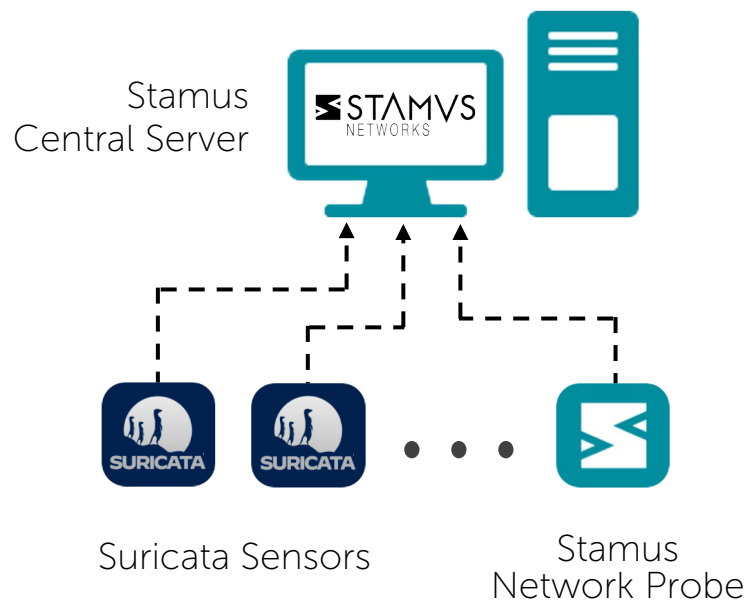


# Supercharge Suricata Sensors with Stamus Security Platform

While Stamus Security Platform (SSP) is optimized for use with Stamus Network Probes, organizations deploying native Suricata sensors in their network will also benefit from using Stamus Security Platform. In addition to providing a convenient way to centrally manage rulesets and logs for multiple Suricata sensors, Stamus Security Platform includes a Suricata sensor post-processing module to provide advanced features, previously only available with Stamus Network Probes.

This document describes the capabilities of Stamus Security Platform that are available to users of native Suricata sensors.



## Foundational Suricata Capabilities in SSP

From its earliest inception, Stamus Security Platform was designed to provide a powerful central management to help scale enterprise Suricata deployments. The following is a summary of the foundational SSP capabilities designed for Suricata sensors.

- **Ruleset and threat intelligence management** – centralized management of Suricata rulesets and third-party threat intelligence
- **Protocol transaction and flow data logging & analysis** – centralized logging and analysis of protocol data, including flow records and transaction logs, captured by Suricata sensors

- **Alert logging & analysis** – consolidated IDS event storage and central integration point for the rest of your security tech stack, such as SIEM, SOAR, Open XDR, IR or messaging systems
- **Guided threat hunting** – because even the most advanced system cannot automatically detect everything, Stamus Management Server integrates a guided threat hunting console that simplifies proactive defense for less-experienced analysts.

Stamus Management Server may be installed on turnkey physical appliances (available from Stamus Networks) or as a software image that you deploy either on bare metal hardware, a virtual machine, or a virtual machine in the cloud.

## Capabilities enabled by Suricata Sensor Post-Processing

In Stamus Security Platform, advanced features such as metadata enrichment, tagging, automated triage classification, and the execution of “Stamus threat” detection logic are performed on Stamus Network Probes. As such, these features have not historically been available to native Suricata sensor deployments.

Beginning with release U37, Stamus Security Platform includes a *Suricata sensor post-processing* function that delivers many of the same functions in the central Stamus Management Server.

These capabilities include:

- Alert data enrichment
- Automated event triage
- Network definitions
- High-fidelity Declaration of Compromise™

The remainder of this document is devoted to explaining these capabilities in greater detail.

## Alert Data Enrichment

When the capability is enabled, SSP enriches the data associated with alerts from Suricata sensors, delivering some key capabilities previously available only with the Stamus Network Probes. Alerts are enriched with metadata about domain/DNS server, JA3/JA3s, and IP geolocation. See the example screenshot below in which some of the alert enrichment is highlighted with blue boxes.

