

Install Osquery, Beats & Wazuh

FleetDM:

Security Onion includes FleetDM to manage your osquery deployment.

I hope you configure your FleetDM during the installer.

Fleet configuration can be found in `/opt/so/conf/fleet/`

osquery

To deploy an osquery agent to an server,

- go to the Security Onion Console (SOC) Downloads page
- download the proper osquery agent for the operating system of that endpoint.
- Use `so-allow` to allow the osquery agent to connect to port 8090 on the manager.
- Then install the osquery agent.

You can find the osquery, which is showing up in FleetDM

Osquery will attempt to connect to the manager via the manager's IP or Hostname - whichever was selected during the manager setup.

If the hostname is used, the endpoints need to be able to resolve that hostname to the manager's IP.

See this value by running the following command on the manager: `sudo salt-call pillar.get global:url_base`.

Shipping Windows Eventlogs

Windows Eventlogs from the local Windows system can be shipped with osquery to Security Onion. Current parsing support extends to core Windows Eventlog channels (Security , Application , System) as well as Sysmon under the default channel location. These logs will show up in Security Onion as `event.dataset: windows_eventlog` OR `event.dataset: sysmon`.

- Confirm that you can successfully live query the logs: `SELECT * FROM windows_events limit 10;`
- Save a new query: Query -> Manage Queries -> Create New Query `SELECT * FROM windows_events;` -> **Save**
- Add the new query to a query pack that targets a Windows host - how often it should run depends on log volume on the local host; start off with 180 seconds, differential logging: Packs -> Manage Packs -> Select + Edit Pack (Modify Targets for Windows only if needed, Modify Logging options as needed)
- Save pack + Enable pack, if needed.

