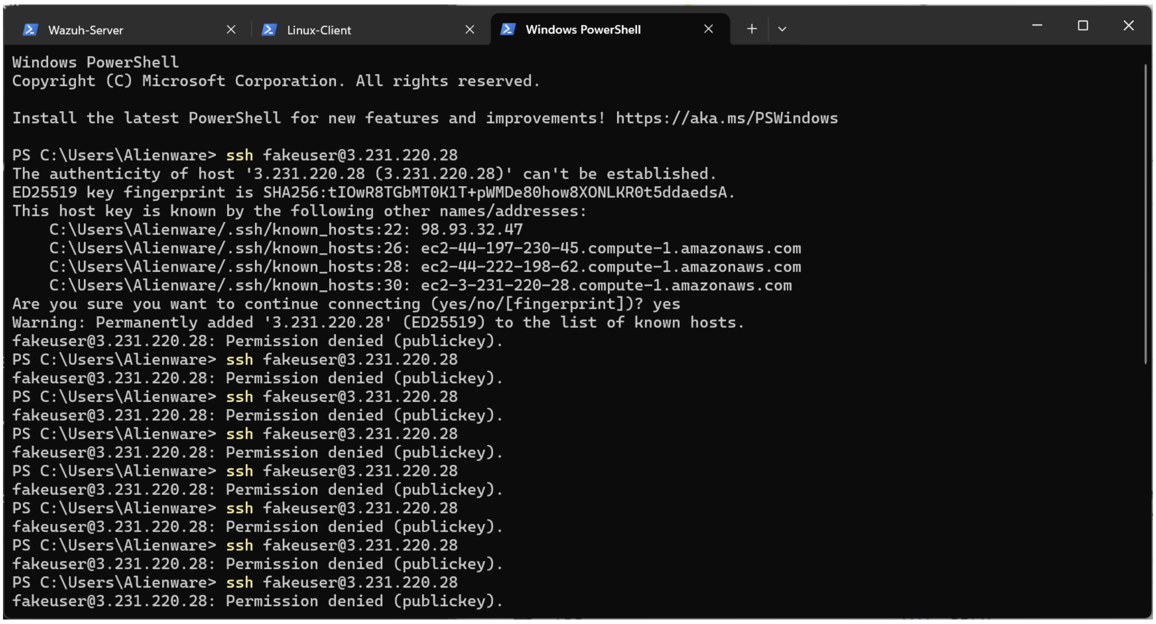

FIGURE 23 – SSH Brute Force Attack Simulation in Terminal

4.1.2 Wazuh Detection

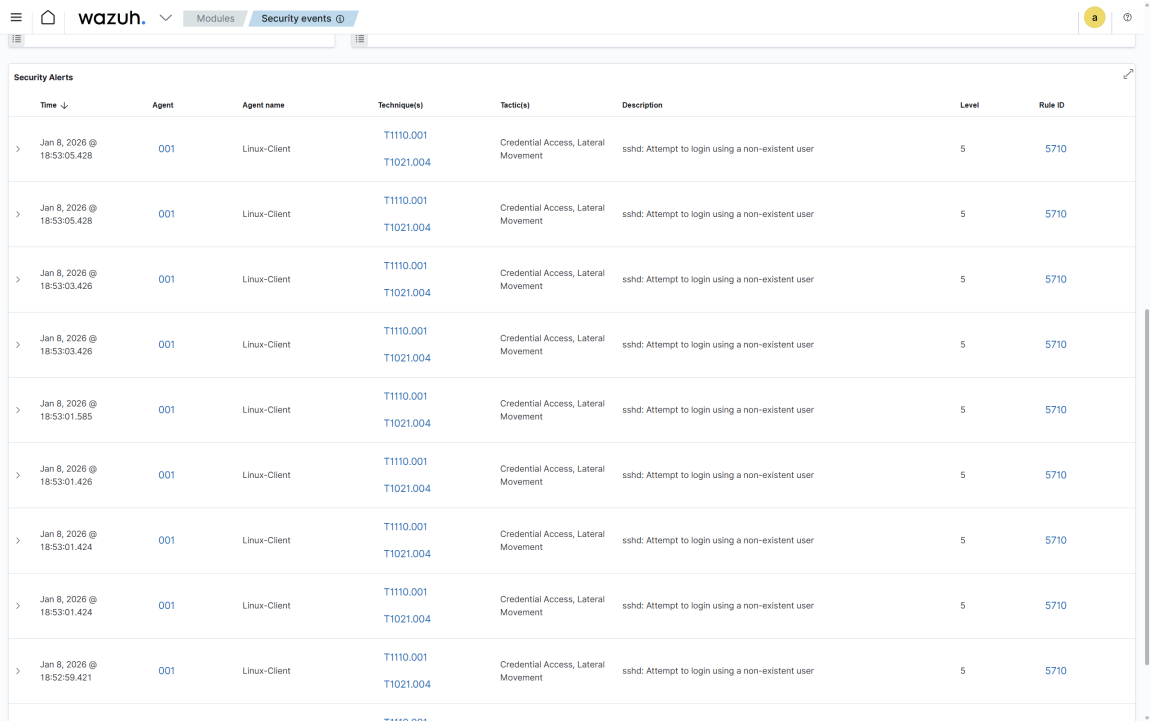

FIGURE 24 – SSH Failed Authentication Events Detected by Wazuh

4.1.3 Event Details

Attribute	Value
Log Source	/var/log/auth.log
Event Type	SSH Authentication Failure
Detection Pattern	Multiple consecutive failed login attempts
Source IP	External attacker IP
Target User	root, admin, ubuntu (common usernames)

