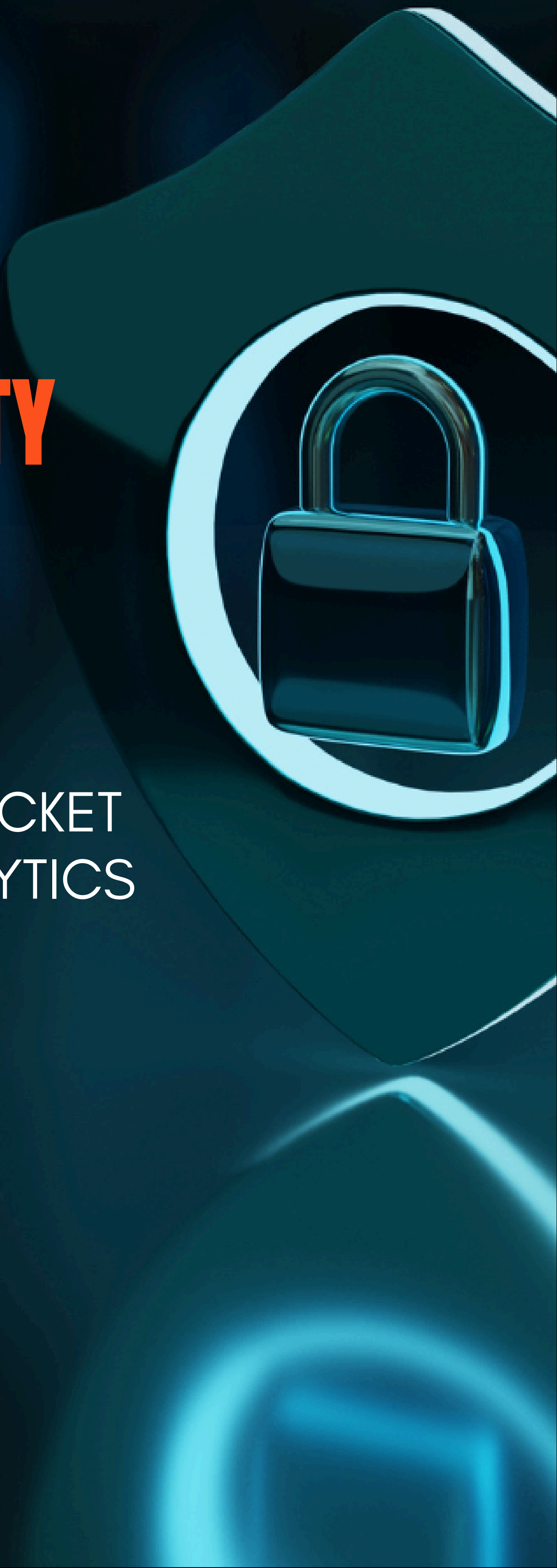
TRISUL NETWORK SECURITY MONITORING

DATASHEET FOR DEEP PACKET INSPECTION BASED ANALYTICS



www.trisul.org

info@unleashnetworks.com

OVERVIEW

01

Trisul Network Analytics is a network traffic analytics platform. Across industries, organizations trust our network solution for real time monitoring of network traffic, detecting anomalies, IPDR regulatory compliance requirements, peering analytics for ISPs. Our Network Security Monitoring solution is our deepest visibility product that leverages analysis at the deepest packet based layer.

Trisul Network Monitoring Solution (NSM) is a full spectrum collection and correlation of network alert events, flows, metadata artifacts, traffic profiles, and packets. Such deep collection and analysis at the packet level enables three powerful benefits.

KEY CAPABILITIES

Better Visibility
Intrusion Detection
Deep Investigation

Trisul 7.0 is designed to make Network Security Monitoring Solution feasible to organizations of all types and sizes.

