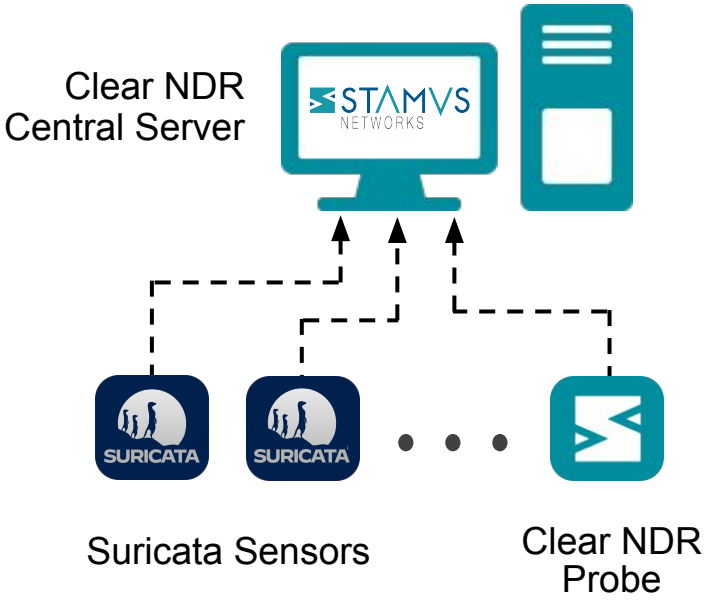
Technical Brief

Supercharge Suricata Sensors with Clear NDR™

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



This document describes the capabilities of Clear NDR that are available to users of native Suricata sensors.

Foundational Suricata Capabilities in Clear NDR

From its earliest inception, Clear NDR was designed to provide a powerful central management to help scale enterprise Suricata deployments. The following is a summary of the foundational Clear NDR 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

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

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

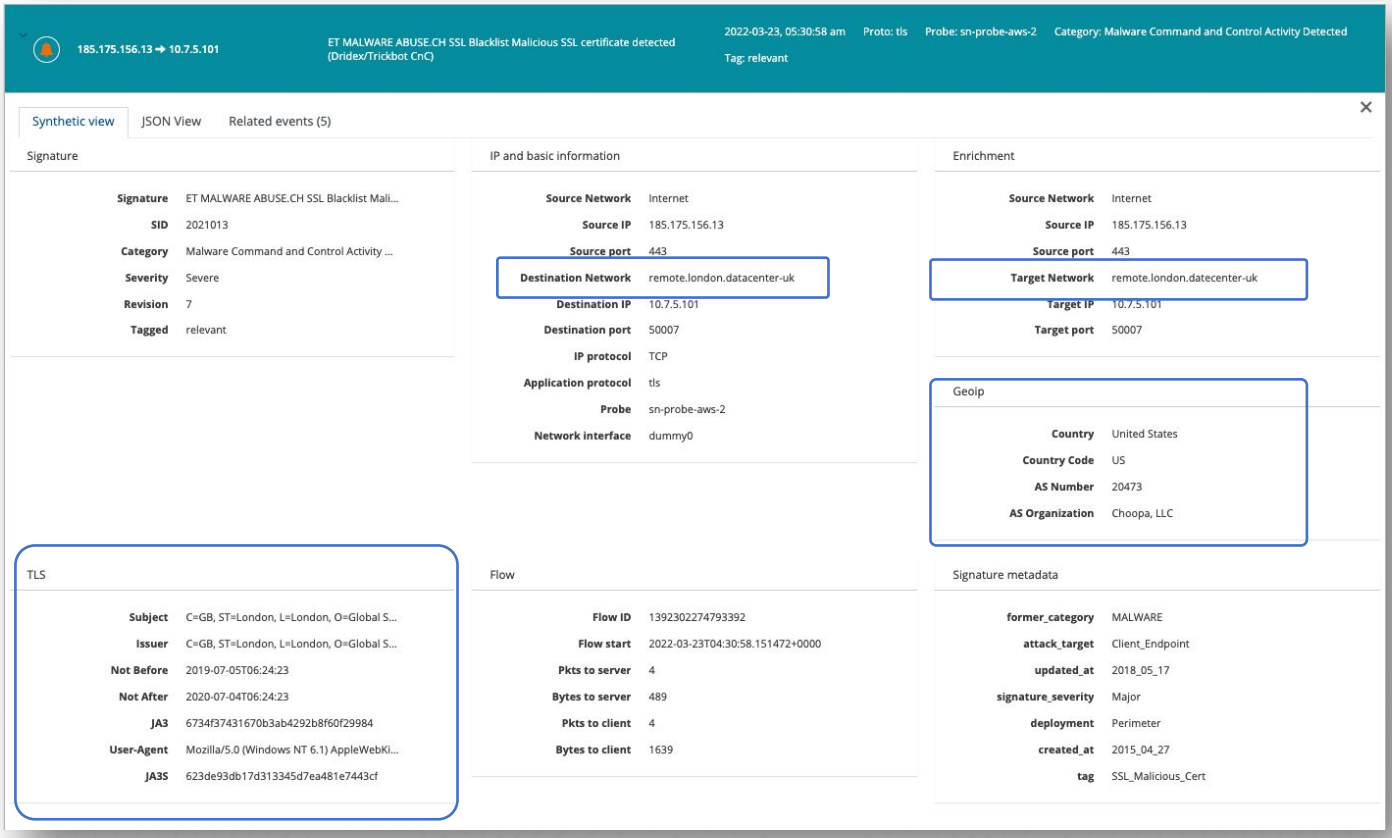
These capabilities include:

- 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

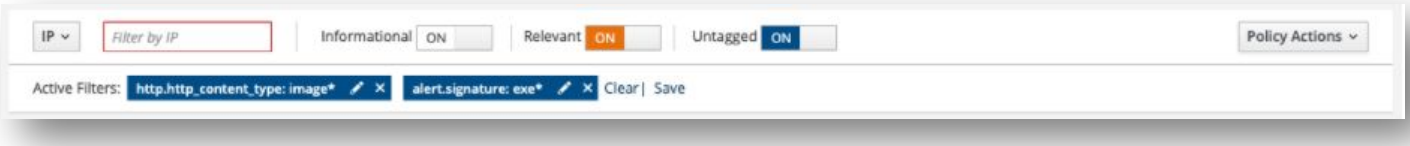
When the capability is enabled, Clear NDR enriches the data associated with alerts from Suricata sensors, delivering some key capabilities previously available only with the Clear NDR Probes. Alerts are enriched with metadata about domain/DNS server, JA4/JA4s, and IP geolocation. See the example screenshot below in which some of the alert enrichment is highlighted with blue boxes.



Automated Event Triage

With the metadata applied to the alerts, users may create and apply Clear NDR 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.

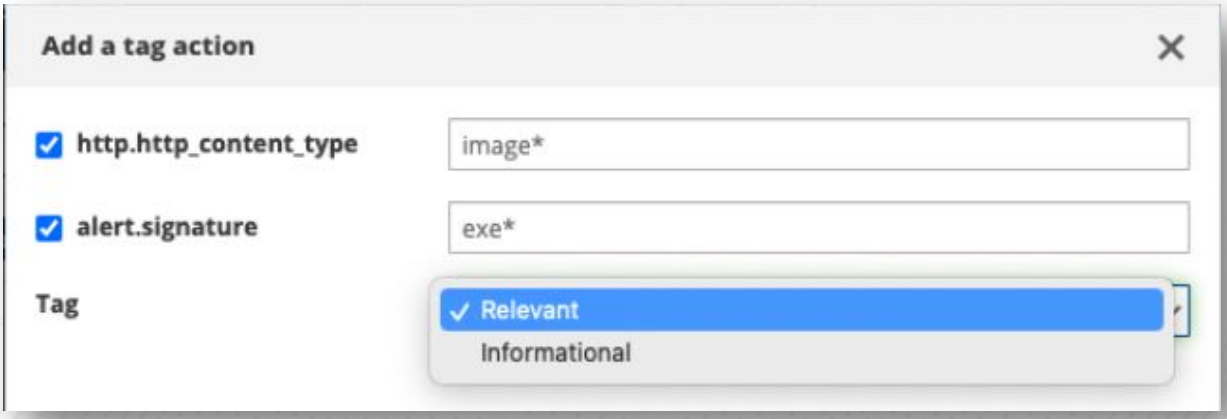
These policies instruct Clear NDR to automatically classify future events, essentially performing the triage automatically. This dramatically reduces the time spent by analysts reviewing security events.