TABLE 4 – SSH Brute Force Alert Details

4.1.4 Security Implication

— **Risk :** Potential unauthorized access attempt via credential guessing

— **Recommendation :** Implement fail2ban, use SSH key authentication, disable root login

— **Response :** Block source IP at firewall, review successful authentications

4.2 Alert 2 : Privilege Escalation (Sudo)

Privilege Escalation Detection

Rule IDs : 5402, 5401
Severity Level : 3-5 (Low to Medium)
MITRE ATT&CK : T1548 - Abuse Elevation Control Mechanism

4.2.1 Wazuh Detection

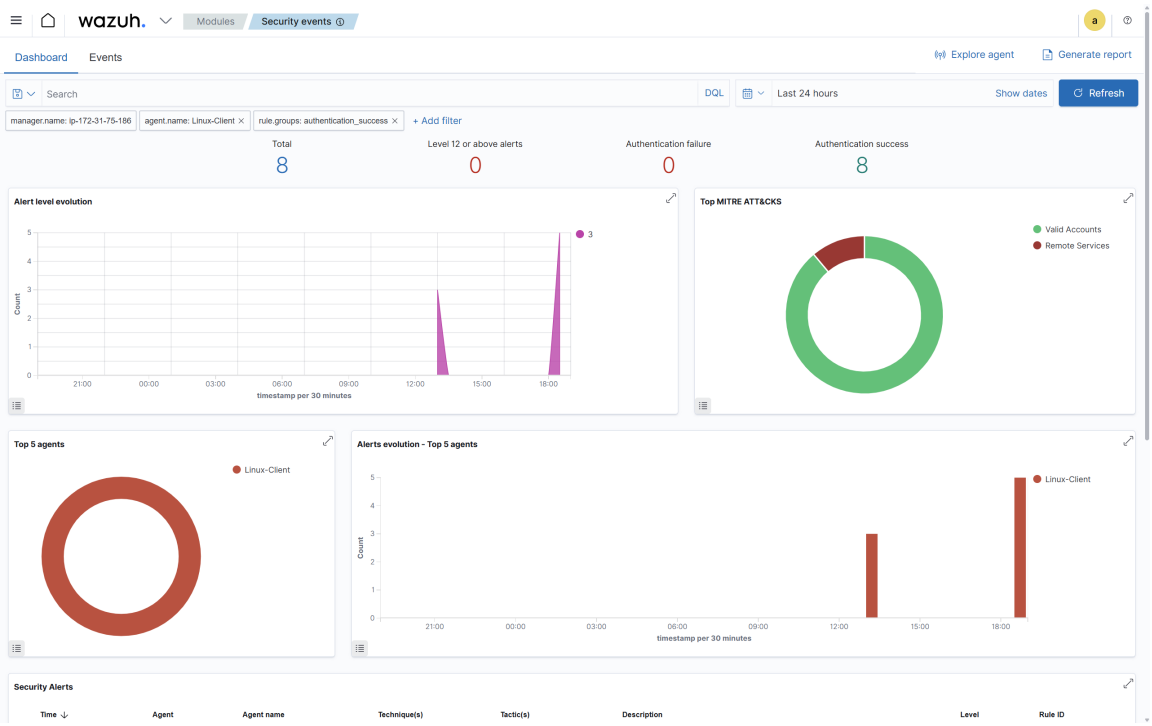

FIGURE 25 – Successful sudo to ROOT Execution Detected

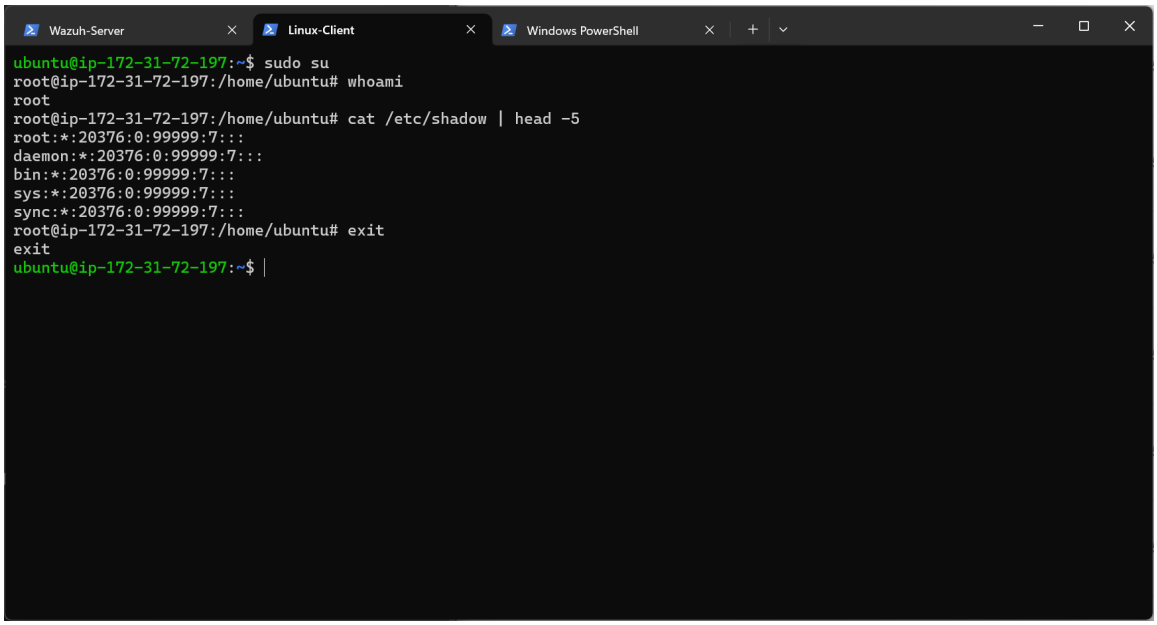

FIGURE 26 – Privileged Root Access Event Details

4.2.2 Event Details

Attribute	Value
Log Source	/var/log/auth.log
Event Type	Successful sudo execution
User	ubuntu
Command	su (switch user to root)
Target User	ROOT

TABLE 5 – Privilege Escalation Alert Details

4.2.3 Security Implication

— **Context :** May be legitimate administrative activity
— **Monitoring Value :** Critical for detecting unauthorized privilege escalation
— **Best Practice :** Implement just-in-time privilege access, log all sudo commands

4.3 Alert 3 : File Integrity Monitoring (FIM)

File Integrity Change Detection

Rule IDs : 550, 553
Severity Level : 7 (High)
MITRE ATT&CK : T1078 - Valid Accounts, T1136 - Create Account

4.3.1 Event Details

Attribute	Value
