Malvertising: A Small SOC Implementation

CMIT-450-80: Senior Seminar Project

Instructor Michael Atwood

Kyle Hathaway

9.22.2025

Contents

Introduction

This project's goal is to build a home SOC lab using an Aruba switch, Cisco ASA, two host machines, Security Onion running in a VM, and three Windows 10 VMs. In this environment, I will ingest logs from the various sources into Security Onion. Additionally, I will conduct an OSINT research on a malvertising campaign, creating an intelligence brief with ATT&CK mapping and IOC tables. The OSINT investigation will be used to develop three detection rules and test them in simulations within the lab.

The product of this project will be a thorough and reproducible Blue Team package utilizing OSINT investigation to create detections, along with a demonstration featuring a timed incident drill in a home SOC lab. Deliverables for this project will be an OSINT intelligence brief on WinSCP malvertising with IOC tables and MITRE ATT&CK mapping. A detection pack of three rules created from the brief. A SOC evidence bundle consisting of configs and dashboards. An incident response playbook and timed drill report. All of this will be presented in a GitHub repository with a reproducible README.

Timeline

Week 3

- SOC Lab: Create repo, draft network diagram, spin up Security Onion and VMs, capture ASA baseline config.
- OSINT: Select a case and write the research question.
- Digital Evidence: Charter PDF, repo tree screenshot, network diagram, and ASA baseline config.

Week 4

- SOC Lab: Finish Security Onion config, enable Zeek/Suricata, configure ASA syslog, set up Aruba SPAN, and confirm first logs.
- OSINT: Start collection using URLScan, Virustotal, WHOIS, and create IOC>csv v0.1.
- Digital Evidence: Security Onion dashboard screenshots, Zeek/Suricata events.

Week 5

- SOC Lab: Spin up Windows VMs, forward security, and PowerShell logs.
- OSINT: Draft ATT&CK techniques list.
- Digital Evidence: Event ID samples,

Week 6

- SOC Lab: Finalize three simulations tied to the case.
- OSINT: Complete collection, draft methods, and findings sections.
- Digital Evidence: Simulation design document.

Week 7

- SOC Lab: Execute simulation #1, verify artifacts, and capture timestamps for MTTD.
- OSINT: Expand IOC tables.
- Digital Evidence: PCAP, Suricata alert detail, IOC.csv v0.2.

Week 8

- SOC Lab: Execute simulation #2. Create the first rule, begin building the FP/TP matrix.
- OSINT: Draft ATT&CK mapping.
- Digital Evidence: Rule v0.1 file, FP/TP matrix v0.1.

Week 9

- SOC Lab: Execute simulation #3, create rules two and three. Start the incident response runbook.
- OSINT: Continue to work on intel brief.
- Digital Evidence: Rules v0.2-0.3, runbook draft.

Week 10

- SOC Lab: Consolidate triage dashboards.
- OSINT: Finalize the intel brief.
- Digital Evidence: OSINT PDF v1.0.

Week 11

- SOC Lab: Drill rehearsal across all simulations, time triage steps for MTTR.
- OSINT: Publish IOC.csv v1.0 in repo.
- Digital Evidence: Simulation rehearsal notes.

Week 12

- SOC Lab: Formal timed drill.
- OSINT: Post-mortem on what intel improved and remaining gaps.
- Digital Evidence: Formal drill document.

Week 13

- SOC Lab: Export rules, dashboards, and runbook.
- OSINT: Polish report.
- Digital Evidence: Rules v1.0. README, screenshots.

Week 14

- SOC Lab: Final time for tweaks, notes.
- OSINT: Final polish.
- Digital Evidence: Submission includes an executive one-pager, an OSINT brief, an IOC.csv, a detection pack, an FP/TP matrix, Security Onion dashboard screenshots, an incident response runbook and drill timing table, and a repo README.

Summary

During the last week, I began building the hardware for the SOC lab. I wiped two host machines and installed Windows 10 Pro. On these two machines, I enabled Hyper-V. On Host 1, I installed Security Onion as a standalone deployment. On Host 2, I installed three Windows 10 Pro devices with moderate specifications. The networking equipment was reset to its defaults and configured with basic settings. Currently, the SOC lab has Security Onion running in a VM, but it is ingesting no logs. The other VMs are up and running. The networking equipment is configured to allow traffic to the internet.