The screenshot displays the SSP alert interface for an alert titled "ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex/Trickbot CnC)". The alert is dated 2022-03-23, 05:30:58 am, with a protocol of TLS, probe of sn-probe-aws-2, and category of Malware Command and Control Activity Detected. The alert is tagged as relevant.

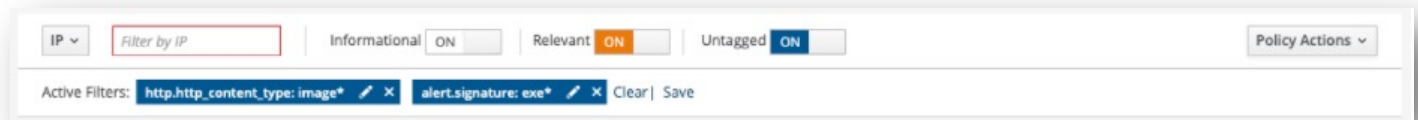
The interface is divided into several sections:

- Signature:** ET MALWARE ABUSE.CH SSL Blacklist Mail..., SID: 2021013, Category: Malware Command and Control Activity ..., Severity: Severe, Revision: 7, Tagged: relevant.
- IP and basic information:** Source Network: Internet, Source IP: 185.175.156.13, Source port: 443, Destination Network: remote.london.datacenter-uk, Destination IP: 10.7.5.101, Destination port: 50007, IP protocol: TCP, Application protocol: tls, Probe: sn-probe-aws-2, Network interface: dummy0.
- Enrichment:** Source Network: Internet, Source IP: 185.175.156.13, Source port: 443, Target Network: remote.london.datacenter-uk, Target IP: 10.7.5.101, Target port: 50007.
- Geoip:** Country: United States, Country Code: US, AS Number: 20473, AS Organization: Choopa, LLC.
- TLS:** Subject: C=GB, ST=London, L=London, O=Global S..., Issuer: C=GB, ST=London, L=London, O=Global S..., Not Before: 2019-07-05T06:24:23, Not After: 2020-07-04T06:24:23, JA3: 6734f37431670b3ab4292b8f60f29984, User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit..., JA3S: 623de93db17d313345d7ea481e7443cf.
- Flow:** Flow ID: 1392302274793392, Flow start: 2022-03-23T04:30:58.151472+0000, Pkts to server: 4, Bytes to server: 489, Pkts to client: 4, Bytes to client: 1639.
- Signature metadata:** former\_category: MALWARE, attack\_target: Client\_Endpoint, updated\_at: 2018\_05\_17, signature\_severity: Major, deployment: Perimeter, created\_at: 2015\_04\_27, tag: SSL\_Malicious\_Cert.

## Automated Event Triage

With the metadata applied to the alerts, users may create and apply SSP filters based on this metadata during incident investigation and hunting. These filters help the user isolate and pivot on events in the system. These filters may be used to create a policy to suppress, threshold or tag alerts associated with the filter criteria.

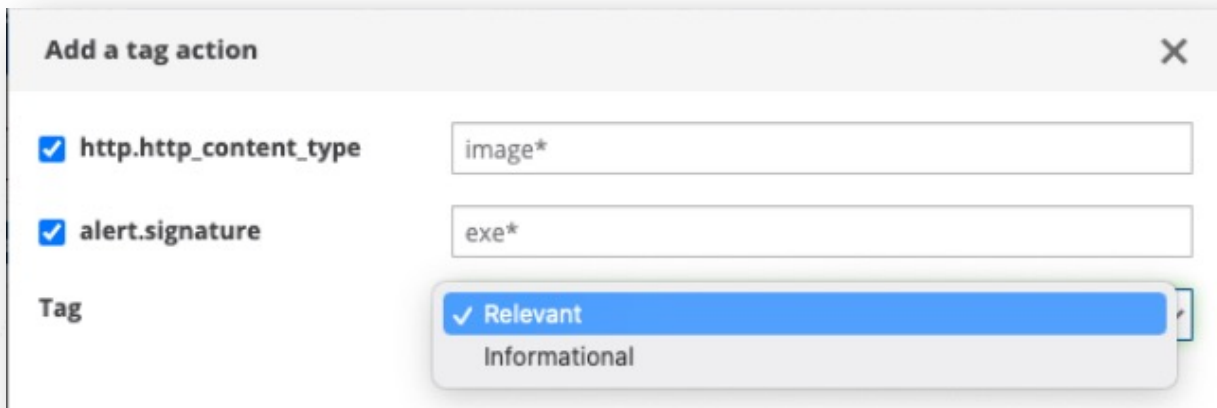
These policies instruct SSP to automatically classify future events, essentially performing the triage automatically. This dramatically reduces the time spent by analysts reviewing security events.



