Public

TDAC Use Case

Global Communications Provider Integrates Telesofts Cyber Security Tools

September 2018

DX-IPF-TDAC-MK-SP-35439-01

Global Communications Provider Integrates Telesofts Cyber Security Tools

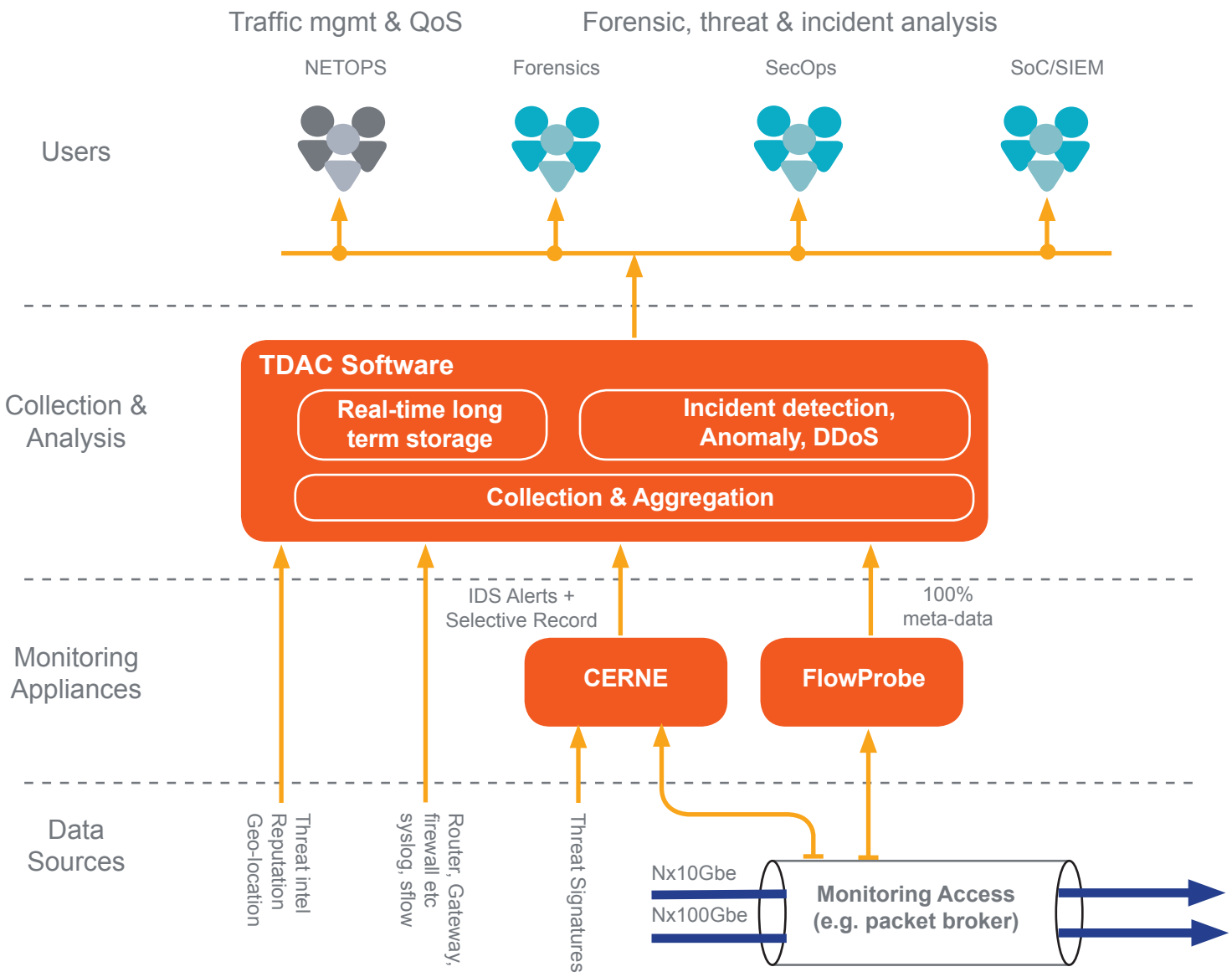
Synopsis

The Telesoft TDAC, CERNE and FlowProbe have been selected by a Global brand communications provider to protect their data, their subscribers and their reputation.

