

10

MONITORING YOUR NETWORK WITH DETECTION AND ALERTING



Network monitoring provides real-time visibility into your network activity, enabling you to stay ahead of potential threats and (ideally) stop adversaries before they've performed any disruptive action.

Monitoring your network is a huge undertaking, so alerts are often a useful starting point for investigations. Without meaningful alerts, network monitoring is like finding a needle in a haystack—trying to identify malicious activity within a very large dataset.

Your firewalls, proxies, antivirus, and other solutions should be up and running for at least a month before you start trying to actively monitor your hosts and network traffic, just to ensure they're functioning correctly. Up until this point, everything has been relatively passive; once set up, no further input from you is required, unless you need to update or change the configuration.

Due to their nature, active monitoring and alerting can take considerable time and effort—not only to implement but to maintain, and that is especially true as a network expands. Not only will you need to

check in regularly to see whether your network monitoring software has identified any threats or unusual behavior, but you'll also need to investigate this behavior and potentially work to mitigate the identified activity. Depending on the size of the network, monitoring it could be a full-time job for one or more people.

This chapter will arm you with the knowledge and tools required to monitor your network and alert you to suspicious behavior successfully. We'll discuss how, when, and where to implement network traffic access points (TAPs) and a switch port analyzer (SPAN) in your network to enable network traffic capture, monitoring, and analysis. Finally, we'll build a network monitoring appliance using Security Onion—a free suite of network security monitoring tools—and discuss how best to utilize its built-in capabilities.

Network Monitoring Methods

You can use several methods to monitor and capture network traffic for real-time or post-facto analysis and alerting. The method you choose depends mostly on your network's hardware, as each device has different capabilities. We'll discuss two of the most common methods in the following sections.

Network Traffic Access Points

In small networks without switches, you can install a network *traffic access point (TAP)* to monitor the data that passes through it. A TAP is an inline device, placed between two nodes on a network; it becomes an extension of the transmission medium (like an Ethernet cable) that already exists between those two devices. In **Figure 10-1**, the TAP is between the firewall and router.

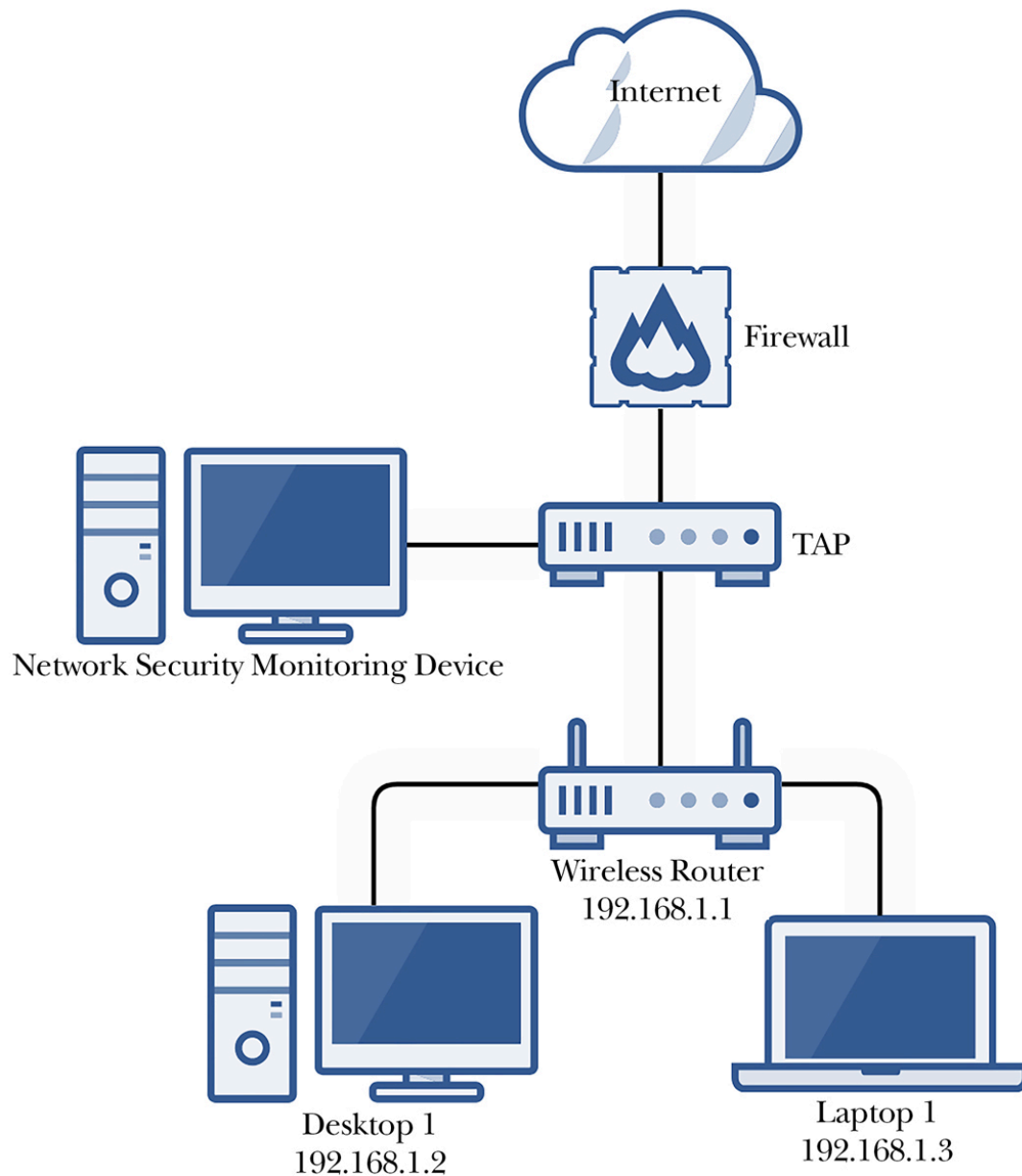


Figure 10-1: Placement of a network TAP

In this configuration, all traffic passing between the router and the firewall is sent by the TAP to a monitoring device, where it's stored for analysis.

TAPS AND INTRUSION DETECTION SYSTEMS

Coupling TAPs with an *intrusion detection system (IDS)* allows administrators to identify suspicious activity occurring across this ingress and egress point. An IDS is a software or hardware tool that uses a set of

rules or signatures to identify known-bad behavior. When an IDS identifies something suspicious in your network traffic, it will generate an alert that you can investigate to decide whether it's actually malicious (a true positive) or benign (a false positive). You can then ignore the alert or take action to mitigate and remediate the problem, which we'll discuss at length later.

When placing a TAP, consider what you actually want to see and investigate. In a configuration like the one shown in [Figure 10-1](#), you'd capture all the traffic between your endpoints and the firewall (the network's boundary). Monitoring your major egress point lets you investigate things like *data exfiltration*, where an adversary is trying to steal your data by sending it outside your network. However, with this configuration, you won't be able to see traffic between your endpoint devices, as that is handled by the wireless router and never reaches the TAP.

If you placed the TAP behind the firewall (as opposed to on the internet side), you wouldn't see any traffic from the internet attempting to reach the internal network that's blocked by the firewall. If the TAP is in front of the firewall, you wouldn't see the outbound traffic being blocked by the firewall; the security monitoring system also would lose the protection of that firewall and become an easy route into your network. Decide which of those scenarios you're comfortable with and place your TAP accordingly. In most cases, it's best to place the TAP behind the firewall (inside your network) and review the firewall logs for what the TAP doesn't see.

A TAP is an inline device. Be aware that if the TAP becomes unavailable or goes offline—if any of its limited network ports fail—your entire network will lose access to the internet. Your endpoint devices should still be able to communicate with each other via the router, but traffic will no longer pass through the TAP.

Several TAP devices are available at reasonable prices. One of the simplest is the *Dualcomm ETAP*. One possible configuration of such a TAP would be to connect the firewall in [Figure 10-1](#) to the A inline port, connect the B inline port to the wireless router, and connect a separate cable to the monitoring port of your network security monitoring device (discussed in the next section). Such a configuration would allow traffic to flow through the TAP as if it wasn't there, except that it would be intercepted, monitored, and analyzed by the network security monitoring system.

Switch Port Analyzers

An alternative to a network TAP is the *switch port analyzer (SPAN)* or *mirror port* (interchangeable terms) functionality provided by a switch. A SPAN does the same thing as a TAP; it mirrors (or copies) all the data passing through a source port(s) to the destination SPAN port on the switch. Your network security monitoring system is then connected to the SPAN port to capture the network traffic for analysis and alerting. In most modern switches, it's possible to create a SPAN configuration with multiple source ports, so you can capture data from any port(s) on a switch.

