Scaling Suricata for Enterprise Deployment

STAMUS NETWORKS

Suricata is a high-performance network threat detection, IDS, IPS and network security monitoring (NSM) engine. It is open source and owned by a community-run nonprofit foundation, the Open Information Security Foundation (OISF). Suricata is developed by OISF, its supporting vendors and a passionate community of volunteers.

From its humble beginnings in 2008 as a signature-based intrusion detection system (IDS), Suricata has now grown into a powerful IDS/IPS/NSM and evolved to include full-featured packet capture, scripting, and network security monitoring capabilities that rivals those of dedicated solutions. In fact, Suricata has in recent years, formed the foundation of many successful commercial products and spawned an incredible ecosystem of independent ruleset/signature and threat intelligence providers.

CHALLENGES OF LARGE-SCALE DEPLOYMENTS

For all Suricata's capabilities, building out an enterprise-scale deployment of Suricata with mostly open-source tools can be a challenge.

For example, in smaller deployments such as in a single office location, keeping the system up to date with the latest signature rulesets and/or threat intelligence can be performed manually and doesn't take too long. But in an Enterprise deployment with multiple network segments, branch offices and cloud applications, you will want to automate that process to make sure that all the sensors are running in lock step.

In this white paper we outline five ways to improve the scalability of Suricata in an enterprise deployment. In each case, we try to offer a free or open-source choice and in some cases, we identify straightforward commercial solutions that can provide a fully-supported alternative.

Technically, Suricata is an "engine" - not a complete IDS/IPS/NSM. But for the sake of this paper, we will assume that you understand how to build and deploy a basic Suricata sensor in your network. If you don't know where to start and would like to begin experimenting with Suricata, we recommend SELKS, a turnkey, no cost, open-source solution for experimenting with and deploying the latest version of the Suricata engine.

MAKING IT BETTER

This paper presents five suggestions that can help you improve the scalability of Suricata in your enterprise. While not an exhaustive list of recommendations, the following should give you a good starting point for improving your installation:

- Optimize the placement of your sensors
- Deploy centralized sensor management
- Tune the network of sensors for maximum performance
- Consolidate Suricata alerts and logs from multiple sensors
- Deploy high-level analytics to focus analysts' time on the the things that matter

1 OPTIMIZE SENSOR PLACEMENT

The foundation for effective network detection and response is based on the proper placement and configuration of the Suricata sensors, effectively your eyes and ears into the network traffic. Improper placement from poor planning or misconfiguration can lead to gaps in network visibility, which can allow attackers to go undetected for prolonged periods of time and to penetrate deeper into your network.

Before we discuss the specifics of placement, it is worth mentioning that Suricata may be deployed in either active (in-line) or passive (monitor only) mode. This paper is focused more on monitoring mode, typically of a SPAN/Mirror port. There are two reasons for deploying in passive monitoring mode: 1) the sensor cannot in any way affect the operations of your network and 2) the passive deployment provides greater visibility and more rich metadata context 3) attackers are much less likely to detect and locate the presence of the monitor and it is therefore less likely to become a target itself.

When considering sensor placement, you must thoroughly understand your network topology as well as which are the critical assets on the network that an attacker may attempt to compromise. You have the strategic advantage of knowing your network topology better than the attackers, so, it is crucial that the security team must work closely with the network and IT architects to identify all the critical monitoring points for your organization. Use this knowledge to your advantage.

While it is not realistic to monitor 100% of the traffic passing among all the systems in your network, it is necessary to look carefully at your options to prioritize your activities and maximize coverage.

