White Paper

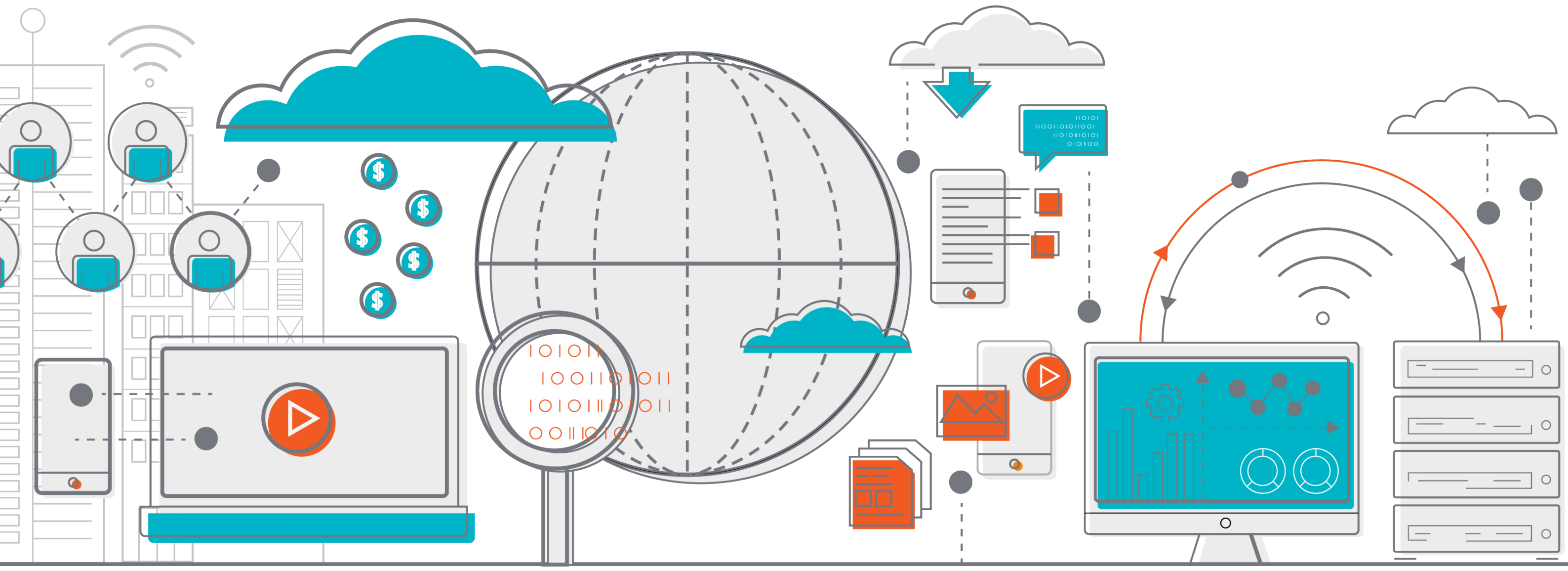
IP Flow Probe

200Gbps Flow Monitoring System

Scaling cyber defence tools, including IDS, Record and Flow monitoring to protect a medium sized mobile network operator's backbone

