

Current State of my Homelab



Introduction

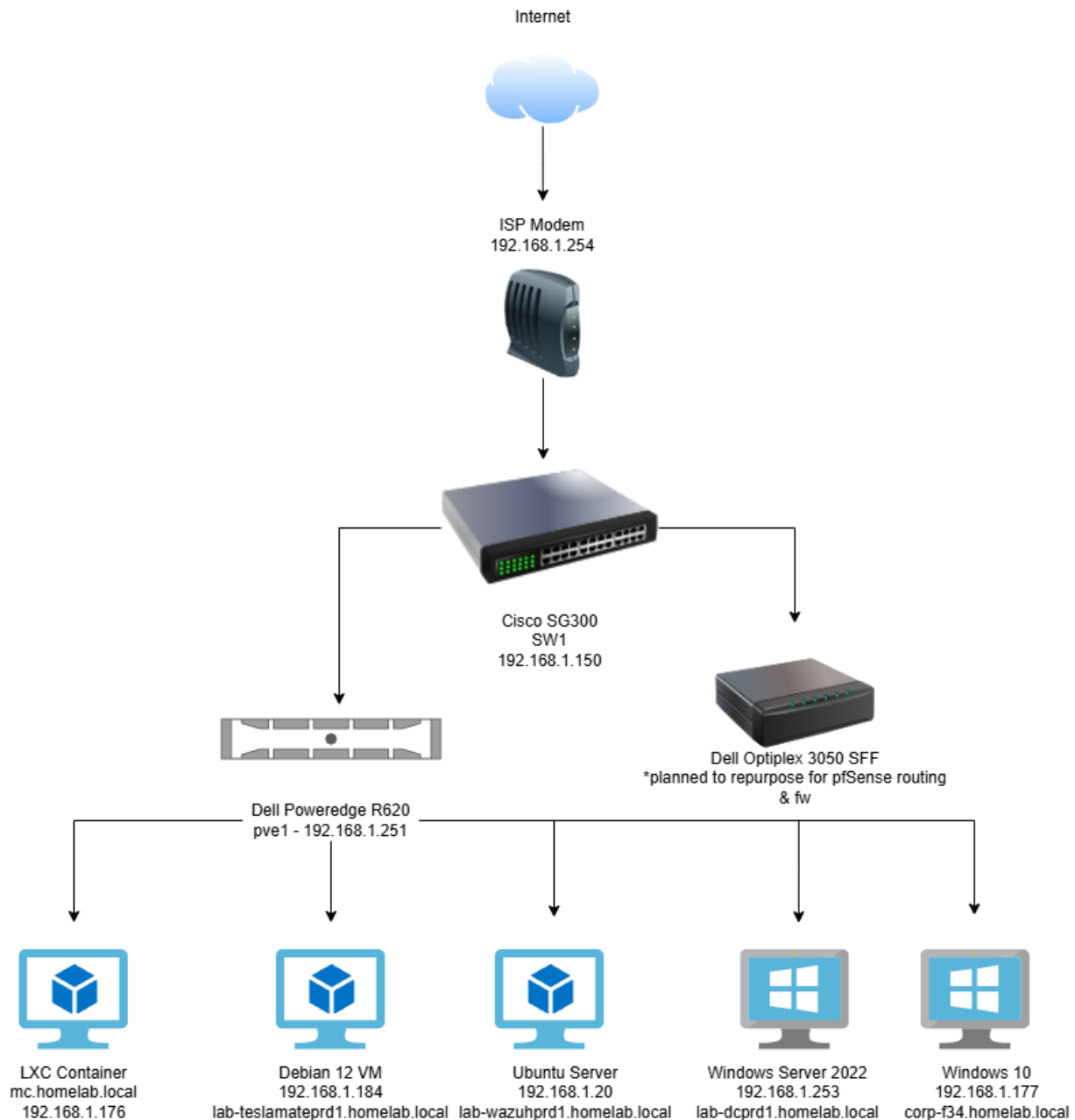
Collectively since October of 2025, I've been getting my hands on some hardware to build up my homelab. I've been able to obtain a Dell Optiplex 3050 SFF, Cisco SG300 switch, Dell Poweredge R620, and a Lenovo Thinkserver RD640 which sadly died on me shortly after purchasing it.

