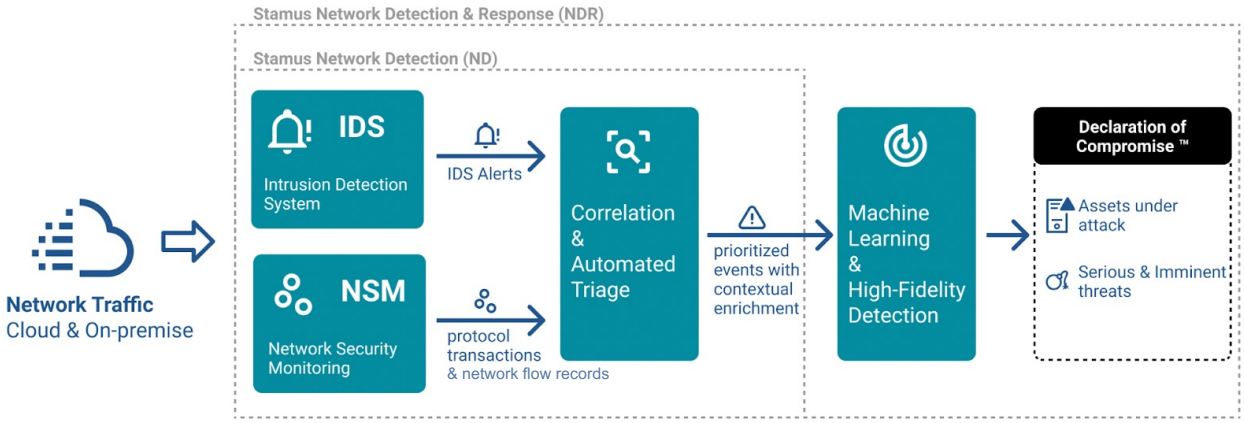
Technical Brief

Splunk Integration with Stamus Networks Solutions

The network doesn't lie. In fact, the network holds the ground truth for an enterprise's security posture. Even as more organizations shift to cloud-based resources, encrypted transmission, and remote workforces, nearly all cyber threats generate communications that can be observed on the network.

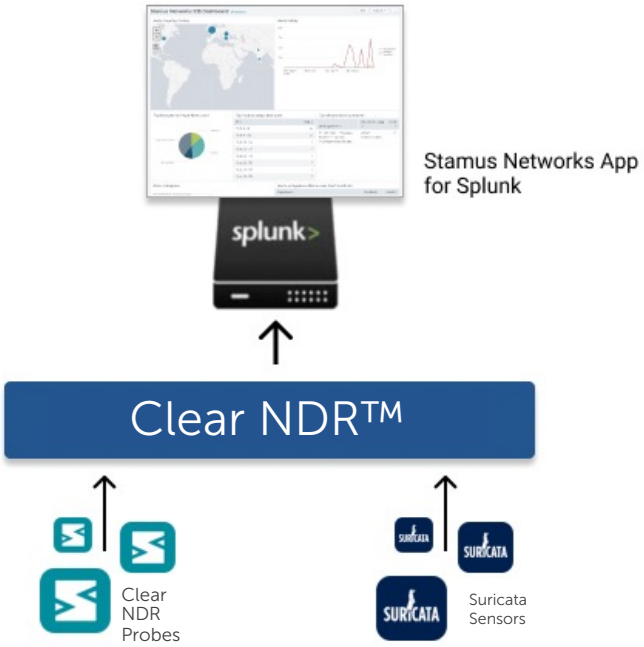
At Stamus Networks, we tap into the inherent power of network traffic to uncover critical threats to your organization. We offer the best possible asset-oriented visibility and automated detection to help practitioners cut through the clutter and focus on only those serious and imminent threats.



The Clear NDR™ is a network detection and response (NDR) solution from Stamus Networks built on a foundation of Intrusion Detection Systems (IDS) and Network Security Monitoring (NSM), enhanced to deliver:

- Correlated IDS alerts (signature-based) and NSM logs – protocol transactions and network flow records
- Tagging & classification for automated triage and alert reduction
- Open access to third-party and custom threat intelligence
- Explainable & transparent results with evidence
- Integrated guided threat hunting
- Declarations of Compromise™ - Response-ready and high-fidelity threat detection from machine learning, stateful logic, and signatures
- Stamus Sightings™ - insights from machine learning that detect suspicious and unusual behavior
- Open interfaces for SOAR, SIEM, XDR, IR via REST-API and Webhooks
- Flexible and turn-key integration with Splunk using native Splunk app

Clear NDR can easily be integrated with third party tools such as Splunk to allow a security team to correlate telemetry data from NDR, EDR and other log sources.