April 2017

DX-IPF-GEN-MK-WP-35223-01



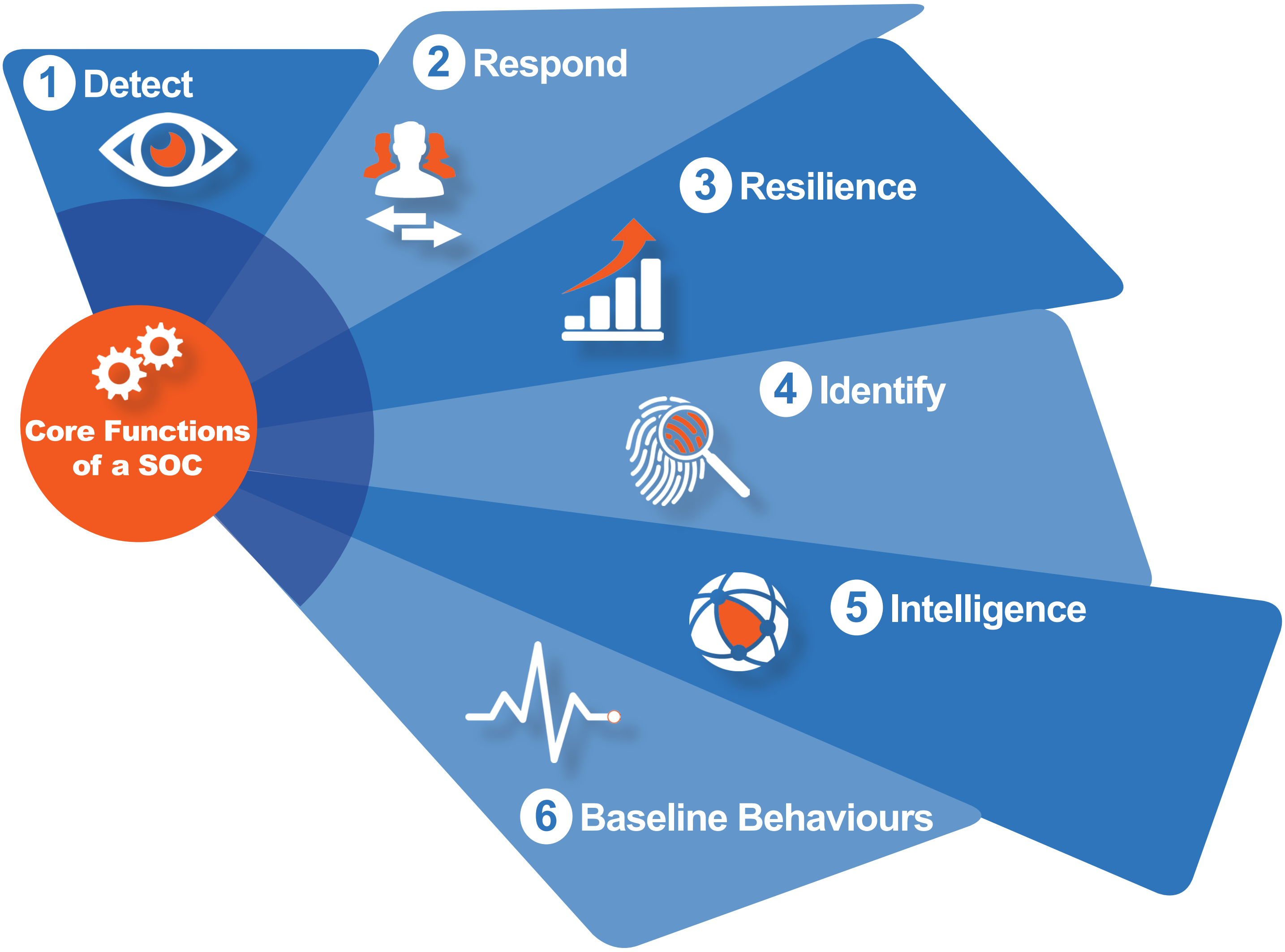
Scaling cyber defence tools, including IDS, Record and Flow monitoring to protect a medium sized mobile network operator’s backbone

Synopsis

There are a number of cyber security tools and techniques that are increasingly used by enterprises in their Security Operations Centre (SOC) to protect their networks and data. In the SOC, the analyst(s) or the ‘blue team’ work flow includes performing traffic and data flow analysis, accessing and analysing event and log data, using a Security Information and Event Management system (SIEM) and garnering threat intelligence information. However, equipment commonly available to run these tasks does not scale well, or at all, to the volumes of data seen across a medium sized carriers network or an ultra-scale datacenter.

This white paper presents a solution to the problem of monitoring and protecting high volumes of data (up to 200Gbps in a 1U appliance) seen on the backbone of a typical carrier network, by using off-the-shelf appliances provided by Telesoft Technologies, combined with open source software and existing enterprise scale tools.