The goal of my homelab is to simulate a mock enterprise environment to simulate blue and red team activity, practice networking, while hosting some quality of life services that I can use on the daily.

Future Plans

- ☒ Deploy Wazuh SIEM and XDR agents on all endpoints
- ☐ Implement VLANs for services, DC, endpoints
- ☐ Enable port security on SG300
- ☐ Deploy [pfSense](#) for firewall and routing outside of ISP modem
- ☐ Tune and customize alert detections in Wazuh based off my environment
- ☐ Implement GPOs to mock an enterprise environment

Network Diagram

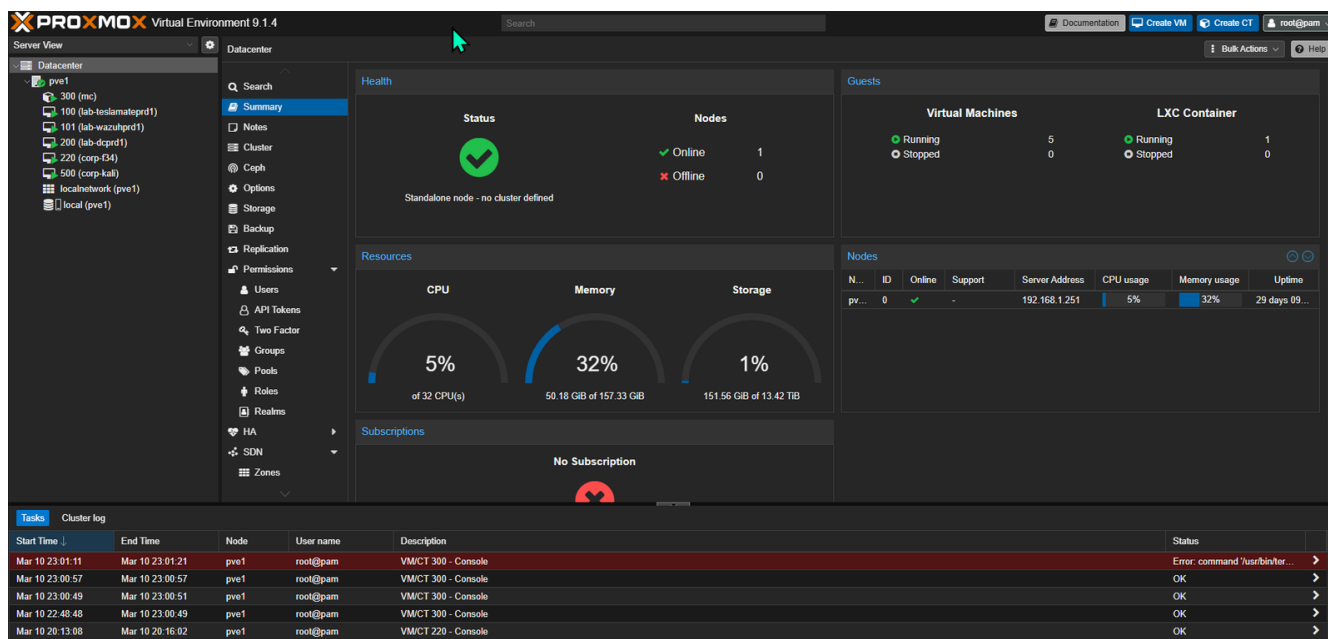


Hardware, VMs, Services

Cisco SG300

I recently obtained a Cisco SG300 in an effort to grow the homelab to mock an enterprise environment for best learning. The switch will also help me practice networking and switching commands as I study for the CCNA. As of right now, I intend to set up VLANs for the Windows DC, Windows endpoints, and different services (i.e., teslamate).

