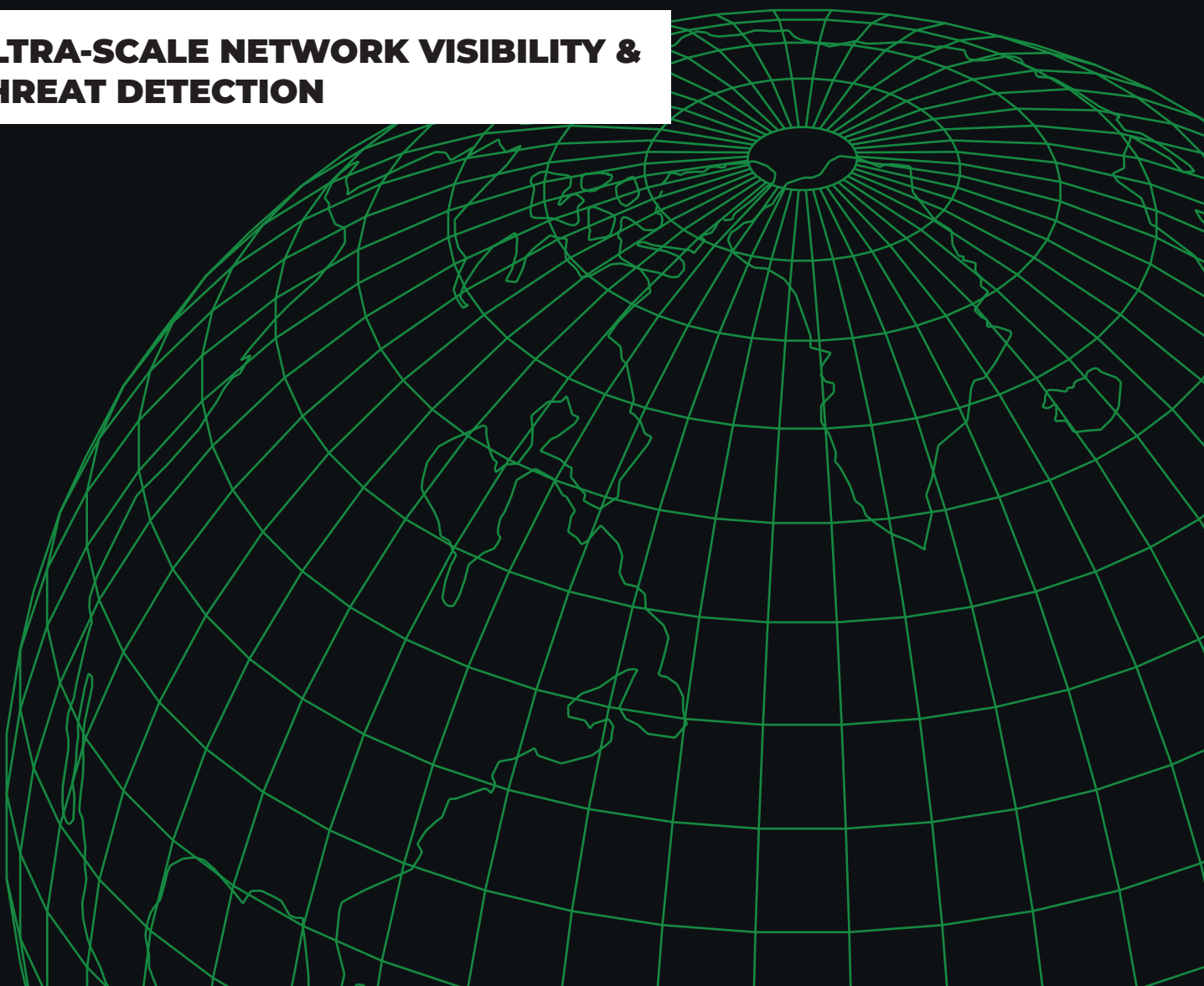
TELESOFT

TDAC PLATFORM

ULTRA-SCALE NETWORK VISIBILITY & THREAT DETECTION

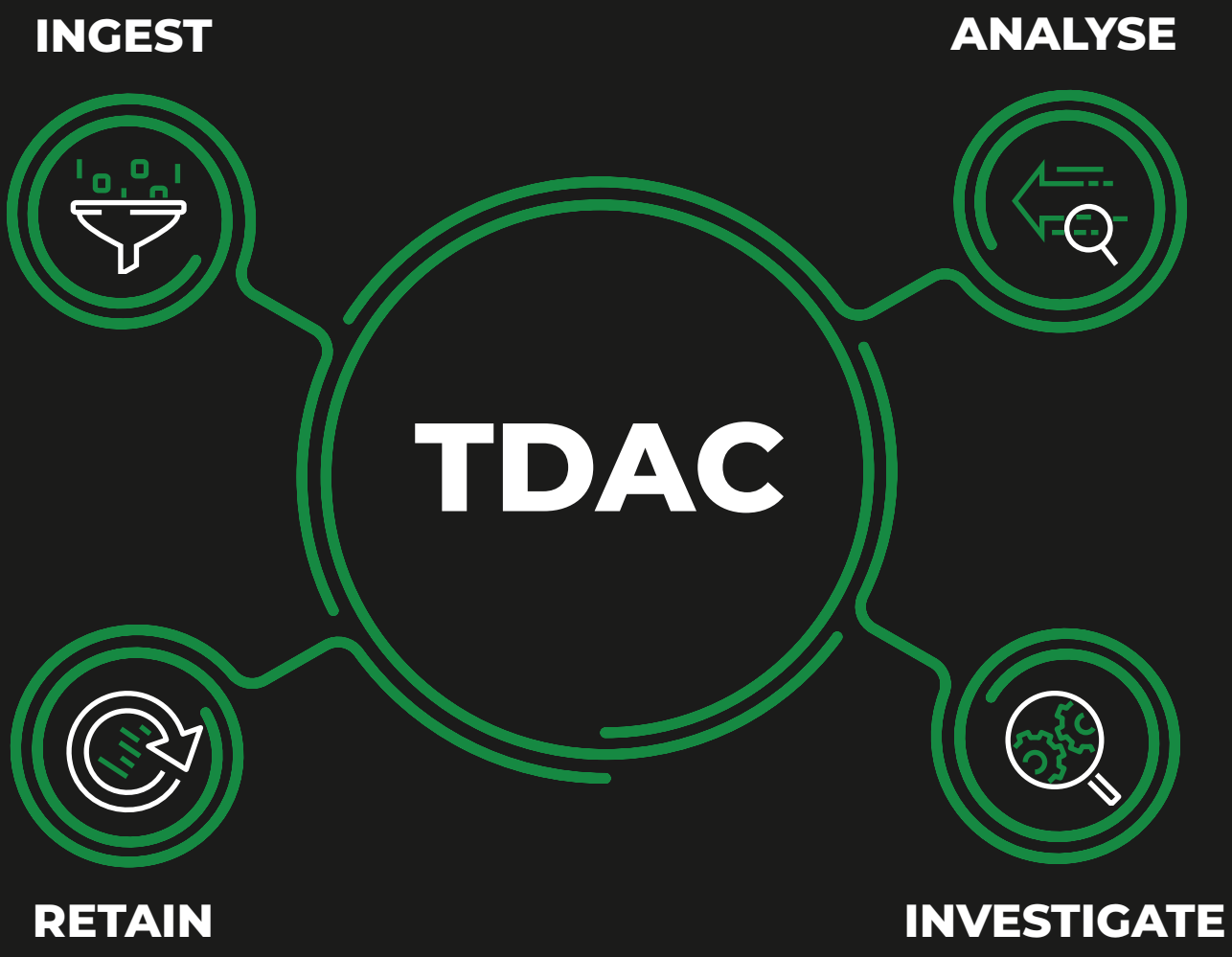


WHAT IS THE TDAC PLATFORM?

The ATCO-TELESOFT TDAC Platform is the complete solution for full network visibility and threat detection at carrier scale.

With experience of monitoring terabits of network data per second and petabyte storage, the TDAC Platform ingests and stores comprehensive and unsampled flow data enhanced with the latest threat intelligence.

Comprised of a number of intelligent hardware and software components, the TDAC Platform utilises purpose built machine learning to detect and alert on anomalous behaviour. Coupled with data analytics and extensive querying capability the TDAC Platform provides the complete comprehensive toolset to support Incident Response, Digital Forensics, and Threat Hunting teams.



INGEST

Probes and sensors deployed within your digital estate capture every communication moving across, around and through your mobile and IP networks. Deep packet inspection and metadata enrichment ensures full, uncompromised visibility, overcoming the deficiency in existing infrastructure and lowering the risk of a sophisticated cyber breach.

ANALYSE

Data is enriched in real time with the latest threat intelligence and grouped into entities based on your specific network configuration. User defined and pre-built threat recipes automatically analyse the data for known threats, while machine learning and behavioural analysis engines identify anomalous activity within your network that could indicate unknown threats.

