Understanding SELKS and the Stamus Networks Commercial Platforms

By Éric Leblond, Peter Manev

White Paper

WP-SELKS-SSP-102022-1

STAMUS NETWORKS

Many SELKS users are pleased with its capabilities. If you are one of those users, you may be wondering if there is any value in upgrading to the Stamus Security Platform (SSP), the commercial product offerings from Stamus Networks. In this white paper we will explain the differences among the platforms and help the reader make an informed decision.

BACKGROUND

Before we explore the distinctions between these two solutions, we first need to establish some baseline understandings.

SELKS

Developed by Stamus Networks, SELKS is a turnkey Suricata-based IDS/IPS/NSM ecosystem with its own graphic rule manager and basic network threat hunting capabilities. SELKS is a Debian-based live distribution built from 5 key open-source components that comprise its name – Suricata, Elasticsearch, Logstash, Kibana and Stamus Community Edition (Suricata Management and Suricata Hunting). In addition, it includes components from Arkime (formerly Moloch) and Evebox, which were added after the acronym was established.

SELKS is a contribution made by Stamus Networks to the open-source community. It is freely available and is released under the GNU GPLv3 license.

The source files, README, issues tracker and wiki may be found on GitHub: https://github.com/StamusNetworks/SELKS

Information on each individual component may be found at the sites listed to the right:

(S) Suricata IDPS - http://suricata-ids.org/
(E) Elasticsearch - https://www.elastic.co/products/elasticsearch
(L) Logstash - https://www.elastic.co/products/logstash
(K) Kibana - https://www.elastic.co/products/kibana
(S) Stamus Community Edition -https://github.com/StamusNetworks/scirius
EveBox - https://evebox.org/
Moloch - https://molo.ch/

STAMUS SECURITY PLATFORM

The Stamus Security Platform (SSP) is a commercial enterprise-scale solution developed and supported by Stamus Networks. SSP is an advanced network detection and response system that exposes serious and imminent threats to critical assets and empowesr rapid response.

It is offered in the two tiers listed below:

Stamus ND is a Suricata-based intrusion detection (IDS) and network security monitoring (NSM) system, that delivers:

- Correlated IDS (signature-based) and NSM (protocol transaction logs) data
- Open interfaces for SIEM
- Turn-key Splunk app
- Support for third-party signatures and threat intelligence
- Tagging & classification for automated triage and alert reduction
- Integrated guided threat hunting

Stamus NDR is a broad-spectrum, open network detection and response (NDR) system built on top of Stamus ND that adds:

- Declarations of Compromise™ - response-ready threat detection from machine learning, stateful logic, and signatures
- Asset-oriented attack insights
- Open interfaces for SOAR, SIEM, XDR, IR
- Includes Stamus threat intelligence and custom threat detection
- Explainable and transparent results with evidence

To learn more about Stamus Security Platform, visit the Stamus Networks website here: https://www.stamus-networks.com/

KEY DISTINCTIONS

While Stamus Security Platform is built using many of the same components as SELKS, it is in fact, much more complete and enterprise class systems. There are seven major dimensions to consider when comparing SELKS to SSP:

- Enterprise Scale and Integration
- Organization-Specific Context
- Threat Detection and Hunting
- Network Security Monitoring
- Event Noise Reduction
- Total Cost of Ownership
- Enterprise Support

This paper looks more closely at each of these.

ENTERPRISE SCALE AND INTEGRATION

Scale is one of the most obvious differences between the SELKS and Stamus Security Platform. In the simplest terms, SELKS includes only a single instance of Suricata and is only capable of managing one sensor. In SELKS, the Suricata rules management and threat hunting interface are directly coupled with the sensor.

