**Security Onion Logging of Cyberattack Patterns**

**Key Contributors:**

**Anthony Jamieson, Abdul Alqarni**



**10/21/2022**

# EXECUTIVE SUMMARY

In today’s world, utilizing a single alert and threat management system often does not give enough data to drive meaningful security decisions. Security information and event management is always critical to monitoring and safeguarding a secure technological ecosystem. Even in smaller companies that may not have the budget for an expensive SIEM or network security management tool, proper security is still a must-have, and the tool must be effective in its purpose. Carrying this issue in mind, we searched as a team for reliable and trusted options for lower cost SIEM options, and through our research, we found that the Security Onion system developed by Security Onion Solutions provided an excellent value for being a free product. On top of being a tool worthy of use in the general workplace, Security Onion is also a great training tool for home labs and hobbyist cybersecurity analysts as well. Security Onion is a system of collected IDS tools and data analytics programs combined into one package, all built from a CentOS 7 64-bit distribution of Linux. It can be installed on a virtual machine or on a bare-metal system. For our purposes, we decided to build our distribution from a virtual machine using their self-installation .iso file for the least number of issues.

Following our online research, we will work as a team to explore the free SIEM system Security Onion, and specifically how Security Onion does its logging and reporting of network traffic. We will go through the process of running simulated network traffic through suspicious PCAP files to test the capabilities of the built-in intrusion detection systems packaged in with the Security Onion SIEM. Following that, we will study the logged alerts, data, charts, and graphs offered through different parts of the service by utilizing the included Security Onion dashboard as well as the additional tools such as the ElasticSearch dashboard for the recorded time of each PCAP. As the data is collected, filtered, and displayed, we will discuss the efficacy of each included intrusion detection tool compared between multiple different samples of suspicious network activity through various PCAPs. We will obtain our PCAP files through the website Malware Traffic Analysis in order to provide consistent, higher quality samples through which we break down in Security Onion. Breaking down the logs, our team will analyze the types of data recorded by the different tools and what key parts are important to focus on.

Project Milestones:

1. Configure Security Onion Deployment
2. Download PCAP from Malware Traffic Analysis
   1. Import PCAP data into Security Onion
3. Filter logs and data through SO dashboard and Elastic
   1. Log and expand on Final Report

Deliverables:

1. Project Report
2. PowerPoint Presentation
3. Security Onion Logs

Professional Accomplishments:

1. Professional understanding of SIEM systems
2. Knowledge of PCAP gathering
3. Log analysis and filtering skills

# PROJECT SCHEDULE MANAGEMENT

# Gantt Chart

Timeline

Description automatically generated

# Trello QR Code

Qr code

Description automatically generated

# GitHub Repository

https://github.com/awjamieson83/IDS-Security-Onion-Project

# TABLE OF CONTENTS

[EXECUTIVE SUMMARY 2](#_Toc120293547)

[PROJECT SCHEDULE MANAGEMENT 3](#_Toc120293548)

[Gantt Chart 3](#_Toc120293549)

[Trello QR Code 3](#_Toc120293550)

[GitHub Repository 3](#_Toc120293551)

[TABLE OF CONTENTS 4](#_Toc120293552)

[MILESTONE 1: CONFIGURING SECURITY ONION DEPLOYMENT 5](#_Toc120293553)

[Initial Deployment Problems 5](#_Toc120293554)

[Current System Issues 6](#_Toc120293555)

[MILESTONE 2: IMPORTING AND PROCESSING PCAPS 6](#_Toc120293556)

[SSH and Importing PCAP Files 6](#_Toc120293557)

[MILESTONE 3: EVALUATING AND SORTING LOG FILES 7](#_Toc120293558)

[Analyzing Network Traffic 7](#_Toc120293559)

[Variety of Data Types and Tools 8](#_Toc120293560)

[CONCLUSION 9](#_Toc120293561)

# MILESTONE 1: CONFIGURING SECURITY ONION DEPLOYMENT

Through the research done through official documentation and hobbyist blogs, we configured our deployment to run a virtual machine primarily from a NAT network with a secondary bridged network connection to the host PC. Because our Security Onion deployment works as a terminal interface, another virtual machine is required to utilize the tools and system dashboard. A secondary deployment of a Kali Linux virtual machine works as our node to the main deployment and allows us to utilize the main security onion dashboard. Additionally, our Kali virtual machine allows us to remotely connect to the original Security Onion terminal through SSH, letting us use command line tools from the original process such as ‘so-allow’ and ‘so-import-pcap’. Our bridged network allows for a simple second half of the deployment process as Security Onion auto-fills IP addresses and ranges which cuts out a lot of hassle and troubleshooting.