Key Aims of Security Operations Centre (SOC)



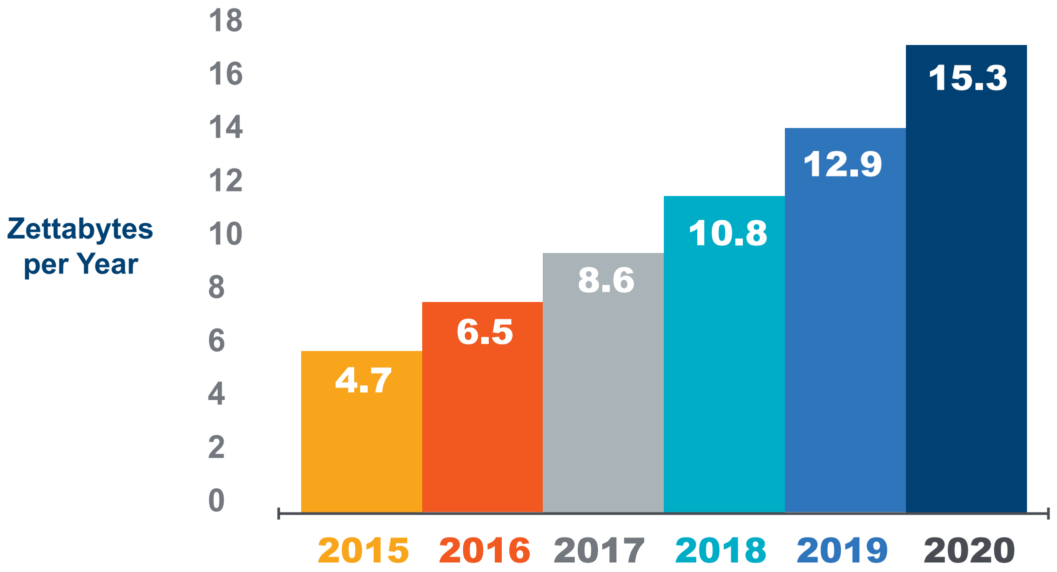
Scaling cyber defence tools, including IDS, Record and Flow monitoring to protect a medium sized mobile network operator's backbone

The Problem

Data throughput on network backbones and at the border of ultra-scale datacenters is constantly rising, to well above the rate at which traditional cyber defence tools operate. The option for a medium sized carrier or ultra-scale datacenter owner is to purchase multiple low throughput branded cyber defence tools and additional monitoring infrastructure to load share traffic across each element, if this is economically viable. Some users have found that the closed approach used by many vendors, preventing signatures and custom user configurations to be added by the user, is not flexible and agile enough to prevent breaches, and many are now looking to build out their own infrastructure and knowledgeable cyber security teams, enabling scaling to significantly large data throughput, reducing OpEx, and providing agile reconfiguration by the internal team to quickly react to threats. For an operator this also enables a new revenue stream of reselling hosted cyber security services.

Global Data Center Traffic Growth

Cisco predicts that data centre traffic will more than triple from 2015 to 2020.