A SPAN configuration in a small network might look like the one shown [Figure 10-2](#), where the firewall or other system provides IP addresses to endpoints. Each host is connected by Ethernet to a port on the switch, and then the network security monitoring device is connected to the SPAN configured on the switch. Unlike TAPs, if a port on the switch fails, the rest of the network continues functioning, but if the entire switch goes offline due to a power failure, the entire network will go down with it.

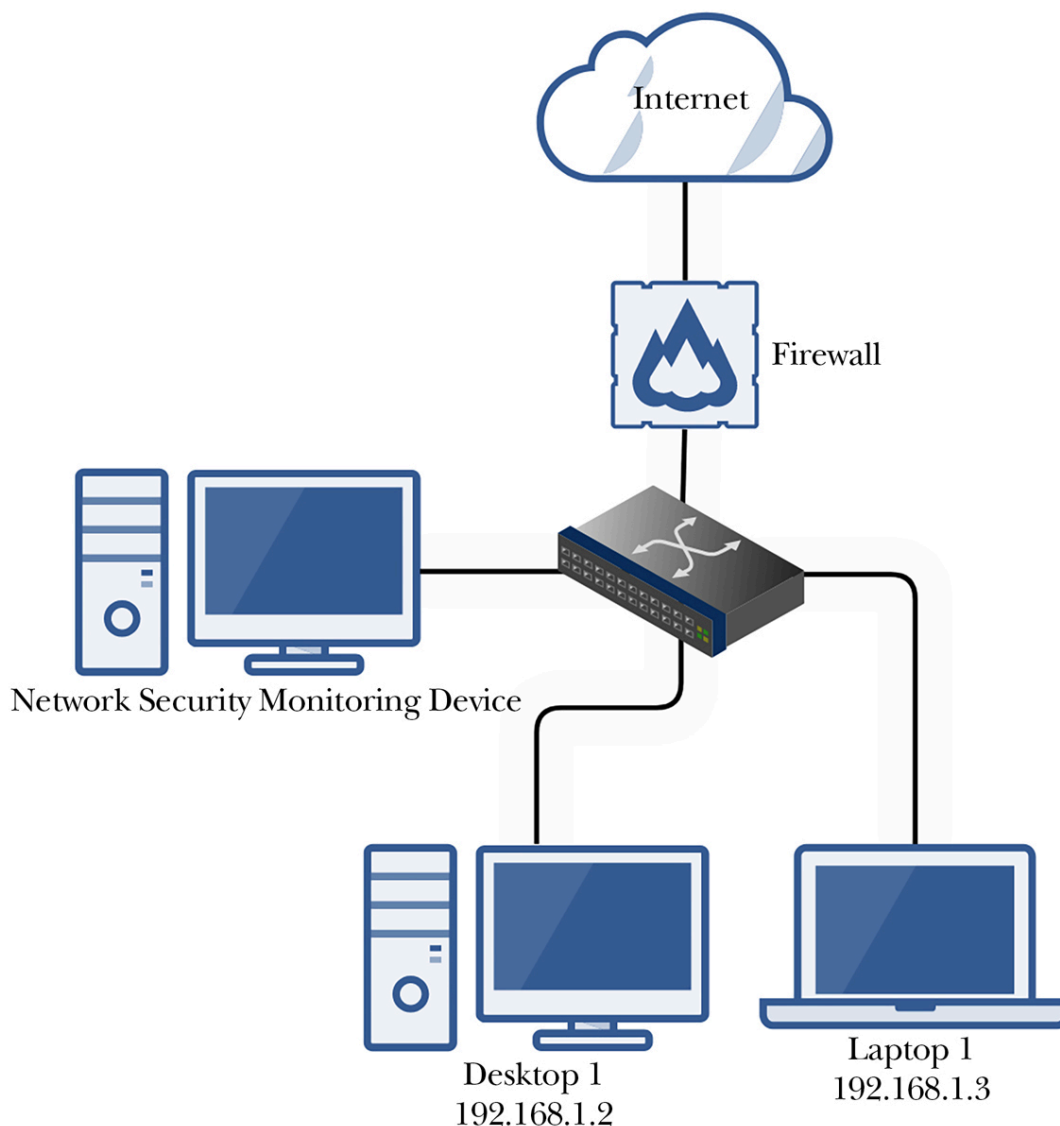


Figure 10-2: A small network with a switch and SPAN port

Unlike a TAP configuration, with a SPAN set up on a switch, you'll be able to capture and analyze computer-to-computer traffic in addition to inbound and outbound data. You'll still have the placement issue, though; when the switch is on the internal side of the firewall (as it should be), your security monitoring system won't have visibility over the traffic blocked by the firewall.

#35: Configuring a SPAN Port

To configure a SPAN port on a managed switch, like the Netgear switch that we used in [Chapter 2](#), follow these steps:

1. Log in to the switch with administrator credentials.
2. Select **System ▶ Monitoring ▶ Mirroring**.
3. In the Port Mirroring Configuration table that appears, click the source ports from which you want to capture network traffic to select them. Selected ports will have a check mark.
4. In the Destination Port drop-down box, enter the port to use as the SPAN port you'll connect to your security monitoring system.
5. Finally, in the Mirroring drop-down menu, select **Enable ▶ Apply**.

Whether you choose to set up a TAP or a switch with a SPAN port, you'll need a network monitoring solution capable of aggregating collected data. The best solution currently available for small networks is Security Onion, which includes various components for capturing and aggregating network data and enables you to quickly analyze that data.

Security Onion

Security Onion is an open source platform for threat hunting, network security monitoring, and log management. It's an operating system, like Ubuntu, that includes several open source tools we'll utilize to monitor our network for security and configuration issues.

Security Onion's tools include suricata, an intrusion detection system, and zeek, a software framework for analyzing network traffic to identify anomalous behavior. Grafana is a set of visualizations and dashboards for monitoring the health of the Security Onion system, and osquery gathers data about the endpoints in your network and the operating systems they're running for analysis. Wazuh is similar to osquery; it's an agent-based tool that gathers analyzable data from your endpoints and is used for active endpoint detection and response (in the case of a security incident). Finally, Strelka is a real-time file-scanning utility that analyzes network traffic and scans any files traversing the network; it's useful for identifying malware or data exfiltration.

SECURITY ONION TOOLS FOR LARGER NETWORKS

Security Onion makes use of the ELK stack (which includes Elastic, Logstash, and Kibana) to create visualizations and dashboards. ELK is similar to Grafana, except where Grafana is used to display information about the system itself, ELK displays information about the network data being captured, allowing the user to view and analyze the data easily. ELK is a powerful tool but is outside the scope of this book as it is more advanced than the tools within Security Onion's security dashboard. However, many online resources discuss ELK and its use in great detail if you'd like to investigate it further.

Security Onion is designed to be scalable and is capable of monitoring very large networks, so it includes tools that aren't necessary on small networks, such as TheHive, an incident management system, and Playbook, a tool for creating incident management playbooks; those tools are primarily used in larger networks, so they aren't covered here.

In the following sections, we'll discuss creating your network security monitoring system using Security Onion and its built-in tools. We'll explore how to utilize these tools to start monitoring your network, and how to triage and investigate problems when they arise. It's up to you whether you'd like to buy or build your Security Onion appliance. Security Onion Solutions has preconfigured appliances ready to go out of the box.

#36: Building a Security Onion System

To build a Security Onion system, you'll need a device with a minimum of two network interfaces: a management interface and a capture interface (connected to the TAP or SPAN). We'll use an Intel NUC (a small form factor computing unit) with two Ethernet ports, which is very customizable and available at various price points depending on

your budget and requirements. The following minimum hardware specifications are detailed in the Security Onion documentation:

- 12GB of RAM
- Four CPU cores
- 200GB of storage
- Two network interfaces

One additional consideration is how much storage you need. For reference, a NUC with an internal storage space of 2TB might be capable of storing around three weeks of data, depending on the number of devices, number of users, and amount of network traffic in your network. After that point, the data will be kept on a rolling cycle, where older data is deleted in favor of newer data. To enable better incident response capabilities in your network, the more data you keep, the better. If you discover an adversary in your network that has been there for 12 months but you have only one month of data, you'll never be able to determine root cause, making it difficult to kick them out and prevent the problem from recurring.

Once you have a NUC (or similar device), you'll install Security Onion. At this stage, it's also a good idea to connect the network port you plan to use for management (*not* the port you'll use for capturing network traffic) to your network so you can set up its configuration. It doesn't matter which of the two network ports you use for management and traffic capture. This device will need a static IP address, and while you could do that on the device itself, it's better to configure the static addressing on your router or whichever device is responsible for IP address leases in your environment (like your wireless router or pfSense device). Having the management port on your NUC (and only this port) connected will make it easier to identify when installing and configuring the rest of the software. After this process is complete, you can then configure the capture port independently. You should configure the static IP address for the management interface now, as some of

the agents we'll install have requirements and dependencies based on this address, so changing it later can create challenges.