There are 5 types of actions that can be performed with policies:

- Suppression, to remove an alert
- Thresholding, to retain an alert under certain conditions
- Tagging, to enrich the alert with a tag (either "relevant" or "informational")
- Escalating, to escalate an alert to a Declaration of Compromise™

The screenshot below illustrates applying the filter above to create a tagging policy.



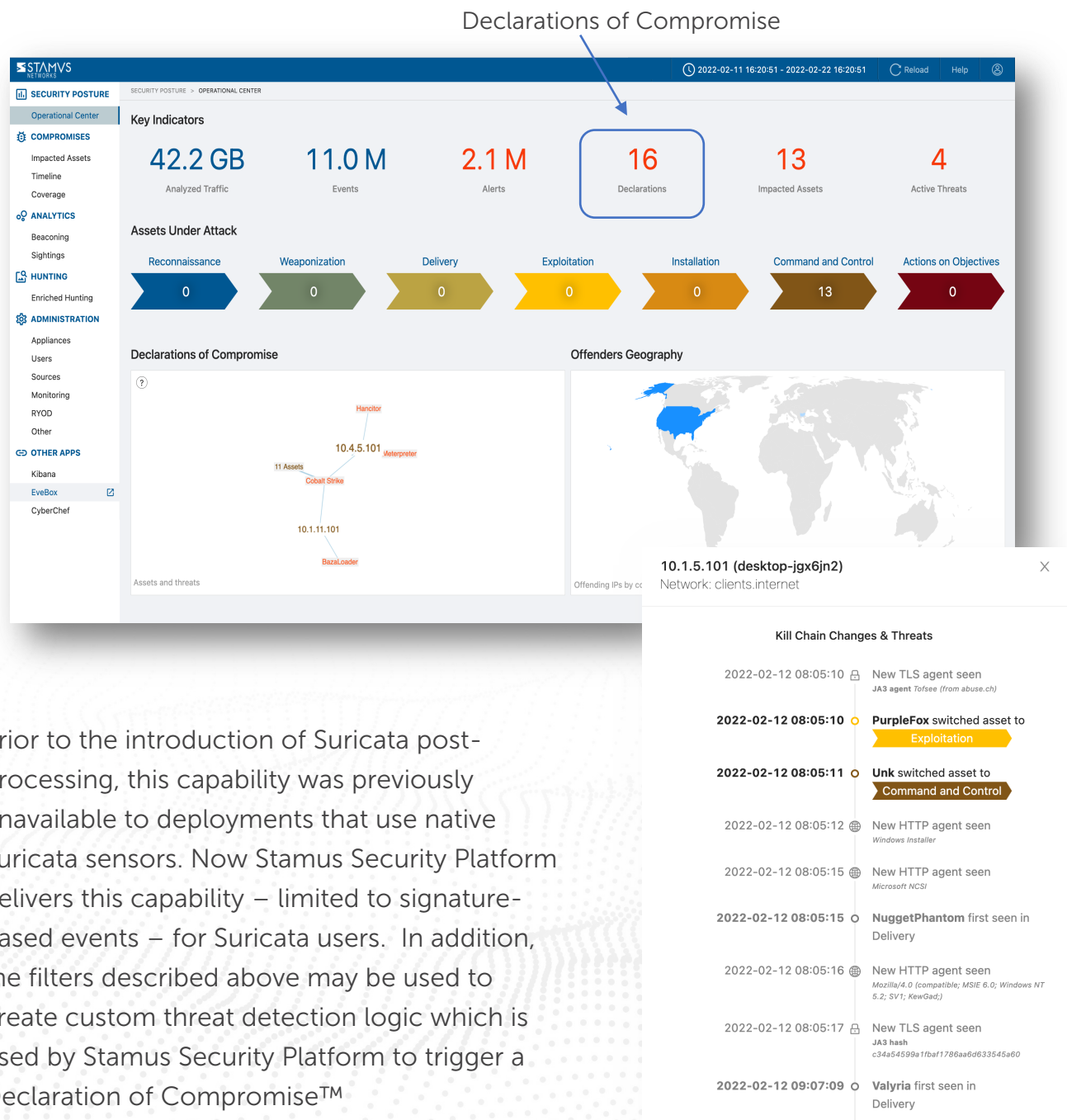
Policy actions can use any fields, including metadata, from an alert. Once an alert is tagged, the analyst can, for example, use the tag to filter only those alerts which the system labeled "relevant" using the tag filter shown below.