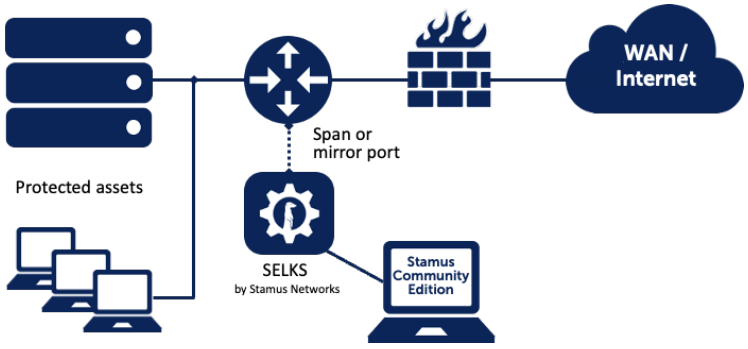

Figure 1. SELKS - a single instance of Suricata with the management system integrated into the sensor.

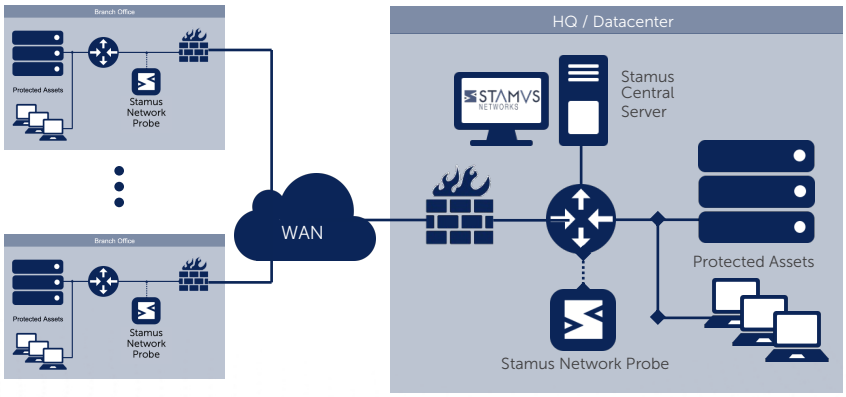

Figure 2. Stamus Security Platform – independent probe management and threat hunting systems may access multiple probes in multiple branch offices or network segments.

With Stamus Security Platform, the management and threat hunting systems are independent of the sensors, providing the operator with a consolidated management and threat hunting view into the event data from many Suricata sensors or Stamus Network Probes from a single pane of glass.

In addition, Stamus Security Platform supports multiple network definitions, allowing each probe or sensor to have its own organizational context applied to its alerts and hierarchical management layers. This multi-tenancy capability allows you to oversee probes deployed in multiple networks and multiple organizations from a single threat hunting and management console.

While SELKS may be installed on a range of hardware options, including virtual machines, installing, tuning, and optimizing your implementation will require some trial and error. Alternatively, with Stamus Security Platform, you have the option to purchase the software integrated on one of the optimized Stamus Network Appliances, which are tested and rated for a given performance level.

Here are several key scalability and integration features available in Stamus Security Platform, but not in SELKS:

Stamus Security Platform Feature Not Available with SELKS	Impact
Management of multiple sensors/probes	Allows you to deploy probes/sensors in multiple network segments and locations, giving you greater visibility into your organization's threat posture from a single pane of glass.
Aggregated event data from multiple sensors/probes	Gives you a centralized view of the security posture for your entire network.
Integration with Splunk	If you already use Splunk for centralized log management, you'll want to include the enriched event data from Stamus ND/NDR
Multiple organization-specific network definitions	Allows you to define different contextual environments for different networks or organizational subsets.
Multi-tenant (MSSP/MDR) operation	Manage multiple distinct organizations from a single pane of glass.
Available on tested, verified and high-performance turnkey appliance	You can deploy with confidence, knowing that your system will not drop packets or miss events due to performance issues.
Online or offline (Air-gapped) software maintenance	Simple installation of software updates does not require an Internet connection.
Integration with LDAP and Active Directory	You can stay compliant with your security policies by integrating Stamus ND/NDR into your existing access control systems.
Backup and restoration of configurations	Ensures you can quickly restore your security monitoring functions in the event of a disaster.

ORGANIZATION-SPECIFIC CONTEXT

When viewed through the SELKS user interface (UI), your organization's network segments, and devices – such as endpoints and hosts – are displayed simply as IP addresses. If you manage a large network, you will likely need to switch to a different system to look up the IP address in order to associate it with your network asset. This takes time and can disrupt your concentration during an intense threat hunting session.

