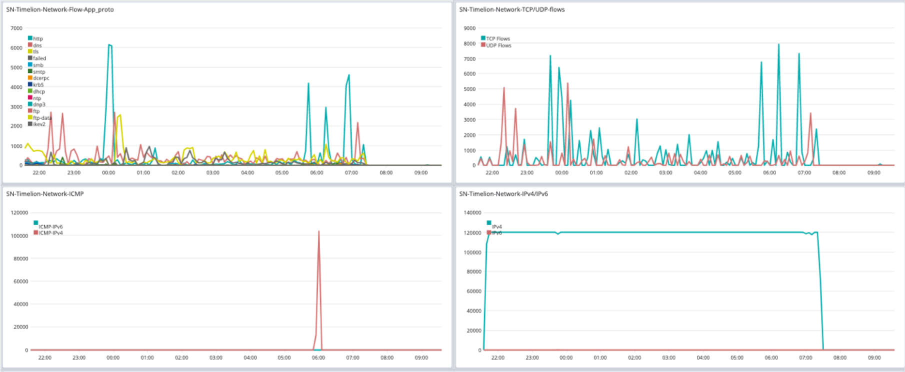
Technical Brief

Clear NDR™ Probes and NetOps

In addition to their intrinsic value for security operations (SecOps), deployment of security monitoring probes in a network or data center can bring value to network operations (NetOps) by providing visibility into network blind spots and allowing NetOps to benefit from a budget previously allocated to SecOps projects.

Clear NDR Probes passively monitor network traffic and provide a broad spectrum of traffic metadata. The data types logged by the probes are configured by the user. When all data types are enabled, security alerts account for only 8% of the data by volume.



IPv4/6, ICMP, TCP/UDP Analysis

The remaining 92% of the data consists of over 4000 unique elements of metadata derived from the network security monitoring logs – protocol transactions – including:

- SMB, KRB5, HTTP, DNS, etc..
- NTA data such as Host Insights and self-learning datasets
- Flow data records

While this information is valuable for SecOps and is used by Clear NDR for automated threat detection, it can also be a powerful resource to help NetOps teams with:

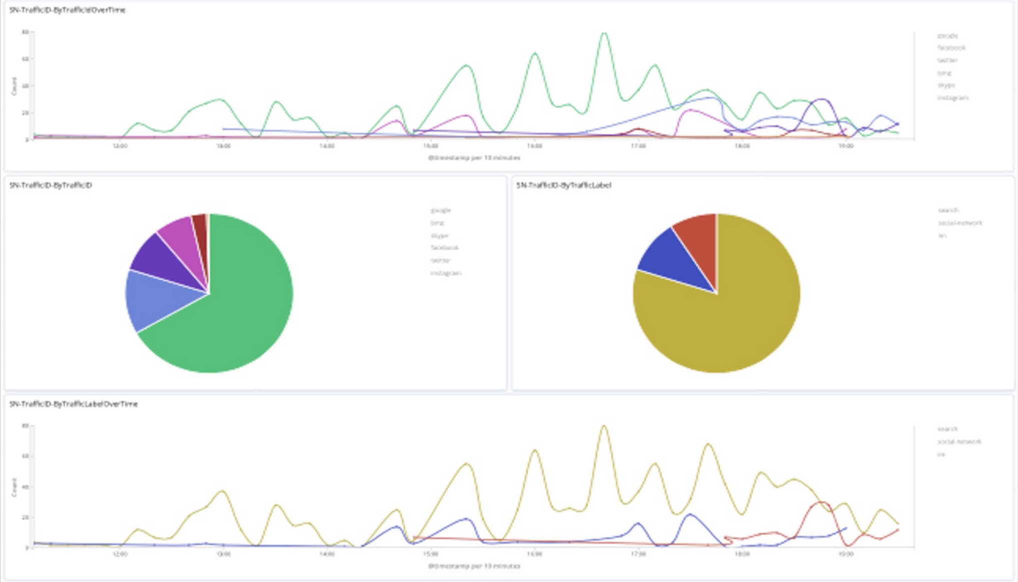
- Understanding what's happening on the network
- Engineering network traffic
- Detecting the use of vulnerable protocols and ciphers
- Troubleshooting a slow network
- Profiling user behavior
- Uncovering shadow IT

This data may be viewed and analyzed in the Clear NDR through Kibana, which is accessed on the task switcher menu. This integrated Kibana toolset provides 25 reports and over 450 visualizations. Finally, this data may be exported to third party NTA log and analysis system such as SolarWinds, Nagios, ManageEngine and others.