Installing Security Onion

You can install Security Onion from an ISO file (available directly from Security Onion Solutions at

<https://securityonionsolutions.com/software/>) or manually using CentOS 7 as the base operating system and then installing the Security Onion package like any other application in a Linux environment (note that CentOS 7 is the only OS supported by Security Onion). Using the ISO file is a simpler and faster method of creating a Security Onion system, whereas manual installation requires slightly more effort. However, manual installation allows you to have more granular control over things like disk partitioning. If that is of interest to you, choose the manual installation method. If not, install Security Onion using the ISO file.

Installing Security Onion from the ISO File

Start by downloading the latest ISO from Security Onion Solutions, and follow the procedure outlined in **Chapter 1's "Creating a Physical Linux System"** to create a bootable USB drive from the ISO file. Plug your bootable USB into your NUC, turn on the NUC, and you'll be presented with the Security Onion installation wizard. Follow these steps to complete the installation:

1. The wizard will prompt you to install Security Onion, destroying all data and partitions. Type **yes** and press ENTER to accept this and begin the installation process.
2. Enter an administrator username when prompted; then press ENTER.
3. Enter a strong passphrase for the user; then press ENTER.
4. Repeat the passphrase to confirm it; then press ENTER to initiate the installation.

5. Once installation completes, the computer will reboot. Log in with your newly created credentials and the Security Onion setup wizard will pop up. Press ENTER to continue.
6. 6. Using the arrow keys, select **Install** to run the standard Security Onion installation; then press ENTER.

At this point, the process for completing the installation of Security Onion is the same for both the ISO file installation and the manual installation paths. Jump to the section “**Completing the Security Onion Installation**” on **page 157**.

Installing Security Onion Manually

You can install Security Onion entirely from scratch by installing CentOS 7 on your NUC and then installing the Security Onion packages and tools on top. To do this, follow these steps:

1. Download the most recent CentOS 7 ISO (the correct format is x86_64) from **<https://www.centos.org/>**.
2. Follow the procedure outlined in **Chapter 1**’s “**Creating a Physical Linux System**” section to create a bootable USB drive from the ISO file.
3. Plug your bootable USB into your NUC and boot from the USB. You’ll be presented with a few options; choose **Test this Media & Install CentOS 7**.
4. At this point, a graphical installation wizard appears. Select your desired language and click **Continue**.
5. Set the correct time zone and keyboard layout.
6. Under Software Selection, it’s recommended to choose **Server with GUI** for ease of administration.
7. Under System ▶ Installation Destination, select the internal disk where you plan to install Security Onion and then choose **I Will Configure Partitioning**. Click **Done** to proceed to the partitioning wizard. Partitioning defines how the hard drive storage will be divided among the users and applications on the system.
8. 8. Select **LVM Partitioning** and create the following partitions:

1. */boot*: CentOS will boot from this partition; it should have at least 500MB of space available.
 2. */boot/efi*: Part of the boot partition; it should be at least 500MB.
 3. */*: The root of the filesystem; should be 300GB.
 4. */tmp*: For temporary files; should be 2GB.
 5. *swap*: For swap files; should be 8GB.
 6. */home*: A space for any user files; should be 40GB.
 7. */nsm*: For all the security tools and captured data; it should be assigned the remainder of drive space.
9. Click **Done** ► **Accept Changes** to write the changes to disk.
10. Click **Begin Installation** to install the operating system.
11. Set your root passphrase and create a non-root, administrative account on the following screen. If you want to connect to this system via SSH, ensure that your administrative account has a strong passphrase.
12. Once the installation is complete, reboot the machine and remove the installation USB. Then, boot to your CentOS operating system.
13. Accept the license information.
14. You might need to turn the network card on to enable the network. Click **Network & Host Name**, toggle the network button to **On**, and then click **Done**.
15. Click **Finish Configuration**.

With CentOS installed, next install Security Onion. First, connect to your server via SSH or log in directly. Change directory to the */nsm* partition you created during the initial setup:

```
$ cd /nsm
```

Use `sudo yum install` to install Git (an application for software management) and then `git clone` to download Security Onion:

```
$ sudo yum install git -y
```

```
$ sudo git clone \
```

<https://github.com/Security-Onion-Solutions/securityonion>

(Whereas Ubuntu is based on Debian Linux and uses the `apt` utility to manage software packages, CentOS is based on Red Hat Linux and uses `yum`.)

Navigate to the newly created *securityonion* directory and run the setup script:

```
$ cd /nsm/securityonion/
```

```
$ sudo bash so-setup-network
```

Running this script starts an interactive installation wizard that leads you through the initial setup and configuration of your Security Onion server.

Completing the Security Onion Installation

Now that the basic configuration of the operating system has been completed, you'll start installing and configuring the tools you'll use to monitor and analyze the network traffic. Zeek is a security monitoring platform that will enable you to analyze network traffic more efficiently and alert on suspicious activity within your network automatically. It does this by utilizing rulesets containing information on suspicious or malicious activity, software, and network traffic, such as the ETOPEN ruleset you'll use here.

Regardless of how you've installed Security Onion, follow these steps to complete the process:

1. Press ENTER to continue past the welcome screen (and to progress to all other screens).
2. On the Installation Type page, navigate to STANDALONE with the arrow keys, and press the spacebar to select the option.

3. If you used the Security Onion ISO, select **Standard** on the next page to indicate that this machine has internet access.
4. If you performed the manual installation of Security Onion, type **AGREE** to accept the Elastic License on the next page.
5. On the next page, keep the default hostname for simplicity or change it if you like (in larger installations that have more than one server, changing the hostname will be beneficial). If prompted to change the hostname, choose to proceed anyway.
6. On the next page, enter a short description for this computer or leave it blank.
7. On the network card configuration page, shown in **Figure 10-3**, select the interface with the words *Link UP* next to it as the management interface. It should be the only interface plugged into the network at this point.

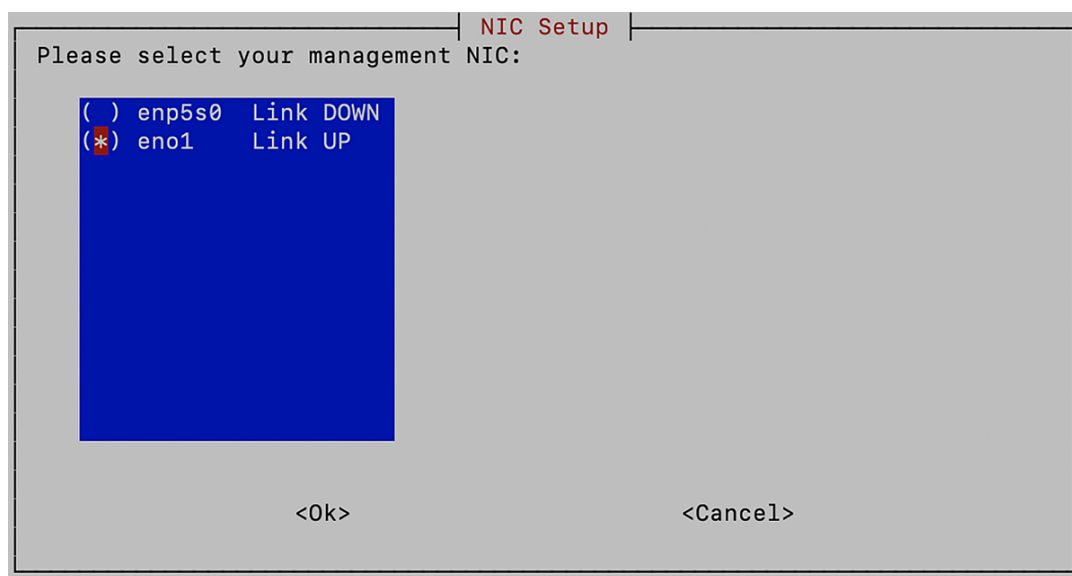


Figure 10-3: NIC setup wizard

1. 8. Press the spacebar to set the monitor interface.
On the management interface page, you may receive an informational error about using DHCP; as long as you've configured a static address for this device, you can ignore this message.
2. When asked how this computer should connect to the internet, select **Direct**.

30. Select **Automatic** on the OS Patch Schedule page to keep your operating system automatically up-to-date.
41. Specify your home network address range, identified in **Chapter 1**. If your network uses 10.0.0.0/8 addresses, leave that in the box provided and delete the other two subnets. If your network uses 192.168.0.0/16 addresses, keep that in the box and delete the other two, and so on.
52. When asked which type of manager to install, select **BASIC**.
63. Select **ZEEK** as the tool to use to generate metadata.
74. Select **ETOPEN** as the IDS ruleset to use to generate alerts.