Consider the following major areas where you may wish improve your network traffic visibility:

- Network edge - most attacks originate from the outside your network, and nearly all incidents result in some sort of communication with a command and control and exfiltration system - also outside your network. If you deploy only one network sensor in your network, it should be at the network edge. Depending upon the scale of your organization, there may be more than one 'edge' to your network. These could include your Internet entry/access points, partner/supplier extranet entry points, and remote office connections.
- Remote data center or colocation facility - in many organizations, some of the most critical assets are located in remote data centers. If this is the case in your network, you will want to deploy at least one sensor in that facility to monitor traffic to and from that facility.
- Public cloud resources - if you are leveraging public cloud infrastructure for hosting any mission-critical enterprise applications, you will want to deploy at least one sensor here. Most of the major cloud service providers now provide mirror interfaces that allow you to send duplicate traffic to a virtual sensor deployed in the cloud. As with other deployments in the public cloud, you have the flexibility to spin up or down new sensors fairly quickly to align with the dynamic nature of the resources you are working to protect.
- Remote/branch offices - if your network includes remote or branch offices that are directly connected to the public Internet and contain high-value network assets, you may wish to deploy a sensor on site. If, however, your branch office connections are architected such that they all home traffic to a central location, you can more easily deploy a single sensor at that location and monitor all remote office traffic from there.
- Network segmentation - in all the above examples, you may wish to deploy multiple sensors inside the network to eliminate blind spots AND to instrument individual sections of the network (e.g. for each department) in order to detect lateral (east-west) movement of adversarial activity.

Note: you may either set up the sensors physically near the correct network segment, or you can direct the appropriate traffic to the sensor network ports via a span/mirror port from a central switch location.

When deployed throughout the enterprise network at strategic locations described above, Suricata sensors can provide your security team with excellent visibility and form the foundation of a formative threat detection and response program.

2 CENTRALIZE SENSOR MANAGEMENT

While Suricata sensors are capable of running extensive signature rulesets, network traffic analysis, and reputation/match lists, each sensor in your enterprise may require different hardware and software configurations based on their network performance requirements and where they are deployed. And you will want to understand how these are performing relative to your expectations.

For example, you may deploy lower performance sensor hardware in your branch office running a subset of your detection rules while you deploy a much higher performance appliance in your datacenter running a complete commercial ruleset and the latest IP and DNS threat intelligence lists. In an enterprise deployment, you may have hundreds of sensors and dozens of different configurations. This presents several challenges for the enterprise.

- How to make sure rules, threat intelligence and data capture is properly deployed and up to date on every sensor
- How to monitor the performance of each sensor to ensure it is processing every packet and every rule, so you won't miss critical events
- How to maintain backup configurations for each sensor so you can quickly replace a sensor in the event of a hardware failure or revert to a previous known state
- How to upgrade and patch the software on your fleet of sensors
- How to keep track of the inventory of various sensors and configurations

As your deployment requirements grow and the Suricata capabilities continue to evolve, the above challenges are amplified. Logging into individual sensors (or SELKS user interfaces) one-at-a-time to monitor and make changes is simply not practical.

In order to address these challenges at an enterprise scale, you will want to install a centralized sensor management system.

