

Home SOC Lab — Wazuh SIEM Deployment

Cybersecurity Portfolio Project

Chas Carden | chascarden.com | github.com/ccard-tech | September 2026

Security Operations

SIEM

Blue Team

Network Security

Linux

Virtualization

Project Overview

I designed and deployed a multi-endpoint home Security Operations Center (SOC) lab using Wazuh as the SIEM platform. The lab simulates a real-world blue team environment: attack traffic is generated from a Kali Linux attacker machine, monitored endpoints report security events to the Wazuh Manager, and I investigate and document the resulting alerts — replicating the core workflow of a Tier 1 SOC analyst.

The goal was to build a practical, portfolio-quality project that demonstrates hands-on security operations skills beyond certifications alone.

Lab Architecture

Component	Role	OS / Tool	IP Address
X1 Carbon (host)	Wazuh SIEM Server	Ubuntu Server 24.04 LTS	10.0.30.10 (static)
Kali Linux VM	Attacker Machine	Kali Linux 2026.2	10.0.30.81
Metasploitable 3 VM	Vulnerable Target	Ubuntu 14.04 (Metasploitable 3)	10.0.30.8
UniFi UCG Max	Network Gateway	UniFi Network 10.37.1	10.0.30.1 (Lab VLAN)

Network Design

All lab machines run on an isolated **VLAN 30 (10.0.30.0/24)** configured on a UniFi UCG Max. Firewall rules prevent lab traffic from reaching the production network (192.168.1.0/24) or IoT VLAN (10.0.20.0/24), ensuring attack traffic stays fully contained. The lab VLAN retains internet access for package updates and threat intelligence feeds.

Attack Flow:

```
Kali Linux (10.0.30.81)
↓ runs nmap, Hydra, Metasploit
↓
Metasploitable 3 (10.0.30.8)
↓ Wazuh agent detects events
↓
Wazuh Manager (10.0.30.10)
↓ correlates & alerts
↓
Wazuh Dashboard (HTTPS)
→ SOC analyst investigates
```

Tools & Technologies

Category	Tool / Technology	Purpose
SIEM Platform	Wazuh 4.9.2 (Manager + Indexer + Dashboard)	Log collection, correlation, alerting, compliance
Hypervisor	VirtualBox 7.0 on Ubuntu Server 24.04	Hosts Kali and Metasploitable VMs
Attacker	Kali Linux 2026.2	Offensive tools: nmap, Hydra, Metasploit, Nikto
Target	Metasploitable 3 (Ubuntu 14.04)	Intentionally vulnerable endpoint
Network	UniFi UCG Max + U6 Pro AP	VLAN segmentation, firewall policy, WiFi
OS (server)	Ubuntu Server 24.04 LTS	Wazuh host — headless, SSH-managed
Monitoring	Wazuh agents on all endpoints	Real-time log shipping to SIEM manager

What I Built & How

1. Network Isolation (UniFi VLAN)

Created a dedicated Lab VLAN (VLAN 30, 10.0.30.0/24) on a UniFi UCG Max with firewall rules blocking lab-to-production and lab-to-IoT traffic. Configured a dedicated Lab SSID for wireless lab device access. Solved a rule ordering limitation in UniFi Network 10.x by using IP range exclusions in the drop rule rather than separate allow/deny rules.

2. Wazuh SIEM Server

Deployed Wazuh 4.9.2 all-in-one (Manager, Indexer, and Dashboard) on a Lenovo X1 Carbon running Ubuntu Server 24.04 LTS with a static IP. Configured the server for headless operation (lid-closed, SSH-only access). Resolved several Ubuntu Server 24.04 boot issues including systemd-networkd conflicts with NetworkManager and WiFi driver dependencies.

3. Attacker VM (Kali Linux)

Imported and configured a Kali Linux VirtualBox VM (4GB RAM) bridged to the Lab VLAN. Enabled headless operation and SSH access. Installed and configured a Wazuh 4.9.2 agent on Kali so the SIEM can monitor the attacker machine itself — useful for detecting if a compromised attacker box is used as a pivot point.

