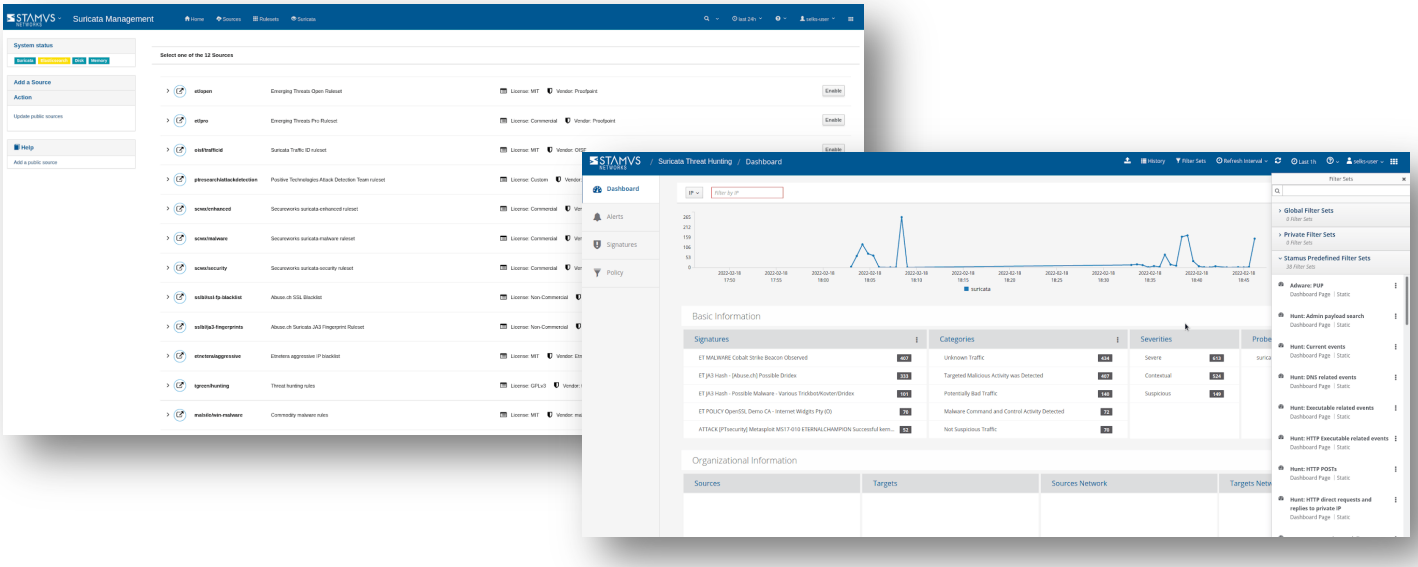
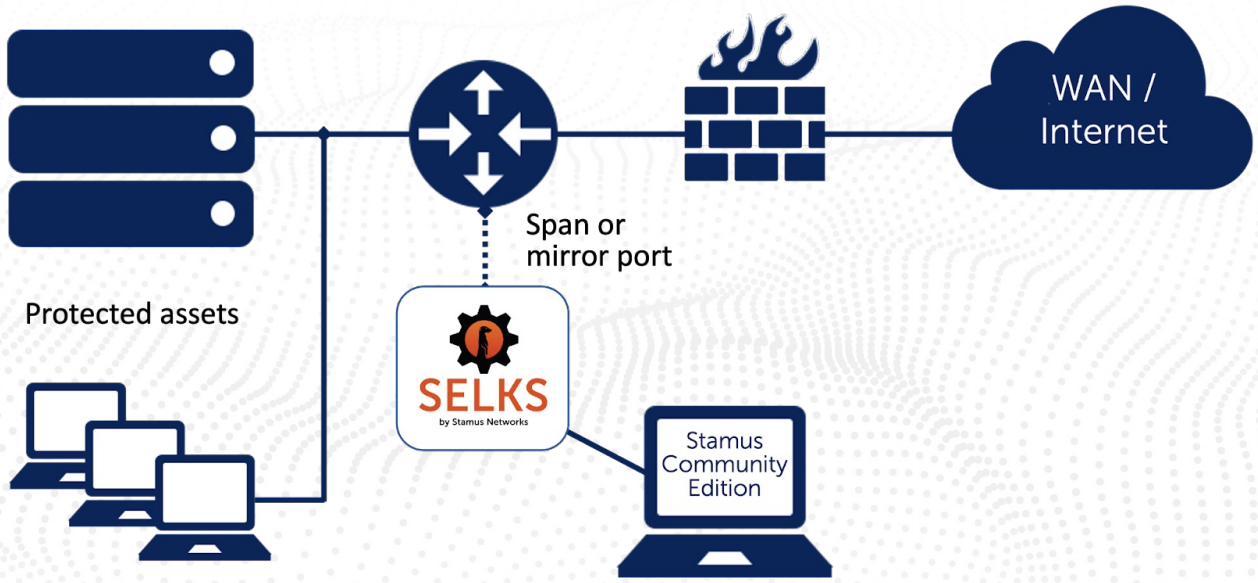
Datasheet

SELKS by Stamus Networks

SELKS is a free, open-source, and turn-key Suricata network intrusion detection/protection system (IDS/IPS), network security monitor (NSM) and threat hunting implementation created and maintained by Stamus Networks.