Detection Module	Syscheck (File Integrity Monitoring)
Monitored File	/etc/passwd
Change Type	Modified
Detection Method	Checksum comparison (MD5, SHA256)
Previous Hash	[Original file hash]
New Hash	[Modified file hash]

TABLE 6 – FIM Alert Details

4.3.2 Security Implication

- **Risk :** Critical system file modification may indicate :
  - Unauthorized account creation
  - Account manipulation by attacker
  - Potential system compromise
- **Response :** Immediately investigate file changes, compare with known-good baseline
- **Forensics :** Review file modification timestamps, correlate with authentication logs

5 Security Events - Windows Client

This section documents the security alerts captured from the Windows client (Windows Server 2022) demonstrating Wazuh's detection capabilities for Windows-specific security events, including enhanced EDR telemetry from Sysmon integration.

5.1 Alert 1 : Failed Logon Attempts

Windows Authentication Failure Detection

Windows Event ID : 4625
Wazuh Rule ID : 60122
Severity Level : 5 (Medium)
MITRE ATT&CK : T1110 - Brute Force

5.1.1 Wazuh Detection

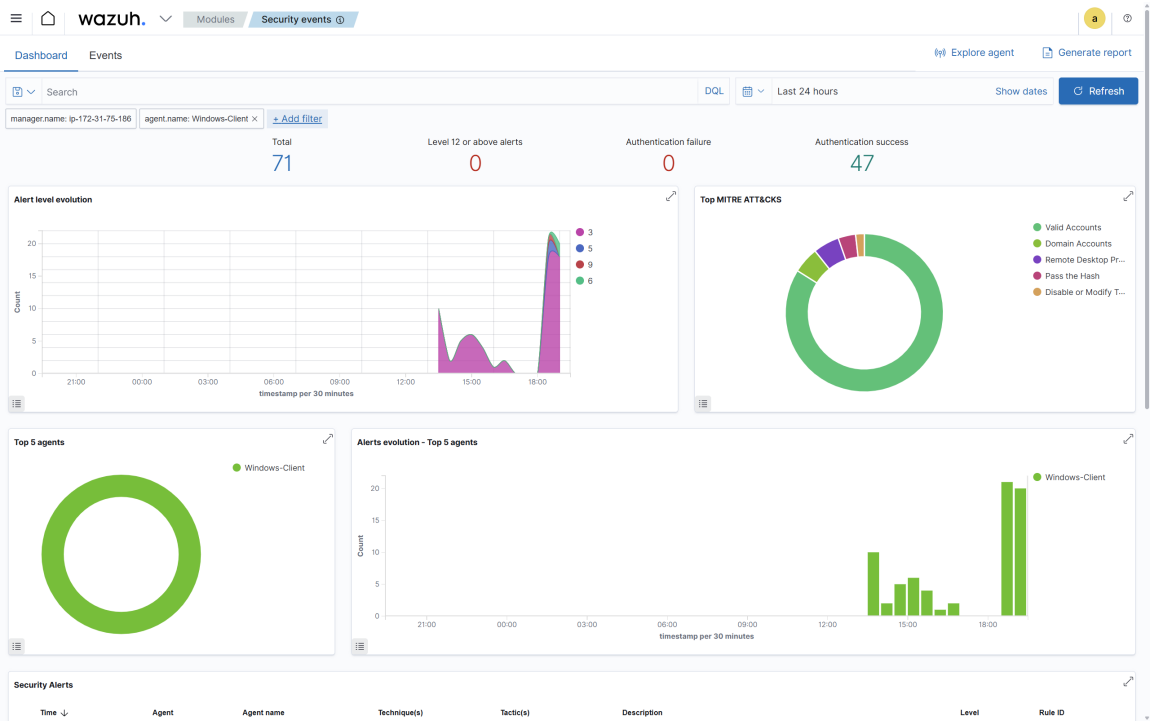

FIGURE 27 – Windows Failed Authentication Events in Wazuh Dashboard

5.1.2 Event Details

Attribute	Value
Event Source	Security Event Log
Event ID	4625 (Failed Logon)
Target Username	FakeUser
Logon Type	10 (RemoteInteractive / RDP)
Failure Reason	Unknown user name or bad password
Source Network Address	Attacker IP