NOTE *ETOPEN is an open source ruleset updated regularly with new and emerging threats and alerts. ETPRO and TALOS are similar to ETOOPEN, but they require a subscription. For small networks, ETOOPEN is sufficient.*

15. The wizard then asks which components of the Security Onion suite of tools you want to install. Select **Osquery**, **Wazuh**, and **Strelka**.
26. If asked if you'd like to keep the default Docker IP range, select **Yes**.
37. Enter your email address for the Security Onion administrator.
48. Enter and re-enter the password for your account.
59. When asked how you will access the web interface, select **IP**.
60. Set a strong passphrase for the *soremote* user account (for performing some administrative actions).
21. Choose **BASIC** to install the network security monitoring components with the recommended settings.
8. 22. Type **2** for the number of Zeek and Suricata processes. The number of processes dictates how much network traffic your system can process. For small networks, two processes should be sufficient; you can change this later if necessary.
23. If asked if you'd like to configure NTP servers, choose **Yes**. Network Time Protocol (NTP) is used to keep endpoints synchronized. It's best to keep your monitoring server in sync with a time

server to prevent time drift, which can cause issues when troubleshooting alerts. Browse to <https://www.ntppool.org/> and choose an NTP server in your region to keep your Security Onion server's time in sync.

104. Select **NODEBASIC** when asked.

125. Run **so-allow** by pressing ENTER when asked to correctly configure the firewall on the system to allow access to all the tools being installed.

When asked for an IP address to allow access to your network monitoring system, you can choose to allow access to the Security Onion web interfaces from a single computer or device or from any host in your network. For security purposes, you allow access only from a single IP address.

26. Enter the IP address you plan to use; then press ENTER.

27. Finally, accept the configuration you've just created by pressing TAB to select **Yes**; then press ENTER to finish the setup wizard and commit the changes.

NOTE *Security Onion and some of its tools, like Zeek, can run in a cluster configuration, where the agents are installed on multiple systems for enhanced data collection and processing. In small networks, a stand-alone system is sufficient. In larger networks with multiple network segments and switches, a cluster configuration might make more sense.*

At the end of the installation, the screen will display the URL to access the Security Onion web interface; write this down (it should be `http://<your_server_ip>/`). The system will reboot. Once it comes back up, you'll be able to log in via the URL using the email address and passphrase you entered earlier. To test the Security Onion configuration, run the following:

```
$ sudo so-status
```

This command lists the tools Security Onion is running and the status of each, which should appear as **OK** if everything worked.

If any services haven't started, wait a few minutes before running the status command again. If they still fail to start, try starting services manually using these commands:

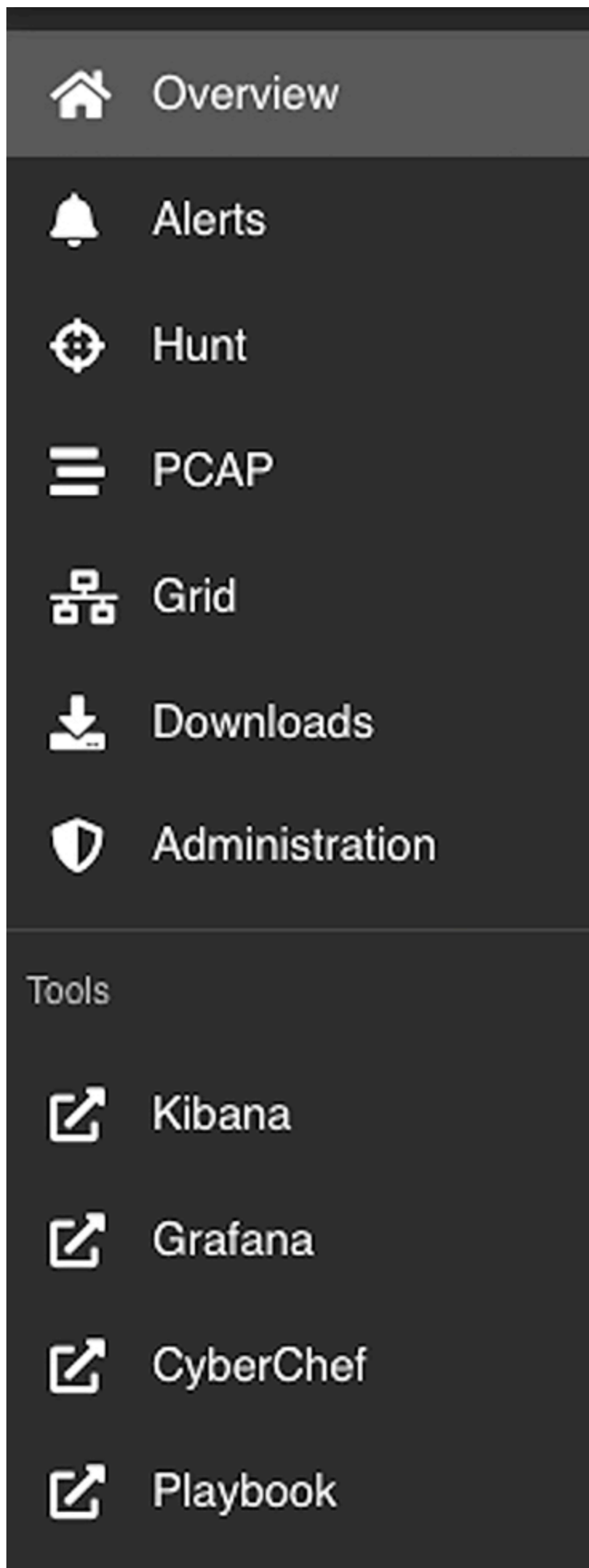
```
$ sudo so-servicename-stop
```

```
$ sudo so-servicename-start
```

```
$ sudo so-servicename-restart
```

If you're still unable to get the services to start, reboot the computer. If all else fails, reinstall Security Onion.

Once you can access the Security Onion console, you'll see a menu on the left side that lists all the tools at your disposal (see **Figure 10-4**).



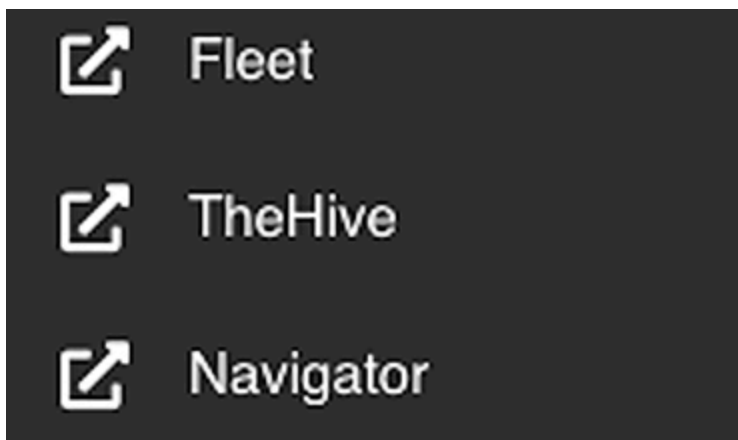


Figure 10-4: Security Onion tools

At this point, click **Kibana**, and a new tab will be launched in your browser. You should see a minimal number of records because you haven't plugged in the capture port on your device.

Connect this port to the SPAN or TAP you configured earlier. Once that's done, refresh the page after a few minutes to see Kibana populated with newly acquired data.

#37: Installing Wazuh

Security Onion's additional tools help you to understand what's happening in your network and take action to investigate, mitigate, and remediate issues when they arise. One of these packages is Wazuh.

Wazuh is an open source *endpoint detection and response (EDR)* platform that monitors your endpoints for malicious activity, alerts you within the Security Onion console, and provides the incident response capabilities of blocking network traffic, stopping malicious processes, and quarantining malware files.

Using agents like Wazuh can be controversial. In larger networks, oftentimes so much is going on that adding something new to the network, especially across all the systems, can cause stability issues or create/exacerbate challenges around limited resources like bandwidth. This is usually less of an issue in smaller networks because ca-

capacity isn't shared between so many devices, users, or processes, and there generally aren't as many solutions competing for resources.

Installing Wazuh won't have a meaningful impact on the daily operations of your small network. Conversely, the value you receive from the additional monitoring and security uplift far outweighs any potential negative consequences of using multiple agents. Ultimately, it's your decision whether to install these agents on one, some, or all of the endpoints in your network. The more complete your coverage and network monitoring, the more secure your network is likely to be.

This section provides instructions for installing the Wazuh agent on Windows, macOS, and Linux.