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™

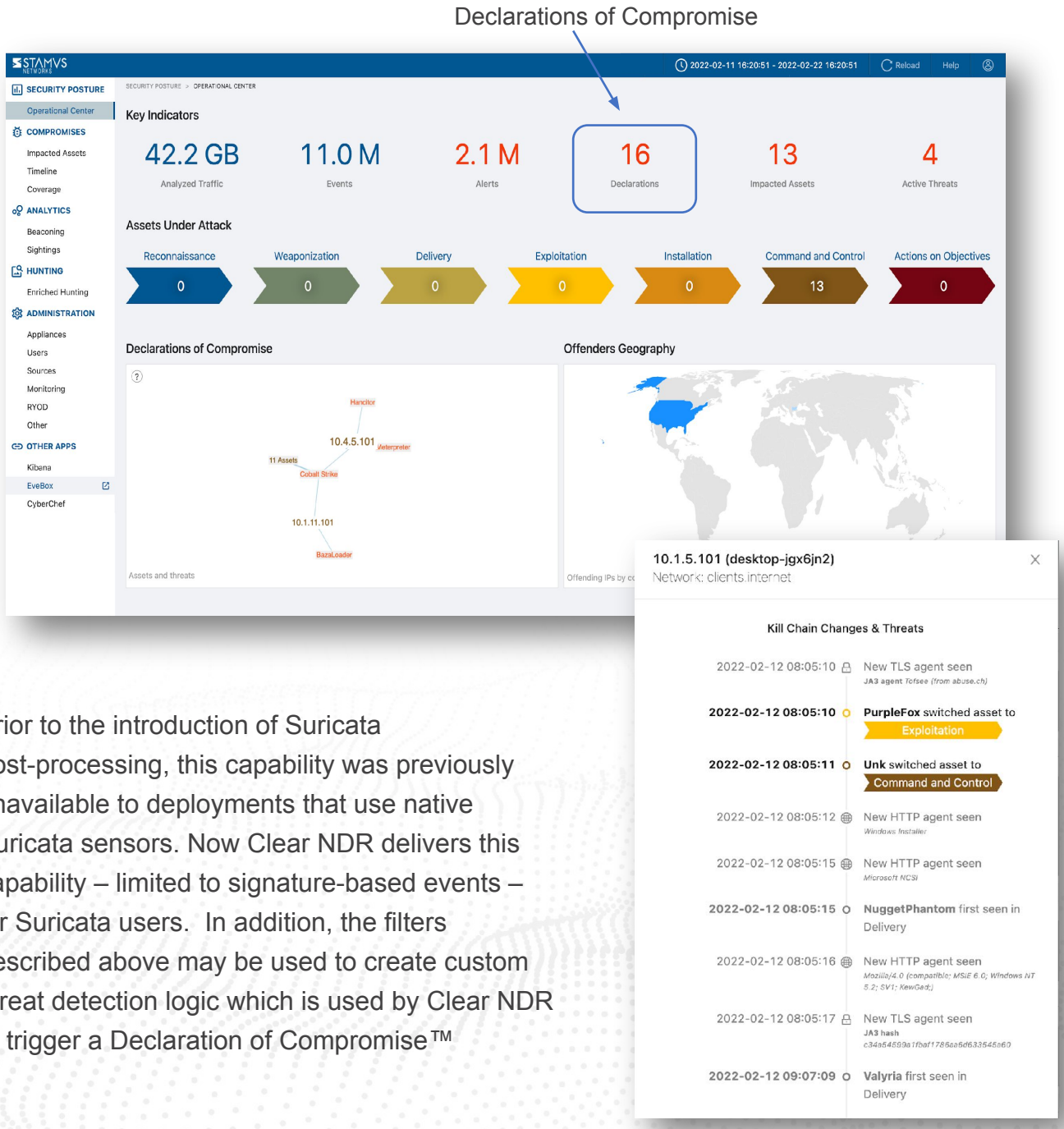
The screenshot below illustrates applying the filter above to create a tagging policy.



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.” Clear 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.