This global brand, provides always on, available everywhere world-wide, on-demand services, connecting users and devices with data in a world of IoT. To do this, they maintain a wide spread data routing and access infrastructure that provides end user services (carrying their own and third-party data and services to their subscribers) and high rate peering (carrying someone else's data to another network). Their network infrastructure is part of our CNI ("Critical National Infrastructure").

The volume of data carried on their network rises daily. It connects with, and can be accessed from almost anywhere on the planet, and it needs protecting from misuse. So when this global brand was looking to roll out a cyber defence system to protect this valuable resource, they selected Telesoft's high density multi-100Gbps monitoring and visibility tools, "Telesoft Data Analytics Capability" (TDAC), CERNE (high rate IDS and event driven record) and FlowProbe.

Telesoft Carrier Scale Monitoring and Visibility Infrastructure Integration



The Challenge

The operator had evaluated multiple suppliers of enterprise scale cyber security tools as used in an enterprise Security Operations Centre (SOC), and found that none would scale up to processing the volume of events seen on their Global network.

Their situation:
- A network supporting 100's of millions of physical and virtual entities, with multiple applications
- Physical infrastructure carrying data in a mixture of multi 10Gbps and 100Gbps fibres.
- Operations spread across multiple countries and continents.
- Existing infrastructure that has limited monitoring capability, usually sampled (reporting 1 in many thousands of sessions or events) and used for Network Performance Monitoring and Diagnostics (NPMD).
- A mixture of own traffic (to own subscribers) and peering traffic.
- Limited visibility of complete network.

Their need:
- Protect network infrastructure from existing known and zero-day attacks in order to maintain subscriber and peering services.
- Method to prioritise monitoring and visibility of physical or virtual assets on a rapidly changing basis.
- Understand how much bad traffic (such as DDoS) is carried across the network and where possible use this information for data scrubbing.
- Have a toolset that allows analysts to hunt for anomalous behaviour across the entire network.
- Discover and disable spread of botnets on own infrastructure.
- Store meta-data for minimum 3-months for post incident analysis.
- Provide rapid query of historical data for Incident Response.
- Integrate with existing legacy tools.
- Be useable by multiple teams across multiple sites.

The Solution

Using a combination of Telesoft FlowProbes, CERNE and TDAC the provider now has flexible, multi-user visibility of Global traffic, with meta-data and selected session pcap record for 3-months. Flexible dashboards, queries and alerting enable analysts to see and modify what is important to them on a rapidly changing basis.

Survey – Meta-data

One key problem was to understand how data was flowing through the network, from where, to where, and in some occasions, what was being sent. This enables baselines of normal behaviour to be set so that anomalies (such as a newly activated botnet) can be quickly discovered and mitigated.

Total network monitoring and record is one solution, but with 10's of 100GbE to monitor this provides a huge challenge for storage, search and query. Much of the data is encrypted and unreadable, and some is known and uninteresting content (streaming video for example). The chosen solution is to monitor and store enhanced meta data generated from every communication session or flow. Hence use of the Telesoft unsampled 2 x 100GbE FlowProbe, which generates and exports unsampled flow data (as IPFIX, NetFlow or JSON). These are deployed at strategic points within the global network, usually key national gateway points where data enters the network.

Collection and Storage

The FlowProbe provides a 100:1 reduction in data volume – but there is still millions of events per second to analyse and store, for a minimum of 3-months. This is the problem solved by Telesoft's TDAC platform, running on a centralised multi-node storage-server farm. Meta-data generated from traffic at national gateways is routed back to the central collection, storage and analysis facility where TDAC provides user programmable visualisations, alerting, historical query and API integration into a variety of tools used by the providers security operations teams.