KEY BENEFITS OF STAMUS NETWORKS INTEGRATION WITH SPLUNK

- **Control data volume** - Stamus Networks solutions allow fine tuning of the data types sent to Splunk to control Splunk license consumption - send everything or very little, it's up to you.
- **Ready to go** - Stamus Networks App for Splunk lets you integrate and investigate alerts, events, metadata and Stamus host identification data in Splunk with pre-built dashboards, reports and advanced queries. And all data complies with Splunk's Common Information Model (CIM).
- **Rich context** - The enriched JSON data from Clear NDR deliver valuable context beyond traditional IDS and NSM data such as GeoIP, tagging, filtering, JA4/JA3S fingerprinting, domain breakdowns, etc.
- **Support for Suricata** - Stamus Networks App for Splunk also supports native Suricata sensors

CONSOLIDATING ALERTS AND LOGS

Enterprise security operations teams consolidate logs from different systems using Splunk or similar systems to gain a single unified view of what's happening in their environment.

Looking closer, network security teams wish to consolidate all the IDS events, protocol transactions, flow records, TLS meta-data, and others produced from multiple network probes – physical, virtual and in the cloud – deployed across a multiple locations. This unified view for correlation, search, and analysis allows a security team to more easily gain insights into their organization's overall network security posture.

Data aggregation from multiple probes is provided by both the Stamus Central Server – the central component of the Clear NDR – and from within Splunk. Of course, within Splunk, aggregation can be further extended to include correlation of other log sources such as those from EDR.

Clear NDR runs automated detection on the network data and provides additional context to Splunk such as a 360-degree view of compromised host activity and response-ready, high-fidelity Declarations of Compromise through Splunk custom commands included in the Stamus Networks App for Splunk.

CONTROLLING DATA INGESTION

Splunk can receive data from native Suricata sensors, Clear NDR Probes and Clear NDR Central Server.

When forwarding data from Clear NDR Probes or Clear NDR Central Server, filtering may be used to control the ingestion volume while meeting your organizational requirements and ensuring your Splunk consumption volume and their associated fees are under control.

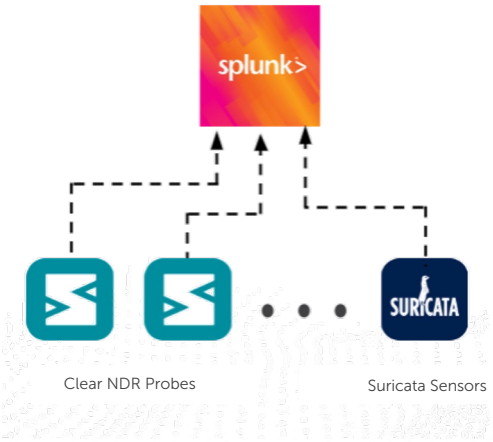
At the highest level, users may select any or a combination of the following data types:

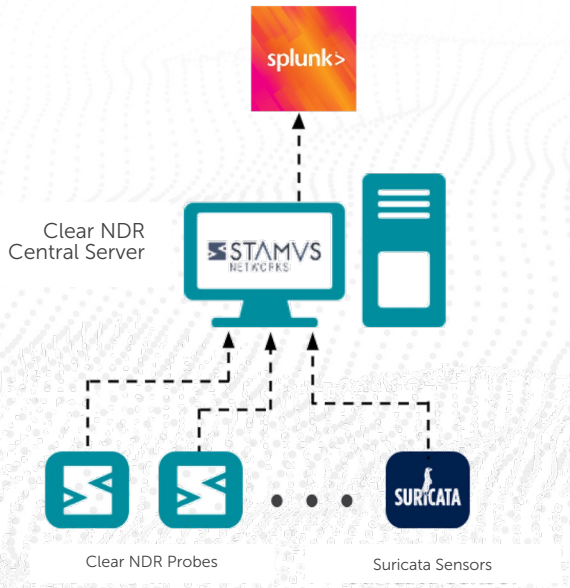
- Security events – IDS alerts enriched with contextual information
- Protocol transactions – network traffic metadata, optionally filtered per protocol (e.g. http, smtp, ssh)
- Network flows – metadata record of any IP session (IPs, ports, bytes, etc)
- The system's internal logs – for audit purposes

Direct Probe Connection

Whether you use native Suricata sensors or Clear NDR Probes, logs can be ingested by Splunk through the usage of Splunk Forwarders or using the syslog protocol.

Stamus Network Probes are already packaged with a Splunk Forwarder, and Clear NDR Central Server allows the administrator to configure which Stamus Network Probes will send logs to Splunk in a matter of a few clicks.