## Declarations of Compromise™

One of the key features of the Stamus NDR license is the ultra high-fidelity detection that generates what we call Declarations of Compromise™ comprised of “Stamus Threats.” Stamus Security Platform applies advanced logic to signature-based alerts, metadata, and raw protocol transactions to identify serious and imminent threats, and to reconstruct the sequence of events that led to the declaration of compromise.



## Network Definitions

Network Definitions allows the user to label certain networks or IPs with organizationally-relevant names which SSP uses to enrich event data. This simple capability can dramatically accelerate the analyst's ability to assess the criticality of an asset or identify suspicious user activity on a particular network segment.

See the example below.

- Datacenter UK
  - London
    - Accounting
      - 📄 10.1.37.0/24
    - DMZ
      - 📄 10.1.32.0/21
      - 📄 10.15.0.0/24
    - Remote
      - 📄 10.1.39.0/26
    - Sharepoint Portal
      - 📄 10.1.36.56
  - Internet
    - 📄 0.0.0.0/0

Configuration of  
Network Definitions

←

Network Definitions  
enriching alert records

↓

IP and basic information	
<b>Source Network</b>	Internet
<b>Source IP</b>	185.175.156.13
<b>Source port</b>	443
<b>Destination Network</b>	remote.london.datacenter-uk
<b>Destination IP</b>	10.7.5.101
<b>Destination port</b>	50007

Signature

Signature ET MALWARE ABUSE.CH SSL Blacklist Malicious...

SID 2021013

Category Malware Command and Control Activity ...

