TDAC Success Story

telesoft

Industry: Retail/ E-commerce

Deployed: TDAC Full System

Date: September 2016

Customer Profile

Being one of the world's largest retailer in a specific sector, with over 2,000 stores across Canada, North and South America and a corresponding e-tailer business offering over 1M products to businesses and consumers, this organisation had a key need to protect business assets, customer data, reputation and revenue.

With several high profile data breaches in the USA retail sector, Telesoft assisted this organisation to ensure that a similar attack could be detected and prevented, and sufficient historical analytics were available for forensic analysis of any potential threat or attack.

Customer Challenge

A number of off the shelf cyber defence tools designed for medium sized enterprises had been previously successfully trialled and deployed, but with rising e-commerce use and business reliance on electronic systems for efficient stock management being crucial to revenue, existing providers were not agile enough to react to emerging threats and were struggling to scale to provide full visibility of the entire organisation's data assets.

Deployment

From understanding our customer's key requirements, the following key issues were addressed:

1. How can I scan ALL traffic for known threats?
Information from passive monitoring points at every network boundary and strategic points on the internal backbone was processed by TDACs IDS signature scanning capability (CERNE), with a single instance running up to 40Gbps and alerts passed to the analyst via a SIEM.

2. How can I gather and analyse forensic data for an investigation from so much traffic?
Full packet capture at maximum data rates was not economically viable; hence un-sampled flow monitoring was selected in order to maintain a 3-month retention window. Flow data can be rapidly queried and data pivoted with TDAC to provide an analyst with answers to when did a suspect IP host first appear on the network, who did it communicate with, what was the lateral data exchange and was there any external network exfiltration.

3. How do I know when I have an extraordinary event happening?
TDAC's intuitive and secure dashboard enables exploration of trends and patterns using in-built queries, custom user configured or a combination, for flexible control of multitenant capable search and analytics, and setting thresholds in order to generate events on unusual or anomalous behaviour.

Summary

The retailer/e-tailer was able to supplement less trusted existing cyber defence infrastructure with Telesoft's TDAC capability, which rapidly became the key cyber visibility and incident response forensics tool owing to its agility and programmability. The cyber team applauded the flexibility of the system to add their own signatures rapidly, configure dashboards, detect and analyse events using their own methodologies. TDAC continues to be a key component for protecting the large-scale infrastructure.

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