Network Traffic Analysis to secure your IT operations

- Provides round-the-clock **security monitoring**
- Gives you powerful rapid **detection & response capabilities**
- Take advantage of the solution’s **powerful detection capabilities**
- Let’s you gain a deep visibility into the internal network
- Powerful and **easy to use**

I.T.S, a Network Traffic Analysis tool helps enterprise, government, and critical infrastructure users make their IT operations secure and reliable through advanced artificial intelligence, machine learning, and big data analysis.

Identify Threats Before Damage Happens

Using advanced artificial intelligence methods, I.T.S goes beyond known threats to detect and identify symptoms of malicious behaviour at the atomic level. Threats are identified in their early stages, decreasing incident response time, preventing further damage, and reducing overall risk.

Easy to Use

The web user interface presents comprehensive information about network traffic: From management overviews, through aggregated information on communication of the network, subnetworks, users and applications, communication of peers, to details concerning individual flows and their content to precisely investigate interesting events.

Identifying Threats in IoT Devices

I.T.S monitors a very rich set of network flow data also in IoT devices, and it is able to identify not only traffic in and out of the network but also communication flows between devices within the network. These are the types of anomalies I.T.S can detect:

- Communication flows between devices
- Additional anomalous devices,
- Excessive communication from one device to another,
- Communication from one device to a host outside the network,
- Periodic communication of the type common in advanced persistent threats.

Much More Capable than NetFlow

I.T.S Analyst collects several times more information on network traffic than NetFlow, IPFIX or similar protocols. NetFlow or IPFIX records are enhanced with security parameters and performance analysis. These include frequency, spectral and traffic content features which are crucial for more sensitive behavioural detection.

Features

Flow-based and Packet-based Technology

Instead of relying on older and limited SNMP polling, I.T.S leverages flow-based and content-based monitoring. Flow-based monitoring provides near real-time (1-minute intervals) visibility into network statistics and other summary and detailed issues. Deep content inspection (DCI) extends this information with real-time comprehensive contextual metadata (user identity, applications, for example).

Application Monitoring and More

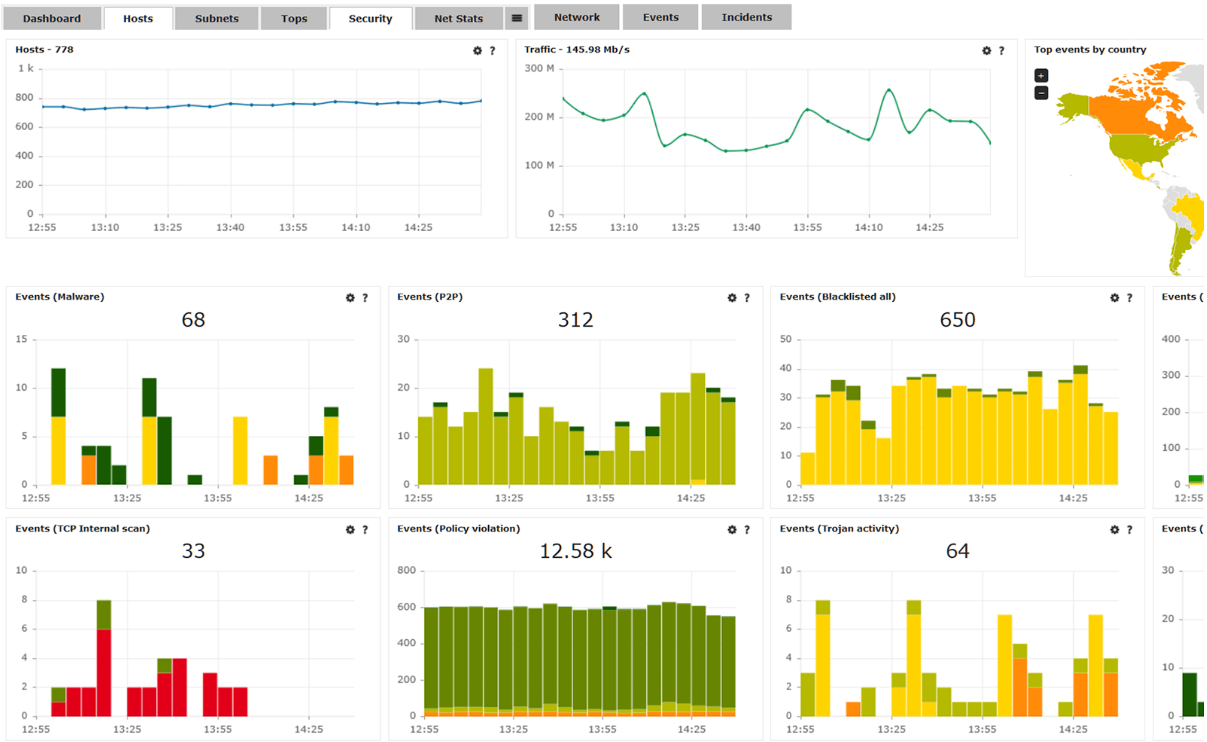
I.T.S Analyst constantly monitors communication of users and network applications of all ports and on TCP, UDP, ICMP and many other protocols. This enables monitoring of current and average bandwidth, response times, transit times, delay, jitter, ports in use, connection peers and more.

Detection Methods

- Signature based detection
- Deep packet inspection
- Network Behaviour Analysis
- Specialized algorithms
- Network performance monitoring
- Application performance monitoring

Powerful Forensics

I.T.S Analyst generates metadata of network communication providing full contextual awareness – for example destination and source, user's identity and application protocol. Unlike technologies based on full packet capture, it allows the metadata on network traffic to be stored for a much longer time with low demands on storage capacity.


Dashboard
Hosts
Subnets
Tops
Security
Net Stats
Network
Events
Incidents
Hosts - 778
1 k
800
600
400
200
0
12:55
13:10
13:25
13:40
13:55
14:10
14:25
Traffic - 145.98 Mb/s
300 M
200 M
100 M
0
Top events by country
Events (Malware)
68
Events (P2P)
312
Events (Blacklisted all)
650
Events (
Events (TCP Internal scan)
33
Events (Policy violation)
12.58 k
Events (Trojan activity)
64
Events (