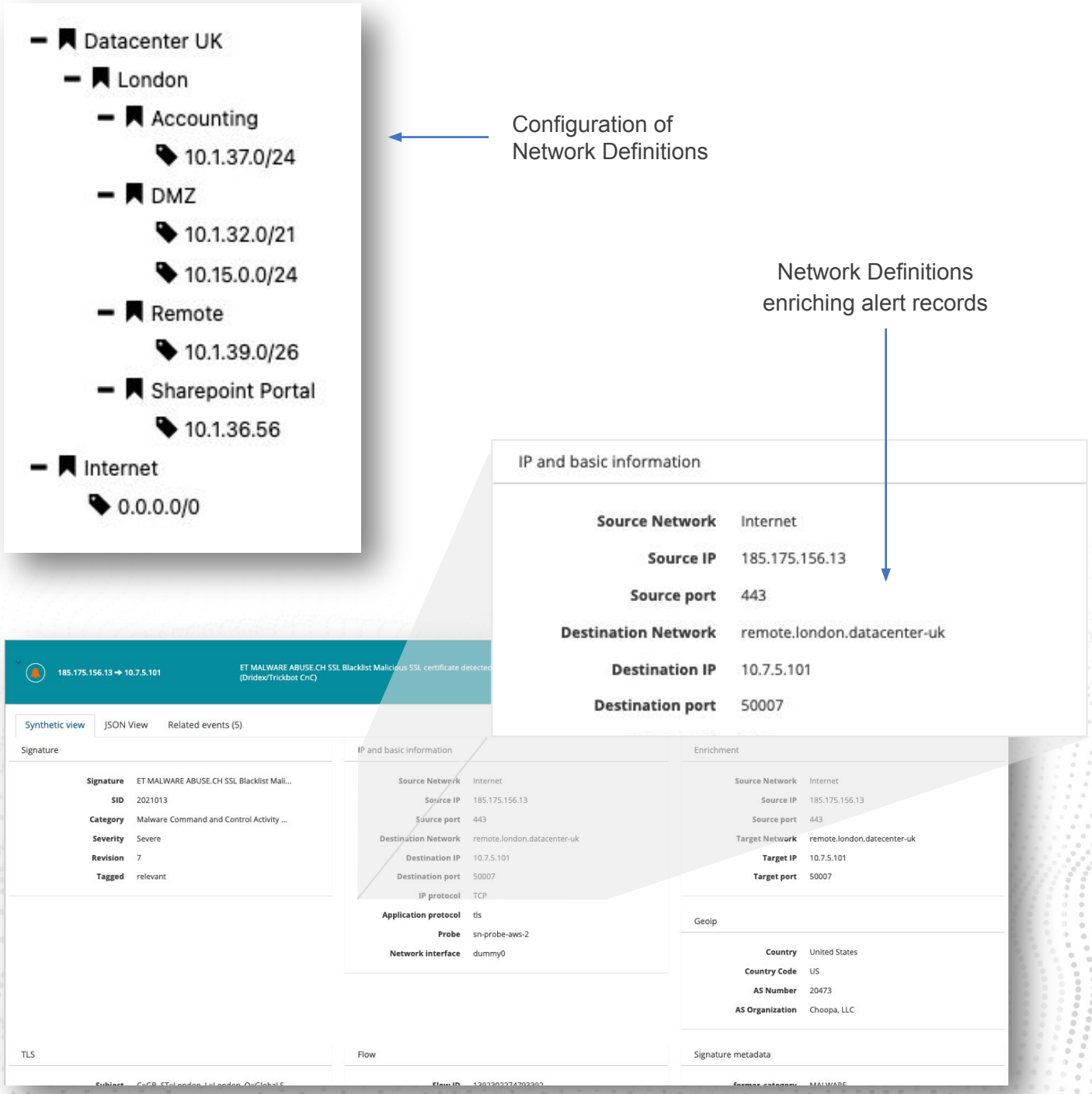


Prior to the introduction of Suricata post-processing, this capability was previously unavailable to deployments that use native Suricata sensors. Now Clear NDR delivers this capability – limited to signature-based events – for Suricata users. In addition, the filters described above may be used to create custom threat detection logic which is used by Clear NDR to trigger a Declaration of Compromise™

Network Definitions

Network Definitions allows the user to label certain networks or IPs with organizationally-relevant names which Clear NDR 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.