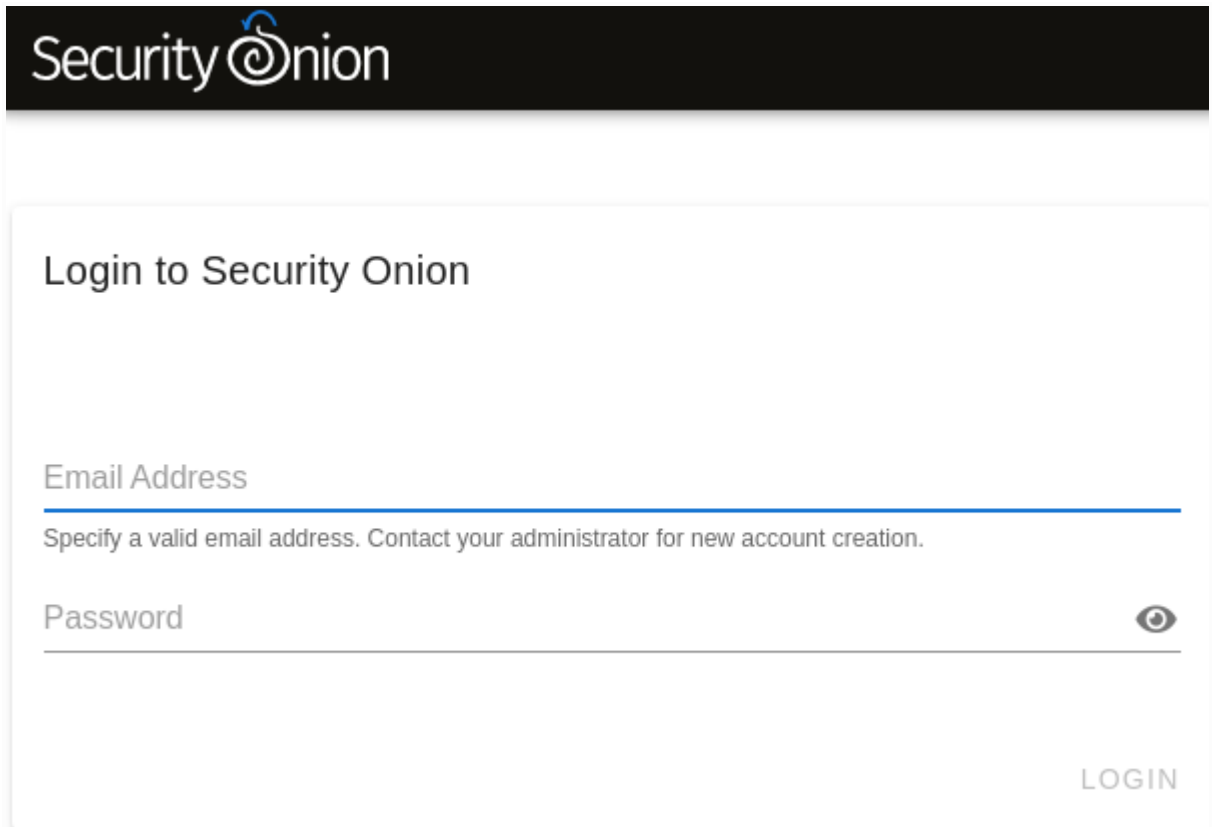
Beats

We can use Elastic Beats to facilitate the shipping of windows server logs to Security Onion's Elastic Stack.

Currently, testing has only been performed with Filebeat (multiple log types) and Winlogbeat (Windows Event logs).

To deploy a beats,

- Run `so-allow` and select the `b` option to allow your Beats agents to send their logs to Logstash port `5044/tcp`.
- When downloading a Beats agent, make sure the version number matches the version of Elastic running on your Security Onion deployment.
- Navigate to the Downloads page in Security Onion Console (SOC) and download the linked Winlogbeat agent. This will ensure that you get the correct version of Winlogbeat for your Elastic version.


The image shows the Security Onion console login interface. At the top is a black header with the 'Security Onion' logo in white. Below the header is a white box with a light gray border. Inside this box, the title 'Login to Security Onion' is displayed. There are two input fields: 'Email Address' and 'Password'. The 'Email Address' field has a blue underline and a note below it: 'Specify a valid email address. Contact your administrator for new account creation.' The 'Password' field has a gray underline and a toggle icon (an eye) to its right. At the bottom right of the white box is a 'LOGIN' button.

Security Onion

Login to Security Onion

Email Address

Specify a valid email address. Contact your administrator for new account creation.

Password 

LOGIN

fig: Security Onion Console

Install Winlogbeat:

Install Winlogbeat and copy `winlogbeat.example.yml` to `winlogbeat.yml` if necessary. Then configure `winlogbeat.yml` as follows:

- Make sure that the `setup.dashboards.enabled` setting is commented out or disabled.
- Disable the `output.elasticsearch` output.
- Enable the `output.logstash` output and configure it to send logs to port 5044 on your management node.
- If you are shipping Sysmon logs, confirm that your Winlogbeat configuration simply collects the Sysmon logs and does NOT use the Elastic Sysmon processors section as Security Onion will do all the necessary parsing.

I will discuss later about Sysmon, which is necessary for forwarding syslogs.

Once winlogbeat.yml is configured properly, start the Winlogbeat service.

Installation

To install a Beat, follow the instructions provided for the respective Beat, with the exception of loading the index template, as Security Onion uses its own template file to manage Beats fields.

Winlogbeat

<https://www.elastic.co/guide/en/beats/winlogbeat/current/winlogbeat-installation.html>

Winlogbeat

C:\Program Files\Winlogbeat\winlogbeat.log

- In Dashboards and Hunt, you can find Beats data by searching for `_index:"*:so-beats-*"`
- In Kibana, you can find Beats data on the Host dashboard or by searching for `_index:"*:so-beats-*"` in Discover.

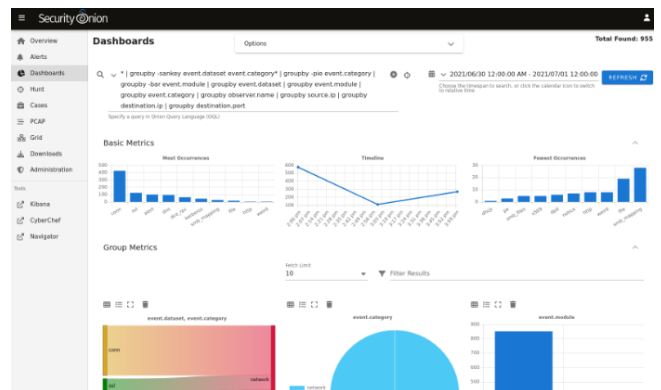
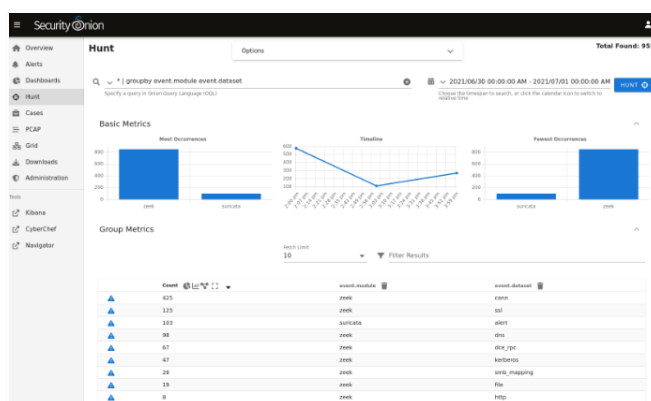