Installing Wazuh on Windows

To install the Wazuh agent on your Windows endpoint(s), follow these steps:

1. Log in to your Security Onion console and click **Downloads** in the left menu.
2. Click the **MSI** installer agent option to download the correct installer; then run the downloaded executable on your Windows computer.
3. Accept the license agreement and click **Install**.
4. Once the installation completes, tick the **Run Agent Configuration Interface** checkbox and click **Finish**.
5. To add this new system to your Security Onion, log in to Security Onion via SSH and run the `manage_agents` script. Following the prompts, add an agent with `A`, list agents with `L` to confirm the addition was successful, and extract the authentication key for your new agent with `E`:

```
$ sudo docker exec -it so-wazuh /var/ossec/bin/manage_agents  
--snip--
```

Choose your action: A,E,L,R or Q: `A`

- Adding a new agent (use '\q' to return to the main menu).

Please provide the following:

❶ * A name for the new agent: Test

* The IP Address of the new agent: 192.168.1.50

Confirm adding it?(y/n): y

Agent added with ID 002.

--snip--

Choose your action: A,E,L,R or Q: L

Available agents:

ID: 001, Name: securityonion, IP: 192.168.1.49

❷ ID: 002, Name: Test, IP: 192.168.1.50

** Press ENTER to return to the main menu.

--snip--

Choose your action: A,E,L,R or Q: E

Available agents:

ID: 001, Name: securityonion, IP: 192.168.1.49

ID: 002, Name: Test, IP: 192.168.1.50

Provide the ID of the agent to extract the key (or '\q' to quit): 002

Agent key information for '002' is:

❸ MDAYIFJvcnkgMTkyLjE2OC4xL...

** Press ENTER to return to the main menu.

--snip--

Choose your action: A,E,L,R or Q: Q

manage_agents: Exiting.

You'll have to provide a name and IP address when you add an agent

❶. For the name, use the hostname of the computer being added.

Run the `hostname` command to find the name:

```
$ hostname
```

```
Test
```

Find your IP address (see [Project 8](#) in [Chapter 1](#)) or consult the asset list or network map you've been maintaining. When you list the agents, verify that an agent with that name and IP address is present ❷. Use the agent's ID number to get its authentication key

3. Return to the main menu with ENTER and use the **Q** option to quit.
6. Open the **Wazuh Agent Manager** on your Windows computer (see [Figure 10-5](#)) and enter the IP address of your Security Onion system and the agent authentication key; click **Save**.

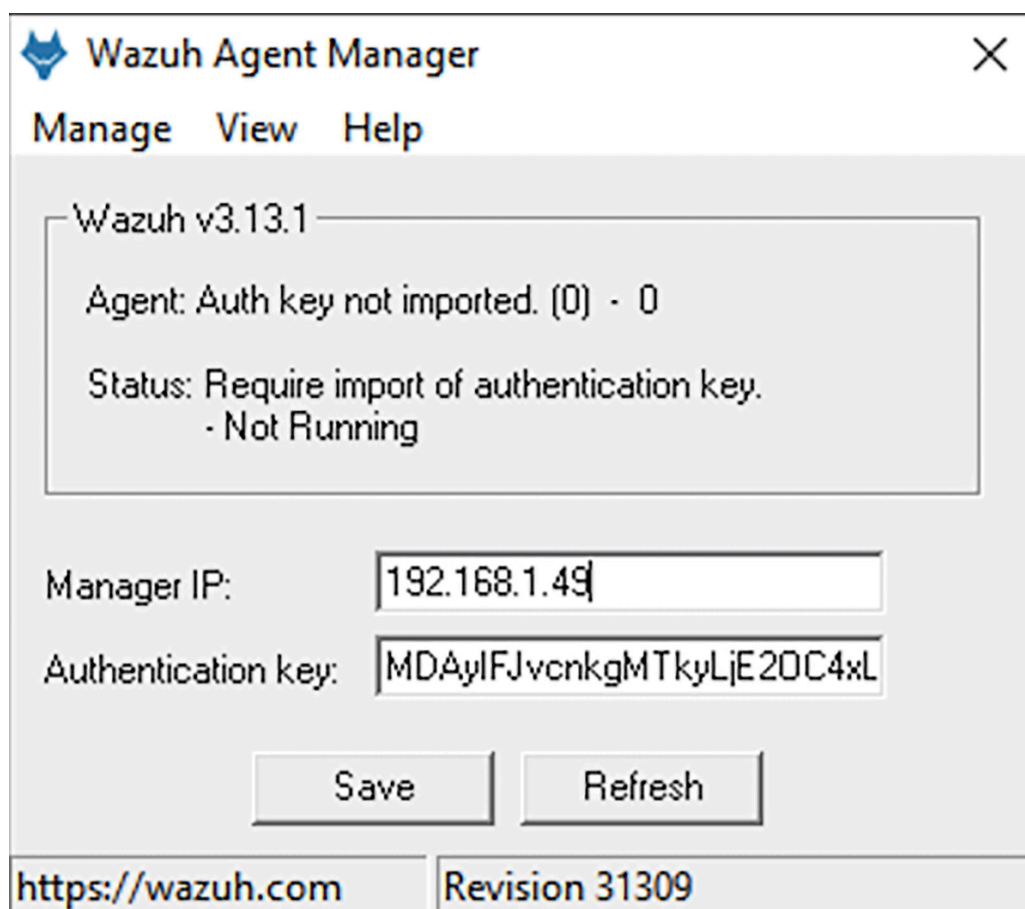


Figure 10-5: Wazuh agent configuration

7. Click **Manage ▶ Start** to start the agent.
8. Every time you add an agent or make a change to Security Onion or the systems that communicate with it, run the **so-allow** script to enable communication between the devices (otherwise, the host firewall on Security Onion will block it). You should do this at the terminal, logged in to the Security Onion system via SSH:

```
$ sudo so-allow
```
9. When prompted, enter **w** to add a firewall rule for a Wazuh agent; then enter the agent's IP address.

Wazuh will now manage this PC. Repeat the process for all other devices (computers, laptops, virtual machines, and so on) in your network that you want to manage in this way. System event logs will then start showing up in your Kibana dashboard, so expect to see new data and alerts in Security Onion.

Installing Wazuh on macOS

To install the Wazuh agent on your macOS endpoint(s), follow these steps:

1. Log in to your Security Onion console, click **Downloads**, and download the macOS package.
2. Run the installation wizard on your Mac.
3. Once complete, log in to your Security Onion system and run `sudo so-allow` to allow your Mac access through the firewall (this must be done before agent registration; otherwise, the agent won't be able to connect to the management server).
4. Following the prompts, choose the Wazuh registration service with `r` and enter the IP address of your endpoint.
5. Now, register the agent with the Security Onion server:

```
$ sudo /Library/Ossec/bin/agent-auth -m security_onion_IP
```

Next, you'll add the Security Onion's IP address to the agent configuration file on your Mac so the agent can communicate with the Security Onion server.

6. Open `/Library/Ossec/etc/ossec.conf` with a text editor.
7. Find the following lines and change `MANAGER_IP` to your Security Onion server's IP address:

```
<client>
<server>
  <address> MANAGER_IP </address>
```

8. Restart the Wazuh agent:

```
$ sudo /Library/Ossec/bin/ossec-control restart
```


4. 9. Confirm the agent has been successfully configured by listing the agents on the Security Onion server; run the *manage_agents* script and enter **L** when prompted for an action:

```
$ sudo docker exec -it so-wazuh /var/ossec/bin/manage_agents
--snip--
```

Choose your action: A,E,L,R or Q: **L**

Available agents:

ID: 001, Name: securityonion, IP: 192.168.1.49

ID: 002, Name: Computer1, IP: 192.168.1.50

ID: 003, Name: MacBook-Pro.local, IP: 192.168.1.51

** Press ENTER to return to the main menu.

```
--snip--
```

Choose your action: A,E,L,R or Q: **Q**

manage_agents: Exiting.

If you see the hostname and IP address of the Mac, the agent is active.

Return to the main menu with ENTER and use the **Q** option to quit.

Installing Wazuh on Linux

To install the Wazuh agent on your Linux endpoint(s), follow these steps:

1. 1. Log in to your Security Onion console, click **Downloads**, and download the relevant package. For Ubuntu, this will be the DEB package (it'll be the RPM package for CentOS and Fedora).

You can download the package directly from your Ubuntu system, or you can download the package to your Windows or Mac computer and transfer it to your Ubuntu system:

```
$ rsync -ruhP wazuh-agent.deb user@linux_ip :/home/ user
```

When installing packages directly from package files (like *.deb* files), use the *dpkg* utility instead of the APT package manager (*dpkg* is the Debian package manager and is used similarly to APT).

2. 2. To install the Wazuh agent, run the following:

```
$ sudo dpkg -i wazuh-agent_ 3.13.1-1 _amd64.deb
```

Your package's version number may be different.