Source: Cisco Global Cloud Index 2015-2020

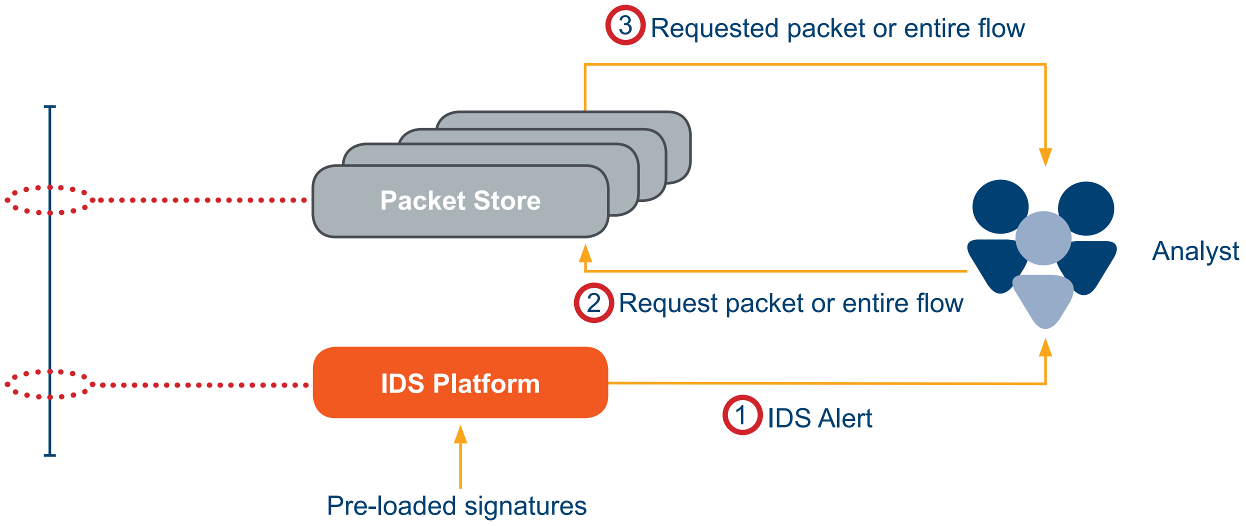
Looking for Known Threats

A common technique for finding known threats uses signature matching in an Intrusion Detection System (IDS). Such a system scans for pre-loaded signatures and generates alerts when a packet containing a signature is seen. Typical IDS platforms scale up to 10Gbps throughput in a single appliance, and often reduce in performance as throughput increases.

To make the IDS alerts usable and hence valuable, an Incident Response analyst will quickly need to know if the event is serious, relevant or just a false positive. The simplest way to achieve this is to record and then inspect the packet that contained the signature that generated the alert. Packet capture can be combined with the IDS engine, but as data throughput rises this causes additional load on the IDS system and impacts performance.

Additionally, in many cases, analysis of a single packet is inconclusive and all of the packets in the TCP or UDP Flow to which the suspect packet belongs will be required. This is usually achieved by capturing and recording all packets from the monitored interface and then retrieving packets belonging to the suspect flow from the packet store.

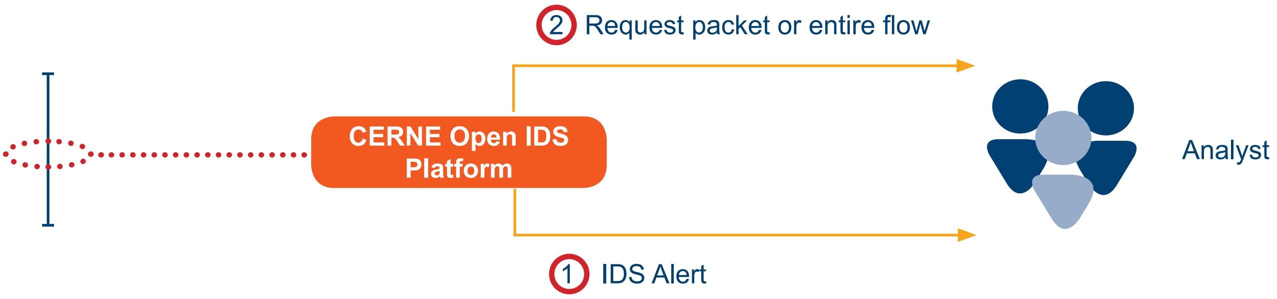
This leads to two issues, one commercial, being the rising cost of storage as data rates rise, the second being operational, the rising time taken to extract all of the packets from a specific flow as throughput, and hence the volume of data stored, increases.


3 Requested packet or entire flow
Packet Store
Analyst
2 Request packet or entire flow
IDS Platform
1 IDS Alert
Pre-loaded signatures

Standard IDS combined with packet store

Telesoft's solution to these problems is the CERNE Open IDS Platform, which is a ready to run, customizable appliance that combines IDS and record functionality running at up to 40Gbps on 4 x 10GbE. Using widely supported Suricata, the CERNE scans for threat signatures specified in user definable rules that include an optional property to extract, record and deliver to your SIEM the TCP or UDP session containing the packet that triggered the alert. Sessions are captured and extracted from a back in time buffer running at the full 40Gbps rate which delivers packets from up to 2 seconds prior to the detected event, providing additional intelligence to the Incident response analyst.