With Stamus Security Platform, the event and log data is enriched - in real-time - with context that is unique to your organization. You can easily import your organization's network definitions, so those network names will appear alongside the IP addresses.

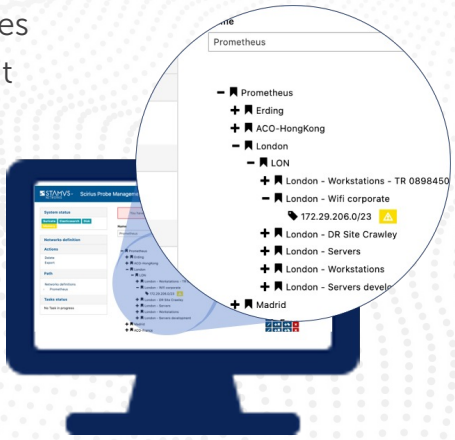

Figure 3. Stamus Security Platform network definition screen allows user to apply organizational context to the system.

In addition, Stamus Security Platform queries your internal domain name server to associate fully-qualified internal domain names (FQDNs) with those IP addresses, bringing even more organizational context to events and investigations without having to leave the tool. Armed with this context you can use those familiar names to develop filters and hunting strategies, allowing you to quickly assess the target or source or host associated with suspicious activity on the network.

Here is a summary view of the organizational-specific context features available in Stamus Security Platform but not in SELKS:

Stamus Security Platform Feature Not Available with SELKS	Impact
Internal IP addresses are identified with internal network names	Easily recognize your organization's assets and networks while threat hunting and incident investigation. Filter on events based on this organizational context. Aids in rapid detection of lateral threats and policy violations.
Internal hosts are identified as fully qualified domain names (FQDN)	
Custom organization-specific threat detection rules	Define custom threat detection rules using the language of your organization's network and assets.

THREAT DETECTION AND HUNTING

The cornerstone of a security practice is effective threat detection and the ability to quickly assess the risk and severity of the indicators of compromise that your systems detect.

Because it includes a Suricata engine, SELKS is capable of using some of the most sophisticated threat intelligence on the market, including signatures/rules from commercial feeds such as Proofpoint ETPro and others. This provides SELKS users with excellent foundation of network-based threat detection, albeit on a single network segment.

In addition, SELKS includes basic cyber threat hunting capabilities, giving you the opportunity to begin a threat hunting session based on, for example, signatures that triggered events, IP addresses and domains.

However, Stamus Security Platform delivers significantly more capability for both detection and hunting.

Stamus Security Platform enriches the detection with context derived through both network traffic analysis and organization-specific network information. In addition, Stamus Security Platform offers you the ability to create your own custom detection policies built around your organization's unique needs. These important features give you the ability to not only detect north-south intrusions, but also lateral threat movement and policy violations, such as disabled virus detection and unauthorized SSL certificate or proxy deployments.

And your ability to proactively hunt for threats is significantly improved with Stamus Security Platform compared to SELKS. This is due to its extensive data enrichment, classification-assisted workflow, advanced search and filtering capabilities, and mapping indicators of compromise to the stages along the cyber kill chain. These features allow you to quickly assess your threat posture from a number of angles and begin your threat hunting from the appropriate starting point.

Here is a summary view of the threat detection and hunting features available in Stamus Security Platform but not in SELKS:

Stamus Security Platform Feature Not Available with SELKS	Impact
Over 40+ additional metadata fields derived from network traffic analysis and organizational context are used to enrich the alert data in real-time.	The improved detection and more-effective threat hunting saves you time and reduces your exposure.
Turnkey integration and automation of ETPro threat intelligence ruleset	Arms you with the industry's most effective commercial threat intelligence that is automatically updated as new rules become available (typically 10-50+ each day)
Detection of lateral threat movement, security policy violations, use of homoglyphs in phishing attacks	More complete coverage of various methods of attack and various stages of the cyber kill chain.
Advanced detection algorithms mapped to cyber kill chain	You can quickly assess the criticality of a given alert and begin your investigation by focusing on indicators that matter most.
Advanced filtering based on Boolean combinations of events and metadata	Allows you to rapidly pivot your investigation as you uncover additional insights. You may save commonly-used filters and/or take advantage of 30+ predefined filters developed by the Stamus Networks threat intelligence team.
Classification-assisted workflow	By tagging events that match a given filter criteria, you are able to suppress informational alerts and identify others as relevant and worthy of further inspection. This lets you focus on what matters most, saving you time and allowing for less skilled team members to make more effective contributions.

