Security Onion

Free and Open Security Platform where you peel back your defenses layer by layer and make your adversaries cry

Garrett Pearsall and Jeffrey Zhang

December 7, 2024
Version 1.0

Summary

This tutorial focuses on learning about the Security Onion Platform, a free and open framework/platform for threat hunting, network security monitoring, and log management. We will demonstrate a few tasks that the Security Onion Platform is capable of performing.

Contents

1 Virtual Machine Passwords

- Windows 11 VM: win11_local_admin/password
- Ubuntu VM: user/password
- Security Onion VM: admin/password
- Security Onion SOCGUI: admin@securityonion.com/password
- LAMP: root/Password1

2 Introduction >

What are the benefits of automated log collection versus manual log collection? How would the benefits of automated log collection assist in the overall defense architecture of the network(s)?

It is important for all of us to understand why is it important to have log collection in general. Automating it via tools such as Security Onion can help assist System Administrators in automatically keeping a watchdog on the network, like an extra pair of eyes. Most applications leave some sort of logs for security purposes, to keep logs of our information up to date. Manual Log Checking is of course, viable, however it isn't scalable and it is inconvenient when compared to automated systems like Security Onion to assist.

3 Major Stats for Security Onion <>

1. 2009 - Security Onion was Established. [1]
2. 2014 - Security Onion LLC gets established.
3. 2021 - Security Onion achieves 2 million downloads.

This lab will be using Security Onion version v2.3. (v2.4 is the latest version, released on August 29, 2024.)

[1] Security Onion Solutions, LLC is the creator and maintainer of Security Onion, a free and open platform for threat hunting, network security monitoring, and log management. Security Onion includes best-of-breed free and open tools including Suricata, Zeek, the Elastic Stack and many others. [1]

4 More Trivia for Security Onion <>

1. For network security, Security Onion is a FRAMEWORK that offers signature based detection via Suricata, rich protocol metadata, and file extraction.
2. It's Highly Scalable.
3. Security Onion and it's tools (i.e. Wazuh) are open source. The source code is on GitHub for review by those seeking to understand how it works behind the scenes.
4. If one is familiar with the "Stellar Cyber" platform, they are both relatively similar in utility.

Security Onion is a free and open platform built by defenders for defenders. It includes network visibility, host visibility, intrusion detection honeypots, log management, and case management. For network visibility, we offer signature based detection via Suricata, rich protocol metadata and file extraction using your choice of either Zeek or Suricata, full packet capture via Stenographer, and file analysis via Strelka. For host visibility, we offer the Elastic Agent which provides data collection, live queries via osquery, and centralized management using Elastic Fleet. Intrusion detection honeypots based on OpenCanary can be added to your deployment for even more enterprise visibility. All of these logs flow into the Elastic stack and we've built our own user interfaces for alerting, hunting, dashboards, case management, and grid management. Security Onion has been downloaded over 2 million times and is being used by security teams around the world to monitor and defend their enterprises. Our easy-to-use Setup wizard allows you to build a distributed grid for your enterprise in minutes!

5 Activity 1: Discussion <>

List 3-5 key benefits of using Network Monitoring in a corporate environment.

How can Security Onion be customized to fit the specific needs of an organization's security posture?

In what ways does Network Monitoring facilitate incident detection and response? Can it be effectively used for real-time monitoring?

Security Onion is a robust, open-source platform designed for threat hunting, network security monitoring, and log management. It integrates tools like Wazuh, Suricata, Zeek, and Kibana, thus providing a comprehensive solution for detecting and responding to cybersecurity threats.

6 Briefing: Wazuh <>

What is Wazuh, and how is it used within Security Onion?

1. Wazuh monitors endpoints for suspicious activities, unauthorized changes, and vulnerabilities.
2. It collects, parses, and analyzes logs from various sources to identify potential security incidents.
3. Leverages signature-based and anomaly-based detection methods to uncover threats.

