Security Onion Solutions Sensor for FireEye Helix

Integration Enablement Guide

The Security Onion Solutions Sensor for FireEye Helix enables customers to gain visibility into the network. Begin using the Security Onion Solutions Sensor by following these two steps:

STEP 1: Download the latest ISO image file from the Security Onion Solutions GitHub:

https://securityonion.net/hybridhunter

STEP 2: Follow the setup instructions listed at the bottom of the page link above

Setup should start immediately when you log in. Follow the prompts and select the **HELIXSENSOR** option (screenshot below). You can skip the prompt for the API key and instead paste the key in an SSH session post-installation by running the "sudo so-helix-apikey" command.

Security Onion Solutions

Security Onion is a free and open source Linux distribution for intrusion detection, enterprise security monitoring, and log management. It includes Elasticsearch, Logstash, Kibana, Snort, Suricata, Bro, Wazuh, Sguil, Squert, CyberChef, NetworkMiner, and many other security tools, helping customers 'peel back the layers' of their networks.

In addition to the sensor, Helix offers over 10 Security Onion Solutions dashboards that enable customers to detect and respond to attacks, identify anomalies quickly, and hunt for attackers using contextual data beyond alerts.