Aggregated Clear NDR Connection

Consolidated data may also be forwarded to Splunk from the central Clear NDR Central Server by using the syslog protocol.

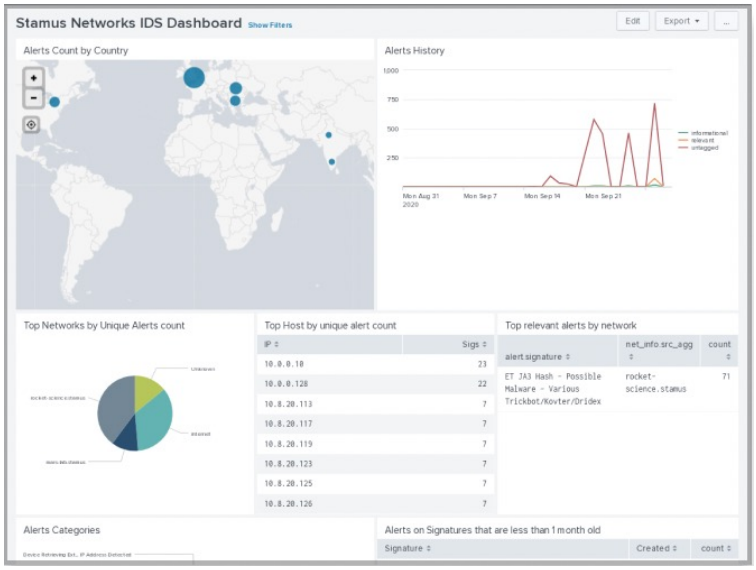
In this case, Clear NDR Central Server serves as a central repository collecting logs from all the Clear NDR Probes and Suricata sensors in your environment.

HOW TO SEND LOGS TO SPLUNK

Stamus Networks recommends sending logs using a Splunk Forwarder via direct probe connection to ensure that the data are forwarded through an encrypted channel (TLS/SSL). However, depending on your architecture, you may choose an alternative mechanism, such as Syslog. The Stamus Networks solutions have the flexibility to fit your requirements.

STAMUS NETWORKS APP FOR SPLUNK

The Stamus Networks App for Splunk provides ready-to-use dashboards, reports and advanced queries that expose the IDS and NSM data being collected by Stamus Probes or Suricata sensors to help Splunk Enterprise users extract information and insights from their network activity.



The data produced by the probes include IDS alerts, protocol transactions (metadata), network flow records, and enrichments such as JA4/JA3S fingerprinting, domain/hostname breakdowns, alert classification, geolocation, and many others.

The Stamus Networks App for Splunk also provides search commands to query data from Clear NDR Central Server. These data are not indexed by Splunk, allowing you to reduce your data ingestion and thus your Splunk license fees. But it nonetheless exposes all the power and unique perspectives of Clear NDR to Splunk users (see Clear NDR host insights feature description below).

Clear NDR "HOST INSIGHTS" FEATURE

The unique Clear NDR host insights capability provides a snapshot view of the network by aggregating information for each host about services, users, agents and uniquely identifying encrypted connections identified over time across the entire network. This information is powerful for network discovery and for providing context for incident response.

Clear NDR Central Server

These data, representing the state of any given host in the network, are updated in real-time and maintained inside Clea3r NDR Central Server. The Stamus Networks App for Splunk, through REST-API calls, provides Splunk commands, queries and dashboards for this consolidated view of the network activity.

SPLUNK SOURCETYPE AND CIM COMPATIBILITY

Suricata began exporting its data as JSON many years ago. This choice makes its data directly compatible with Splunk Enterprise and even with the Splunk Common Information Model (CIM) used for Splunk Enterprise Security by normalizing the field names such as "src_ip" for an IP source.