Wazuh is a powerful open-source platform that complements Security Onion by extending its capabilities to endpoint detection, log analysis, and compliance monitoring. Security Onion focuses on network security monitoring, providing tools like Suricata and Zeek for traffic analysis. Wazuh enhances this setup by adding endpoint-level visibility, ensuring that organizations have a holistic view of their infrastructure. By integrating these two platforms, analysts can monitor both network and endpoint activity in a unified dashboard, such as Kibana, enabling seamless threat detection and response.

One of the key benefits of using Wazuh with Security Onion is the ability to correlate data from network traffic and endpoint logs. For instance, while Security Onion might identify suspicious network traffic patterns, Wazuh can analyze logs from the affected endpoints to pinpoint the root cause, such as unauthorized file modifications or anomalous user behavior. This integrated approach helps security teams detect and respond to multi-vector threats more effectively.

In addition to threat detection, Wazuh aids in compliance monitoring by auditing endpoint configurations and ensuring adherence to regulatory standards like PCI DSS, HIPAA, and GDPR. Security Onion, on the other hand, focuses on network-level compliance, such as monitoring for data exfiltration. Together, they provide a comprehensive compliance solution that spans both network and endpoint levels.

Finally, the integration between Wazuh and Security Onion enhances incident response. When Security Onion generates an alert for potential malicious activity, Wazuh provides detailed endpoint context, such as system logs or process activities, allowing analysts to investigate thoroughly. Wazuh can also automate response actions, like isolating compromised systems, which accelerates containment efforts. This synergy between Wazuh and Security Onion makes them a powerful combination for organizations aiming to strengthen their cybersecurity posture.

7 Task 1: Catching Events Within the "Alerts" Tab <>

Open the Security Onion WebGUI

- Navigate to the "Windows Client" VM
- Open Chrome, and input the URL 192.168.1.100
- Navigate to alerts on the left sidebar, and then check the previous logs that have already been captured.
- log off the current machine and log back in. Navigate back to the WebGUI, and there should be a new windows client event catching the logon and logout events. Click Drilldown and find the specific event.

Wazuh should've captured this new event while it was running. As mentioned in the previous page, it runs within the framework of Security Onion to catch new events under the network that Security Onion was set up in.

8 OSSEC Method (Linux) <>

- Host-Based Intrusion Detection
  - It identifies suspicious activities on individual hosts, such as unauthorized file modifications or privilege escalation.
- Log Analysis
  - Collects and parses logs from Linux services like SSH, Apache, and systemd to detect potential security threats.
- It's basically Wazuh but for Linux

- OSSEC and Wazuh are both open-source security platforms designed for intrusion detection and log management, but they differ in scope and functionality. OSSEC is primarily a host-based intrusion detection system (HIDS) focused on monitoring file integrity, analyzing logs, and detecting rootkits. It provides a lightweight solution for monitoring Linux, Windows, and macOS systems and has a strong emphasis on simplicity and performance. However, its feature set is relatively basic, offering limited support for modern use cases such as advanced threat detection, endpoint response, or compliance reporting.

- Wazuh, on the other hand, is a fork of OSSEC that has evolved into a more comprehensive security platform. It expands on OSSEC's capabilities by integrating modern features such as vulnerability detection, compliance auditing, and enhanced endpoint detection and response (EDR). Wazuh also provides a more user-friendly interface and integrates seamlessly with tools like Elasticsearch and Kibana for advanced visualization and analytics. Additionally, Wazuh offers improved scalability and central management, making it better suited for large, complex environments. For convenience we will use OSSEC to monitor Linux, and Wazuh to monitor Windows for the remainder of this tutorial.

9 Activity 2: Triggering an event from the Ubuntu Machine <>

- Log onto the Ubuntu Machine.
- Fail to log onto the "bobbob" user account at least 3 times.
- Tab back into the Security Onion WebGUI and look for a new OSSEC Alert Type regarding the failed logons, then click drilldown on that specific alert to see the details of the incident.

