Malvertising: A Small SOC Implementation

CMIT-450-80: Senior Seminar Project

Instructor Michael Atwood

Kyle Hathaway

11.16.2025

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 a detection and test it in a lab simulation.

The product of this project will be an attempt at an example of a 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 malvertising with an IOC table. With one detection rule created from the brief. A SOC evidence bundle consisting of configs and dashboards. 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: Working through the initial OSINT and beginning a more refined second investigation.
- Digital Evidence: OSINT v1.

Week 7

- SOC Lab: Finish SOC lab.
- OSINT: Work on the second OSINT investigation and begin building the IOC table.
- Digital Evidence: OSINT v2, IOC.csv v1.

Week 8

- OSINT: Draft OSINT v2.
- Digital Evidence: OSINT v2.

Week 9

- OSINT: Continue to work on intel brief.
- Digital Evidence: OSINT v2.

Week 10

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

Week 11

- SOC Lab: Troubleshoot issues with the SOC lab.
- OSINT: Publish IOC.csv v1.0 in repo.
- Digital Evidence: GitHub.

Week 12

- SOC Lab: Begin detection rule testing.
- Digital Evidence: Detection rule screenshots.

Week 13

- SOC Lab: Export rule and dashboard.
- OSINT: Polish report.
- Digital Evidence: Complete readmes.

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, and a detection rule. Security Onion dashboard screenshots, and a repo README.

Summary

These past few weeks, I reconsidered my timeline and deliverables. I began to scale back what I think I can deliver in the time left. I have cut the timed drills. I have cut the rules back to one and dropped the ATT&CK brief for now. Scaling back the project has made me feel more comfortable with the timeline.

Due to a power outage two weeks ago, my SOC lab went down. When I brought it back up, I did not have any internet in the environment. During the course of troubleshooting the issue, I settled on rebuilding the environment. I am not sure why it lost the ability to pass traffic. It may have been because of the outdated firewall, but for whatever reason, I could not fix the issue. I was spending too much time chasing theories and guesses and ultimately decided it would be more time efficient to rebuild it. I completed the rebuild and set about trying to test my first and simplest detection rule. I will not be submitting anything about that, as I am not happy with how it is going.

In addition to revisiting my timeline, I have begun restructuring and filing out my GitHub. I am very happy to have begun tackling this step. It was giving me the most anxiety. I wasn't sure how I would build it out and tie everything together, but now I am beginning to see how it will all work together. The next big hurdle, as far as GitHub is concerned, is to fill out the readmes and tie all the evidence in. I do have some experience with markdown syntax, but I am a bit rusty.

Evidence

The evidence this week will consist of my GitHub link. I am most worried about the structure and reporting of this project. I believe I see the weak spots and know the extra evidence I need to produce, but I will be grateful for feedback. The GitHub contains most of the evidence I have submitted up to this point, as well as some extras, including new configs, screenshots, and revised charters.

Conclusion

Scaling back this project has given me room to breathe. I felt overwhelmed by the end goals and tasks I had before me. Revisiting the timeline and deliverables has given me room to breathe. Reframing my goals and setting some of them as reach goals has allowed me to focus on the tasks at hand. My biggest worry now is whether the work I have done and will have done will satisfy the requirements of the project. I believe they will, but it all remains to be seen.

In the coming weeks, I aim to complete the README in my GitHub, tying all of it together. I hope to begin building a final submission packet. Once I begin to form my final submission, I would like to try to reach the goals I initially set. Some may not be attainable, but I believe that a few will be. I do think that a timed demonstration and a runbook may be beyond what I have the time or knowledge to complete in the time left to me. I am looking forward to feedback and guidance.