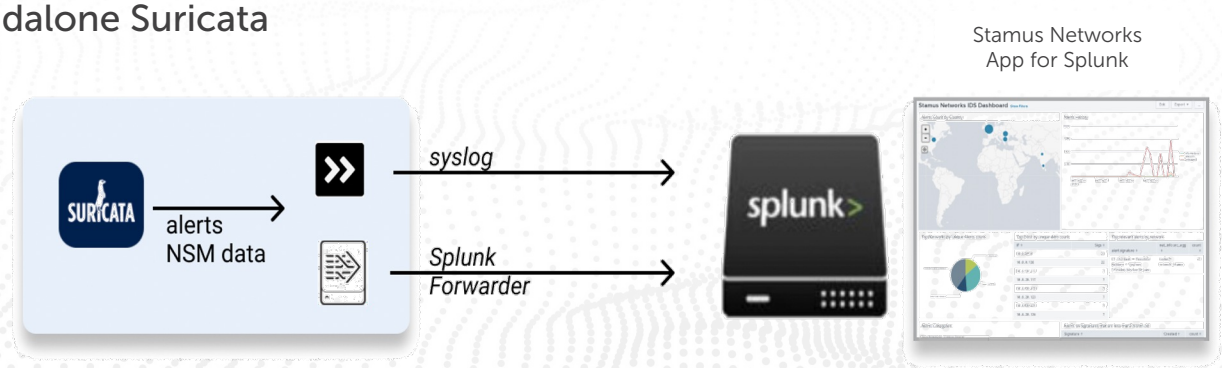
The Stamus Networks App for Splunk delivers a sourcetype definition 'suricata' that is compatible with the data produced by Stamus Network Probes and with native Suricata sensors. The app includes a Splunk technology add-on (TA) which conforms to the Splunk CIM and provides dashboards as well as new keywords.

With the roots of Stamus Networks firmly planted in the Suricata open-source community, the Stamus Networks App for Splunk offers ready-to-use dashboards and reports that will expose the IDS and NSM data being generated by Suricata sensors and help those with large Suricata deployments integrate their NDR, IDS and NSM data with their other sources for highly accurate detection and detailed context.


```
"flow" : {
  "pkts_toclient" : 3
  "src_ip" : "172.16.10.97"
  "bytes_toclient" : 470
  "src_port" : 49944
  "dest_ip" : "198.199.96.164"
  "bytes_toserver" : 1241
  "start" : "2021-06-21T03:53:37.725931+0200"
  "pkts_toserver" : 4
  "dest_port" : 443
}
```


DEPLOYMENT MODES

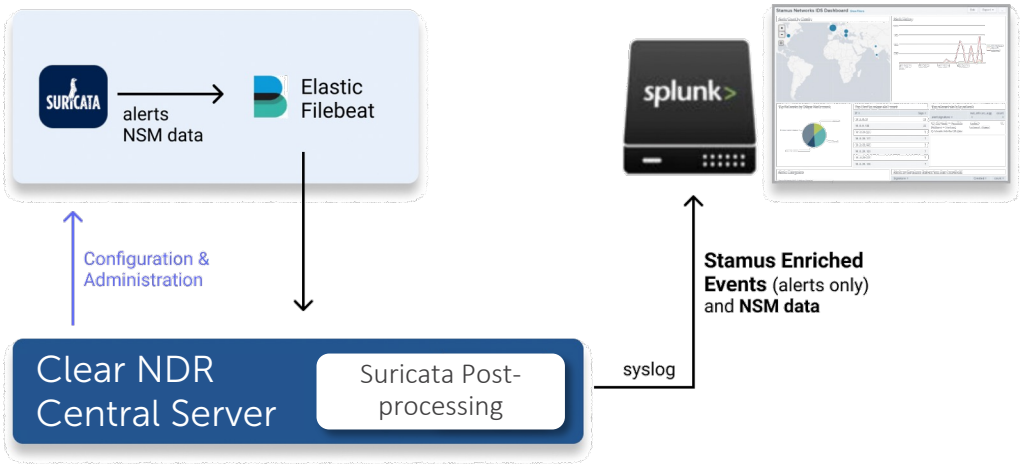
Standalone Suricata



What: Configure the alerts, protocol transaction logs and flow records forwarded to Splunk from your Suricata sensors using syslog or by installing a Splunk Forwarder.

Why: Become more productive when your organization has a large Suricata deployment