- The new triggered alerts should add onto the number of existing alerts due to our testing earlier.
- The name of the alert should be pretty obvious.

10 Security Onion Downloads

<>

- Five main configuration types for Security Onion. These are dependent on what you want to get our of security onion on various sizes of networks.
- Import - This one is for deep packet inspection where you provide the pcap files and you can use the security onion interface to delve and find the alerts in the file.
- Eval - Is for smaller classroom examples to help learn and understand the security onion system.
- Standalone - Is a single node setup for production. Mainly for smaller systems.
- Distributed - Is a multi-node system for larger networks with lots of network traffic.

In this instance we are using the Eval configuration. This will be helpful because it is a single node system that is used for examples and do not have the large system requirements that other systems need.

11 Kibana <>

- Kibana is a front-end for another look at all of the data gathered by security onion.
- It is very similar to the SOC-GUI but it has some major differences.
- It is more focused on the where and when the incident happened rather that looking doing full packet inspection.

Kibana is within the elastic application and reads the data stored by Elasticsearch. It is a visualization tool that we can create graphs of the data to find more simplified views of our alerts with options like filtering that only takes data from a certain data set.

12 Grafana <>

- Is an open source data visualization software that looks at the network and the traffic data that is passing through.
- This can show things like network bandwidth usage, sensor activity, and system health with real time data.
- You can also set up alerts so if something is detected that is not usual activity you can set it up so an alert will pop up in security onion stating what went wrong.

This is really helpful on a larger distributed network setup. With a distributed network it might be too much strain on a one node system and you can implement and monitor each node with this software to see that each node is within a normal work load for the system.

13 CyberChef <>

- This is a web based tool that you can use to decode, analyze, and manipulate different types of data.
- If you have a packet that you want to decode into plain text you can input the data and then add different limiters so that when you decode it will reduce it to plain text.
- You can follow along or just watch how easy you can manipulate data within this tool.

This can be really helpful for when you want to do some deep packet inspection and instead of looking at large blocks of data you can reduce it to more readable and useable data.

14 Playbook <>

- This is a web based database for storing different ”plays” related to alerts that come up in the SOC-GUI.
- This provides your personnel with what is going on and what to do in certain scenarios where an alert came up and they do not know where to start.
- We can lookup and find the pre-configured plays that come with security onion while also having the option to create new plays and edit previously made plays if needed.

This is very helpful when you have multiple people who monitor and look through the logs stored in your SOC-GUI. It can provide the needed knowledge to shut down and prevent incidents that are caught early.

15 FleetDM <>

- Fleet Device Manager is an online software that provides a easy to use device manager where you can look up and check the status of agents that use osquery agent software.
- We are not able to implement this within our tutorial because you need internet connection to install multiple tools to allow this to run on your computer.
- This is very helpful when using the osquery agent software to record and send logs back to security onion.

There are three different applications that are recommended to use on all agent devices, elasticsearch, wazuh, and osquery. In this implementation we were only able to use two for device endpoint monitoring.

16 Navigator <>

- This is an integrated and version of the MITRE ATTCK Navigator tool that maps and analyzes threats methods as they appear.
- This is used hand in hand with the playbook but this provides a framework of what might happen in certain scenarios when a incident has been detected.
- In the playbook we can see references to the ATTCK navigator tool about certain incidents and more knowledge on what to do in said incidents.

MITRE ATTCK framework is a database that shows what an attacker would do in a certain scenario when they are attacking a system.

17 Walkthrough Activity: More Functions <>

A lot of the services that Security Onion offers require internet, and/or are beyond the scope of this lab. The presenter will demonstrate some of these functions, and the audience is requested to follow along.

Duration: 10-15 minutes

18 Challenge 1: Capturing and logging ICMP packets <>

- Find a way to make more ICMP alerts show up on the "alerts" tab of the Security Onion SOCGUI (Security Onion Console GUI).
- Then look in the Kibana interface to find the alert so it shows where ICMP traffic originated, where it went and the timestamp associated.