Looking for Known Threats



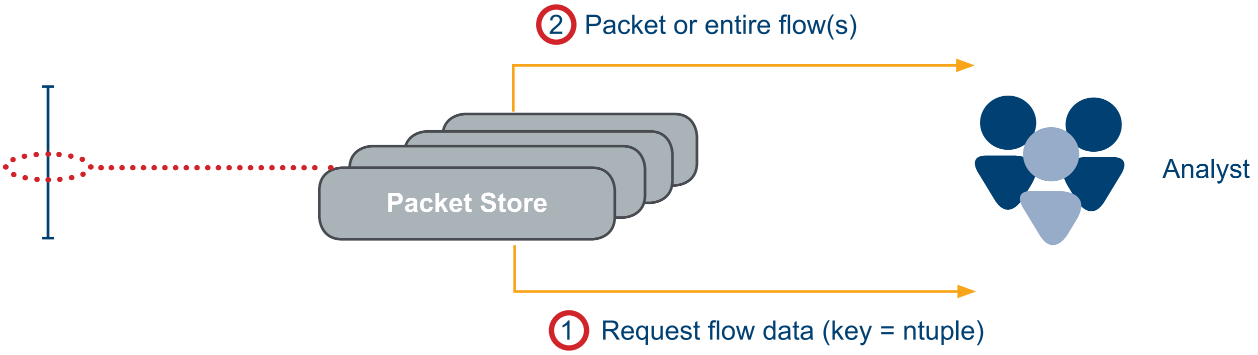
Telesoft CERNE IDS/Recorder

Session extraction and recording can also be controlled from threat intelligence logic from within the SIEM, enabling even greater control and intelligence over storage management.

Historical Analysis for High Rate Networks

Once a breach has been detected, (possibly using the IDS technique described above), an analyst will want to quickly know the history of the breach. When did the associated remote IP address first contact the network? How many times? What nodes on the network did that IP address contact? For how long? Was any data exfiltrated?

The obvious method for this is to store all IP traffic for as long as economically possible and to be able to rapidly search and retrieve relevant information. The problem with this is that for a network running at 100GBps, this would require approximately 1PB of storage for one day of traffic. Standard practice seen in many SOCs typically implements three months of storage or about 90PB of data. As well as the sheer volume of storage, all of this data needs to be searchable, and as quickly as possible.



2 Packet or entire flow(s)
Packet Store
Analyst
1 Request flow data (key = ntuple)

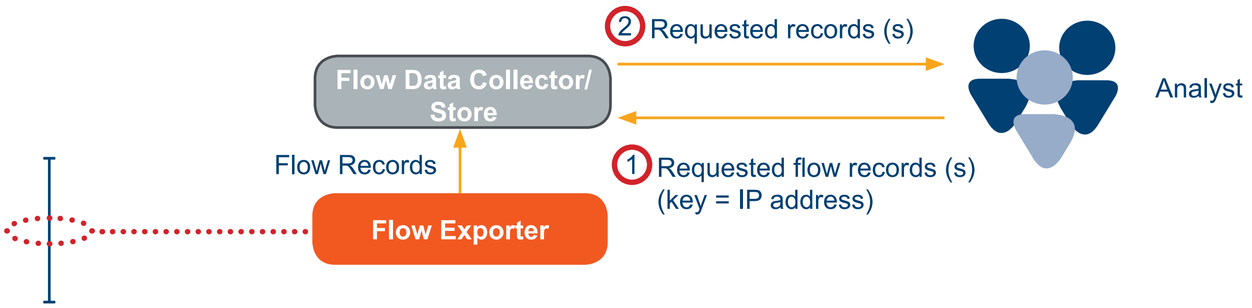
Complete packet capture and retrieval

For the majority of investigations, minimal information is required such as; IP addresses, volume of data and time, or more simply only flow meta-data. All of which can provide a 100 times reduction in the data volume stored. Flow data, in the form of industry standard IPFIX or NetFlow records are provided by network infrastructure such as switches. Traditionally flow data has been sampled, so that the performance of the primary infrastructure function, the switching, is not impacted at high traffic rates. For cyber defence analysis, un-sampled flow records are required. Generating un-sampled flow records is imperative to create a network baseline and pinpoint accurately network issues at high traffic rates which requires a dedicated monitoring appliance.

Historical Analysis for High Rate Networks

The Telesoft IP Flow Probe is a 1U appliance that generates un-sampled flow statistics on traffic monitored from two 100GbE or up to 20 10GbE. Processing up to 150 Million concurrent flows at a churn rate of up to 1.5 Million active flows/s enables the collection of flow statistics from ultra scale networks.

Distributing flow records across multiple collectors such as Elastic Search and Apache Kafka using the universal standard IETF Internet Protocol Flow Information export (IPFIX) protocol and JSON allows existing collection and recording infrastructure to scale up to monitor a large network backbone, allowing you to accurately gather, process, compare and analyse network behaviour in real-time.