TABLE 7 – Windows Failed Logon Alert Details

5.1.3 Security Implication

- **Risk :** Potential RDP brute force attack targeting the system
- **Recommendation :** Enable account lockout policies, implement Network Level Authentication (NLA)
- **Response :** Block source IP, enable MFA for RDP access

5.2 Alert 2 : User Account Creation and Group Modification (IAM)

User Account and Group Modification Detection

Windows Event IDs : 4720 (User Created), 4732 (Group Modified)
Wazuh Rule IDs : 60103, 60137
Severity Level : 8-10 (High to Critical)
MITRE ATT&CK : T1136 - Create Account, T1078.003 - Local Accounts

5.2.1 Wazuh Detection

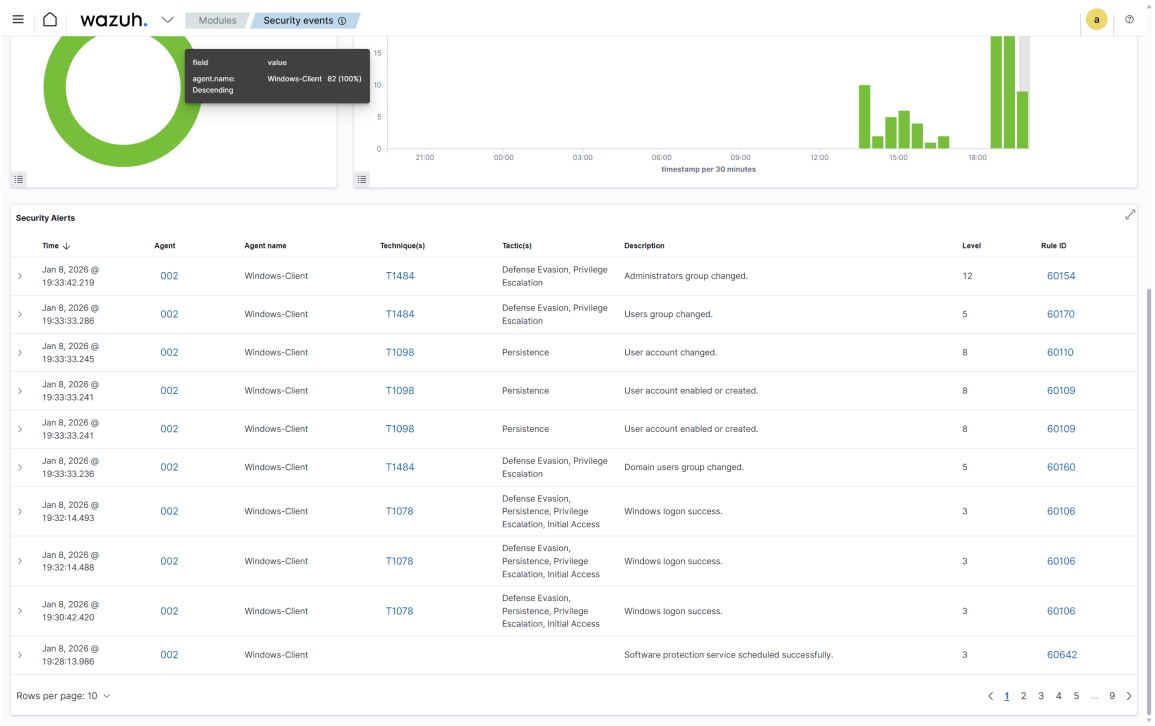

FIGURE 28 – User Account Creation and Security Group Modification Events

5.2.2 Event Details - User Creation (4720)

Attribute	Value
Event Source	Security Event Log
Event ID	4720 (User Account Created)
New Account Name	labuser
Created By	Administrator
Account Domain	WINDOWS-CLIENT

TABLE 8 – User Account Creation Alert Details

5.2.3 Event Details - Group Modification (4732)

Attribute	Value
Event Source	Security Event Log
Event ID	4732 (Member Added to Security-Enabled Local Group)
Target Group	Administrators
Member Added	labuser
Modified By	Administrator

TABLE 9 – Security Group Modification Alert Details

5.2.4 Security Implication

— **Monitoring Value :** Tracks all account creation and privilege changes
— **Risk :** Privilege escalation - new administrator account created
— **Response :** Validate authorization, review admin activity, check for lateral movement
— **Compliance :** Essential for SOX, PCI-DSS, HIPAA audit requirements