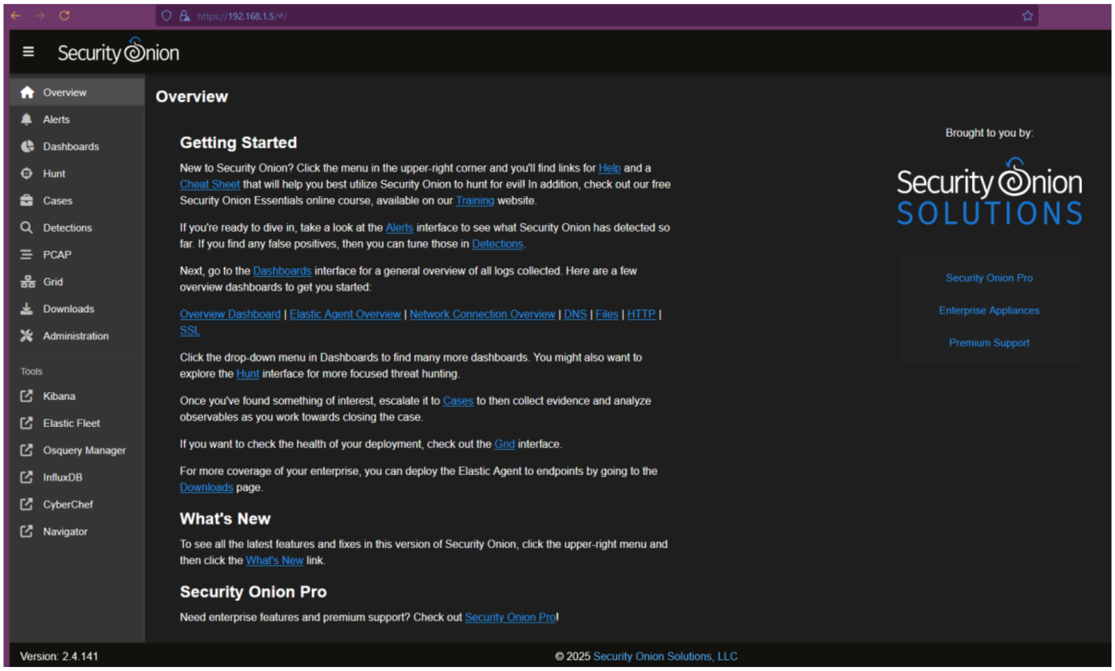
I ran into several issues this week. Starting with the hardware issues, my plans were immediately derailed when I realized that the devices I have would not run Security Onion 2, and getting Security Onion to run on what I have will be a stretch. Luckily, I dug out some extra RAM to plug into each machine. The extra RAM will allow Host 1 to run Security Onion with its required 16 GB. Host 2 will split its RAM between the three VMs and itself. Host 1, running SO, only has one NIC. It needed two to function properly. I used a USB to Ethernet cable for the monitoring NIC.

Installing the software was another problem. It took several attempts and a lot of googling to install SO properly. After which, I discovered that I had assigned the switch and the SO management console the same IP. I addressed that by changing the switch's IP address. Installing the Windows operating systems was more straightforward but still came with some struggles. On Host 2, I had to enable Hyper-V in the BIOS. After installing and spinning up the operating systems, I needed to assign network adapters and modify firewall rules so that I could ping each machine and access the internet.

I also created a GitHub repository and built out its structure. I had never used GitHub before, and understanding how to commit and push changes to the repository took me quite a while, and again, more googling. I built a network diagram, fleshed out a charter for the project, and pulled the initial configs for the firewall and the switch.

Evidence

Evidence this week will consist of a photo of the SOC lab, screenshots of Security Onion and GitHub repository, networking equipment configs, a network diagram, and a Project Charter. The Project Charter and network equipment configs will be submitted separately.



