TDAC Success Story

Industry: Telecommunications | Deployed: TDAC Full System | Date: Jan 2017

Customer Challenge

Serving tens of millions of home and business subscribers, Telesoft's customer represents one of the largest technology providers in the US market. Considering the quantity of information to be protected through their telecommunication, video, and internet channels, running security for this corporate giant is no small task, requiring an approach and products which tackle both the scale and value of the project. Telesoft's TDAC has been employed to provide complete real time network visibility and intelligence across all data and network assets. Taking millions of events from this massive network, TDAC applies automated intelligence, for rapid incident response, performance monitoring and reporting.

Deployment

In order to successfully protect, map and understand the target network activity at hyper scale, the Telesoft engineering team began the integration by answering a few basic questions that show how implementation of the TDAC will streamline the SOC team's day to day security monitoring.

1. What does my system look like typically?
Information from distributed large scale data warehouses is collected using TDAC's cutting edge flow monitoring sensor, which is a 1U appliance that generates un-sampled flow statistics on traffic up to 200Gbit/s. External network events reaching out to subscribers are collected from existing network infrastructure and all information routed into TDAC's distributed data store for a minimum 3-months retention. A multi-user, distributed monitoring, query and alerting interface allows our customer to set a baseline of normal network activity and investigate anomalies.

2. What are the normal operating boundaries?
The customer had many variables to consider when putting together a strategy for baselining operating boundaries that included a need for full network visibility inside geographically distributed multi-100Gbps data warehouses and across network infrastructure delivering content and services to end users. TDAC has been developed from the ground up to scale horizontally according to the resources allocated to it, enhanced database features allow all network data, including that from different geographical locations to be queried at low-latency as an entire mass or sliced by source/site.

3. How do I know when I have an extraordinary event happening, and how do I chase it down quickly and get to the root cause?
One of the key focuses for us and our customer, was usability and ensuring that time from incident to action is minimal, which is why automation is a key component of this product. TDAC's intuitive and secure dashboard enables exploration of trends and patterns using our in-built queries, configuring your own or combining both for flexible control of multitenant capable search and analytics, returning search results in seconds. This advanced insight is invaluable for determining whether an issue stems from an application, the network itself, or from a security incident.

Summary

The customers approach to cyber security is an integrated layered system with different kinds of products that either work together or in tandem to give visibility across a massive scale network. The TDAC has provided protection and detection of DDoS attacks, DNS tunnelling and TCP SIN flood. While automatic 'forensic pathway' tracking allows for investigative route tracing through the data lake in order to be post analysed, replayed and downloaded as a report. This enables auditing and enhanced intelligence during incident management and response.

To find out more information about the TDAC or to request a datasheet, please contact us on **+44 (0) 1258 480880** or **sales@telesoft-technologies.com**

telesoft-technologies.com