NETWORK SECURITY MONITORING

Both threat detection and proactive threat hunting benefit from the visibility and context provided by network security monitoring (NSM), also known as network traffic analysis. Without details such as usernames, user agents, network segments, network flow data and fully qualified domain names, many threats will go undetected and even your most sophisticated analyst will have difficulty separating important indicators of compromise from simple informational alerts.

While a SELKS system will collect some of this raw data for a single network sensor, you will need to also deploy a standalone network traffic analysis solution if you hope to gain visibility into that host-oriented data. In addition, you will need to feed logs from both systems into a SIEM or SOAR in order to correlate the context with the alerts.

With Stamus Security Platform, all the NSM metadata context is correlated -- in real time -- with events and is available to you in a single web interface for all of your network probes/sensors. And you may create filters that incorporate many of the metadata fields to investigate, for example, all alerts associated with a given hostname and attack target type. Deploying Stamus Security Platform eliminates your need to run a separate NSM, reducing your costs and your management overhead.

Here are several examples of the network traffic analysis features available in Stamus Security Platform, but not in SELKS:

Stamus Security Platform Feature Not Available with SELKS	Impact
Protocol-independent hostname Split (FQDN, TLD, domain, subdomain)	Form of event data enrichment facilitates easier and more flexible thread detection by allowing for use of advanced Boolean combinations and criteria, ultimately saving time and expense during hunt and detection
Host fingerprinting using user agents, services, host name, TLS agents and username	Cyber situational perspective provides invaluable fingerprinting of end points for not only data threat detection but also compliance and anomaly profiling.
Geolocation, AS number, AS Organization information for IP	Saves your team time and cost during hunt and incident investigation
Metadata integration with SIEM, SOAR, and data lakes	Streamlines reduces the volume of transactions and expense associated with hunting and investigation.

For a complete list of NTA-based metadata attributes, please contact Stamus Networks.

EVENT NOISE REDUCTION

Given the sheer volume of events that may be generated by a network security monitoring system, it is critical that you deploy mechanisms to streamline and optimize your efforts. You may also wish to ask your most experienced SOC analysts to create automated policies that further streamline the work for your less experienced staff.

SELKS gives the user some basic tools to classify events for suppression or for logging only when a specified threshold has been reached. This can help reduce the number of events required for the analyst to review and the system to store.

Stamus Security Platform takes this much further and provides additional classification criteria using the more extensive metadata fields that Stamus Security Platform maintains as a result of its network traffic analysis. While this allows you to create complex filters for interactive investigation into the data, the real power comes when you apply those filters into even more meaningful classifications.

And Stamus Security Platform gives you two additional filter actions that you may use to classify events and dramatically transform your workflow: "tag" and "create STR events" actions.