3. Next, log in to your Security Onion system via SSH and run `sudo so-allow` to allow your Linux system access through the firewall.
4. Following the prompts, choose the Wazuh registration service with `r` and enter your endpoint's IP address.
5. 5. Register the Linux agent and connect it to the Wazuh management server (that is, the Security Onion server):

```
$ sudo /var/ossec/bin/agent-auth -m security_onion_IP
```

6. 6. Then, modify the configuration file on your Linux system to allow it to communicate with the management server by changing the `MANAGER_IP` placeholder in the `ossec.conf` file to the IP address of your Security Onion server:

```
$ sudo nano /var/ossec/etc/ossec.conf
```

```
--snip--
```

```
<client>
```

```
<server>
```

```
<address> security_onion_IP </address>
```

```
--snip--
```

7. 7. Restart the Wazuh agent to start sending data to Security Onion with this:

```
$ sudo systemctl restart wazuh-agent
```

8. 8. Finally, confirm the agent has been successfully configured by listing the agents on the Security Onion server; run the `manage_agents` script and enter `L` when prompted for an action:

```
$ sudo docker exec -it so-wazuh /var/ossec/bin/manage_agents
```

```
--snip--
```

```
Choose your action: A,E,L,R or Q: L
```

```
Available agents:
```

```
ID: 001, Name: securityonion, IP: 192.168.1.49
```

```
ID: 002, Name: Computer1, IP: 192.168.1.50
```

```
ID: 003, Name: MacBook-Pro.local, IP: 192.168.1.51
```

```
ID: 004, Name: Linux1, IP: 192.168.1.52
```

```
** Press ENTER to return to the main menu.
```

```
--snip--
```

Choose your action: A,E,L,R or Q: Q

manage_agents: Exiting.

9. If you see the Linux computer's hostname and IP address, the agent should be active. Press ENTER to return to the main menu, and enter Q to quit.

You can now manage all types of computers in your network with Wazuh.

#38: Installing osquery

osquery provides improved visibility within your network. It gathers endpoint data such as the operating system details, installed software, command-line history, and details of running processes; you can then query this data to identify suspicious activity or devices not in compliance with your security policies or configurations. When used together with Wazuh, these tools provide a detailed view of the systems in your network and what each of them is doing or being used for, legitimately or not. Once installed, osquery uses a user interface called Fleet to display and manage the details of your monitored endpoints.

Installing osquery on Windows

To install the osquery agent on your Windows endpoint(s), follow these steps:

1. Log in to your Security Onion console, click **Downloads**, and download the osquery package for Windows (the MSI file).
2. Execute this file on your Windows system and complete the installation wizard.

Once osquery is installed, it'll be invisible and run in the background; there's no user interface to deal with.

3. Next, log in to your Security Onion system via SSH and run `sudo so-allow` to allow your computer and osquery access through the

firewall. Enter `o` (for osquery) and the IP address of your Windows system when prompted.

4. To view and manage systems with osquery, log in to your Security Onion console. In the left menu, click the **Fleet** link to open the Fleet Manager Dashboard.

When you install osquery on an endpoint and after you run `so-allow` to enable communication between the osquery agent and the Security Onion server, your managed hosts should show up here as cards; it can take a few minutes for communication to begin.

Installing osquery on macOS

To install the osquery agent on your macOS endpoint(s), follow these steps:

1. Log in to your Security Onion console, click **Downloads**, and download the osquery package for Mac (the PKG file).
2. Run `sudo so-allow` on your Security Onion server and add your Mac to the list of allowed agents for osquery. Enter `o` (for osquery) and the IP address of your Mac when prompted.
3. Execute the file you downloaded and complete the installation wizard on your Mac.
4. Log in to the Fleet Manager Dashboard and click **Add New Host** to find your Fleet Secret.
5. Add your Fleet Secret to the `/etc/so-launcher/secret` file using any text editor.
6. Update `/etc/so-launcher/launcher.flags` so the hostname value is `security_onion_IP :8090` and the root directory value is `/var/so-launcher/ security_onion_IP -8090 :`

autoupdate

hostname 192.168.1.200:8090

root_directory /var/so-launcher/192.168.1.200-8090

osqueryd_path /usr/local/so-launcher/bin/osqueryd

enroll_secret_path /etc/so-launcher/secret

```
update_channel stable
```

```
root_pem /etc/so-launcher/roots.pem
```

7. Copy the contents of the `/etc/ssl/certs/intca.crt` file on your Security Onion server into the `/etc/so-launcher/roots.pem` file on your Mac.

After a few minutes, your Mac should show up as a new card in the Fleet Manager Dashboard.

Installing osquery on Linux

To install the osquery agent on your Linux endpoint(s), follow these steps:

1. Log in to your Security Onion console, click **Downloads**, and download the osquery package for Linux (the DEB file for Ubuntu, RPM for CentOS, and so on).
2. Run `sudo so-allow` on your Security Onion server to add your Linux system to the list of allowed agents for osquery. Enter `o` (for osquery) and the IP address of your Linux system when prompted.
3. 3. Install the downloaded file on your Linux system; here's an example using `dpkg` on Ubuntu:

```
$ sudo dpkg -i deb-launcher.deb
```

Your Linux system should automatically show up as a new card in your Fleet Manager dashboard.

A Network Security Monitoring Crash Course

You've now installed the necessary hardware and software to monitor your network for suspicious and malicious activity. You need to be able to identify issues, respond to incidents when they occur, and keep your network, users, and data secure. In this section, we'll cover the fundamentals of how to configure and make use of osquery, Wazuh, and the Security Onion Alerts Dashboard.

Using osquery

If you're familiar with *relational databases* and *Structured Query Language (SQL)*, using osquery will be reasonably easy for you. If not, here are the basics. You can view all the data for the devices in your network that osquery manages in the Fleet Manager Dashboard. To reach the dashboard, log in to your Security Onion console at https://<security_onion_IP>/ and click **Fleet** in the administrator menu on the left.

Data is stored in a series of *data tables*, wherein each table contains two or more columns (also called *tuples*) that include information such as hostname, IP address, MAC address, uptime, last shutdown time, and so on, for each device. Each row in the table relates to a specific entity, such as a computer or laptop, or something more atomic, like a specific user account on a device. For example, the *users* table looks similar to **Table 10-1**.

Table 10-1: The osquery Users Table

UID	GID	UID_Signed	GID_Signed	Username	Description
0	0	0	0	testuser	A test user account

The Username column's first row of data pertains to the *testuser* account on a device. Each of these tables is related to one or more of the other tables in the database (of which there are more than 200). These tables and their relationships allow you to perform powerful queries about the details and status of each managed device.

We can ask questions of this data using a query language called SQL, a high-level language for accessing and manipulating databases. A SQL query looks like this:

```
SELECT c1,c2 FROM tablename
```

In this query, the uppercase commands, `SELECT` and `FROM`, indicate the action you want to perform—in this case, asking for the data in columns 1 and 2, represented by the `c1` and `c2` parameters, from the table called `tablename`.

In practice, that query would look like this:

```
SELECT username FROM users
```

```
SELECT * FROM users
```

The first command returns (displays to the user running the query) all the usernames that exist in the `users` table and no other columns. The second command returns all (`*`) of the columns and rows from the `users` table.

NOTE Several SQL commands are available for retrieving data in different ways; see the SQL cheat sheet at <https://www.sqltutorial.org/sql-cheat-sheet/> for more details. See also the osquery documentation at <https://osquery.io/> for a listing of all available tables and their data.

Fleet stores a lot of queries in your Fleet dashboard. Click the **Query** menu on the left of the page (see [Figure 10-6](#)).