Overview

Getting Started

New to Security Onion? Click the menu in the upper-right corner and you'll find links for Help and a Cheat Sheet that will help you best utilize Security Onion to hunt for evil! In addition, check out our free Security Onion Essentials online course, available on our Training website.

If you're ready to dive in, take a look at the Alerts interface to see what Security Onion has detected so far. If you find any false positives, then you can tune those in Detections.

Next, go to the Dashboards interface for a general overview of all logs collected. Here are a few overview dashboards to get you started:

Overview Dashboard | Elastic Agent Overview | Network Connection Overview | DNS | Files | HTTP | SSL

Click the drop-down menu in Dashboards to find many more dashboards. You might also want to explore the Hunt interface for more focused threat hunting.

Once you've found something of interest, escalate it to Cases to then collect evidence and analyze observables as you work towards closing the case.

If you want to check the health of your deployment, check out the Grid interface.

For more coverage of your enterprise, you can deploy the Elastic Agent to endpoints by going to the Downloads page.

What's New

To see all the latest features and fixes in this version of Security Onion, click the upper-right menu and then click the What's New link.

Security Onion Pro

Need enterprise features and premium support? Check out Security Onion Pro!

Brought to you by:

Security Onion SOLUTIONS

Security Onion Pro

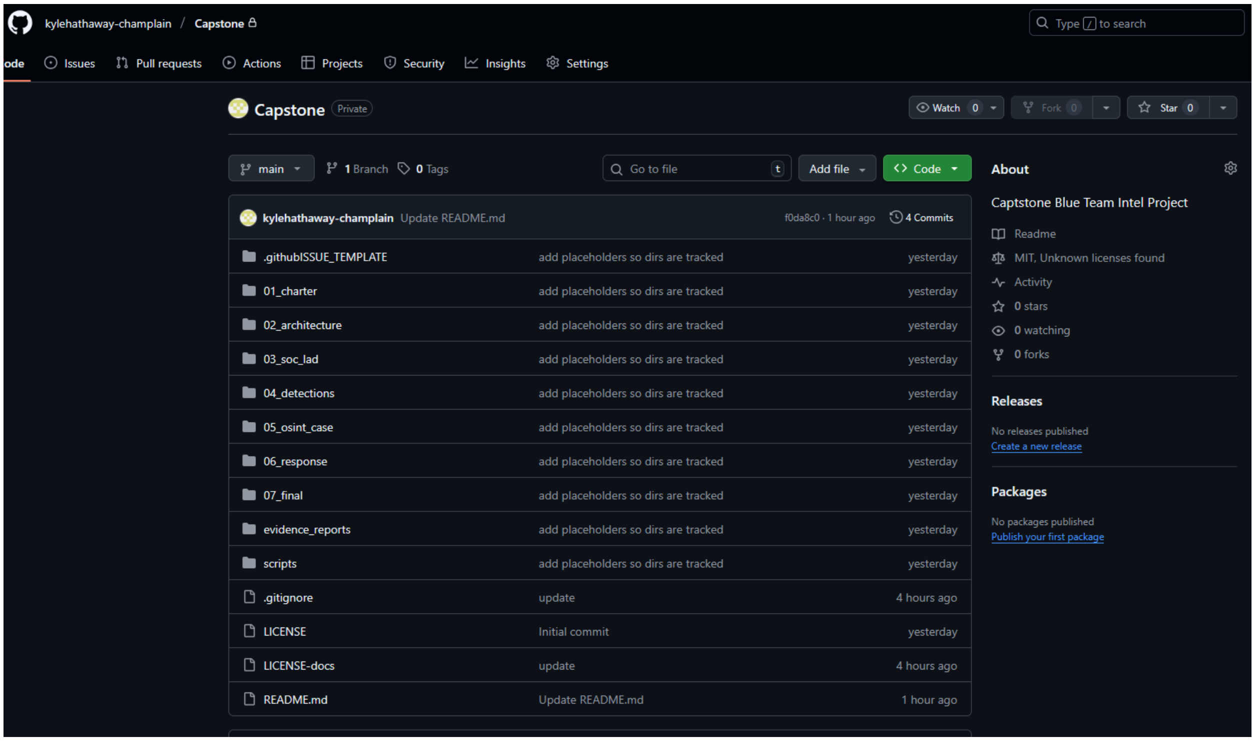
Enterprise Appliances

Premium Support

Version: 2.4.141

© 2025 Security Onion Solutions, LLC

Figure 1: Security Onion Management Dashboard



kylehathaway-champlain Update README.md f0da8c0 · 1 hour ago 4 Commits

.githubISSUE_TEMPLATE	add placeholders so dirs are tracked	yesterday
01_charter	add placeholders so dirs are tracked	yesterday
02_architecture	add placeholders so dirs are tracked	yesterday
03_soc_lad	add placeholders so dirs are tracked	yesterday
04_detections	add placeholders so dirs are tracked	yesterday
05_osint_case	add placeholders so dirs are tracked	yesterday
06_response	add placeholders so dirs are tracked	yesterday
07_final	add placeholders so dirs are tracked	yesterday
evidence_reports	add placeholders so dirs are tracked	yesterday
scripts	add placeholders so dirs are tracked	yesterday
.gitignore	update	4 hours ago
LICENSE	Initial commit	yesterday
LICENSE-docs	update	4 hours ago
README.md	Update README.md	1 hour ago

About

Captstone Blue Team Intel Project

- Readme
- MIT, Unknown licenses found
- Activity
- 0 stars
- 0 watching
- 0 forks