Included Reports

The ZIP package that accompanies this document contains example Kibana reports and analysis for approximately half the data types produced by the probes, and includes:

- Summary of all recorded meta-data [SN-ALL]
- DHCP traffic analysis [SN-DHCP]
- DNP3 traffic analysis [SN-DNP3]
- DNS traffic analysis [SN-DNS]
- File transfer analysis [SN-FILE-Transactions]
- Flow data analysis [SN-FLOW]
- HTTP protocol analysis [SN-HTTP]
- Kerberos traffic analysis [SN-KRB5]
- Overview of all network traffic over time [SN-Network-Overview-1]
- Overview of all network traffic [SN-Network-Overview-2]
- NFS protocol analysis [SN-NFS]
- Overview of protocol throughput and top events [SN-OVERVIEW]
- SMB protocol analysis [SN-SMB]
- SMTP protocol analysis [SN-SMTP]
- SSH protocol analysis [SN-SSH]
- TFTP protocol analysis [SN-TFTP]
- TLS protocol analysis [SN-TLS]
- Traffic type analysis [SN-TrafficID]
- IDS Alert (triggered by a signature) analysis [SN-IDS]



Traffic Type Analysis

For Splunk® Users

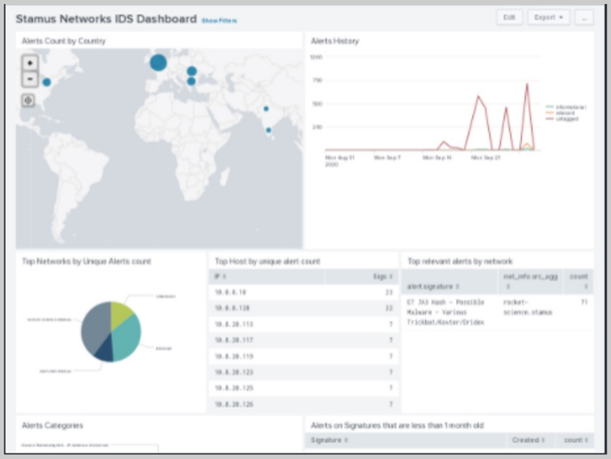
For Splunk users, there is a Stamus Networks Splunk application available at https://splunkbase.splunk.com/app/5262/. This includes multiple reports and visualizations for network security monitoring, including:

For Clear NDR Users

- Intrusion Detection System Dashboard
- Network Traffic Analysis Dashboard
- Stamus NDR Dashboard
- Stamus Networks Host Anomaly
- Stamus Networks NSM Anomaly
- Investigate an IP

For Suricata Users

- Intrusion Detection System Dashboard
- Network Security Monitoring Dashboard
- Network Security Monitoring Anomaly Detection
- Investigate an IP


Stamus Networks IDS Dashboard
Show Filters
Edit
Export ▾
...
Alerts Count by Country
Alerts History
1000
750
500
250
Mon Aug 31 2020
Mon Sep 7
Mon Sep 14
Mon Sep 21
informational
relevant
untagged
Top Networks by Unique Alerts count
Top Host by unique alert count
Top relevant alerts by network
Alerts Categories
Alerts on Signatures that are less than 1 month old

IP ⇕	Sigs ⇕
10.0.0.18	23
10.0.0.128	22
10.0.20.113	7
10.0.20.117	7
10.0.20.119	7
10.0.20.123	7
10.0.20.125	7
10.0.20.126	7

alert signature ⇕	net_info.src_agg ⇕	count ⇕
ET JA3 Hash - Possible Malware - Various Trickbot/Kovter/Dridex	rocket-science.stamus	71

Signature ⇕	Created ⇕	count ⇕

Traffic Type Analysis
in Splunk

Learn More

Visit stamus-networks.com

or contact us via email at contact@stamus-networks.com

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.

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