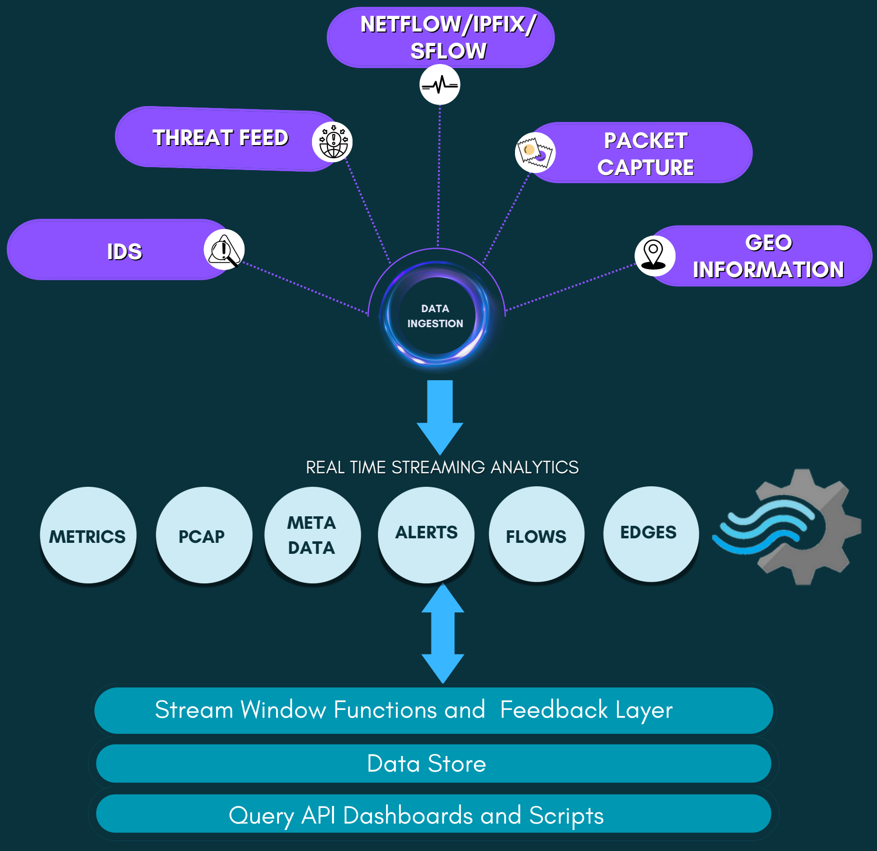
NSM FEATURES

02

TRAFFIC ANALYSIS

L2 to L7 Packet Based Metrics

Trisul NSM delivers multi layer network visibility through high resolution traffic metrics. Out of the box you get 200+ metrics and dozens of Top-Talkers at all layers, fully customizable metric, and real time analytics. Trisul NSM works at the packet level, so you miss nothing.



Multiple Data Types

FLOW ANALYSIS

Full record of conversations

Trisul reconstructs IP conversations (flows) from packets, indexing and storing them in a custom-built database designed to scale billions of flows with sub-second query response times. The Explore Flows tool allows you to search for any flow in the past. Flow Trackers and Flow Taggers allow you to mark flows of interest in real time. Trisul NSM stores all flows without rollups so you can rely on it as a reliable source of truth for long term investigations.

EXTENSIBILITY

LUA API and Trisul Apps

Get creative with our powerful LUA API which enables integration of custom detection and metrics into the streaming analytics engine. The TRP API enables database integration with other systems. Trisul APP are free pluggable extensions to provide enhanced functionality to Trisul NSM.

METADATA

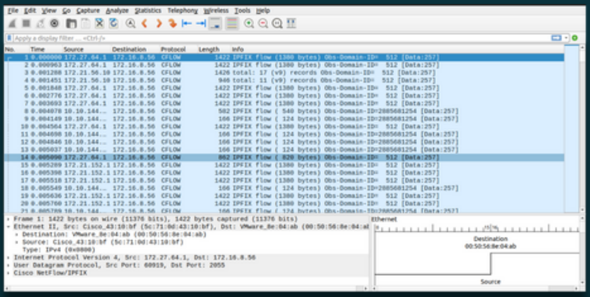
Extracts objects from network

Trisul NSM continuously tracks packets, reconstructs them using TCP analysis, and extracts metadata. These metadata are stored as searchable resources and FTS documents. Examples are DNS records, HTTP headers, SSL certs, file hashes, and reconstructed binaries. This enables query-based investigation and scanning for threat analytics Indicators of Comrpromise.

RAW PACKETS FROM ANY ANALYSIS POINT

Jump to raw packets from anywhere

TrisulNSM works at the packet level. Hence it indexes packets with flows, alerts, metrics, and resources. Click to get PCAPS (Packet Captures) from any point in your analysis and pull it into Wireshark for further bit level analysis.