5.3 Alert 3 : Sysmon Process Creation (EDR)

Enhanced EDR Telemetry - Process Creation

Sysmon Event ID : 1 (Process Create)
Severity Level : Informational to High (context-dependent)
MITRE ATT&CK : Multiple (T1059, T1203, T1204)

5.3.1 Sysmon Events in Wazuh

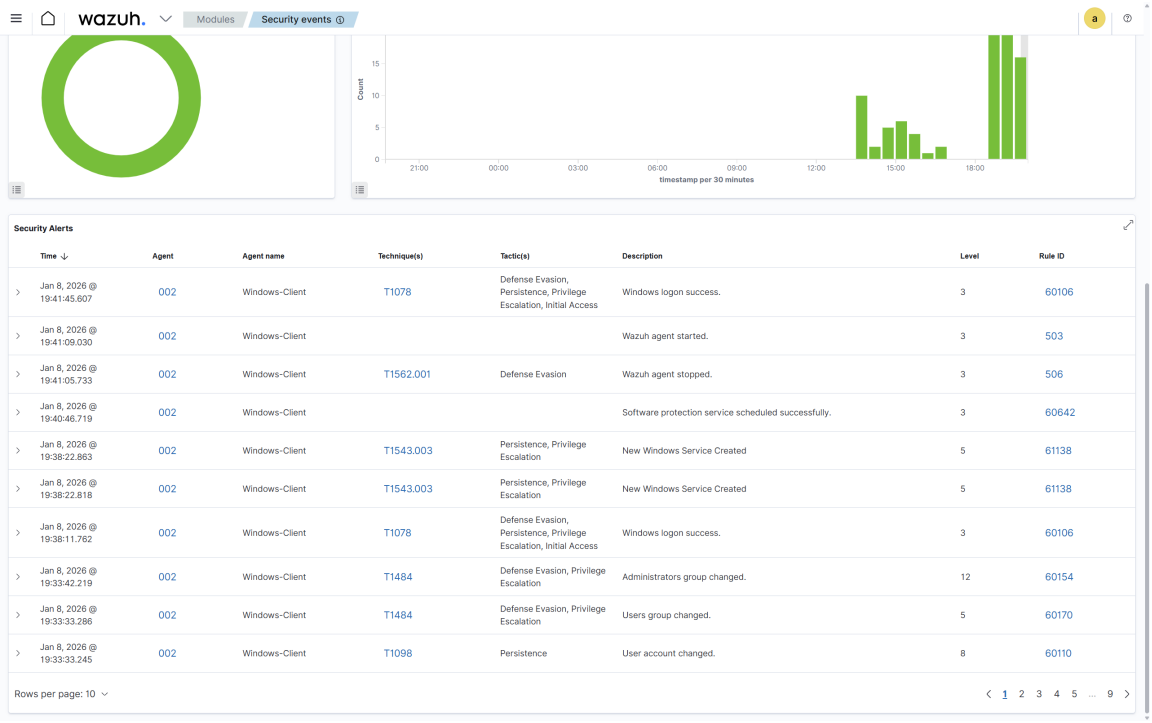

FIGURE 29 – Sysmon Events Overview in Wazuh Dashboard

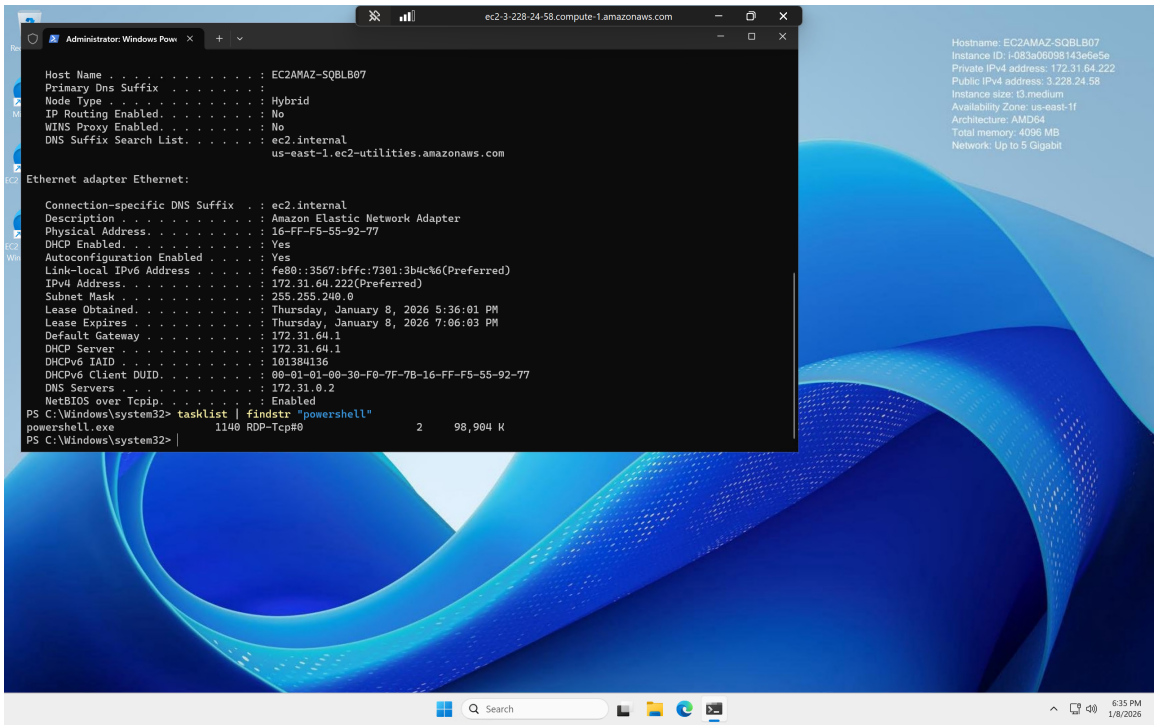

FIGURE 30 – Process Creation Events (Sysmon Event ID 1) Details

5.3.2 Event Details

Attribute	Value
Event Source	Microsoft-Windows-Sysmon/Operational
Event ID	1 (Process Create)
Image	Full executable path captured
CommandLine	Complete command-line arguments
ParentImage	Parent process that spawned this process
User	Execution context
Hashes	MD5, SHA256 file hashes

TABLE 10 – Sysmon Process Creation Event Details

5.3.3 EDR Value

- **Granular Visibility :** Full command-line arguments captured
- **Process Ancestry :** Parent-child process relationships tracked
- **Hash Collection :** File hashes enable threat intelligence correlation
- **Detection Capabilities :**
  - Living-off-the-land binary (LOLBin) attacks
  - Malicious script execution
  - Lateral movement patterns
  - Fileless malware detection

6 SIEM vs EDR - Comparative Analysis

6.1 SIEM (Security Information and Event Management)

Definition

SIEM is a centralized platform for log aggregation, correlation, and analysis that provides holistic visibility across an organization's IT infrastructure.

6.1.1 Key Capabilities Demonstrated in Lab

- **Log Collection :** Aggregation from multiple sources (Linux auth.log, Windows Event Logs)
- **Real-time Correlation :** Event correlation and alerting across systems
- **Centralized Visibility :** Single dashboard for heterogeneous environments
- **Compliance Support :** Audit trails for regulatory requirements