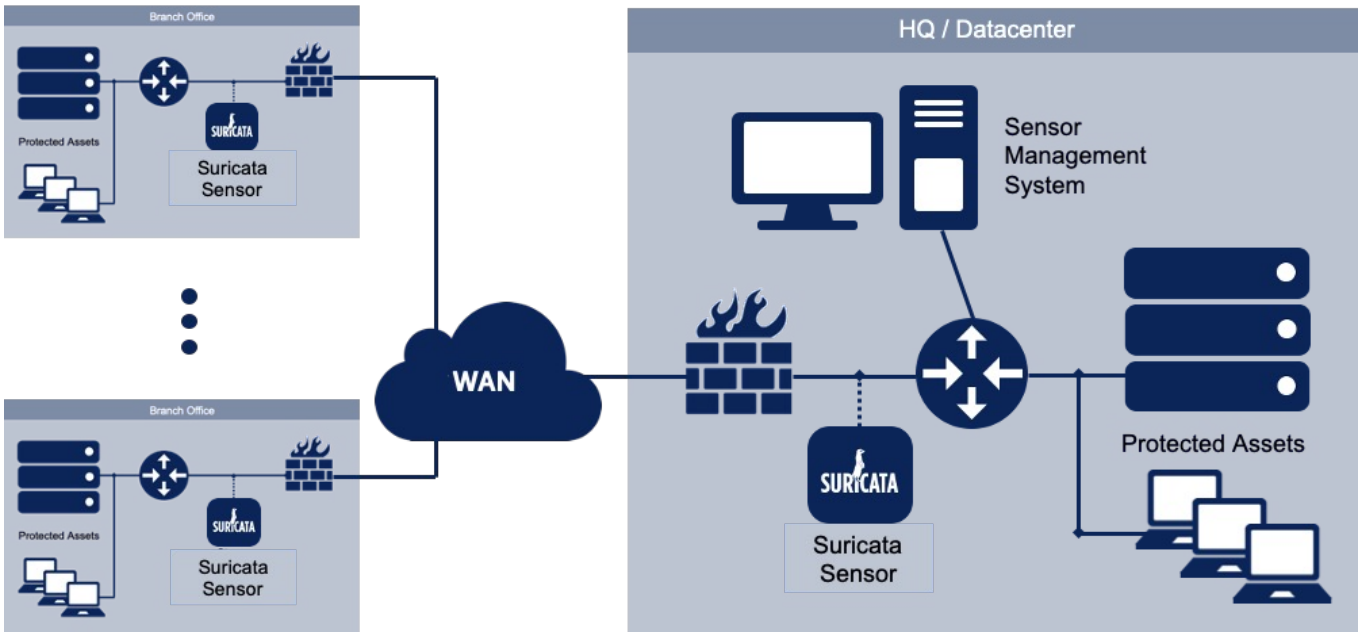


Figure 2. Sample architecture of a Suricata deployment

The options for a centralized management system include in-house development, open-source and commercial solutions.

The advantages of in-house development include the flexibility to include any and all features required for your enterprise and zero out-of-pocket expense. Of course, the challenges include securing the resources needed to develop the sensor management system and having access to those resources for support and continuous improvement. And there are indirect opportunity costs associated with consuming those resources when they could be used to develop other systems.

The advantages of deploying an open-source solution are similar to those of an in-house developed system in that there is typically zero out-of-pocket expenses, and you will preserve the flexibility of making customizations in the future. The biggest disadvantage to open-source solutions is that your team is 100% responsible for support. We have spent time researching this problem and have unfortunately not found a reasonable open-source solution for this problem. If you know of any, please let us know and we will update this paper.

Finally, there are several commercially available solutions for sensor management, including Stamus Security Platform (SSP) from Stamus Networks. Solutions such as SSP include IDS ruleset and match list management, network sensor administration (both Suricata and Stamus Network Probes), application and OS updates, and a RESTful API for integrating with your security stack. The advantages of a commercial solution include dedicated ongoing support and a roadmap of continuous product improvements.

Commercial solutions such as SSP do require a modest out-of-pocket investment - typically an annual subscription - and the development of any enterprise-specific customizations are dependent upon your vendor partner to implement.

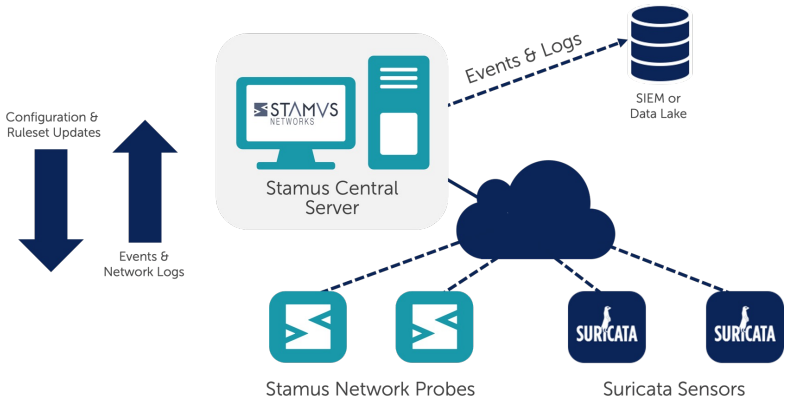


Figure 3. Stamus Security Platform from Stamus Networks

3 TUNE THE SENSORS

Modern versions of Suricata have deployed successfully on 100Gps links with off-the-shelf hardware outfitted with a specialized capture network interface card (NIC). This was shown as part of a public demonstration in 2017 using Suricata 4.0 dev edition with Napatech NT200A02 NIC . Your specific requirements may vary across the enterprise. As mentioned above, Suricata sensors often require different hardware and software configurations based on their network performance requirements and where they are deployed.