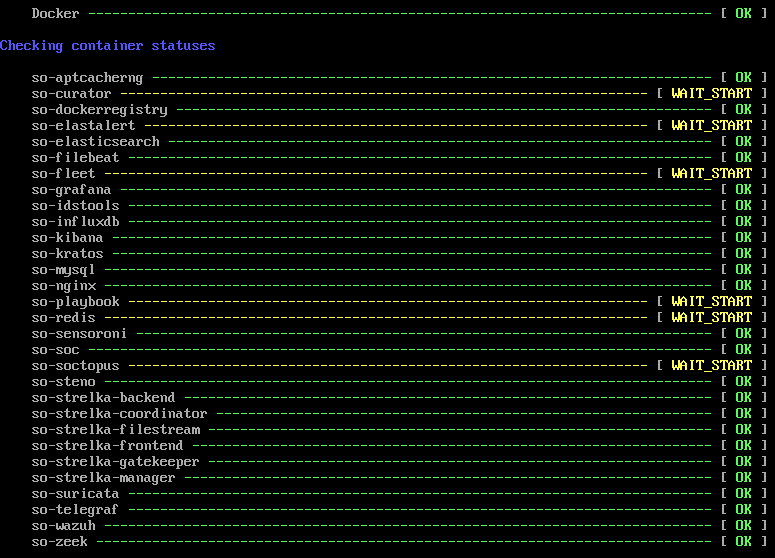


Fig 1. Executing so-status on Security Onion to display services and their current status

Initial Deployment Problems

The process of setting up Security Onion was an initial arduous process for the project. Utilizing VMWare Player 16 and the .iso file for Security Onion 2.3 alongside a Kali VM node, we encountered numerous errors in initially getting the SIEM system to run correctly. The set-up process worked nearly perfectly, but the issue of setting up multiple NAT networks for the system to communicate on was quite confusing, and the documentation provided little in terms of assistance with getting the issues figured out. Eventually, after consulting multiple guides, videos, and a chat or two with Dr. Parra, I managed to get the system to boot on my home system. Getting Security Onion to work on a laptop was also a difficulty, as the recommended specifications were very high and hard to manage on anything less than a more expensive machine. One issue that our team still runs into is not having the recommended amount of RAM to allocate to the VM; on our home computer, we were not able to allocate the requested amount while also running a secondary VM to act as a node for the SIEM.

Current System Issues

As the Security Onion system currently stands, there are still some unresolved issues that we must work around as a team. After utilizing the system for a consistent period of time, the VM errors out with a hard CPU lockup, requiring a full reboot of Security Onion. This takes the dashboard offline for the time it takes for the system to come back online; in our experience, for the VM to get back up to full functionality, a reboot could take anywhere from ten to twenty minutes for the system to reconnect and for the dashboard to reflect the system’s state on our Kali node. With this in mind, we needed to work around the system’s crashing issue when working on the VM. Another issue we encountered is a general sluggishness in system performance once activity started to climb; we would feel a lag in typing system commands and find simpler functions hanging for longer than we would like them to. We contribute many of these issues to the environment we are running Security Onion on, but we also find serious difficulty in solving these issues because of a lack of concise documentation, especially for beginner or low-level cyber security analysts.

# MILESTONE 2: IMPORTING AND PROCESSING PCAPS

To test the efficacy of the system in analyzing network activity, our team decided to utilize PCAP files that can be imported straight into the Security Onion system. A key feature of Security Onion is its native PCAP import tool which simplifies the analysis process into significantly fewer steps. In order to use the native PCAP import tool, we needed to SSH from our secondary Kali machine’s root terminal into the main Security Onion system and process our commands directly through it. This makes the process more streamlined and easier to follow, however it does require saving more files into the storage of the Security Onion system itself.