- **Historical Analysis :** Long-term data retention for forensic investigations

6.1.2 Lab Use Cases

- SSH brute force detection through authentication log analysis
- Centralized monitoring of multi-OS environment
- Rule-based alerting on security events
- Cross-system correlation (e.g., authentication events across Linux and Windows)

6.1.3 Strengths & Limitations

Strengths	Limitations
Broad infrastructure visibility	Relies on logs (may miss activity)
Compliance and audit support	Less granular endpoint visibility
Pattern recognition across systems	Reactive detection model
Long-term data retention	Requires proper log forwarding setup

TABLE 11 – SIEM Strengths and Limitations

6.2 EDR (Endpoint Detection and Response)

Definition

EDR is an agent-based solution providing deep endpoint visibility, behavioral analysis, and threat response capabilities at the process and file level.

6.2.1 Key Capabilities Demonstrated in Lab

- **Process Monitoring :** Sysmon Event ID 1 - detailed process creation tracking
- **Network Visibility :** Sysmon Event ID 3 - network connection monitoring
- **File Integrity :** FIM module detecting critical file changes
- **Command-line Visibility :** Full command-line argument capture
- **Process Ancestry :** Parent-child process relationship tracking
- **Hash Collection :** File hashes for threat intelligence correlation

6.2.2 Lab Use Cases

- Sysmon providing detailed process creation data with full command lines
- Process hash collection enabling malware analysis
- Behavioral analysis for detecting suspicious patterns
- Network connection monitoring for C2 detection

6.2.3 Strengths & Limitations

Strengths	Limitations
Deep endpoint visibility	Agent required on each endpoint
Behavioral detection capabilities	Higher resource consumption
Proactive threat hunting	Endpoint-focused (may miss network attacks)
Rich forensic data	Can generate high data volume