2 Requested records (s)
Flow Data Collector/ Store
Analyst
Flow Records
1 Requested flow records (s) (key = IP address)
Flow Exporter

Flow export and store rapid analysis

Intelligent load balancing across flow collectors reduces load and storage on a single collector instance, flow safe load balancing ensures duplex flows are forwarded to the same collector for accurate and rapid analysis. The traffic monitoring interfaces work in passive mode and do not require any protocol handshake or keep alive in order to process incoming traffic, ensuring plug and play and seamless integration.

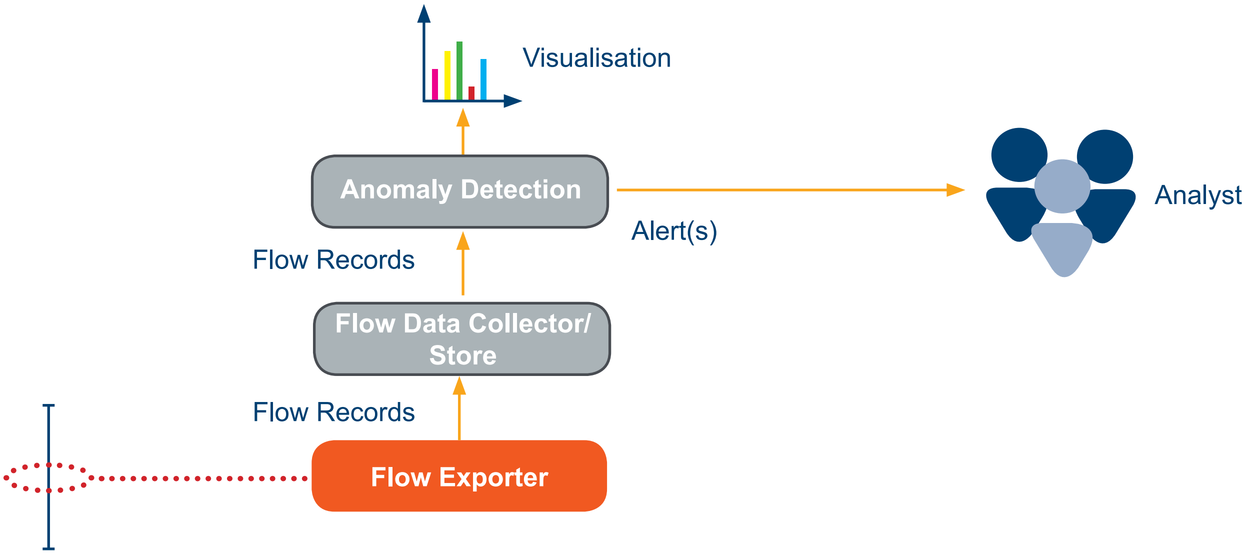
Looking for Known Threats

IDS and signature scanning tools provide the ability to detect previously identified threats. But how can new threats and attacks be detected?

One technique is to monitor and analyse the traffic flows within a network to profile normal behaviour, and detect anomalies that may indicate a breach or attack.

Detection of some threats, such as Denial Of Service (DoS) can be achieved by monitoring sampled flow records to indicate traffic trends. Specific attacks targeting a single network node require un-sampled flow record generation to ensure that no events are missed.