The performance of your Suricata deployment depends on a number of factors, including traffic volume for each sensor, the specifics of the underlying hardware, the nature of your detection, file extraction, and protocol monitoring needs and your requirements for data retention time.

The goal of any tuning exercise is to create a few baseline packages/configurations for each of your scenarios to use a solid starting point for each deployment.

Here are the macro variables to consider when tuning your sensors:

- **The scale of the ruleset and/or threat intelligence you are using** - for example, will you be using 100% of a commercially available ruleset with 50,000 signatures? How extensive is your internally-developed threat intelligence? Are you attempting to match a list of 1 million domains and 270,000 URLs?
- **The type of traffic mix and volume the sensor will see on the network** - while not actually something you can control directly; it is important to understand that the traffic mix running on a monitored network segment has an impact on performance. This should be considered when determining the sensor placement.
- **The specific type of hardware or virtual machine Suricata is running on** - the OS/kernel version, the processor, number of cores, memory, disk space, network interface card (NIC) are all important factors. Obviously, if the sensor is deployed in the cloud and/or in a virtual machine, your choices will have an impact on performance and subsequently your optimized configuration.
- **The version of Suricata you are running** - with each new release of Suricata, new features are added. While usually new releases bring some performance improvements, sometimes the new features impact your performance in your particular environment.

Begin your tuning exercise by locking down 3 out of the 4 factors listed above and adjusting the fourth until you maximize your performance in that setting. For example, start with a known version of Suricata, the threat detection and intelligence you will likely want to deploy, and a particular network traffic type/mix. Then experiment with several hardware or container configurations to see if you achieve the performance targets you are looking for.

Here are two high-performance open source packet generation tools we have found useful in testing 100Gbps+ systems

TRex (contributed by Cisco)
https://trex-tgn.cisco.com/

Pktgen (contributed by Intel)
https://pktgen-dpdk.readthedocs.io/

Once you have baselined this set up, you can move it to a different network segment and revalidate the performance. If you find that this new installation has substantially lower traffic volume for example, you may wish to downsize the hardware and retest to see if you can save some money on all your low traffic network segments.

Keep in mind that any time one of the variables is changed, you will want to revalidate or retest that particular tuning.

After you've created one or more deployment packages, you may wish to move to an advanced set of adjustments of the secondary variables that have the potential to impact your performance. Here is a list of those features that may have performance implications in your environment:

- Kernel/NIC driver version
- Rules/match/drop lists adjustments
- eBPF filters adjustments
- Protocol detection and logging changes
- Multitenancy
- Per interface configs

Ideally, the tuning above can be performed remotely using a central management system as discussed above with the ability to save 'golden' configurations for each scenario you wish to deploy in.

The efforts required to tune the deployment are very different if you have chosen to go with pure open source (e.g. SELKS or other Suricata stack) or if you are using a commercial system such as Stamus Security Platform (SSP) from Stamus Networks.

If you have chosen the open-source route, there are a number of very valuable resources available to help. These include online guides such as https://github.com/pevma/SEPTun and https://github.com/pevma/SEPTun-Mark-II and workshops sponsored by the OISF such as those listed here; https://suricata-ids.org/tag/training/.

If you wish to minimize the time your team and you dedicate to tuning and optimizing your deployment, you may opt for a commercially available solution for which the Suricata installation is pre-optimized for the hardware it is installed on and fully supported . An example of this pre-optimized hardware can be purchased from Stamus Networks. Learn more about the Stamus Networks Appliances here.