Dell Poweredge R620 / Proxmox VE Hypervisor



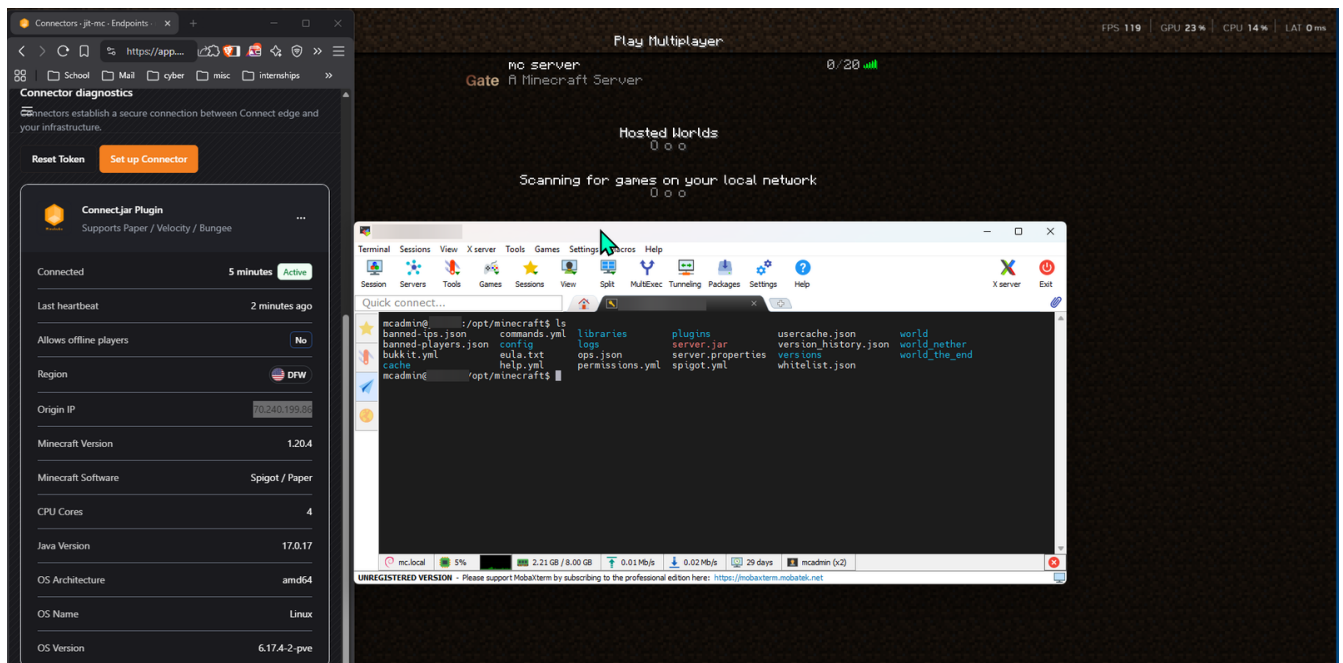
The absolute bread and butter of my homelab, I was able to snag this Dell Poweredge R620 with 160GB RAM, 2x Xeon E5-2640 v2 CPUs, and 3x 5TB HDD.

I deployed [Proxmox Virtual Environment \(VE\) 9.1](#) as my T1 Hypervisor. Within Proxmox, I deployed a LXC for self-hosting a minecraft server which rarely gets used, but why not? A Debian 12 VM for hosting [Teslamate](#), a self-hosted data logger via the Tesla API. Additionally, I've deployed Windows Server 2022 as a Domain Controller (homelab.local), which supports 1 Windows 10 endpoint (vulnerable). Lastly, a Kali Linux VM for practicing penetration testing/red teaming. Lastly, I deployed [Wazuh](#), an open source SIEM and XDR solution.

