Malvertising: A Small SOC Implementation

CMIT-450-80: Senior Seminar Project

Instructor Michael Atwood

Kyle Hathaway

10.8.2025

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

These past few weeks have been very challenging. The project I have picked is more involved than I had initially thought. As I work through the phases, I am finding that I need to adjust the scope of what I am trying to accomplish with the time, tools, and skills that I have. I ran into multiple issues over the course of the last couple of weeks. My first and biggest issue is time management. There doesn't seem to be enough time in the day to make the necessary headway to meet the deadlines I have for this class. Moving forward, I

will need to allocate four or more hours a day to stay on track and to feel comfortable with my progress. The next biggest issue is gathering and organizing my data, evidence, and process in a way that makes sense. I have yet to understand GitHub and how best to organize everything. My OSINT investigation was another major struggle. I have been struggling to find relevant malicious domains that I can trace to a specific campaign. For now, I have begun finding malicious domains that seem to serve malicious files targeting IT professionals. These programs are WinSCP, TeamViewer, PuTTY, and AnyDesk. Additionally, I struggled to ingest logs into Security Onion. After fighting with both the Cisco firewall and the Aruba switch, I decided to pivot and focus on ingesting logs from the hosts and VMs.

Despite the struggles I have faced over the last few weeks, I have found some success. I was able to begin ingesting logs from a host machine. I fought with Winlogbeat for a number of days before I discovered that I could use the Elastic agent downloaded from Security Onion itself. Once the agent is installed, the IP range needs to be added to the host group in Security Onion to allow the logs to be ingested. In Figure 1, you can see the logs beginning to come into the Security Onion dashboard. Opening the Elastic Agent tab opens a new browser window. Once signed in, I was able to go over the configuration of the agent and manage what logs would be pulled into Security Onion. Figure 2 shows what can be managed in the console.

I have made good progress on the OSINT investigation. I have found a few malicious domains from which I will be able to derive IOCs and build detections off of. However, I need to reevaluate my research question and reframe exactly what I am searching for. At the moment, my investigation feels a little unfocused. Despite that, I am feeling good about the progress I have made with the investigation.

Evidence

The evidence this week will consist of my initial OSINT investigation, along with an appendix with screenshots of the evidence gathered. Additionally, I have provided evidence of logs being ingested into Security Onion.

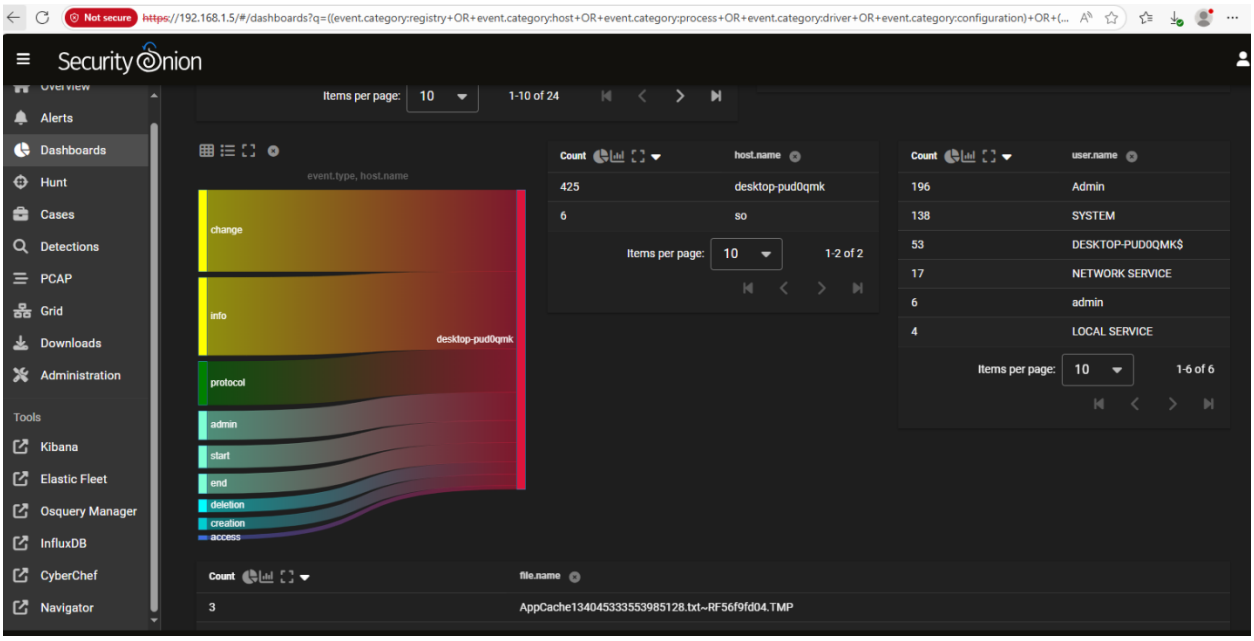

Figure 1: Host group dashboard showing Windows logs coming into Security Onion.

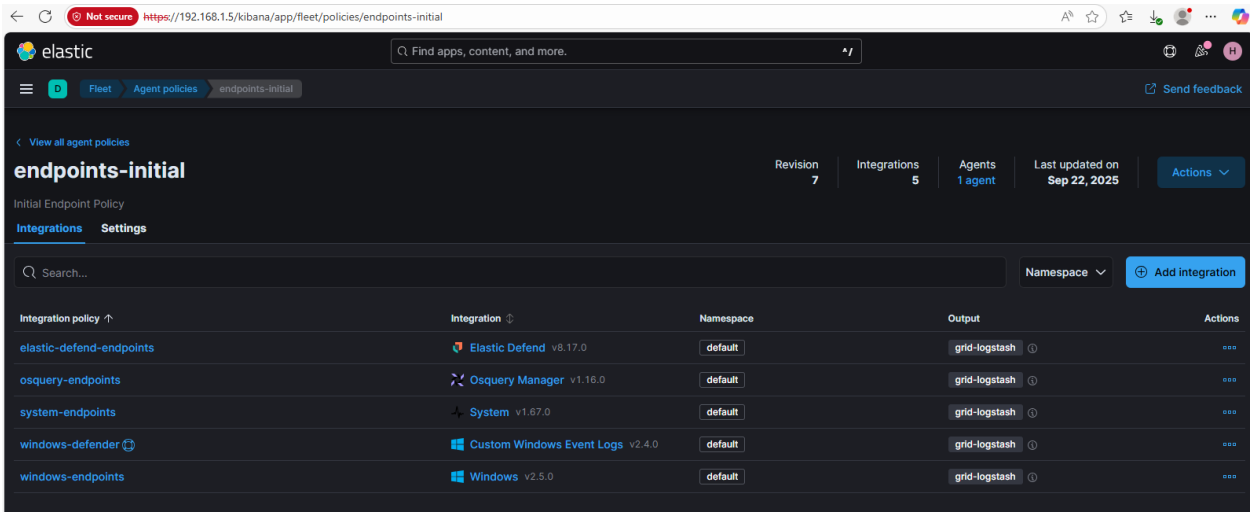

Figure 2: Elastic Agent management console showing what can be managed in the agent.

Conclusion

Despite my struggles with time management and my unclear path to my goal, I am feeling optimistic. I have made good progress and have overcome some obstacles that frankly challenged me greatly. The next few days, I will finalize installing and ingesting logs from the hosts and VMs. I will complete my OSINT investigation and build an IOC table. I would like to begin filling out my GitHub a bit more. If I can do these things by the end of the week, I will feel much better about where I am in my project.