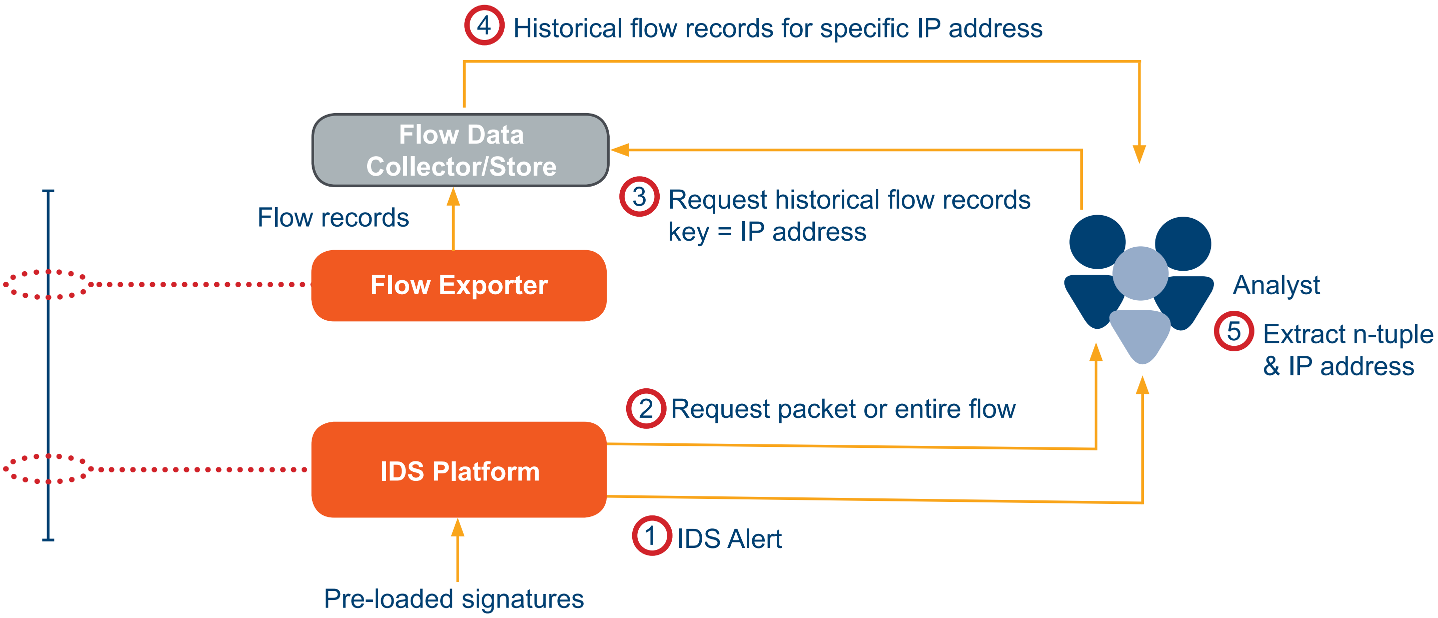
Looking for Known Threats



Using flow analysis to detect anomalies

Combining IDS and Un-sampled Flow in Incident Response

A common SOC workflow involves threat detection, either through an IDS function or anomaly detection, then if signature based, investigation of the packet or if possible the entire flow that generated the alert, then further investigation of historical data (for example pivoting retained flow records by the source IP address of a detected threat) to understand any impact the threat has had in the past.


4 Historical flow records for specific IP address
Flow Data Collector/Store
3 Request historical flow records key = IP address
Flow records
Flow Exporter
Analyst
5 Extract n-tuple & IP address
2 Request packet or entire flow
IDS Platform
1 IDS Alert
Pre-loaded signatures

Combined IDS/Flow

Storage and Analysis

There are a number of industry proven toolsets for threat detection, traffic profiling and anomaly detection, however these are dimensioned to operate at the scale of a small to medium sized enterprise, and would not operate at the scale of a whole network operator backbone or ultra-scale datacenter.

One solution is to implement a retention, aggregation and filtering capability between the monitoring and collection infrastructure, and pass up pre-analysed data to the toolsets, a second alternative is to implement high capacity analysis using scalable, open source software.

The Telesoft IP Flow Probe generates flow records for collectors such as Elastic Search and Apache Kafka using the universal standard IETF Internet Protocol Flow Information export (IPFIX) protocol and JSON.

Multiple toolsets, many of which are open source are available, for data normalisation (such as logstash), data brokering (kafka), retention and rapid search (elastic, hadoop), analysis and visualisation (Apache Spark, Apache Storm). These tools are becoming increasingly popular since they have far more flexible licensing (or non licensing) that makes their commercial packaged counterparts, many of which charge licensing fees based on data volumes, uneconomical at the scale of monitoring and protecting an entire mobile networks data traffic.

Headquarters
Telesoft Technologies Ltd
Observatory House, Stour Park
Blandford DT11 9LQ UK
t. +44 (0)1258 480880
f. +44 (0)1258 486598
e. sales@telesoft-technologies.com

Americas
Telesoft Technologies Inc
430 National Business Parkway
Suite 480, Annapolis Junction
MD 20701
USA
e. salesusa@telesoft-technologies.com

Asia
Telesoft Technologies Ltd
Tapasya Corp Heights
Ground Floor, Sector 126
Noida, 201301, India
t. +91 120 612 7725
e. salesindia@telesoft-technologies.com

telesoft

telesoft-technologies.com