mc-homelab.local

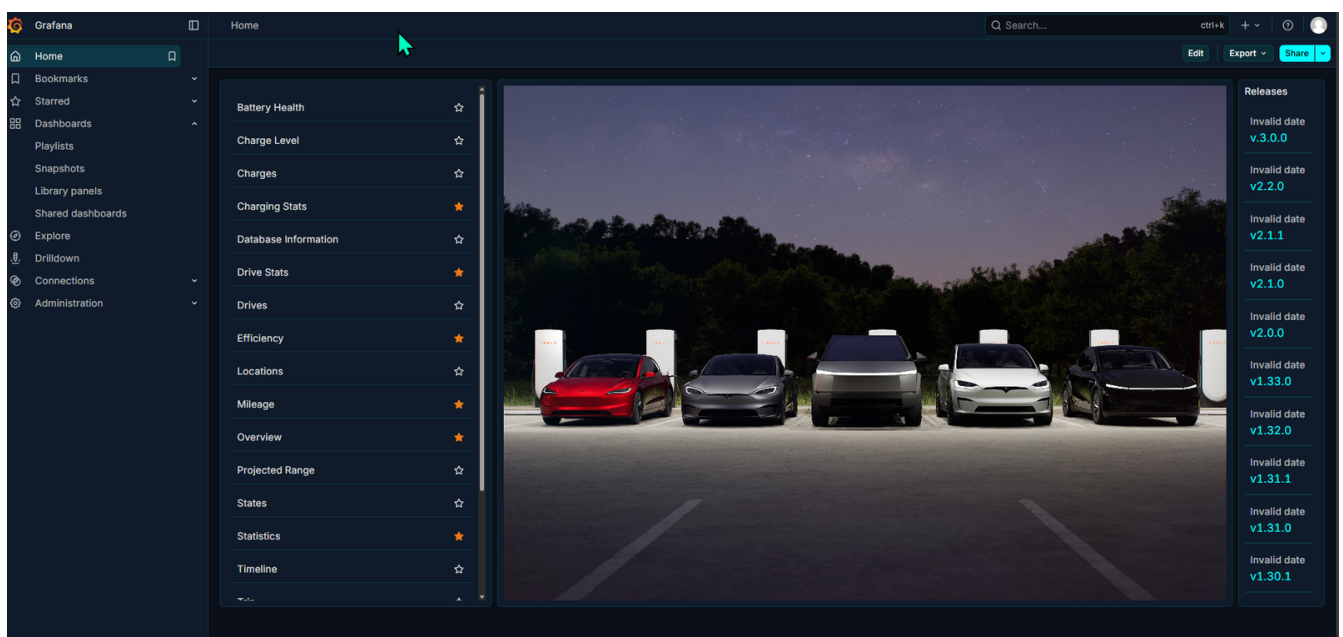
The Linux Container (LXC), supports a self-hosted minecraft server, averaging a daily 0 player count. To avoid port forwarding on my home network, I utilized a service called [Minekube Connect](#), functioning as a managed, cloud-based proxy network which allows me to serve a secure connection, without exposing my public IP, while also providing anti-DDoS protections.

I really just host this incase myself or any of my friends want to play on a server for us with 24/7 uptime to avoid purchasing a [Realm](#).