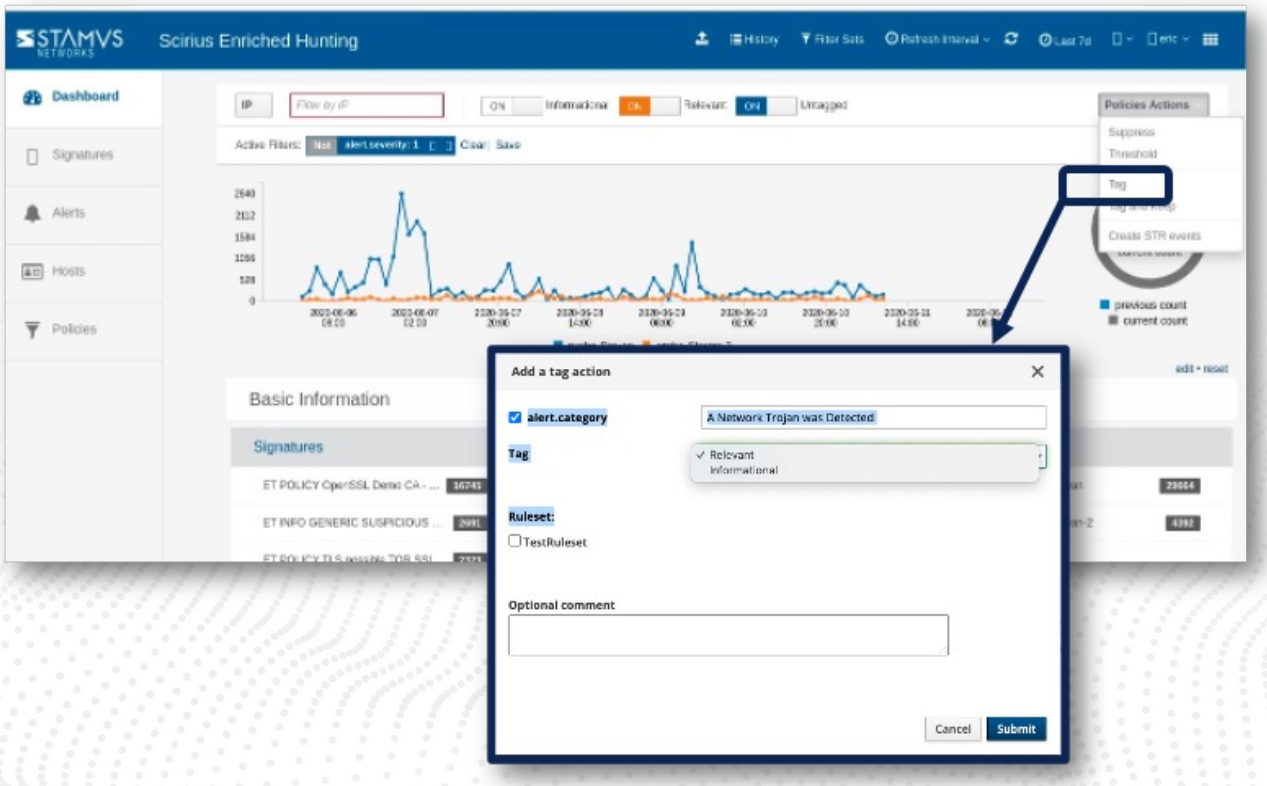

Figure 4. In Stamus Security Platform, the "Tag" action allows you to tag events matching the filter criteria as either "Informational" or "Important", which can be used to improve your team's efficiency.

With Stamus Security Platform, you may tag events matching the filter criteria with one of three "tag" states:

- Untagged - the default state
- Tagged "Informational" - indicating these alerts are worth keeping, but not necessarily the highest priority
- Tagged "Important" (formerly known as "relevant") - indicating these alerts should be investigated

Here's an example of how this powerful feature can be used to improve your team's efficacy:

1. As a senior analyst / engineer, you implement a periodic (daily?) routine to categorize and classify "Untagged" events as either "Important" or "Informational", using the Filter Set "tag" action.
2. Your Tier 1 analyst focuses the daily investigations on those events that are identified as "Important", ignoring those you've marked as "Informational"
3. Each day you review the "Untagged" events and refine your classification rules (Filter Set "tag" actions) to make sure all events are tagged as "Important"' or "Informational"
4. Repeat steps 1-4

With this process in place, you've created a mature deployment in which your team dedicates their energy only on issues you've deemed "important." And an "Untagged" event in the system is an exception, and one that has not previously been encountered on the network.