INVESTIGATE

TDAC Platform arms your SOC & NOC teams with Threat Hunting, Threat Detection, Incident Response, and Intelligent Querying to help keep one step ahead of malicious actors by proactively monitoring your networks.

RETAIN

TDAC Platform's highly scalable, secure storage element stores all network telemetry and anomaly data based on your retention period requirements. Intelligent indexing and data correlation ensures data can be readily accessed and investigated.

FEATURES AND BENEFITS

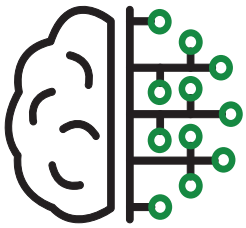
UNRIVALLED 800G NETWORK VISIBILITY WITHIN 1U

TDAC Platform monitors network data to produce unsampled, enhanced IPFIX records for every communication passing through your digital estate. Deployable in 1U probes, each supporting 800Gbps of traffic, TDAC Platform can ingest your network data from around the globe, providing full visibility from a central location.

DATA ENRICHMENT

TDAC Platform imports 3rd party feeds to provide several layers of data enrichment to the unsampled traffic flows, enabling enhanced network visibility and detection of malicious or suspicious events.

- IP and domain reputation lists enable alerting of known threats
- Geographic location and ASN mappings allow unexpected endpoints to be quickly identified and flagged
- Detailed enrichment of DNS flows aids the detection of attacks hidden within DNS, including APT and data exfiltration



UNKNOWN THREAT DETECTION BASED ON MACHINE LEARNING

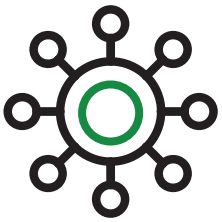
Utilising machine learning, behavioural analytics, and historical baselining, TDAC Platform monitors network activity and identifies anomalous flows. By alerting the user with full flow analysis in real-time, the TDAC Platform enables SOC teams to quickly assess suspicious behaviour for unknown threats and take the relevant actions.

PETABYTE STORAGE

The TDAC Platform features a data lake, this is a multi-petabyte data store that enables the TDAC Platform to ingest and record all records generated by the probes. This intelligent data store allows the end user to rapidly receive queried data at unbelievable speeds.

ACCELERATED INTRUSION DETECTION

Based on up-to-date threat intelligence, IoCs and reputation databases, TDAC Platform performs full line rate intrusion detection at 200G speeds. With fully integrated alerting, TDAC Platform provides the user with real-time updates of known threat detection via the 'single pane of glass' monitoring interface.



ENTITY TAGGING

Every flow passing through the TDAC Platform is tagged based on entity, enabling anomaly detection algorithms to monitor for unexpected behaviour based on predefined entity characteristics and historical statistical analysis. In large carrier-grade networks, where data rates are into the Tbps, enabling users to categorise and monitor the subsystems within their network allows high value resources to be ring-fenced and protected.

DATA VISUALISATION

TDAC Platform supports a multitude of user roles to enable tiered access to the vast data stored. Dashboards enable data to be visualised and enhanced querying allows users to create specific expressions to search the data for potential threats. With built in reporting and automated alerting, TDAC Platform ensures the user has active updates on the networks security posture.

ENCRYPTED TRAFFIC MONITORING

Utilising fingerprinting, TDAC Platform provides encrypted traffic analysis without requiring access to the decrypted packet payload. Employing JA3, JA3S, and HASSH methods, TDAC Platform generates hashes from the initialisation packets of TLS, SSL, and SSH flows. These calculated fingerprints can be cross-referenced against known bad fingerprint databases to identify potential malicious flows without the need for decryption.

1 CERNE

The CERNE is an intelligent IDS situated in a 1U server. The CERNE runs at 200Gbps throughput and supports 1 million user-defined signatures. With its 2.5 seconds back-in-time visibility, the CERNE creates PCAPs of every detected threat activity.

2 FLOWPROBE

The FlowProbe provides detailed unsampled traffic statistics in the form of flow records at 8 x 100GbE per 1U appliance, passively monitoring at a rate of 14 million flows a second.

3 MOBILE SIGNALLING PROBE

The Mobile Signalling Probe provides visibility of mobile networks by monitoring signalling messages and creating records with the relevant metadata. The Mobile Signalling Probe ingests protocols from 2G, 3G, 4G, and 5G networks including protocols such as SS7, Diameter, and GTP-C.