Releases

No releases published
Create a new release

Packages

No packages published
Publish your first package

Figure 2: GitHub Repository

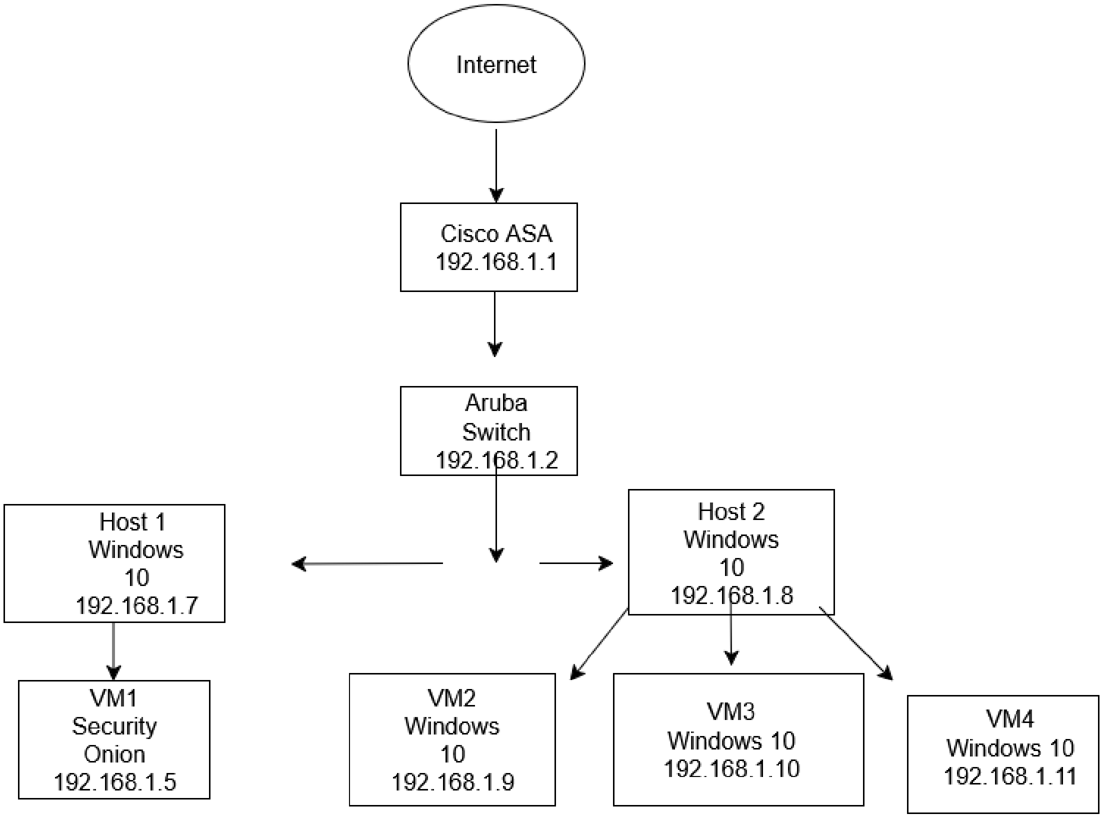

Internet
Cisco ASA 192.168.1.1
Aruba Switch 192.168.1.2
Host 1 Windows 10 192.168.1.7
Host 2 Windows 10 192.168.1.8
VM1 Security Onion 192.168.1.5
VM2 Windows 10 192.168.1.9
VM3 Windows 10 192.168.1.10
VM4 Windows 10 192.168.1.11

Figure 3: SOC Lab Network Diagram

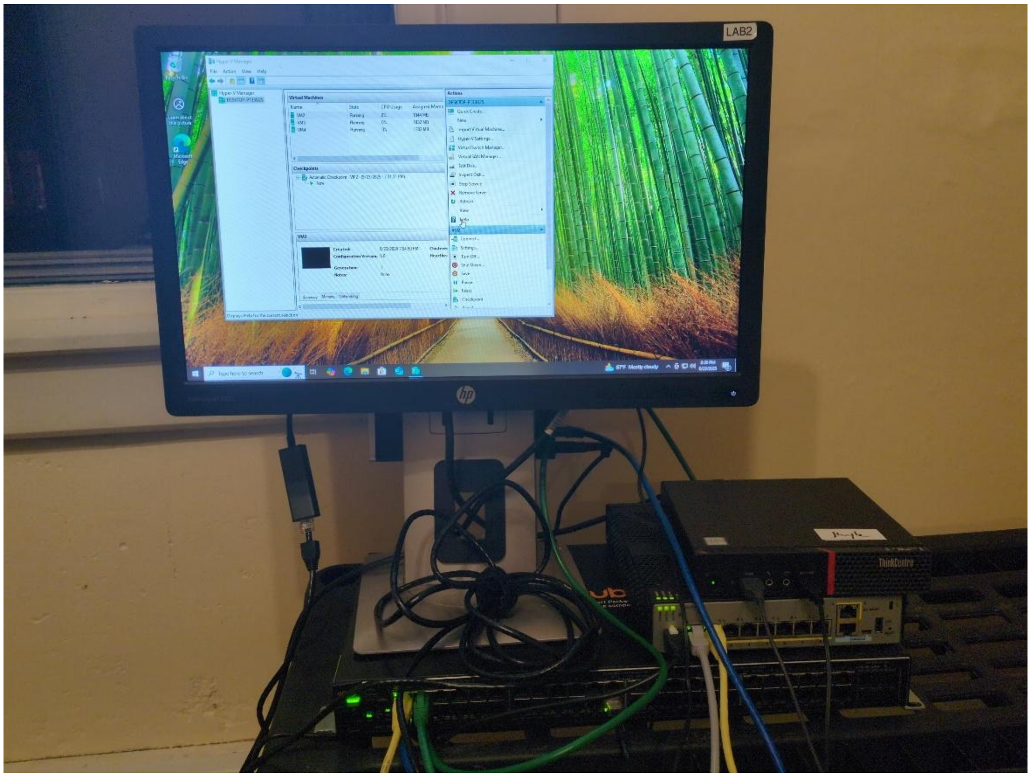


Figure 4: SOC Lab Physical Setup

Conclusion

These past few weeks have been challenging. I haven’t had the time, energy, or motivation to put towards this project. This past week has been great. Despite the issues and problems I ran into, I feel that this project is off to a good start. I am working hard to get back on my timeline, and I am hoping to begin to get a head start on this project. I am happy with where I am currently in this project. When I initially began to put this together, I thought I had taken on more than I could handle. I think now that I have started and things are starting to come together, I think this will be a manageable project. The only issue I am having now is staying on track and getting the work done in a timely fashion.