SSH and Importing PCAP Files

To gather the necessary data for Security Onion to process, we utilized the website Malware Traffic Analysis to find good examples of malicious network traffic. In this website, many different types of attacks are logged and posted for research and use in training datasets. From this site, we pulled a select few sample PCAPs to load into Security Onion for analysis. With Security Onion running, we were able to access the machine through our Kali node utilizing SSH. In this process, we can use the ‘wget’ command to pull download links from Malware Traffic Analysis and unzip them inside the Security Onion machine. Once the PCAP is removed from the zip file, we used the command ‘so-import-pcap’ to utilize Security Onion’s built-in PCAP analyzer tool. This tool makes use of Suricata and Zeek/Bro to break down the traffic data carried inside the PCAP and outputs both results into the dashboard as well as ElasticSearch.

A screenshot of a computer

Description automatically generated with medium confidence

Fig 2. Suricata alerts in Security Onion dashboard from “TA578 IcedID (BOKBOT) with DarkVNC and Cobalt Strike”

# MILESTONE 3: EVALUATING AND SORTING LOG FILES

Once the files have been imported and processed through the Security Onion import system, the data that is output can be manipulated and filtered using the built-in search functions. Logs can be sorted by time period or sorted by using SQL-like commands to pull for specific aspects, modules, IP addresses, timestamps or more. These commands can help in narrowing the scope of searches down to a fine level of detail, giving administrators a greater amount of control over what traffic goes through their systems and assists them in finding exactly what they are searching for.

Analyzing Network Traffic

Once the data has been pulled and analyzed by the security tools, we can drill down to specific triggers and notifications that would be flagged and alerted by either Suricata or Zeek monitoring. Security Onion is also quite helpful in this regard, allowing the use of multiple IDS modules to further increase the chances of detecting and alerting for malicious network activity. Each packet can be broken down to see carried information and each attack’s starting point can be clearly defined. Every alert created can be sorted by which module detected it to focus in on specific intrusion detection systems. In Elastic, the data is laid out in different displays, such as line charts and graphs to compare different aspects of the PCAP traffic. Both Elastic and the Security Onion dashboard have their own graphs and tables for viewing and analyzing data; in addition, form the Security Onion dashboard, you can pull specific entries from the PCAP to create threat hunting cases and narrow down who and what caused the attacks on the systems. Related info is logged in data tables, such as source and destination IPs, source and destination ports and timestamps for every entry. All of this information is collected in tables that make the data easy to read and handily keeps all related fields grouped up in the same space.

Graphical user interface

Description automatically generated

Fig 3. Elastic data tables from “TA578 IcedID (BOKBOT) with DarkVNC and Cobalt Strike”

Variety of Data Types and Tools

The dashboards of both Security Onion and ElasticSearch provide multiple types of data visualizations for many configurable variations. Charts, graphs, and timelines accompany data tables and resource lists, providing handy visual aids to be used for many different purposes. Having different sources of these data visualizations also provides more choice to the user based on which tool they prefer the most. Among other tools that we have seen thus far, there are also more niche free tools available such as Grafana and CyberChef that have their own dashboards for viewing. As opposed to Kibana and SO dashboard, Grafana’s default setup shows more of the real time system metrics that would be useful for a session monitoring current web traffic and system usage. CyberChef is a neat little package of different cybersecurity tools with hex converters, encryption tools, hashing, forensics tools and more, all wrapped up in a fun little interface resembling a chef’s recipe. On the other hand, Playbook and FleetDM did not work in our EVAL session of Security Onion, giving a 404 error in place of any useful data. Finally, Navigator brings up an interactive diagram of the MITRE ATT&CK killchain which can be useful for tracing through certain attacks performed on a client’s services.

A screenshot of a computer

Description automatically generated with medium confidence

Fig 4. Security Onion dashboard for “TA578 IcedID (BOKBOT) with DarkVNC and Cobalt Strike”

# CONCLUSION

After spending time as a team researching, configuring, troubleshooting, utilizing, and reviewing Security Onion, we were impressed with the amount of functionality available in a free SIEM system by a smaller company. Each useful program is tied together well in a consistently updated user interface with intuitive and useful tools. However, alongside this point, many tools may not be the full version or contain every feature that they might otherwise have. The Elastic integration, for example, does not include the more in-depth tools of Elastic SIEM and instead only keeps the more basic tools of Kibana. There are other trade-offs with the tools included being free, also including paid-only customer support through Security Onion Solutions if you need assistance or the slim and often vague documentation. However, with the value of all other included tools, commands and professional environment layout, it is hard to argue the value or worth of Security Onion for being free. It will provide many of the important tools that security administrators will need and can be easily supplemented by other outside resources and distributions.