4. Vulnerable Target VM (Metasploitable 3)

Deployed Metasploitable 3 (Ubuntu 14.04) as the primary attack target with a Wazuh agent reporting to the SIEM. This VM has dozens of intentional vulnerabilities across web, network, and system services — providing a realistic target for documented attack scenarios.

5. Multi-Agent SIEM Dashboard

Both endpoints (Kali and Metasploitable 3) appear as active agents in the Wazuh dashboard, generating real-time security events. The dashboard provides visibility into file integrity monitoring, vulnerability detection, log analysis, and network anomalies across all endpoints.

Attack / Detect / Document Cycle

The core workflow of this lab mirrors a real SOC environment. For each scenario:

- Run an attack technique from Kali against Metasploitable 3
- Monitor the Wazuh dashboard for triggered alerts
- Investigate the alert: identify the rule fired, affected endpoint, source IP, and timeline
- Map the technique to the MITRE ATT&CK framework
- Document what Wazuh caught, what it missed, and recommended remediation

Example Attack Scenarios

Technique	Tool	MITRE ATT&CK	Wazuh Detection
Network port scan	nmap -sV	T1046 — Network Service Discovery	Multiple connection attempts alert
SSH brute force	Hydra	T1110 — Brute Force	Authentication failure threshold alert
Web vulnerability scan	Nikto	T1190 — Exploit Public-Facing App	Web server anomaly alerts
FTP anonymous login	ftp / Metasploit	T1078 — Valid Accounts	Anonymous auth event logged

Skills Demonstrated

Skill Area	Specifics
SIEM Deployment & Admin	End-to-end Wazuh deployment, agent management, dashboard configuration
Network Segmentation	VLAN design, inter-VLAN firewall policy, UniFi UCG Max configuration
Linux Administration	Ubuntu Server 24.04, netplan/NetworkManager, systemd, SSH hardening
Virtualization	VirtualBox VM management, bridged networking, headless operation

Threat Detection	Alert investigation, MITRE ATT&CK mapping, rule analysis
Offensive Security (basic)	nmap, Hydra, Metasploit, Nikto — generating realistic attack traffic
Troubleshooting	Diagnosed VPN routing conflicts, boot service ordering, agent version mismatches

Key Challenges & How I Solved Them

Real-world problems encountered during setup — each one required diagnosis and a targeted fix:

ProtonVPN routing conflict: ProtonVPN on the Mac intercepted all 10.x.x.x traffic including the lab subnet, causing SSH to time out. Diagnosed by checking the routing table (`route get`) and identifying `utun4` as the culprit. Fixed with a static route: `sudo route add -net 10.0.30.0/24 192.168.1.1`, made permanent via a macOS LaunchDaemon plist.

UniFi 10.x firewall rule ordering: UniFi Network 10.37.x forces Accept rules below Drop rules in the policy table with no way to reorder them. Solved by redesigning the Drop rule to use IP range exclusions that skip the Mac's IP (192.168.1.1–.30 and .32–.254), eliminating the need for a preceding Accept rule.

Wazuh agent version mismatch: Kali's apt repo installed Wazuh agent 4.14.7 but the manager was 4.9.2 — agents must be equal or lower version. Pinned the install to the matching version: `apt install wazuh-agent=4.9.2-1`.

Ubuntu Server 24.04 WiFi boot hang: Server hung on boot waiting for the unused ethernet port before WiFi came up, requiring a physical console login before SSH became available. Fixed by masking `systemd-networkd-wait-online` which is not needed when NetworkManager handles networking.

Planned Enhancements

- Add Raspberry Pi 4 as a third monitored endpoint (IoT/embedded device simulation)
- Configure Wazuh active response to auto-block attacker IPs after failed login threshold
- Deploy DVWA (Damn Vulnerable Web App) for dedicated web attack scenarios (SQLi, XSS, LFI)
- Write custom Wazuh detection rules for lab-specific attack patterns
- Add a cloud VPS honeypot to generate and analyze real-world attack traffic
- Document full attack chains with evidence screenshots for each MITRE ATT&CK; technique

GitHub: github.com/ccard-tech **Portfolio:** chascarden.com **LinkedIn:** linkedin.com/in/chas-carden-12b931399