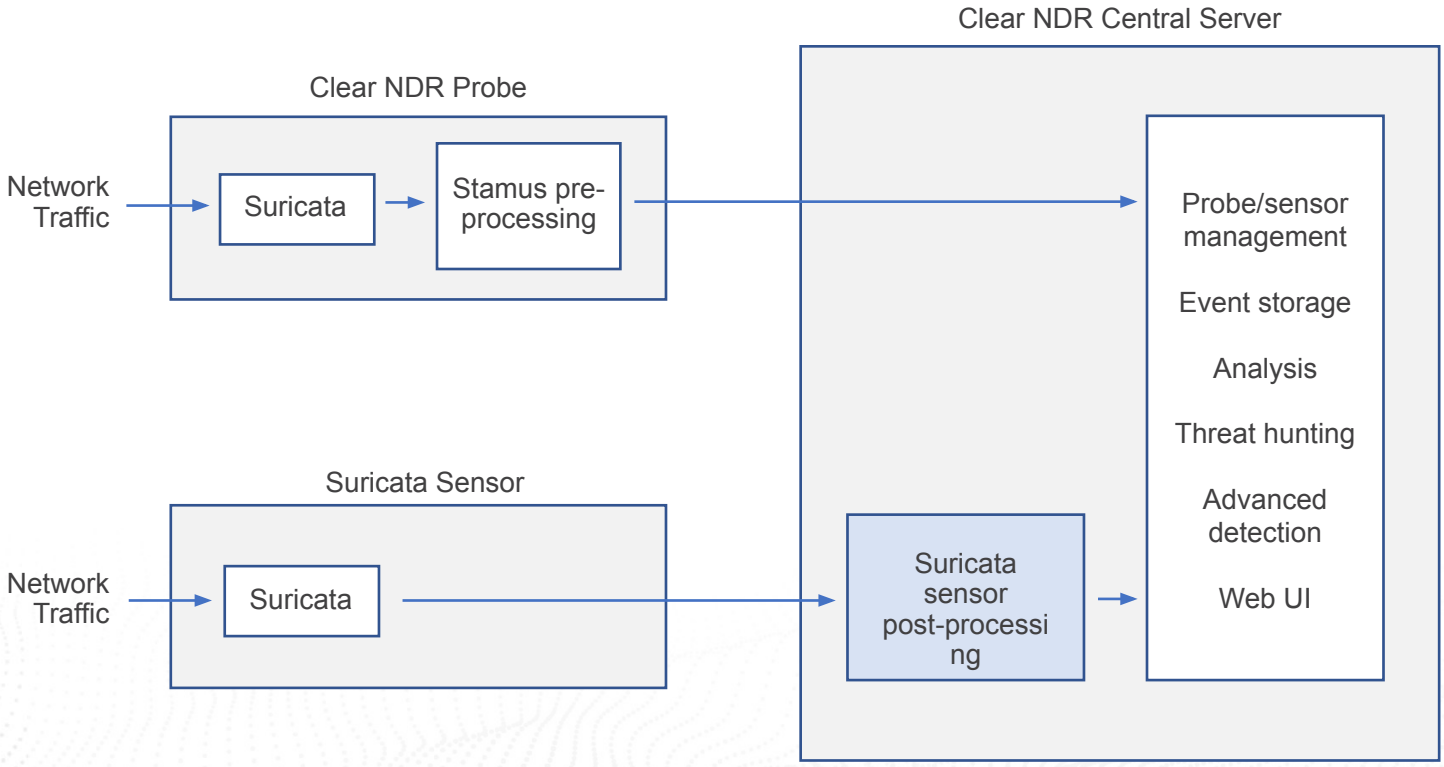
See the example below.



How it Works

In a typical Clear NDR deployment, the Clear NDR 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 Clear NDR Suricata post-processing becomes important. In order to bring organizations using native Suricata sensors some of the same capabilities that are available with Clear NDR Probes, Clear NDR Central Server now includes a component called *Suricata sensor post-processing*. The diagram below provides a visual explanation.



Understanding the Differences with Clear NDR Probes

While Stamus Networks continues to advance its support for native Suricata sensors, organizations wanting to take advantage of the most advanced capabilities in Clear NDR should consider upgrading to the Clear NDR 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 Clear NDR Probes is the most complete way to receive all the advantages of Clear NDR including advanced features such as:

- Host and user insights
- Dynamic datasets for IOC matching
- Protocol transaction-based (non-signature) advanced threat detection
- Machine learning, sightings, and other anomaly detection

Another important consideration when deciding between Clear NDR Probes and Suricata sensors is the performance impact of scaling to multiple sensors. Using native Suricata sensors requires more centralized computational power and resources because the post-processing component runs on the Clear NDR Central Server. Deployments that use Clear NDR Probes tend to be more scalable as they perform the processing directly on the Clear NDR Probes, focusing the work of Clear NDR Central Server on aggregating events and additional detection analytics. Be sure to evaluate your actual bandwidth and throughput requirements before deciding.

Finally, the Clear NDR Probe software and license are included – at no additional cost – with the Stamus ND and Stamus NDR license packages.

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

