TELESOFT

CASE STUDY

THREAT VISIBILITY FOR HIGH RATE TRAFFIC

INDUSTRY: Retail/E-Commerce
DEPLOYMENT: FlowProbe/CERNE/TDAC

CUSTOMER PROFILE AND CHALLENGE:

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 US retail sector, Telesoft assisted this organisation to ensure that a similar attack could be detected and prevented, whilst providing sufficient historical data for forensic analysis of any potential threat or attack.

A number of off the shelf cyber defence tools designed for medium sized enterprises had been previously 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 digital assets.

DEPLOYMENT — FLOWPROBE/CERNE/TDAC

1. How can I scan ALL traffic for known threats?

Data was monitored at passive monitoring points (SPAN/TAP) at every network boundary and strategic point throughout the internal network backbone and was processed by the CERNE Intrusion Detection System (IDS). Information from every network flow was checked against a repository of known threat signatures looking to identify malicious activity.

At the point when a signature match was identified, even if identification happened part way through the flow, an alert would be sent to the SecOps teams immediately, alongside a PCAP of the entire flow. This capability is delivered through the 'Back in time Buffer' a unique feature which allows the CERNE to capture traffic up to 2.5 seconds prior to an alert being triggered, providing SecOps and Incident Response teams vital information regarding the last known movements of the malicious activity.

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

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

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

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. The FlowProbe monitors the flow data in multi-100Gbps networks, extracting only the metadata from each and every communication on the network, therefore ensuring unsampled network visibility of the traffic. Additionally, due to exporting the metadata only, the storage capacity was reduced significantly, to around 2% of the line rate.

The flow data can then be rapidly queried and exported to the TDAC, where the data can be investigated and pivoted to provide an analyst with answers to questions such as 'when did a suspect IP host first appear on the network?', 'who did it communicate with?' or '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 queries or a combination or both, for flexible control of multitenant capable search and analytics. Furthermore, thresholds are able to be set in order to generate events on unusual or anomalous behaviour that is identified outside of the preconfigured settings, which in turn alerts the SecOps teams and enables them to investigate further.

SUMMARY

The retailer/e-tailer was able to supplement less trusted existing cyber defence infrastructure with Telesoft's Cyber Portfolio, which rapidly became the key cyber visibility and incident response forensics tool owing to its scalability and visibility.

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.

TELESOFT

DX-TTL-GEN-MK-GU-35786-01
Telesoft Public