Released under GPLv3 license, the live distribution is available as either a live and installable Debian-based ISO or via Docker compose on any Linux operating system.



SELKS is a showcase for the powerful Suricata IDS/IPS/NSM engine and the network protocol logs and security alerts it produces. All data in SELKS is generated by Suricata

WHY IT IS CALLED SELKS

SELKS derives its name from the five major components that comprise it:

- **S**uricata - Ready to use Suricata
- **E**lasticsearch - Search engine
- **L**ogstash - Log injection
- **K**ibana - Custom dashboards and event exploration
- **S**tamus Community Edition - Suricata ruleset management and threat hunting user interface

In addition, SELKS now includes Arkime, EveBox and CyberChef

STAMUS COMMUNITY EDITION

Stamus CE is the Stamus Networks open-source application that brings all these components together. Stamus CE provides the web interface for the entire system, giving you the ability to:

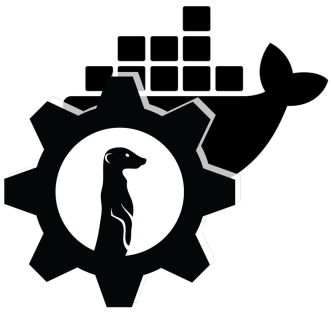
- Manage multiple Suricata rulesets and threat intelligence sources
- Upload and manage custom Suricata rules and IoC data files
- Hunt for threats using 24 predefined filters and enhanced contextual views
- View all protocol and file transactions and flow logs generated by Suricata
- Access to over 28 default dashboards and more than 400 visualizations
- Apply thresholding and suppression to limit verbosity of noisy alerts
- View Suricata performance statistics and information about Suricata rule activity
- Apply Kibana, EveBox, and Cyberchef to the Suricata NSM and alert data

Note: Stamus CE is bundled with the other elements into a single system. It is not possible to manage multiple SELKS instances with Stamus CE.

THREE SELKS INSTALLATION OPTIONS

SELKS is available either as a portable Docker Compose package or as turnkey installation images (ISO files).

SELKS Docker Compose Package



Use the Docker Compose package to install SELKS in any LINUX environment and ensure you are including the very latest containers, including Evebox and Suricata.

Complete Image with Desktop

For turnkey installation that includes the Debian Linux desktop environment. Can be deployed on bare metal hardware or VM. Works well in air-gapped environments or when the full operating system is required.

Complete Image without Desktop

For turnkey SELKS installation in a headless environment. Can be deployed on bare metal hardware or VM. Works well in air-gapped environments or when the full operating system is required.

PLATFORM REQUIREMENTS

The following are the minimum requirements for installing SELKS

- 2 cores
- 8-10 GB of free RAM
- 100GB (10 GB for Docker package) of free disk space (high-performance SSD is recommended)

Because both Suricata and Elasticsearch are multithreaded, performance will improve with additional cores. Likewise, by allocating additional memory, SELKS will more easily support additional traffic loads. Finally, more disk space is required to support higher traffic rates and longer data retention.

WHO IS SELKS DESIGNED FOR?

For many small-to-medium sized organizations, SELKS can be a suitable production-grade network security monitoring (NSM) and intrusion detection (IDS) solution.

And because all the data available in SELKS is generated by the Suricata engine, SELKS is widely used by network security practitioners, educators, and hobbyists to explore what is possible with Suricata IDS/IPS/NSM and the network protocol monitoring logs and alerts it produces.

For enterprise scale applications, please review our commercial solution, Stamus Security Platform (SSP), described below.

WHAT ABOUT ENTERPRISE SCALE DEPLOYMENTS?

While SELKS is an excellent platform to explore the power of Suricata for intrusion detection and threat hunting, it was never designed to be deployed in an enterprise setting. For enterprise applications, please review our commercial solution, Stamus Security Platform.

To learn more about the differences between SELKS and our commercial solutions, refer to the white paper, Understanding SELKS and Stamus Commercial Platforms.

Download it here: https://www.stamus-networks.com/selks#enterprise

REPORT ISSUES AND GET SELKS SUPPORT

To access README documentation, the issues tracker, and the SELKS wiki, please visit the SELKS GitHub page here: https://github.com/StamusNetworks/SELKS

To ask questions or ask for help, join the Stamus Networks Discord server here: https://discord.com/invite/e6GQKGS5HN

ABOUT STAMUS NETWORKS

Stamus Networks believes in a world where defenders are heroes, and a future where those they protect remain safe. As defenders face an onslaught of threats from well-funded adversaries, we relentlessly pursue solutions that make the defender's job easier and more impactful. A global provider of high-performance network-based threat detection and response systems, Stamus Networks helps enterprise security teams accelerate their response to critical threats with solutions that uncover serious and imminent risk from network activity. Our advanced network detection and response (NDR) solutions expose threats to critical assets and empower rapid response.

STAMUS NETWORKS

5 Avenue Ingres
75016 Paris
France

450 E 96th St. Suite 500
Indianapolis, IN 46240
United States

contact@stamus-networks.com
www.stamus-networks.com