4 CONSOLIDATE ALERTS AND LOGS

A single instance of Suricata deployed as a SELKS installation provides you with a turnkey Suricata intrusion detection and prevention system and NSM platform with the ELK stack to collect, store, and analyze alerts and events, EveBox to correlate flows, archive/comment on events, reporting and PCAP download. The SELKS user interface is the Scirius (Stamus) Community Edition which allows an analyst to perform basic incident investigation and basic threat hunting (along with configuration and management of the Suricata ruleset).

But enterprises deploying multiple sensors must find a way to consolidate the logs, events and alerts from those sensors into a "single pane of glass" to efficiently correlate, analyze, search, and gain insights into their overall enterprise network security posture.

Figure 4. Consolidate logs, events and alerts from Suricata sensors to simplify the SOC

This is the function typically provided by a security information and event management system (SIEM), a software system that analyzes log and event data in real time to provide threat monitoring, event correlation and incident response.

The good news is that there are a number of free and open-source options to choose from. Three examples of this genre are listed below.

- ELK stack - also known as "ELK", this set of tools is built and maintained by Elastic and includes Elasticsearch the JSON-based search and analytics engine; Logstash data collection pipeline; and Kibana for visualizations. Note: there is a free set of Suricata dashboards available here.
- OSIM - offered by AlientVault (now AT&T), this SIEM offers event collection, normalization, and correlation functionality. It also includes basic logging and monitoring, threat assessment and some automated response, data analysis, and data archiving tools.
- SIEMonster - an integrated collection of the best open-source security tools, as well as some custom development that includes incident reporting, advanced correlation with threat intelligence and active response.

Naturally, the challenges of these open-source tools is that no single one of these is capable of solving all your organization's needs, so you may find yourself augmenting your selection with other open source or commercial tools to get the coverage you need.

Ideally, the network security information detected, collected and logged by the Suricata sensors is combined with other indicators generated by systems such as endpoint detection systems. But at a minimum, all events from Suricata sensors should be consolidated into a single console.

Of course, many commercial options are also available. These tend to be more full-featured and newer offerings include functionality such as advanced analytics, threat intelligence, incident response and user monitoring.

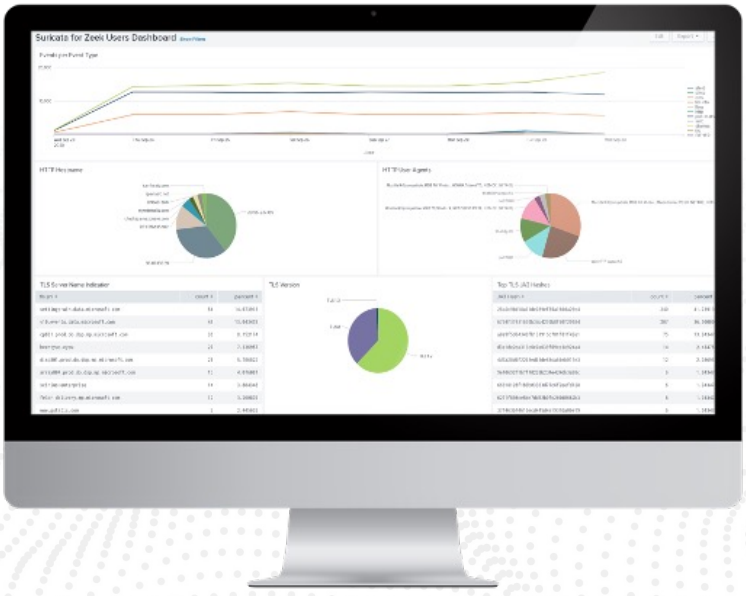


Figure 5. Stamus Networks App for Splunk delivers native support for Suricata in Spunk

One of the most popular commercial options is Splunk, an open platform for which many security vendors have developed custom apps to optimize their system's integration into the platform. This particular one bears mentioning in this paper because of the recently introduced Stamus Networks App for Splunk which includes native support for Suricata.