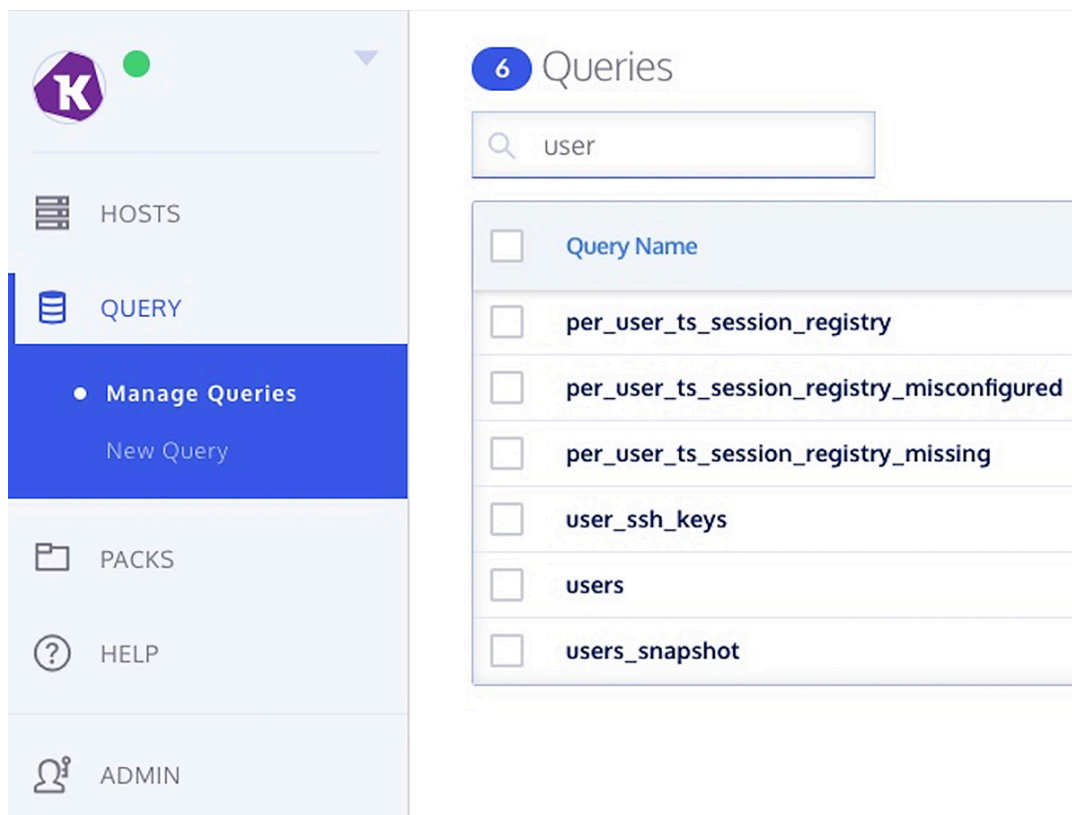


Figure 10-6: Stored SQL queries in Fleet Manager

From this menu, you can scroll through the available queries or search for a specific query using the search bar at the top of the page. Once you've identified a query you want to run, click to select it, and then click the **EDIT/RUN QUERY** button on the right side. Before you're able to execute the query, you need to select the devices you want to query for this information. Select the relevant device(s) from the Select Targets drop-down menu and then click **Run**. When the query completes, Fleet will present you with the results of the query at the bottom of the screen; you can filter the results using the column filters provided.

It's up to you which queries you run, and it depends on what kinds of problems or examples of noncompliance are most concerning to your network. However, these are a few good places to start:

users Useful for identifying user accounts that should or should not exist on given endpoints

browser_plugins Shows all browser plug-ins on a device(s); useful if your users install potentially malicious browser plug-ins

chrome_extension As previously, specifically looking for Chrome plug-ins

crontab Identifies scheduled tasks on Linux systems performing suspicious or malicious activity

disk_free_space_pct Identifies devices with low disk space

installed_applications Identifies malicious or potentially unwanted applications installed on devices

The Hosts dashboard in Fleet shows the details for each managed device at a glance in the form of cards (see **Figure 10-7**).

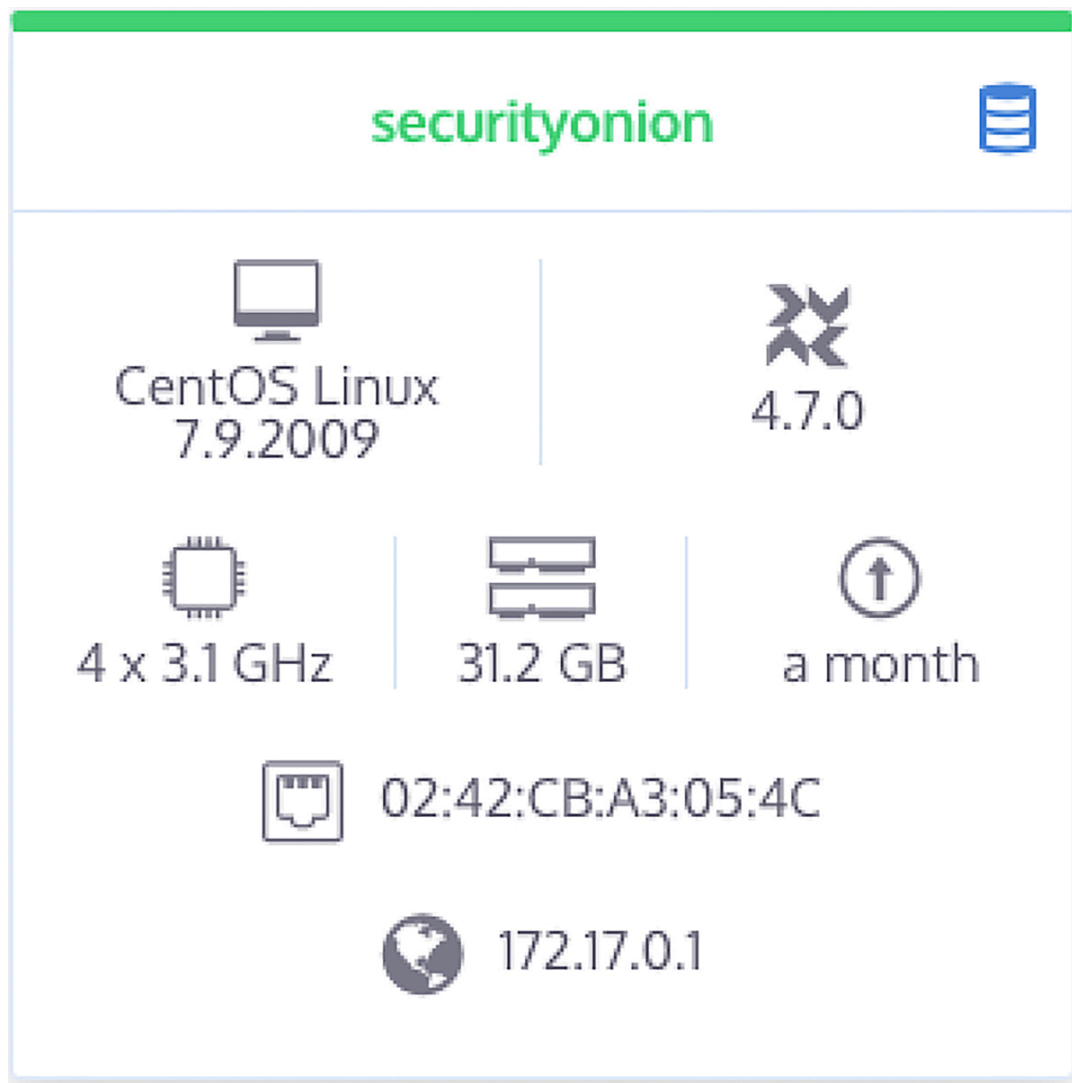


Figure 10-7: Fleet Host dashboard view

Here you can see the hostname, operating system, osquery version, processor details, amount of RAM, uptime, MAC address, and IP address of this host. Clicking the blue query button (the stacked cylinders) at the top right will allow you to easily query this device.

Spend some time familiarizing yourself with the available queries and do some online research to find other potentially useful queries. Try reviewing some of the saved queries and edit or copy them to get the queries you want.

Using Wazuh

We installed the Wazuh agent in [Project 35](#), and we'll configure it in this section. Wazuh allows us to review the logs and alerts in Security Onion, which we'll explore in the next section.

The primary Wazuh config file is located at `/opt/so/conf/wazuh/ossec.conf` on the Security Onion system. Each section of this configuration file is separate and identified with a line like the following:

```
<!-- Files/directories to ignore -->
```

You can revise the settings in this file to change the way Wazuh behaves, which can be useful if, for example, Wazuh reacts to a false positive detection and stops you from doing something benign. Review this file to get an understanding of the types of things Wazuh monitors for.

The section shown in the following snippet specifies files that contain lists of files that are known or expected to be malicious based on identified adversary behaviors, followed by files that are expected to contain trojans (a type of virus) and then files and folders to audit for various vulnerabilities:

```
--snip--
```

```
<rootkit_files>/var/ossec/etc/shared/rootkit_files.txt</rootkit_files>
```

```
<rootkit_trojans>/var/ossec/etc/shared/rootkit_trojans.txt</rootkit_trojans>
```

```
<system_audit>/var/ossec/etc/shared/system_audit_rcl.txt</system_audit>
```

```
<system_audit>/var/ossec/etc/shared/system_audit_ssh.txt</system_audit>
```

```
<system_audit>/var/ossec/etc/shared/cis_rhel7_linux_rcl.txt</system_audit>
```

```
--snip--
```

Each of these files contains a list of things Wazuh will monitor. If the agent detects a file or configuration on a device that matches a behavior or setting in the *rootkit_files.txt* file, it will take action to remediate that threat. If you don't want it to take that action, delete or comment out that line in the configuration file with a `#`.

