

Malvertising: A Small SOC Implementation

CMIT-450-80: Senior Seminar Project

Instructor Michael Atwood

Kyle Hathaway

11.30.2025

## Contents

Introduction .....	1
Timeline .....	1
Summary .....	3
Evidence .....	3
Conclusion .....	3

## 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 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**

- 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**

I have begun to build Readme files for GitHub. I am beginning to see how GitHub will tie everything together. I also started putting the finishing touches on documents for the final package.

## **Evidence**

The evidence this week will consist of my GitHub link. I have pushed a couple of readmes to GitHub.

## **Conclusion**

I am trying to wrap everything up as best I can. I am still trying to get my detection to work. I will keep working on it. I would like to have one detection for my project. I will not feel successful in my project if I don't have one detection rule that works in the lab environment.

I am working to build out the final package for this project. I am aiming to have the bones of the final package put together next week and to use the remaining time to polish it as best I can.