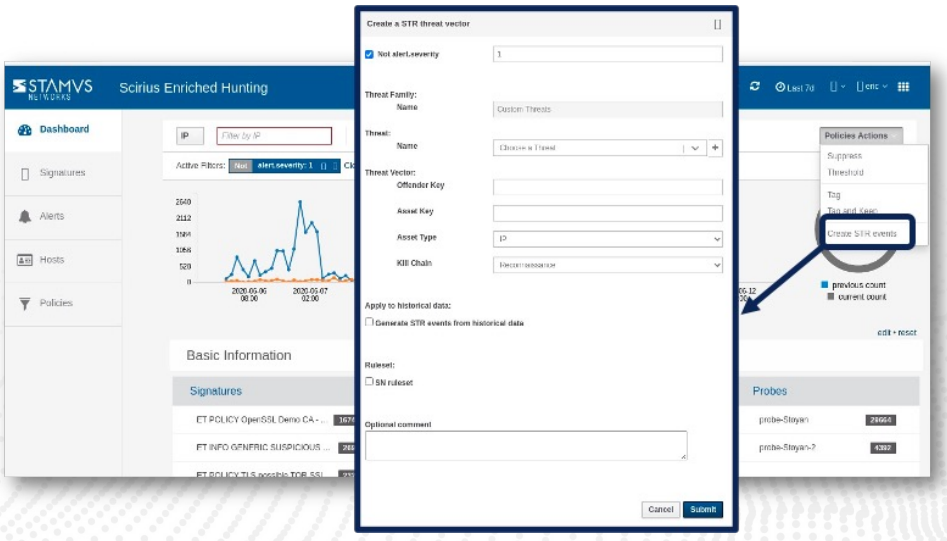

Figure 5. In SSP, the "create DoC events" action allows you to generate an event that appears as a "threat" in Stamus Security Platform, mapped to the cyber kill chain.

Similarly, the "create DoC events" action may be used by a senior analyst during the above process to create custom threat detection policies based on filters you define to classify events. When SSP algorithms determine a match based on your custom threat policy, the new custom threat is registered in Stamus Security Platform

Here is a summary view of the event noise reduction features available in Stamus Security Platform but not in SELKS:

Stamus Security Platform Feature Not Available with SELKS	Impact
Advanced filtering based on Boolean combinations of 100+ types of alert metadata	Allows you to rapidly pivot your investigation as you uncover additional insights. You may save commonly-used filters and/or take advantage of 30+ predefined filters developed by the Stamus Networks threat intelligence team.
Classify events using the "Tag" action for filters	By classifying events that match a given filter criteria, you are able to suppress informational alerts and identify others as important and worthy of further inspection. This lets you focus on what matters most, saving you time and allowing for less skilled team members to make more effective contributions.
"Threat" action for filters to create custom threat detection policies based on that criteria	Identify superset events that are meaningful to your organization and allow for less skilled team members to make more effective contributions.

For more concrete examples of this virtuous circle at work, please check out our solution brief, entitled "Pump Down the Volume." You can find it on the Stamus Networks website here.

TOTAL COST OF OWNERSHIP

As we mentioned earlier, SELKS is freely available and is released under the GNU GPLv3 license. Free, open-source software can be a cost-effective alternative at the beginning of a new installation. But in order to understand the true costs of a project, it is important to factor in both the direct and the indirect costs associated with owning and operating the solution.

Here are several items to evaluate when evaluating the cost of an open source SELKS solution versus the commercial Stamus Security Platform platforms:

Upfront licensing fees for the software - clearly the SELKS has the edge here. Afterall, it's free.

Installation and onboarding - while SELKS is a turnkey ISO image intended to install quickly and easily on a bare metal server, installing, tuning, and optimizing your implementation will require some time and expertise - both of which have real costs for your organization. As a Stamus Networks customer of Stamus Security Platform, you will enjoy complimentary support during the installation and onboarding process. And the burden of the expertise falls on the Stamus Networks support team.

Technical support and maintenance - As a SELKS user, you are ultimately responsible for supporting your organization's technical needs with respect to the SELKS installation. Yes, there are numerous online resources and a very active community, nurtured in large part by the Stamus staff, available to assist you in your efforts. As a Stamus Networks customer of Stamus Security Platform, you will enjoy complimentary technical support, patches and feature enhancements throughout the term of your license. Once again, the burden of the expertise falls on the Stamus Networks support team.

Filling in the missing capability gaps - since SELKS is not as full-featured as the commercial Stamus Security Platform alternatives, you may wish to augment SELKS capabilities with standalone network traffic analysis (NTA) and SIEM or SOAR system to fill the gaps. Even if you obtain open-source versions of these functions, there are significant indirect costs associated with integration, maintenance, and support that you must consider. Stamus Security Platform not only fills capability gaps, but it eliminates the need for time-consuming integrations while reducing the operating expense of SIEM and SOAR deployments.