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Ethernet
Destination
00:50:56:8e:04:ab
Source

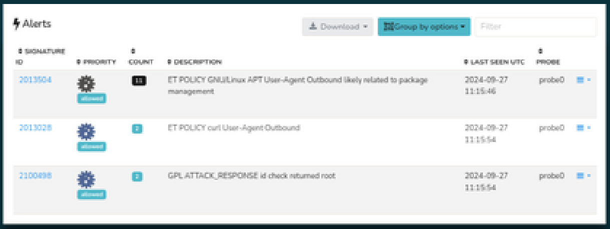
```
No.  Time     Source          Destination  Protocol  Length  Info
  1 0.000000 172.27.64.1     172.16.8.56  CFLOW     1422 IPFIX flow (1380 bytes) Obs-Domain-ID=  512 [Data:257]
  2 0.000963 172.27.64.1     172.16.8.56  CFLOW     1422 IPFIX flow (1380 bytes) Obs-Domain-ID=  512 [Data:257]
  3 0.001288 172.21.56.10    172.16.8.56  CFLOW     1426 total: 17 (v9) records Obs-Domain-ID=  512 [Data:257]
  4 0.001451 172.21.56.10    172.16.8.56  CFLOW      946 total: 11 (v9) records Obs-Domain-ID=  512 [Data:257]
  5 0.001848 172.27.64.1     172.16.8.56  CFLOW     1422 IPFIX flow (1380 bytes) Obs-Domain-ID=  512 [Data:257]
  6 0.002776 172.27.64.1     172.16.8.56  CFLOW     1422 IPFIX flow (1380 bytes) Obs-Domain-ID=  512 [Data:257]
  7 0.003693 172.27.64.1     172.16.8.56  CFLOW     1422 IPFIX flow (1380 bytes) Obs-Domain-ID=  512 [Data:257]
  8 0.004078 10.10.144...    172.16.8.56  CFLOW      582 IPFIX flow ( 540 bytes) Obs-Domain-ID=2885681254 [Data:257]
  9 0.004149 10.10.144...    172.16.8.56  CFLOW      166 IPFIX flow ( 124 bytes) Obs-Domain-ID=2885681254 [Data:257]
 10 0.004564 172.27.64.1     172.16.8.56  CFLOW     1422 IPFIX flow (1380 bytes) Obs-Domain-ID=  512 [Data:257]
 11 0.004698 10.10.144...    172.16.8.56  CFLOW      166 IPFIX flow ( 124 bytes) Obs-Domain-ID=2885681254 [Data:257]
 12 0.004846 10.10.144...    172.16.8.56  CFLOW      166 IPFIX flow ( 124 bytes) Obs-Domain-ID=2885681254 [Data:257]
 13 0.005037 10.10.144...    172.16.8.56  CFLOW      166 IPFIX flow ( 124 bytes) Obs-Domain-ID=2885681254 [Data:257]
 14 0.005090 172.27.64.1     172.16.8.56  CFLOW      862 IPFIX flow ( 820 bytes) Obs-Domain-ID=  512 [Data:257]
 15 0.005289 172.21.152.1    172.16.8.56  CFLOW     1422 IPFIX flow (1380 bytes) Obs-Domain-ID=  512 [Data:257]
 16 0.005398 172.21.152.1    172.16.8.56  CFLOW     1422 IPFIX flow (1380 bytes) Obs-Domain-ID=  512 [Data:257]
 17 0.005518 172.21.152.1    172.16.8.56  CFLOW     1422 IPFIX flow (1380 bytes) Obs-Domain-ID=  512 [Data:257]
 18 0.005549 10.10.144...    172.16.8.56  CFLOW      166 IPFIX flow ( 124 bytes) Obs-Domain-ID=2885681254 [Data:257]
 19 0.005636 172.21.152.1    172.16.8.56  CFLOW     1422 IPFIX flow (1380 bytes) Obs-Domain-ID=  512 [Data:257]
 20 0.005760 172.21.152.1    172.16.8.56  CFLOW     1422 IPFIX flow (1380 bytes) Obs-Domain-ID=  512 [Data:257]
 21 0.005789 10.10.144...    172.16.8.56  CFLOW      166 IPFIX flow ( 124 bytes) Obs-Domain-ID=2885681254 [Data:257]

› Frame 1: 1422 bytes on wire (11376 bits), 1422 bytes captured (11376 bits)
˅ Ethernet II, Src: Cisco_43:10:bf (5c:71:0d:43:10:bf), Dst: VMware_8e:04:ab (00:50:56:8e:04:ab
  › Destination: VMware_8e:04:ab (00:50:56:8e:04:ab)
  › Source: Cisco_43:10:bf (5c:71:0d:43:10:bf)
    Type: IPv4 (0x0800)
› Internet Protocol Version 4, Src: 172.27.64.1, Dst: 172.16.8.56
› User Datagram Protocol, Src Port: 60919, Dst Port: 2055
› Cisco NetFlow/IPFIX
```

