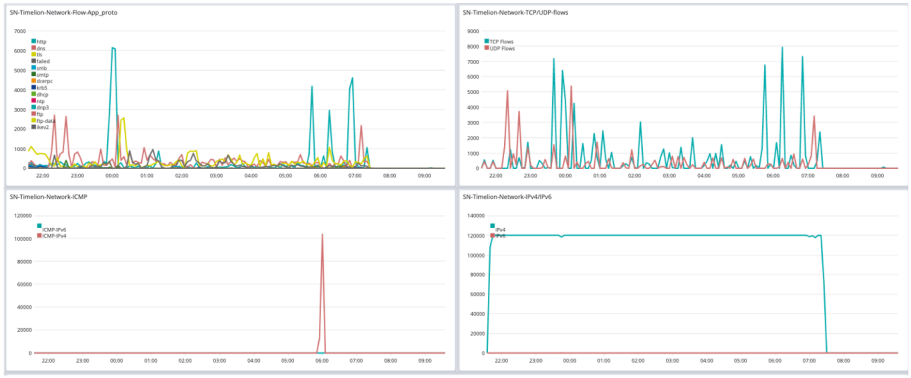
Stamus Network Probes and NetOps

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.

Stamus Network 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 HostID and self-learning datasets
- Flow data records

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

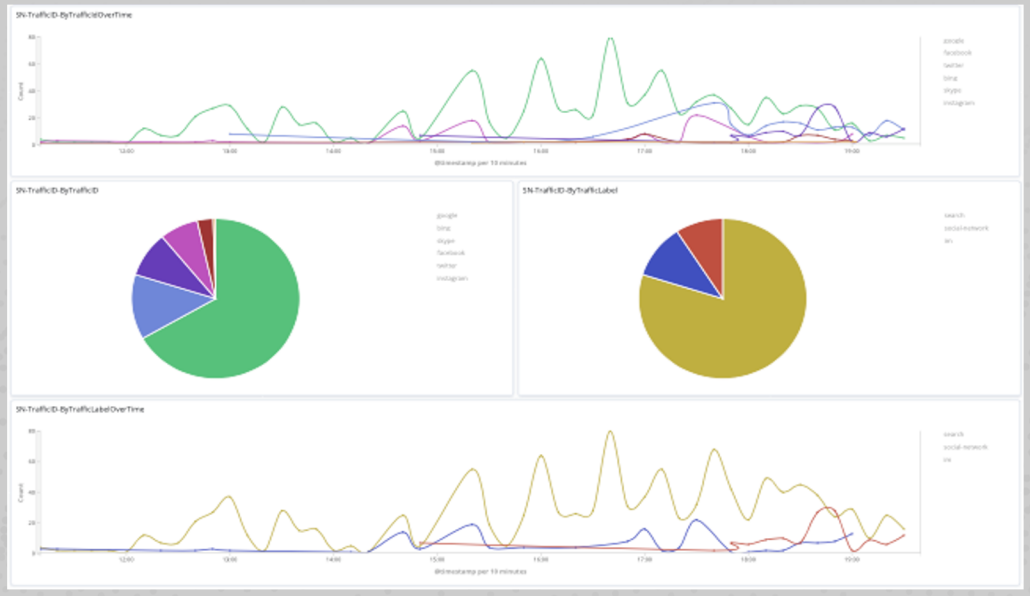
- Understanding what's happening on the network
- Engineering network traffic
- Detecting the use of vulnerable protocols and ciphers
- Troubleshooting a slow network
- Profiling user behavior
- Uncovering shadow IT

This data may be viewed and analyzed in the Stamus Security Platform (SSP) 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

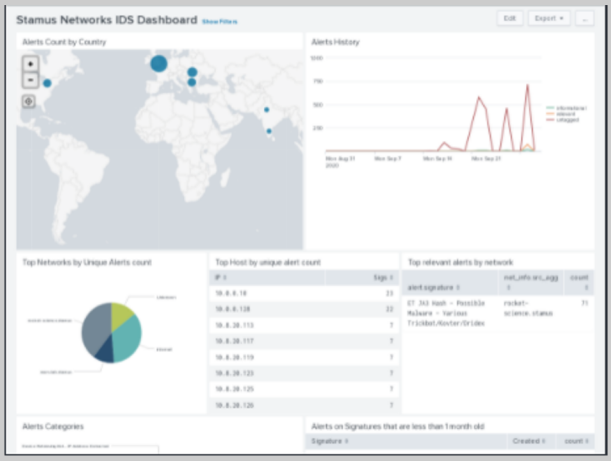
For Splunk users, there is a Stamus Networks Splunk application available at https://splunkbase.splunk.com/app/5262/. This includes multiple reports and visualizations for network security monitoring, including:

For Stamus ND and Stamus NDR Users

- Intrusion Detection System Dashboard
- Network Traffic Analysis Dashboard
- Threat Radar 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



Traffic Type Analysis in Splunk

Learn More

Visit stamus-networks.com

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

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.

STAMUS NETWORKS

For more information, contact

KIPPEO
GET STARTED IN HOLISTIC SECURITY

https://kippeo.com
sales@kippeo.com