The Stamus Networks App for Splunk allows Splunk Enterprise users to extract information and insights from Suricata sensors. It provides ready-to-use dashboards and reports that expose the IDS and NSM data being collected by Suricata sensors and help those with large Suricata deployments become more productive.

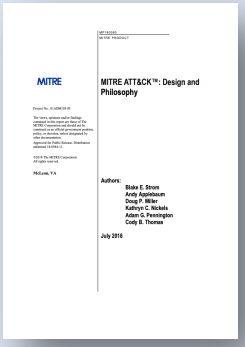
5 ADVANCED ANALYTICS FOR INSIGHTS

With an enterprise-scale deployment, the sheer volume of alerts being generated by the 10s or 100s of Suricata sensors can be overwhelming. Even when organizations have operationalized a SIEM to collect, normalize, and correlate all the activity, security teams find it nearly impossible to know what is important or urgent and what does not deserve their attention.

In order to effectively deploy Suricata at an enterprise scale, it is critical that organizations consider advanced analytics or higher order threat detection algorithms in order to know where to begin their hunt. Without such systems, the number of individual indicators can appear as false positives which leads to alert fatigue which ultimately leads to inaction. This is a big data problem that requires advanced automation solutions.

So, the goal is to reduce the noise and provide automation to guide the threat hunter towards the most important issues of the day. As in other areas, there are several open source and do-it-yourself options as well as a long list of commercial options. In this paper we will touch on a few of the open-source options and explore one commercial solution in some detail.

With a limited set of open-source options available, in order to solve this problem organizations must either develop home grown systems or invest in commercial solutions. Here are three resources that could be helpful when considering developing your own visualization and threat hunting interface:

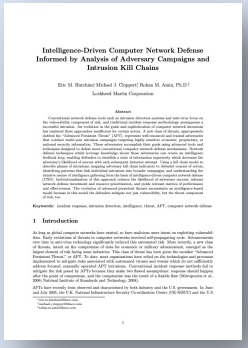

MITRE

MITRE ATT&CK™: Design and Philosophy

Authors:
Blake E. Strom
Andy Applebaum
Doug P. Miller
Kathryn C. Nickels
Adam G. Pennington
Cody B. Thomas

July 2018

[MITRE ATT&CK™: Design and Philosophy] - The MITRE ATT&CK knowledgebase describes cyber adversary behavior and provides a common taxonomy for both offense and defense. It has become a useful tool across many cybersecurity disciplines to convey threat intelligence, perform testing through red teaming or adversary emulation, and improve network and system defenses against intrusions.

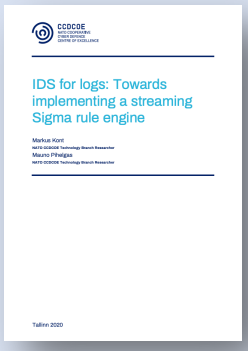

Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains

Eric M. Hutchins[1] Michael J. Cloppert[1] Rohan M. Amin, Ph.D.[1]
Lockheed Martin Corporation

Abstract

1 Introduction

[Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains] - Using a kill chain model to describe phases of intrusions, mapping adversary kill chain indicators to defender courses of action, identifying patterns that link individual intrusions into broader campaigns, and understanding the iterative nature of intelligence gathering form the basis of intelligence-driven computer network defense (CND).


CCDCOE

IDS for logs: Towards implementing a streaming Sigma rule engine

Markus Kont
NATO CCDCOE Technology Branch Researcher
Mauno Pihelgas
NATO CCDCOE Technology Branch Researcher

Tallinn 2020

[IDS for logs: Towards implementing a streaming Sigma rule engine] - The Sigma rule format has emerged in recent years as a signature-like ruleset for event logs for use by security operations and threat hunting communities. This paper provides a detailed technical outline of our implementation.