Fig: Hunt

Fig: Dashboard

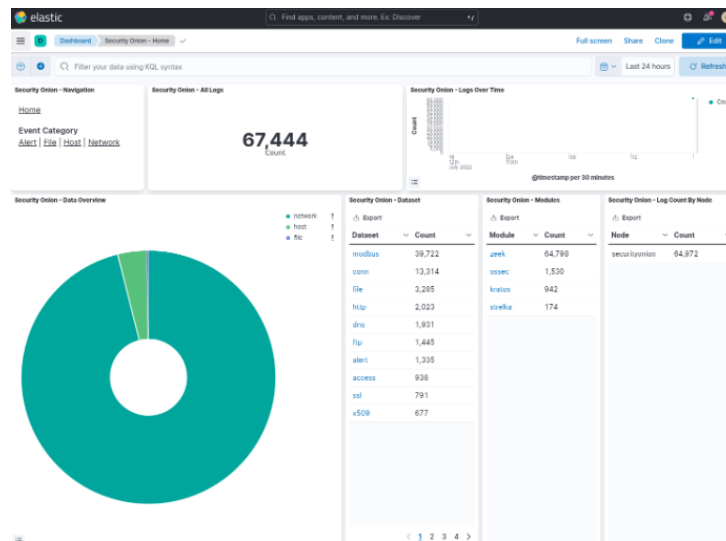


Fig: Kibana

Wazuh

Wazuh is a free, open source and enterprise-ready security monitoring solution for threat detection, integrity monitoring, incident response and compliance.

Usage

Security Onion utilizes Wazuh as a Host Intrusion Detection System (HIDS) on each of the Security Onion nodes.

The Wazuh components include:

manager - runs inside of `so-wazuh` Docker container and performs overall management of agents

API - runs inside of `so-wazuh` Docker container and allows for remote management of agents, querying, etc.

agent - runs directly on each host and monitors logs/activity and reports to manager

The Wazuh API runs at TCP port 55000 locally, and currently uses the default credentials of user:foo and password:bar for authentication. Keep in mind, the API port is not exposed externally by default. Therefore, firewall rules need to be in place to reach the API from another location other than the Security Onion node on which the targeted Wazuh manager is running.

Since the manager runs inside a Docker container, many of the Wazuh binaries that you might want to run will need to be run inside the Docker container. For example, to run agent_upgrade:

```
sudo so-wazuh-agent-upgrade
```

- The main configuration file for Wazuh is /opt/so/conf/wazuh/ossec.conf.
- If you want to send logs to an external system, you can configure Logstash to output to Syslog.

Sysmon

System Monitor (Sysmon) is a Windows system service and device driver that, once installed on a system, remains resident across system reboots to monitor and log system activity to the Windows event log.

You can download sysmon from Microsoft at

<https://download.sysinternals.com/files/Sysmon.zip>

Once you've downloaded sysmon, you probably also want to download a sysmon config to use as a starting point. Here are a few options to choose from.

<https://github.com/Neo23x0/sysmon-config>

<https://github.com/SwiftOnSecurity/sysmon-config>

<https://github.com/olafhartong/sysmon-modular>

- Sysmon logs can be collected and transported using Beats, osquery, or Wazuh
- If you are shipping Sysmon logs via Winlogbeat (see the Beats section), confirm that your Winlogbeat configuration does NOT use the Elastic Sysmon module. Security Onion will do all the necessary parsing.
- Once Security Onion is receiving and parsing Sysmon data, you can search for that data and visualize it via [Dashboards](#), [Hunt](#), or [Kibana](#).