Raw Packet Analysis

SECURITY ANALYTICS

Integrate with IDS and Threat Intelligence systems

Trisul integrates with IDS systems, processing alerts through its streaming analytics pipeline. A built in integration with leading threat intelligence feeds lets you scan all traffic against known indicators of malware. With TrisulNSM you can jump from security alerts to flows to packets to complete your investigation.



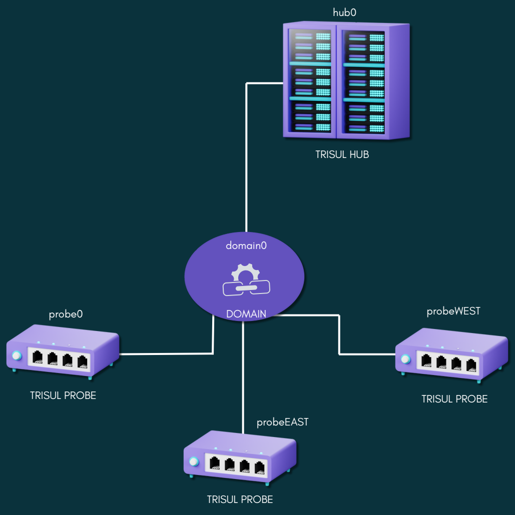
SIGNATURE ID	PRIORITY	COUNT	DESCRIPTION	LAST SEEN UTC	PROBE
2013504	allowed	11	ET POLICY GNU/Linux APT User-Agent Outbound likely related to package management	2024-09-27 11:15:46	probe0
2013028	allowed	2	ET POLICY curl User-Agent Outbound	2024-09-27 11:15:54	probe0
2100498	allowed	2	GPL ATTACK_RESPONSE id check returned root	2024-09-27 11:15:54	probe0

Intrusion Detection Alerts

DISTRIBUTED MULTI-TENANT ARCHITECTURE

03

Trisul NSM works on packet capture which can mean tapping traffic at remote office locations. TrisulNSM supports a scalable *Hub* and *Probe* architecture, where Probes capture packets and run streaming analytics, storing packets locally while forwarding other data types to the centralized Hub for database and reporting functions. Multi Tenancy allows customers to host more than one instance of Trisul on the same hardware monitoring different segments or end customers.



Trisul Distributed Multi-tenant Architecture

SYSTEM REQUIREMENTS

04

< 300Mbps **Single Probe+Hub**	**< 1Gbps** **Single Probe+Hub**	**10Gbps+** **One Hub + multiple probes**
• 2.4Ghz 8 core / • 16GB RAM/ • 1TB HDD/ • 1Gigabit NIC for capture / • 1Gigabit NIC for management	• 2.4Ghz+ 12Core/ • 16GB RAM/ • 2TB HDD/ • 2x1Gigabit NIC for capture/ • 1x1 Gigabit NIC for management	• Hub:2.4Ghz 24Core/ • 32 GB/ • 8TB HDD with INTEL X520/ • X540 10G
Separate disk 1TB and above for Packet Storage	Separate 1TB in RAID 0 (striping) for Packet Storage	Dedicated packet capture cards are supported.

COMPARISON WITH OTHER SECURITY APPROACHES

05

Trisul Network Analytics	Intrusion Prevention System	Intrusion Detection System
Passive – does not block traffic	Inline – blocks traffic	Passive
Historical storage	Limited, focused on blocking	–
Deep visibility Traffic Metrics	–	–
Flow reconstruction and storage	–	–
Database included	No DB. Export to 3rd party	No DB
Category of Network Management System	Category of Network Device	Category of Network Device
Use Cases Visibility, Security, Analytics, Alerting, Incident Response, Audit, and Compliance	**Use Cases** Protection, Firewall role, Attack detection like DoS, Throughput.	**Use Cases** Detection, Performance, Signature quality, forwarding alerts to SIEM, Splunk, Elastic.