TABLE 12 – EDR Strengths and Limitations

6.3 Wazuh : Unified SIEM + EDR Platform

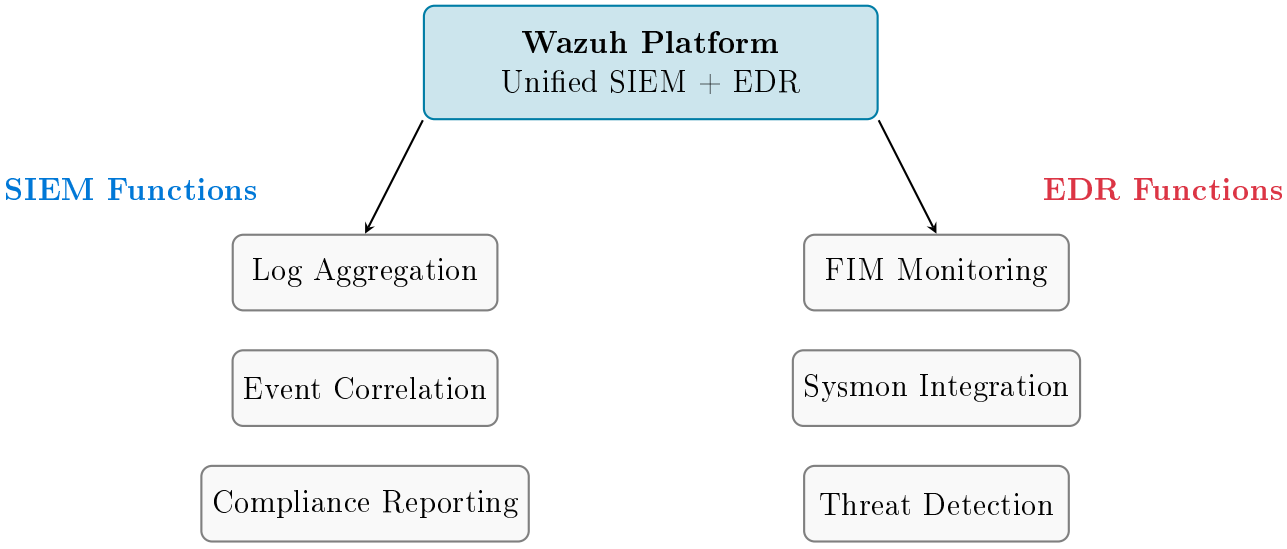

FIGURE 31 – Wazuh Unified SIEM + EDR Architecture

6.3.1 Demonstrated Integration Benefits

— **Single Pane of Glass :** Unified dashboard for all security operations
— **Cross-Domain Correlation :** Link endpoint activity with network/system logs
— **Reduced Tool Sprawl :** One platform instead of multiple point solutions
— **Cost-Effective :** Open-source solution with enterprise capabilities
— **FIM Bridge :** File Integrity Monitoring spans both SIEM and EDR domains
— **Enhanced Telemetry :** Sysmon integration provides deep EDR visibility

7 Identity and Access Management (IAM) & Privileged Access Management (PAM)

7.1 IAM Concepts Demonstrated

7.1.1 Authentication Monitoring

Event	ID	Security Value
Windows Failed Logon	4625	Track unauthorized access attempts
SSH Auth Failure	Rule 5710	Detect brute force attacks
Successful Auth	Various	Establish baseline behavior

TABLE 13 – Authentication Monitoring Events

7.1.2 Account Lifecycle Management

— **Windows Event 4720 :** User account creation detected and logged
— **Account Modifications :** All changes tracked through audit logs
— **Compliance Value :** Supports joiner/mover/leaver processes

7.1.3 Authorization & Privilege Changes

— **Windows Event 4732 :** Group membership changes monitored
— **Linux Sudo Tracking :** Full command history with user context
— **Detection :** Unauthorized privilege escalation attempts identified

7.1.4 Identity-Based Threat Detection

— Multiple failed logins indicate credential stuffing attempts
— Unusual authentication patterns signal compromised accounts
— Lateral movement detection through authentication correlation

7.2 PAM (Privileged Access Management) Relevance

7.2.1 Privileged Activity Monitoring

Activity	Monitoring Capability
Sudo Executions	Logged with timestamp, user, and full command
Windows Admin Actions	Tracked through security event logs
Root/SYSTEM Access	High-severity alerts generated

TABLE 14 – Privileged Activity Monitoring

7.2.2 Compliance Support

— **Least Privilege :** Visibility into who uses privileged accounts and when

— **Just-In-Time Access :** Logs validate that privileges used were authorized
— **Audit Trail :** Full documentation for SOX, PCI-DSS, HIPAA compliance
— **Anomaly Detection :** After-hours privileged access flagged

7.3 Lab Demonstration Summary

IAM/PAM Lab Activities

1. Created user "labuser" on Windows (Event 4720)
2. Added "labuser" to Administrators group (Event 4732)
3. Monitored sudo usage for privilege escalation (Rule 5402)
4. Tracked authentication attempts and failures across platforms
5. Established complete audit trail for identity-related activities

8 Threat Hunting - Sample Queries & Analysis

8.1 Query 1 : Failed Authentication Analysis

Objective

Identify potential brute force attacks or credential stuffing attempts across the infrastructure.

8.1.1 Wazuh Query

```
rule.groups:"authentication_failed" AND agent.name:"Linux-Client
    "
```

8.1.2 Analysis Approach

1. **Pattern Recognition :** Look for multiple failures from same source IP
2. **Timing Analysis :** Check intervals between attempts (automated vs manual)
3. **Correlation :** Link with successful authentication after failures
4. **User Enumeration :** Investigate which accounts are being targeted

8.1.3 Detection Indicators

— $>$ 5 failures within 5 minutes = likely automated attack
— Failures for multiple usernames = scanning/enumeration
— Geographic anomalies = authentication from unusual locations

8.1.4 Response Actions

1. Block source IP at firewall/security group
2. Implement account lockout policies
3. Enable MFA for targeted accounts
4. Review for any successful authentications from same source

8.2 Query 2 : Privileged Account Activity

Objective

Monitor for unauthorized privilege escalation or suspicious administrative activity.

8.2.1 Wazuh Query

```
(rule.id:5402 OR data.win.eventdata.eventID:4672)
AND NOT user.name:"expected_admin"
```

8.2.2 Analysis Approach

1. **Identify :** All sudo/administrator usage
2. **Filter :** Exclude known legitimate administrators
3. **Timing :** Check for unusual timing (after-hours, weekends)
4. **Correlate :** Link with other suspicious activities

8.2.3 Detection Indicators

— Privilege escalation by non-admin users
— Service accounts used interactively
— Unusual commands with elevated privileges
— Privilege use from unexpected systems/IPs

8.2.4 Response Actions

1. Validate whether privilege use was authorized
2. Review command history for malicious activity
3. Disable compromised accounts immediately
4. Initiate incident response if unauthorized

8.3 Query 3 : Process Anomaly Detection (EDR)

Objective

Identify suspicious process execution patterns indicating malware or living-off-the-land attacks.