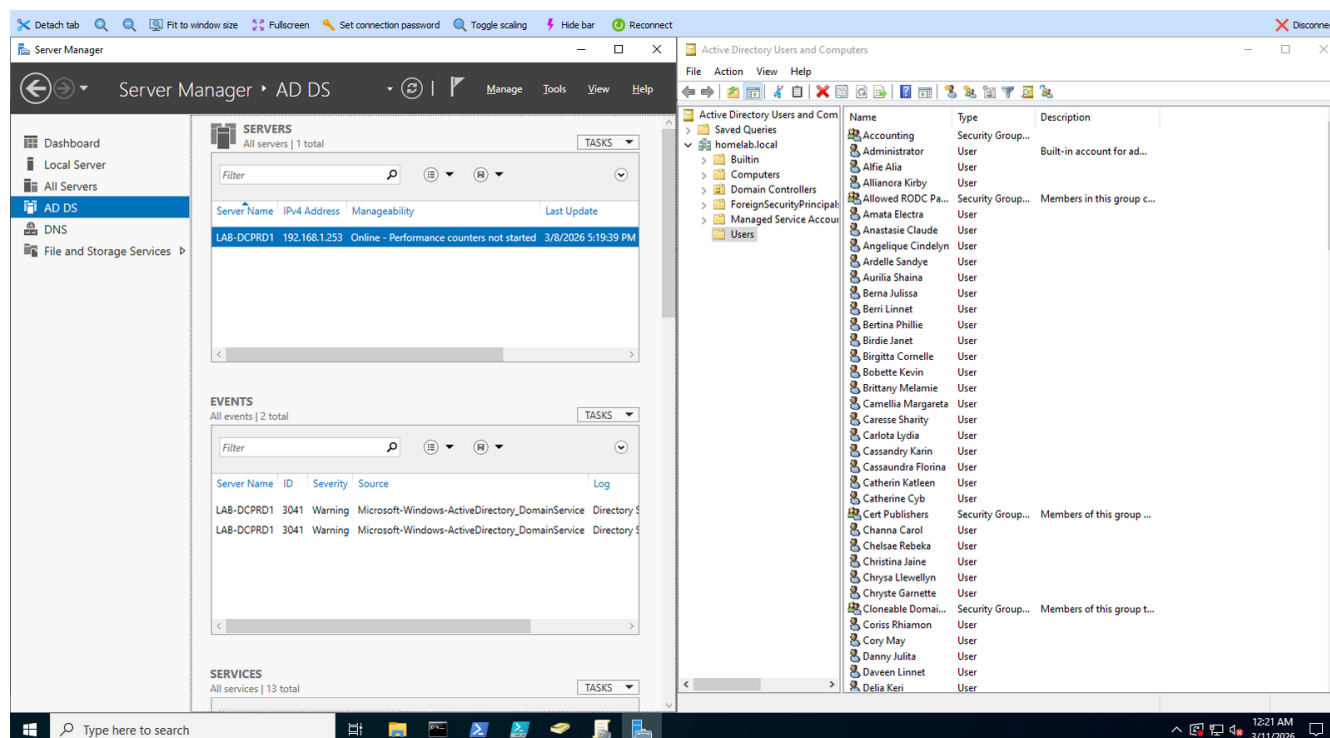
teslamateprd1.homelab.local

Teslamate, supported by a Debian 12 VM, is deployed through a Docker container, with a PostgresDB, which hosts the teslamate instance, and the main Grafana data visualizations. Teslamate provides a ton of analytics all passed through the Tesla API, which honestly provides more analytics and insight to your car than you need, but it is helpful for tracking the battery efficiency and degradation.



lab-dcprd1.homelab.local

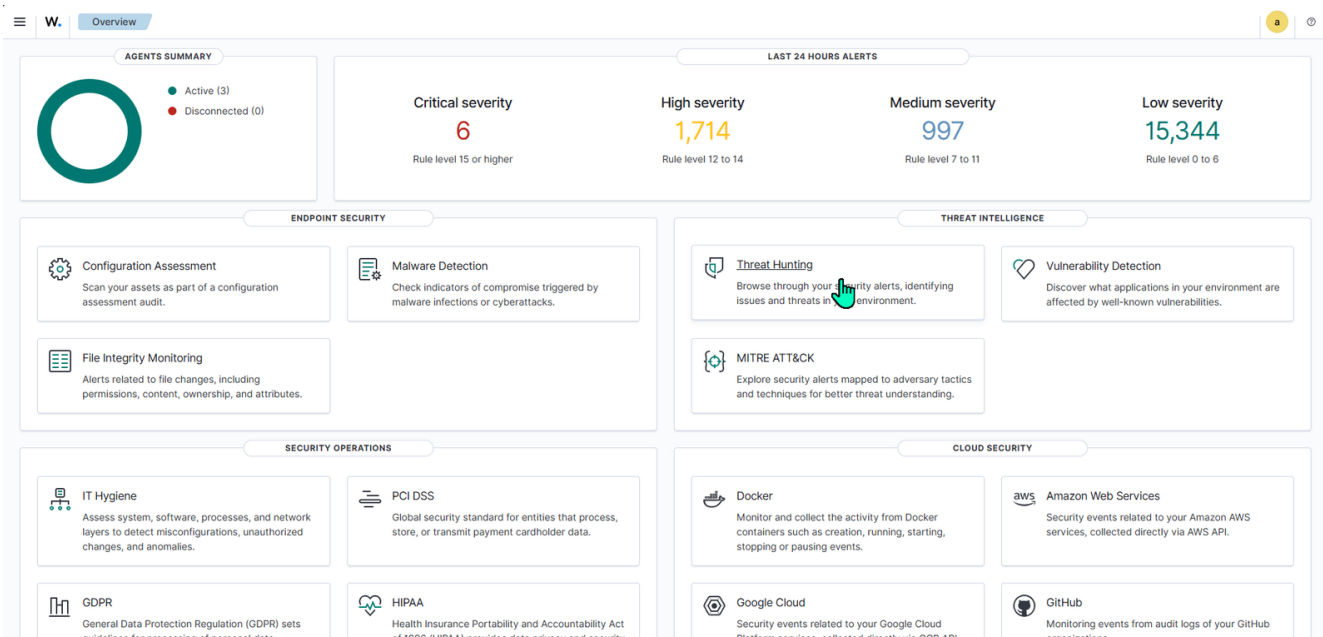
lab-dcprd1 functions as the domain controller for *homelab.local*, supporting 1 windows endpoint (*corp-f34*), in which I utilized [vulnerable AD](#) to purposefully deploy a vulnerable Active Directory environment for red teaming purposes. I have future plans to reset the Active Directory environment, and create automations for creating users, assinging/creating GPOs, etc.