Severity Severe

Revision 7

Tagged relevant

IP and basic information

Source Network Internet

Source IP 185.175.156.13

Source port 443

Destination Network remote.london.datacenter-uk

Destination IP 10.7.5.101

Destination port 50007

IP protocol TCP

Application protocol tls

Probe sn-probe-aws-2

Network interface dummy0

Enrichment

Source Network Internet

Source IP 185.175.156.13

Source port 443

Target Network remote.london.datacenter-uk

Target IP 10.7.5.101

Target port 50007

Geolip

Country United States

Country Code US

AS Number 20473

AS Organization Choopa, LLC

Signature metadata

Subject C/CB-ST/London-London-G/GlobalS

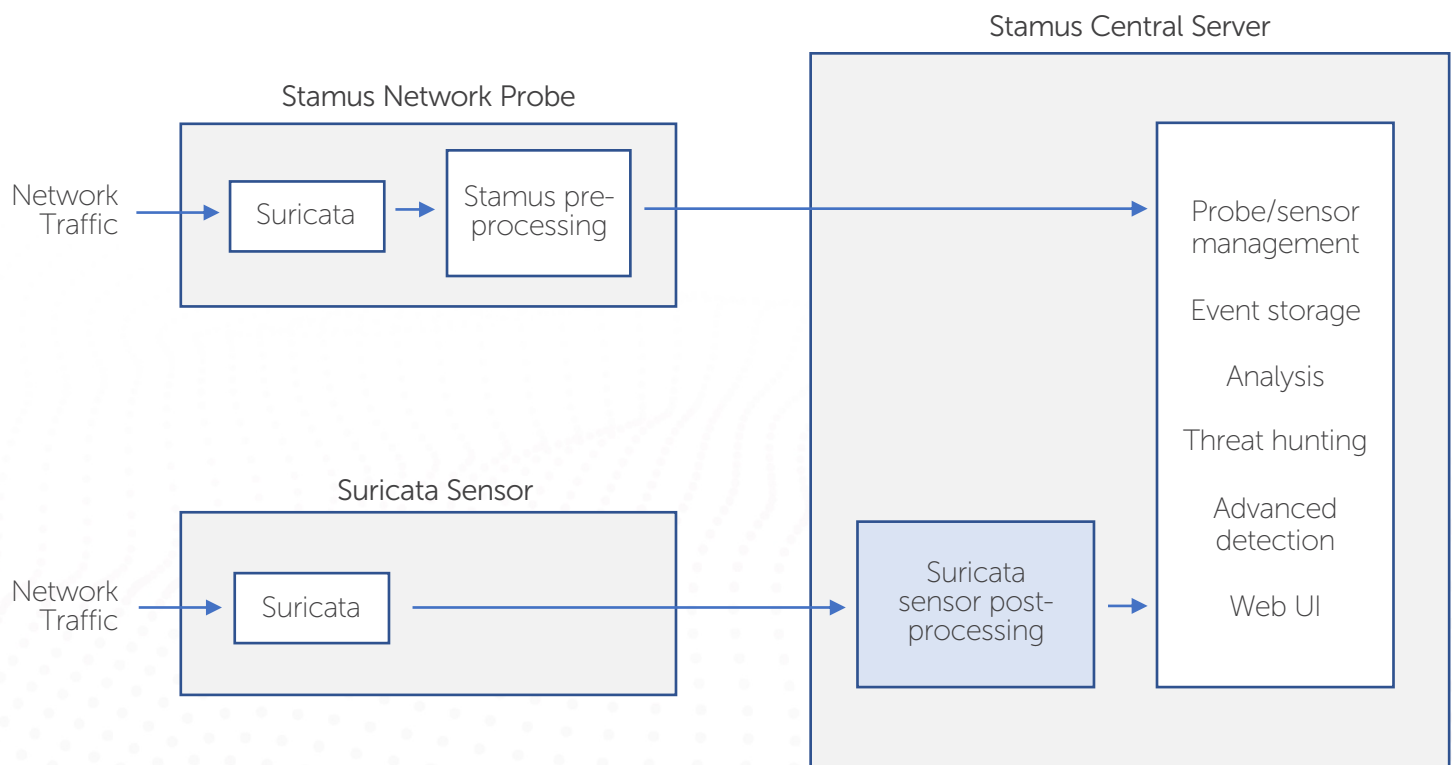
Flow ID 1203203274703203

former category MALWARE

## How it Works

In a typical SSP deployment, the Stamus Network Probes perform extensive local pre-processing of events (alerts, flow data, and protocol transactions), for alert tagging, data enrichment, filtering, and advanced detection.

Native Suricata sensors do not do this, so this is where the Stamus Security Platform Suricata post-processing becomes important. In order to bring organizations using native Suricata sensors some of the same capabilities that are available with Stamus Network Probes, Stamus Central Server now includes a component called *Suricata sensor post-processing*. The diagram below provides a visual explanation.



## 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](mailto:contact@stamus-networks.com)

🌐 [www.stamus-networks.com](http://www.stamus-networks.com)