ENTERPRISE SUPPORT

Most enterprises want their staff focused on leveraging the capabilities of a best-in-class solution rather than spending their valuable time to build and support one.

As an open source solution, SELKS asks that you assume most of the responsibility for installing, troubleshooting, maintaining and supporting the system in your environment. For those who are equipped and funded to do so, this can be quite rewarding. For others, it can cause a substantial distraction from their primary task of protecting the organization's network.

With Stamus Security Platform , you get the full support of Stamus Networks throughout the lifecycle of your deployment. Beginning with system onboarding and throughout the lifetime. This includes tuning and enablement, training, troubleshooting, new feature upgrades, patches and threat intelligence updates. Each Stamus Networks customer is given access to a dedicated channel on our online support system and access to a team of technicians.

Here is a summary view of the support available with Stamus Security Platform but not in SELKS:

Stamus Security Platform Support Not Available with SELKS	Impact
Onboarding	Reduces the time to impact. You will be up and productive within a few days with your organizational specific context in place.
Technical support	When you have questions, Stamus Networks technical experts are available to help.
Ongoing software maintenance	You'll know you have access to the most current version and the latest available features.

For more information on the enterprise support, please request a copy of the Stamus Networks support agreement.

SUMMARY

The table on the following page summarizes the similarities and differences between SELKS and the Stamus Security Platform.

Feature (partial list)	SELKS	Stamus Security Platform license tier	
		Stamus ND	Stamus NDR
IDS administration for one probe	✓	✓	✓
IDS ruleset management for one ruleset	✓	✓	✓
Basic threat hunting on IDS events	✓	✓	✓
Real-time network traffic analysis	✓	✓	✓
Onboarding assistance, technical support, and online maintenance		✓	✓
IDS administration for multiple probes		✓	✓
IDS ruleset management for multiple rulesets		✓	✓
Multiple Stamus Networks Probes and/or Suricata Sensors		✓	✓
Automated health and wellness monitoring		✓	✓
Automated application and OS updates		✓	✓
Unified network Threat Hunting tool		✓	✓
Guided hunting that drives detection		✓	✓
Real-time correlation of IDS events, network traffic analysis and organizational data		✓	✓
Automated event classification and advanced tagging		✓	✓
Network definitions providing enhanced detection of lateral threat proliferation		✓	✓
Enriched data provides context and increase network visibility		✓	✓
Unique metadata for perspective and investigation		✓	✓
Metadata integration with SIEM, SOAR, and data lakes		✓	✓
Highest probability indicators mapped into the cyber kill chain - Declarations of Compromise™			✓
Unified threat detection results drive insightful threat detection algorithms from Stamus Networks			✓
User defined algorithms detect high probability threats specific to your environment			✓
Host fingerprinting details network services, user agents, host name and logged in users			✓
Prioritizes high probability events to direct investigations			✓
Proofpoint ETPro Ruleset subscription with automated updates			✓

LEARN MORE

If you need a powerful investigative toolset to support your threat hunters. Stamus Security Platform provides a proactive threat hunting user interface that allows you to pivot from detection right to investigation by providing packet-level visibility and integrated data enrichments to help investigate threats in real time.

There are numerous factors to review when evaluating and considering the upgrade from SELKS to Stamus Security Platform. If you would like to have a detailed conversation to discuss, please contact us via email at contact@stamus-networks.com or complete the form on our website.

ABOUT THE AUTHORS

Éric Leblond

Chief Technology Officer

Éric is an active member of the security and open-source communities. He is a Netfilter Core Team member working mainly on communications between kernel and userland. He works on the development of Suricata, the open source IDS/IPS since 2009 and he is currently one of the Suricata core developers.

Peter Manev

Chief Strategy Officer

Peter has 15 years of experience in the IT industry, including enterprise-level IT security practice. He is an adamant admirer and explorer of innovative open-source security software. He is the Lead QA on the development of Suricata, the open-source IDS/IPS.

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