Prioritised Visibility and High Risk Assets

One problem was how to provide prioritised visibility and analysis for high value or high risk assets, such as the operators own physical and virtual infrastructure, or mapping of known botnets and threat actors, in an analysis environment of 100's of millions of physical endpoints, virtual entities, applications and millions of events per second.

TDAC solves this problem with user configurable, and auto discoverable entity sets that group records by IP address, IP reputation, domain or other common information element. Each set can then be monitored as a single entity without loss of granularity down to a single node. Queries for these are cached, giving analysts access to sub-second queries for key data.

Using this technique allows groups of infrastructure that do not normally communicate to be configured as separate entity sets, so any anomalous communication can be quickly identified. Records for known threat actors, such as botnets, can also be configured as a single entity either manually or automatically, allowing botnet activity and spread to be mapped and mitigated.

Finding Unknown or Zero Day Threats – Anomaly Detection

High rate near real-time anomaly detection on meta-data enables the providers analysts to hunt for unusual patterns of traffic or unusual and unexpected communications routes. Such anomalies can be an indicator of previously unseen or zero-day threats. These are further investigated by the providers analysts using custom data queries on endpoints, communications routes, infrastructure and correlation with external data sources.

Finding Known Threats - Signatures and IP Reputation

Known threats are identified by the provider using shared and commercial intelligence data, including threat signatures and reputation data fed into the Telesoft Tools.

The Telesoft CERNE is a high rate (40Gbps per 2U appliance) IDS/Signature analysis engine and event driven recorder, pre-programmed and dynamically upgraded by the provider with signatures (byte patterns or information element field values) of known threats or interesting communications flows. As each is detected, an alert is generated, added to the TDAC data store alongside flow meta-data and the entire flow recorded as a pre-indexed and assembled pcap format flow, for rapid off-line analysis of the event.

IP reputation data enables records from known bad IP endpoints (such as botnets or known sources of malware), to be rapidly alerted and investigated.

Selective Record

The provider did not want to capture all traffic, since some would be useless for post event analysis (for example encrypted data or media streaming), and recovering individual sessions from mass capture can be slow, a key factor in rapid incident response and analysis. This was solved using the Telesoft CERNE appliance which provides selective record of individual communication sessions or flows, from a rolling back-in-time buffer, as an easily recoverable pcap. Record is based on signatures or information element value, ensuring only potentially interesting traffic is recorded, reducing both volume of storage required and retrieval time.

Historical Analysis – Accelerated Query and Data Partitioning

Speed of analysis for incident response is critical to minimise impact, especially so for a provider serving 100's of millions of end users. TDAC has been built around a horizontal scalable big data architecture, sharing storage, search and analysis across multiple server-storage nodes. Accelerated cached queries give the providers analysts near second response times. Other techniques, including data partitioning (based on the providers physical and virtual infrastructure architecture and security work-flow) further accelerate data access and retrieval over the 3 month storage period for rapid incident response analysis.

Multi-user Access and Integration into other Toolsets

The Telesoft tools allows the provider to configure user roles and access rights, query priorities and scheduling, ensuring the highest impact events are given maximum resource. The tools provide their own rapidly user configurable GUIs and also APIs with data throttling and filtering to third party tools for teams that need a slower migration to complete Global network coverage.

Summary

A combination of flow monitoring in real time, data prioritisation and aggregation through auto-discovered or user configured entity sets, use of IP reputation, Signatures and Selective Record, has enabled the providers security analysts to discover anomalous behaviour, evaluate impact and take corrective action to remove or redirect traffic. APIs to existing well known toolsets ensure that the benefits of the tools can be used by all security operations teams.

If you have a network of multiple 10Gbps or multi-100Gbps, with M's of endpoints and would like to discuss how we can help you understand the volume of threats carried on your network and potential impact, get in touch today, we would love to talk.

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-technologies.com

DX-IPF-TDAC-MK-SP-35439-01