Managed Suricata



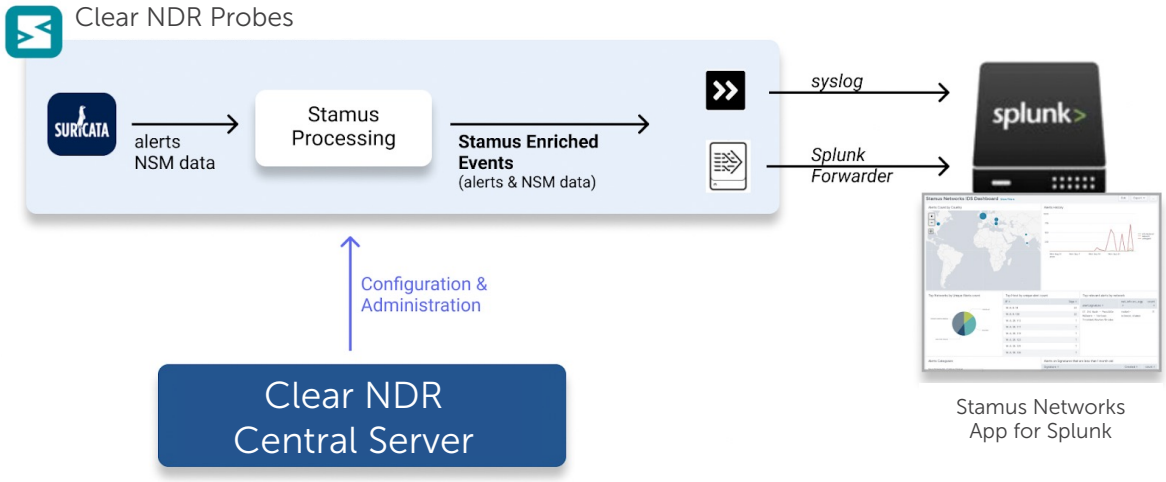
What: Clear NDR Central Server centrally manages Filebeat on your Suricata sensors to collect and aggregate alerts, protocol transaction logs, and flow records. Clear NDR forwards protocol transaction logs (unenriched) and enriched Stamus events to Splunk through syslog. Clear NDR can optionally filter the received protocol transaction logs based on protocols (http, smtp, etc).

Clear NDR Central Server uses an embedded Suricata Post-Processing component to enrich native Suricata alerts – similar to the enriched Stamus events generated by Clear NDR Probes. Protocol transactions and flow records are not enriched as they are with a Clear NDR Probe. Note, enabling this Suricata Post-Processing feature does impact the performance of SCS. This setup should be selected only when it is not possible to replace a native Suricata sensor with a Clear NDR Probe.

Why: Enrich native Suricata alerts in cases where it is not possible to deploy Clear NDR Probes and where you wish to centrally manage Suricata sensor rulesets and threat intelligence.

NOTE: Data may still be forwarded directly from the Suricata sensor to Splunk, but it will not include enrichment. And caution must be taken to not duplicate the data sent to Splunk.

Managed Clear NDR Probes



What: Clear NDR centrally manages Clear NDR Probes, and the probes deliver logs using either Syslog or the Splunk Forwarder which is pre-installed on Clear NDR Probes. Clear NDR Central Server allows the user to configure the type of data (protocol transactions, Stamus Events, flow records, system's internal logs) forwarded to Splunk. Stamus events may also be sent to Splunk

Why: Clear NDR Probes enrich both IDS alerts and NSM data before sending their data to Clear NDR Central Server and Splunk.

Summary of capabilities for each deployment mode

	Data Source Deployment Mode		
	Clear NDR Probes	Managed Suricata	Standalone Suricata
Stamus App for Splunk	Supported	Supported	Supported
Data is forwarded from	Clear NDR Probes or Clear NDR Central Server	Clear NDR Central Server	Suricata sensors
Splunk forwarder	Pre-installed, centrally managed by Clear NDR Central Server	Manually installed on Suricata sensors	Manually installed on Suricata sensors
Stamus enriched events	Yes	Yes, partial	No
Protocol transactions and flow records	Enriched	Raw	Raw
Data filtering per protocol	Yes	Yes	No
Clear NDR Declarations of Compromise™ and Declarations of Policy Violations	Yes	Yes, partial	No
Clear NDR host insights data	Yes	No	No
Clear NDR central Filebeat mgmt	Yes	Yes	No

SUMMARY

For many years, users of Stamus Networks network detection and response (NDR) solutions have been able to view and analyze their security events and logs with Splunk. The integration is simple and flexible though clear configuration, multiple integration options that align with the needs of each organization, and a ready-to-run Splunk Application.

Most Stamus Networks users are also long-time Splunk users and have integrated the enriched JSON Stamus Network Probe data with their instance of Splunk, to gain valuable context beyond what is available from traditional IDS and NSM data.

The Stamus Networks App for Splunk provides users with ready-to-use dashboards, reports and advanced queries that expose all the power and unique perspectives of Stamus NDR/ND. The data presented by the Stamus Networks App for Splunk adhere to the Splunk Common Information Model (CIM) allowing Splunk to normalize data from multiple sources for maximum efficiency at search time.

ABOUT STAMUS NETWORKS

Stamus Networks believes that cyber defense is bigger than any single person, platform, company, or technology. That's why we leverage the power of community to deliver the next generation of open and transparent network defense. Trusted by security teams at the world's most targeted organizations, our flagship offering – Clear NDR™ – empowers cyber defenders to uncover and stop serious threats and unauthorized network activity before they harm their organizations. Clear NDR helps defenders see more clearly and act more confidently through detection they can trust with results they can explain.

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