When you update Wazuh as part of your efforts to consistently update and patch your Security Onion and other systems, the configuration files such as *rootkit_files.txt* may also receive updates. This ensures that as new threats are identified and indicators of compromise are made publicly available, your network stays protected. To avoid losing any changes you make to these files, consider creating new, custom configuration files (such as *my_custom_trojans.txt*) and adding a reference to this file in the *ossec.conf* file, such as the following example:

```
--snip--
```

```
<rootkit_files>/var/ossec/etc/shared/rootkit_files.txt</rootkit_files>
```

```
<rootkit_trojans>/var/ossec/etc/shared/rootkit_trojans.txt</rootkit_trojans>
```

```
<rootkit_trojans>/var/ossec/etc/shared/my_custom_trojans.txt</rootkit_trojans>
```

```
--snip--
```

Adding files to the *ossec.conf* file will result in Wazuh referring to those files for its configuration and settings, in addition to its default configuration files. Using custom files is a good way to add custom configurations that you might have.

If you want Wazuh to ignore a directory or list of directories on any of the endpoints on which it's installed, add that information in the relevant section. You can also tell the agent to ignore specific files or file types, to exclude certain devices from active response (if you want the

agent to never block activity on a specific device that might impact your network), and to set various other options. Familiarize yourself with these configuration files so you can tailor them to your environment.

Using Security Onion as a SIEM Tool

Security Onion, in addition to the other useful capabilities it provides, acts as a *security information and event management (SIEM)* tool. Several SIEMs are available on the market, including Splunk, SolarWinds, or ManageEngine, all of which are commercial solutions and can be very expensive. Security Onion, on the other hand, is open source and free.

A SIEM is designed to aggregate data from devices in a network and act as a central repository for logs and other data. Implementing a SIEM like Security Onion centralizes your logs, making it harder for an adversary to hide their tracks by deleting the logs on any one system. It also enables you to query your logs and other system data in one location so you don't have to check every system or device individually, streamlining the process. Security Onion then analyzes this data and alerts you to potentially malicious activity. **Figure 10-8** shows a list of alerts, found by logging in to the Security Onion console and clicking the Alerts option in the menu on the left.

























	Count	rule.name	event.module	event.severity_label
 	14,102	Windows Logon Success	windows_eventlog	low
 	9,769	ET POLICY GNU/Linux APT User-Agent Outbound likely related to package management	suricata	low
 	6,281	Listened ports status (netstat) changed (new port opened or closed).	ossec	low
 	5,889	ET POLICY Outgoing Basic Auth Base64 HTTP Password detected unencrypted	suricata	high
 	4,169	Service startup type was changed	windows_eventlog	low
 	3,614	ET INFO [eSentire] Possible Kali Linux Updates	suricata	high
 	2,380	ET USER_AGENTS Steam HTTP Client User-Agent	suricata	high
 	1,812	Integrity checksum changed.	ossec	low
 	1,503	ET INFO TLS Handshake Failure	suricata	medium
 	1,430	ET JA3 Hash - [Abuse.ch] Possible Adware	suricata	low
 	1,348	ET POLICY curl User-Agent Outbound	suricata	medium
 	707	ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers	suricata	high

Figure 10-8: Security Onion alerts

When you click an alert, a context menu is displayed with filtering options; you can include, exclude, show only, or group by the alert you’ve selected. You can also drill down into an alert to show every instance of the alert in the timeframe you’re filtering for. By expanding any of these alerts, you can see all of its information, including metadata (see [Figure 10-9](#)) such as the alert’s timestamp, the source and destination IP address of the network traffic, the full message associated with the alert, the actual decoded network data that caused the rule or alert to fire, the rule itself, and often a reference so that you can learn more about the alert, including potential remediation steps or other solutions.

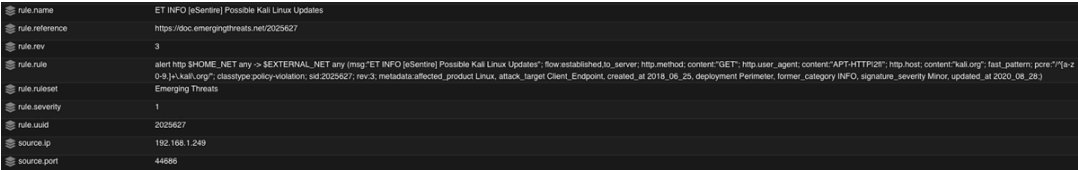


Figure 10-9: Security Onion alert metadata

In practice, the alerts dashboard will show a lot of different categories and types of activity; you’ll almost always see alerts that require further investigation. Let’s discuss a few to help get you started.

Table 10-2: Examples of Potentially Unwanted Software in an Environment		
Rule name	Event module	Severity
ET INFO [eSentire] Possible Kali Linux Updates	suricata	high
ET USER_AGENTS Steam HTTP Client User-Agent	suricata	high

Table 10-2: Examples of Potentially Unwanted Software in an Environment

Rule name	Event module	Severity
ET POLICY curl User-Agent Outbound	suricata	medium
ET POLICY Dropbox.com Offsite File Backup in Use	suricata	high
ET SCAN Possible Nmap User-Agent Observed	suricata	high
ET TFTP Outbound TFTP Read Request	suricata	high
ET P2P eMule KAD Network Connection Request	suricata	high

Table 10-2 shows several examples of software that is potentially vulnerable, could lead to or be used for malicious activity, or shouldn't be on your network in the first place. Kali Linux, for example, is typically used for penetration testing, but attackers can also use it to compromise your network. If you receive this alert, investigate it, identify the system responsible, and remove it from the network. Security Onion provides all of the information you need to do this. You could choose to take the source IP address in the alert and add firewall rules (on your hosts as well as your border firewall) to block all traffic to and from that address, as an example of one mitigation strategy.

Looking at the other alerts in **Table 10-2**, several pieces of software have been identified that might not be allowed or necessary in your network. Steam is a game client. Curl is a utility for transferring data to or from a server and can be used to exfiltrate data from your net-

work or download malware. Dropbox is a cloud storage solution that can likewise be used to exfiltrate or steal data. Nmap is a network mapping tool that attackers can use to identify potential targets and vulnerabilities within your network. Trivial File Transfer Protocol (TFPT) is a vulnerable protocol used for transferring files, and eMule is a peer-to-peer application typically used for file sharing.

Generally, if you aren't using a tool or application, you should uninstall or otherwise remove it to prevent attackers from using it and make your network more secure. If you don't use curl, for example, track down the client responsible for this alert using the hostname, source and destination IP address, or other metadata in the alert itself, and uninstall or remove the offending software. If you use Dropbox, you can safely ignore the alert. Otherwise, investigate and remove it from your network. Do this for all software-related alerts.

Then, use the same process to investigate and remediate all the alerts related to potential malware activity; **Table 10-3** shows an example. Drill down into each alert, identify the device(s) related to the alert, look at the references for the rule behind the alert, and identify and resolve the root cause. If you get stuck, an internet search is usually the best tool to solve a lot of problems.

Table 10-3: Possible Malware Alerts in Security Onion

Rule name	Event module	Severity
ET JA3 Hash - [Abuse.ch] Possible Adware	suricata	Low
ET JA3 Hash - Possible Malware - Neutrino	suricata	Low
ET INFO Packed Executable Download	suricata	Low

Table 10-3: Possible Malware Alerts in Security Onion

Rule name	Event module	Severity
ET INFO EXE IsDebuggerPresent (Used in Malware Anti-Debugging)	suricata	Low
ET EXPLOIT Possible OpenSSL HeartBleed Large HeartBeat Response (Client Init Vuln Server)	suricata	Medium
ET EXPLOIT Possible OpenSSL HeartBleed Large HeartBeat Response (Server Init Vuln Client)	suricata	Medium

Other alerts of interest are those related to account login or log-off actions and elevation of privileges, such as Successful sudo to ROOT executed, as shown in [Table 10-4](#).

Table 10-4: Successful and Failed Login Alerts in Security Onion

Rule name	Event module	Severity
Windows Logon Success	windows_eventlog	Low
PAM: Login session closed.	ossec	Low
PAM: Login session opened.	ossec	Low
Successful sudo to ROOT executed.	ossec	Low

Table 10-4: Successful and Failed Login Alerts in Security Onion

Rule name	Event module	Severity
Logon Failure - Unknown user or bad password	windows_eventlog	Low

While successful logon attempts alert you to accounts that may already be compromised, failed logon attempts can alert you to an attacker trying to break in. In both cases, investigate those alerts to determine whether it's legitimate activity. If, for example, you see an account increasing their privileges to root on a Linux system, determine whether it was you or another trusted user in your network. If it wasn't you or another administrator in your network, change your passwords and investigate any related activity that occurred around the same time.

Summary

Security Onion's alerts provide a starting point for you to identify and chase down suspicious activity; use them to your advantage when securing your network. Use every tool you have at your disposal, as you can be sure that adversaries are doing the same. Simply increasing the visibility of activity on your network enables you to better protect it. With the instructions and tools described in this chapter, you'll soon find a multitude of potential activity to investigate and remediate. Expect this investigation activity to be ongoing and try to keep up with the alerts in Security Onion as your network continues to grow and evolve over time.