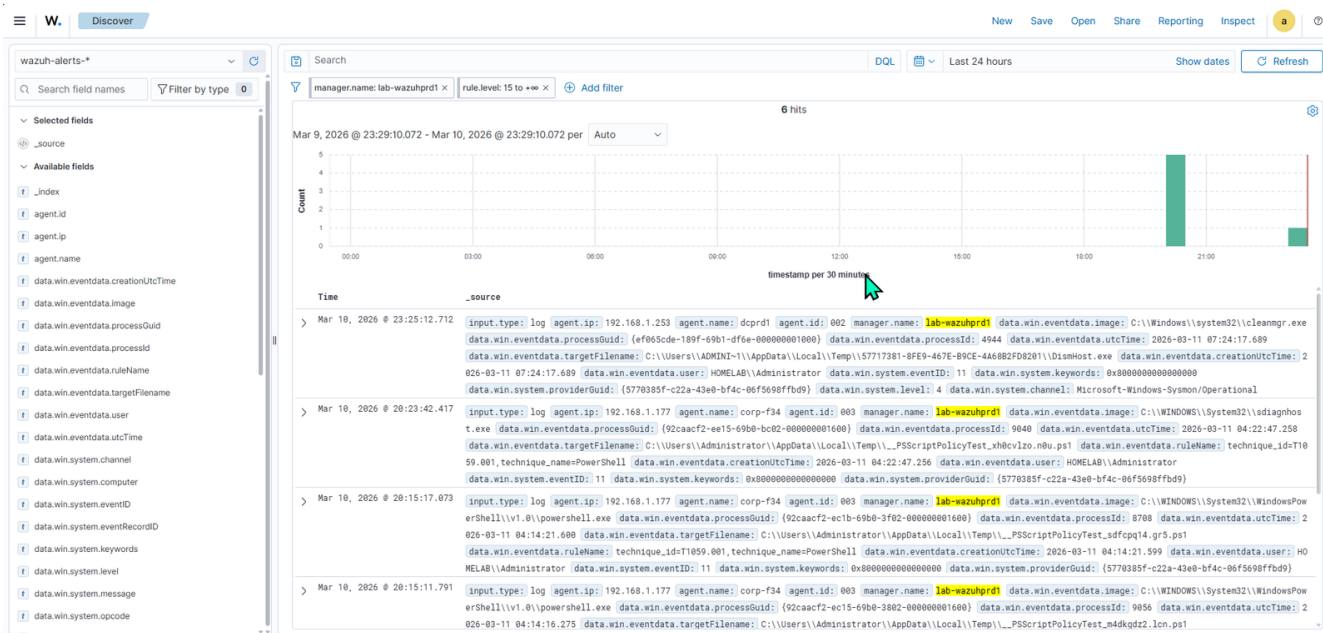
lab-wazuhprd1.homelab.local

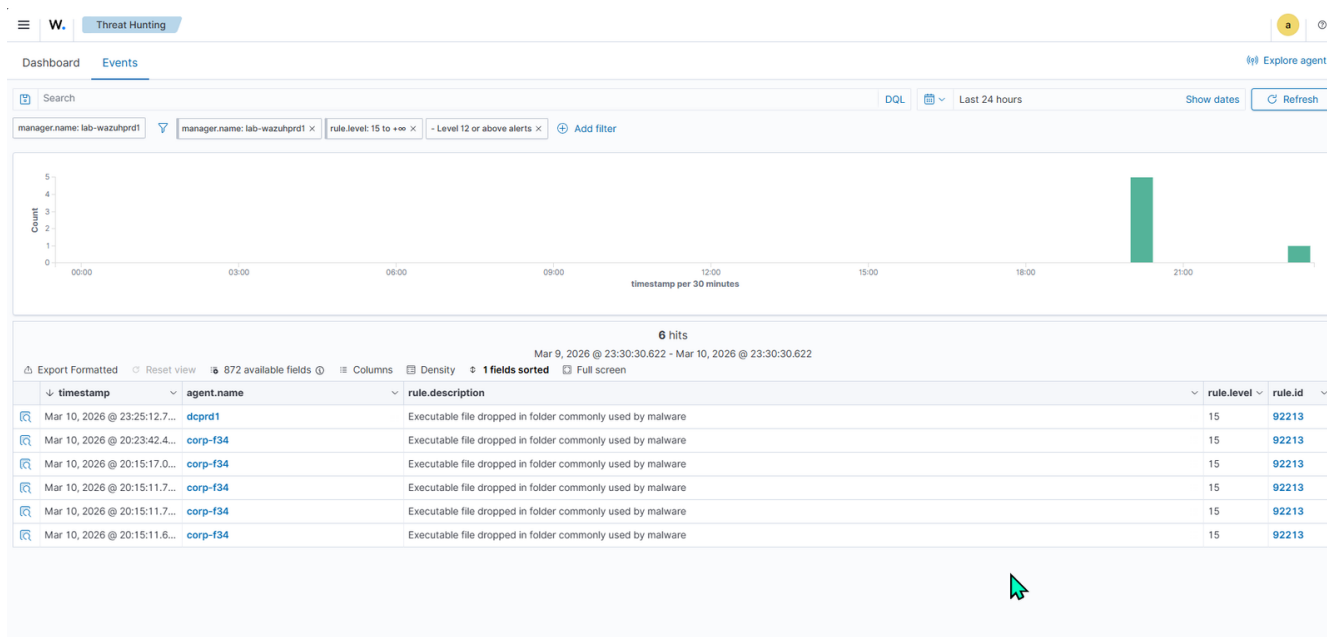
In an effort to get more hands on with SIEM and XDR tools, I deployed an open-source SIEM and XDR solution called [Wazuh](#). Currently I have the Wazuh XDR agent sitting on all endpoints and applicable VMs, with Sysmon telemetry ingesting into Wazuh. I have future plans to practice creating custom detections in my environment, while also tuning some alerts to avoid false-positives such as alerting on processes like Medal, Steam, which I have installed on my main computer.

This is the Wazuh dashboard, overviewing the amount of alerts in the last 24 hours.



This is the Explore/Threat Hunting section of Wazuh, visualizing ingested logs and providing alert information.





I do have future plans to migrate away from the Wazuh log visualization side of things, and implement the ELK Stack (Elasticsearch, Kibana, Logstash) to provide better visualization into log telemetry. Additionally, I'd like to explore the Elastic agent and see what it can offer alongside the Wazuh XDR agent.

Closing Thoughts & Future Plans

I've really enjoyed learning through this homelab, and I'm really excited to start practicing networking and start segmenting my home network. I'd really like to start diving deep into Active Directory, networking, and pfSense as mentioned in my future plans. pfSense will be a great project and great addition to securing my home network rather than relying on the generic ISP modem.



hunts.dev

Originally published on hunts.dev

<https://hunts.dev/blog/homelab/>