When evaluating alternatives, keep in mind that a common, perhaps overly-simplified, solution is to aggregate events based on the source, destination, or other common factors present in each event. This results in a more condensed display of information that allows for simpler analysis.

The problem with this method is that it fails to address the current attack mechanisms, which are multi-stage. These attacks - modeled by the cyber kill chain - can begin by exploiting a system vulnerability, then installing on the system and communicating with the control server to collect and perform desired actions on the target. Aggregating events by metadata doesn't allow the cyber kill chain to be considered. An additional abstraction is needed, or we won't be able to observe the exploitation from one server and the command-and-control beacon which is part of the same process.

Spotlight on One Commercial Solution - Stamus Security Platform

Developed by Stamus Networks, Stamus Security Platform can provide a single alert, and the SOC analyst sees only that - for example - the malware appeared on the server in the command-and-control phase of the kill chain. The analyst also sees the specific time that the communication was detected and when it was last seen. All those repeated noisy alerts are suppressed, but they remain available in the system logs as important corroborating evidence for the incident investigation.

This approach completely changes the paradigm of how security teams view individual events drawn directly from network traffic, by moving to a whole new way of identifying incidents. Getting warned about events such as a new threat detected on an asset or a change in the progression along the kill chain is now a reality. The great news - it will warn analysts only when something meaningful happens on the network.

SUMMARY

In smaller deployments a Suricata deployment can be fairly straightforward and provide significant visibility into network threat activity. And while even in smaller deployments, efficiency and efficacy are important, an enterprise scale deployment brings a unique set of challenges. Sensor optimization and placement as well as centralized management and event aggregation are crucial. We hope this paper provided a few ideas to help you scale and improve the results of your Suricata deployment.

Finally, it is important to note that free, open-source software can be a cost-effective alternative at the beginning of a new installation. And in the right circumstances, can provide an enterprise with significant capabilities when managed by the appropriate internal resources. 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.

ADDITIONAL RESOURCES

If you are interested in exploring this topic further, we recommend the following resources:

- Suricata website
- OISF website
- SELKS web page
- SELKS github page
- Just released: Suricata 6 (blog article)
- Suricata dashboards for any ELK stack (open source contribution by Stamus Networks)
- Grafana dashboards for SELKS (open source contribution)
- Suricata user forum
- Strategic Sensor Placement for Intrusion Detection in Network-Based IDS (academic paper)
- Suricata Extreme Performance Tuning (SEPTun) guide - Part 1
- Suricata Extreme Performance Tuning guide - Mark II
- Official Suricata training resources
- Understanding SELKS and Stamus Commercial Solutions (white paper)
- 11 Open Source SIEM Tools (article)
- Splunk enterprise security solutions
- Introducing the Stamus Networks App for Splunk (blog article)
- Stamus Security Platform (web page)

LEARN MORE FROM STAMUS NETWORKS

Stamus Networks believes in a world where defenders are heroes, and a future where those they protect remain safe. As organizations face 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 know more, respond sooner and mitigate their risk with insights gathered from cloud and on-premise network activity. Our solutions are advanced network detection and response systems that expose serious and imminent threats to critical assets and empower rapid response.

Stamus Networks was founded by Éric Leblond and Peter Manev, both members of the Open Information Security Foundation leadership team and developers on the Suricata project, the world-class IDS/IPS network monitoring engine. Under the leadership of Éric and Peter, Stamus Networks applies its extensive Suricata and network security technology experience to develop our advanced security products.

Visit http://www.stamus-networks.com for more information.

ABOUT THE AUTHOR

Peter Manev

Chief Strategy Officer

Peter is the co-founder and Chief Strategy Officer (CSO) of Stamus Networks and a member of the executive team at Open Network Security Foundation (OISF). Peter has over 20 years of experience in the IT industry, including enterprise-level IT security practice. He is a passionate user, developer, and explorer of innovative open-source security software, and he is responsible for training as well as quality assurance and testing on the development team of Suricata – the open-source threat detection engine. Peter is a regular speaker and educator on open-source security, threat hunting, and network security.

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.

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