19 Conclusion <>

- Network monitoring is a cornerstone of modern Cybersecurity, enabling organizations to detect, analyze, and respond to threats in real time.
- It provides deep insights into network traffic, helping identify anomalies, unauthorized activities, and potential breaches.
- It combines network monitoring with endpoint security and log analysis enhances overall security posture and reduces attack surfaces.

Proactive and continuous network monitoring is no longer optional—it's a necessity for safeguarding data, maintaining operational integrity, and ensuring business continuity in today's interconnected world.

[?]

20 Appendix: Setting Up the VM, Solutions, and Change-log <

1. Steps for setting up the virtual machine
2. Solutions to the challenges and questions
3. Change-log

Steps for Virtual Machine setup:

1. This Tutorial requires following VM's
   - Security Onion VM
   - Windows 11 VM Connected to Security Onion VM
   - Ubuntu VM Connected to Security Onion VM
   - LAMP webserver

Solutions:

- Activity 1: Discussion
  - Possible Answers: Real-time intrusion detection, Saves Manpower, Saves time
  - Possible Answer: Agents can be added or removed, like modules, within the Security Onion Framework.
  - Possible Answers: Network Detections are printed to a log, and yes, it can be used effectively for real-time network monitoring.
- Task 1: Catching Events Within the ”Alerts” Tab
  - Login into the Windows 11 Machine
  - Go to 192.168.1.100 (Security Onion)
  - Navigate to the Alerts tab on the left of the SOCGUI
  - Log out and Log back in
  - Navigate to the Alerts tab on the left of the SOCGUI
  - Inspect the new event via the ”Drilldown” function
- Activity 2: Triggering an event from the Ubuntu Machine
  - Boot Ubuntu Machine
  - Fail to Log onto the user ”bobbob” three times
  - Switch back to the SOCGUI
  - Navigate to the Alerts tab on the left of the SOCGUI
  - Inspect the new event via the ”Drilldown” function
- Walkthrough Activity
  - Follow the On-Screen Demonstration, what could go wrong?
- Challenge 1: Capturing and logging ICMP Packets
  - Open Terminal on the Ubuntu VM
  - Ping the Security Onion VM (Generate some ICMP traffic)
  - Navigate to the Alerts tab on the left of the SOCGUI
  - Inspect the new ICMP event via the ”Drilldown” function

Changelog:

Security Onion			
Ver.	Date	Authors	Changes
v1	December 2nd 2024	Jeffrey Zhang and Garrett Pearsall	Initial Commit.

References

[1] Security Onion LLC. *Security Onion History Timeline as displayed on their website* `https://securityonionsolutions.com/#about`

[2] ATTCK navigator. ATTCK Navigator - Security Onion Documentation 2.4 documentation. (n.d.). https://docs.securityonion.net/en/2.4/attack-navigator.html

[3] Configuration. Configuration - Security Onion Documentation 2.4 documentation. (n.d.). https://docs.securityonion.net/en/2.4/configuration.html

[4] CyberChef. CyberChef - Security Onion Documentation 2.4 documentation. (n.d.). https://docs.securityonion.net/en/2.4/cyberchef.html

[5] Focus, D. V.-C. (2023, August 25). Security onion-(part 2) tools. Medium. https://medium.com/@itdanny/security-onion-part-2-tools-1cd95e350811

[6] Kibana. Kibana - Security Onion Documentation 2.4 documentation. (n.d.). https://docs.securityonion.net/en/2.4/kibana.html

[7] A new fleet. Fleet. (n.d.). https://fleetdm.com/announcements/a-new-fleet

[8] YouTube. (n.d.). Security Onion Essentials 2.3 - Detection Engineering. YouTube. https://www.youtube.com/watch?v=IS2SOlDedPc