Technical Brief

Advanced capabilities in U37 for Suricata Sensors

In Stamus Network Detection (ND) and Stamus Network Detection and Response (NDR) systems, the 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 ND and Stamus NDR include a centralized extract, transform and load (ETL) function that delivers many of the same functions in the central Stamus Security Platform (SSP) admin server.

Enrichment

When the capability is enabled, SSP performs the enrichment and tagging of alerts from Suricata sensors, delivering some key capabilities previously available only with the Stamus Network Probes. Alerts are enriched with domain/DNS server, JA3/JA3s, and IP geolocation metadata.

Filters for Tagging and Classification

With the metadata applied to the alerts, users may create and apply SSP filters during incident investigation and hunting. Additionally, these filters may be used to tag events as either “relevant” or “informational” for bulk event triage. Creating these tagging filters allows SSP to similarly classify future events, essentially performing the triage automatically.

Advanced Threat Detection from Stamus NDR

One of the key Stamus NDR features is the ultra high-fidelity detection that generates what we call declarations of compromise™ or “Stamus Threats.” Stamus NDR 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.

This capability was previously unavailable to deployments that use native Suricata sensors. Beginning with release U37, Stamus NDR delivers this capability - limited to signature-based events - for Suricata users. In addition, the filters described above may be used to create custom threat detection logic which is used by Stamus NDR to trigger a "Stamus Threat" or declaration of compromise™

More Available with Stamus Network Probes

While Stamus Networks continues to advance its support for native Suricata sensors, organizations wanting to take advantage of the most advanced capabilities in Stamus ND or Stamus NDR should consider upgrading to the Stamus Network Probes. And because the probe software is based on Suricata, current Suricata users will not lose any of the functionality they are familiar with.

Deploying Stamus Network Probes is the most complete way to receive all the advantages of Stamus ND and Stamus NDR including host identification, dynamic datasets, and organizational context through network definitions. Other benefits of deploying Stamus Network Probes with Stamus NDR include protocol transaction-based (non-signature) advanced threat detection as well as future machine learning and other anomaly detection capabilities.

Finally, the Stamus Network Probe software and license are – at no additional cost – with the Stamus ND and Stamus NDR licenses.

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.

STAMVS 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