8.3.1 Wazuh Query

```
data.win.system.eventID:1 AND
(data.win.eventdata.commandLine:(*powershell* AND *-enc*) OR
 data.win.eventdata.commandLine:(*cmd* AND */c* AND *certutil*))
```

8.3.2 Analysis Approach

1. **Encoded Commands :** Look for encoded PowerShell (common in malware)
2. **Process Relationships :** Identify unusual parent-child patterns
3. **LOLBins :** Check for system binaries used maliciously
4. **Network Correlation :** Link process creation with network connections (Sysmon Event 3)

8.3.3 Detection Indicators

— PowerShell with encoded commands (-enc, -EncodedCommand)
— cmd.exe spawning unusual children (certutil, bitsadmin, wmic)
— Processes running from temporary directories
— Suspicious parent processes (e.g., Excel spawning PowerShell)
— Processes with network connections to unknown IPs

8.3.4 Response Actions

1. Isolate affected endpoint immediately
2. Collect process memory dump for analysis
3. Check file hashes against threat intelligence
4. Review network logs for C2 communication
5. Initiate full forensic investigation

8.4 Threat Hunting Best Practices

Practice	Description
Time Correlation	Look for events within short timeframes
Baseline Normal	Understand typical activity before hunting anomalies
Pivot on Indicators	One suspicious event often leads to others
Document Findings	Maintain a hunting journal with queries and results
Continuous Improvement	Refine queries based on findings and new threats

TABLE 15 – Threat Hunting Best Practices

9 Conclusion

9.1 Skills Acquired Summary

This practical laboratory enabled the acquisition and validation of essential skills in operational cybersecurity :

- **Secure Cloud Architecture :** Design and deployment of AWS infrastructure with VPC, subnets, and security groups following the principle of least privilege
- **SIEM Administration :** Installation, configuration, and management of a Wazuh Manager server with its dashboard
- **Agent Deployment :** Enrollment and configuration of monitoring agents on heterogeneous systems (Linux/Windows)
- **Security Analysis :** Interpretation of alerts and correlation of security events
- **Threat Hunting :** Creation of proactive search queries for anomaly detection
- **EDR with Sysmon :** Configuration of advanced telemetry for Windows process monitoring

9.2 Importance of SIEM/EDR in a Modern SOC

In the current cyber threat landscape, SIEM and EDR solutions constitute the fundamental pillars of an effective Security Operations Center (SOC) :

Function	Value for SOC
Centralized Visibility	Aggregation of all security events in a single point
Real-Time Detection	Automatic alerts on suspicious behaviors
Incident Response	Rapid investigation and remediation capability
Compliance	Report generation for audits and regulations
Threat Intelligence	Alert enrichment with threat data

Table 16 – SIEM/EDR Value for SOC

9.3 Future Improvements

Several improvement areas can be considered to enhance this laboratory :

1. **SOAR Integration :** Incident response automation with playbooks
2. **Threat Intelligence Feeds :** Connection to external sources (MISP, VirusTotal)
3. **Machine Learning :** Anomaly detection based on machine learning
4. **Red Team Exercises :** Simulation of advanced attacks (APT, ransomware)
5. **Cloud SIEM :** Extension to other cloud providers (Azure, GCP)
6. **Kubernetes Monitoring :** Containerized environment surveillance

9.4 Acknowledgments

I would like to express my gratitude to :

— **Prof. Azeddine KHIAT** for his guidance and valuable advice throughout this Cloud Computing module

— **The Wazuh Team** for providing a professional-grade open-source solution

— **The Cybersecurity Community** for shared resources and documentation

Key Takeaway

This laboratory demonstrates that an open-source SIEM/EDR solution like Wazuh can provide enterprise-level protection while remaining accessible. The integration of SIEM and EDR capabilities in a unified platform reduces operational complexity and costs while providing comprehensive security visibility—an essential asset for modern security operations in cloud environments.

Project Source Code

https://github.com/yassernamez03/wazuh-siem-edr-cloud-lab

10 References

[1] **Wazuh Documentation** - Official Wazuh Platform Documentation
`https://documentation.wazuh.com`

[2] **AWS EC2 Documentation** - Complete Guide to Amazon EC2 Services
`https://docs.aws.amazon.com/ec2`

[3] **Sysmon Documentation** - Microsoft Sysinternals System Monitor
`https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon`

[4] **MITRE ATT&CK Framework** - Knowledge Base of Adversary Tactics and Techniques
`https://attack.mitre.org`

[5] **AWS VPC Documentation** - Virtual Private Cloud Configuration
`https://docs.aws.amazon.com/vpc`

[6] **NIST Cybersecurity Framework** - Cybersecurity Reference Framework
`https://www.nist.gov/cyberframework`

[7] **CIS Benchmarks** - System Hardening Guidelines
`https://www.cisecurity.org/cis-benchmarks`