4 INTELLIGENCE GATEWAY

The TDAC Platform incorporates MISP to provide a simple, single gateway to manage and distribute threat intel across the system. The gateway enables end-users to apply their own threat intelligence sources and feeds.

5 CYBERENGINE

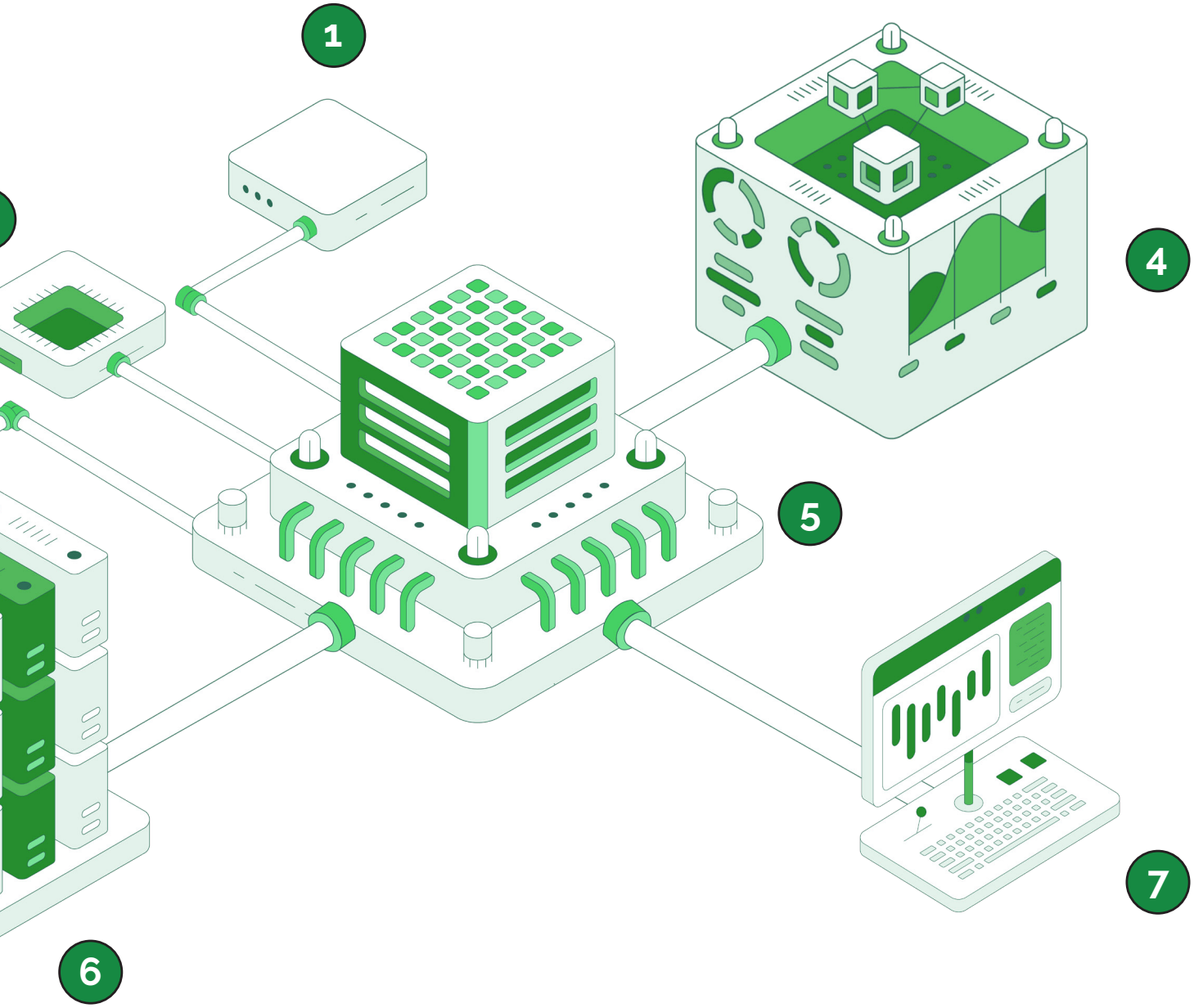
The CyberEngine acts as the brains of the TDAC. A 1U appliance designed to apply threat intelligence to network flows and utilise machine learning to identify anomalies.

6 DATA LAKE

This intelligent highly scalable storage ingests all flow and anomaly data. The data lake provides data storage in the petabytes with rapid retrieval of data over >12 months.

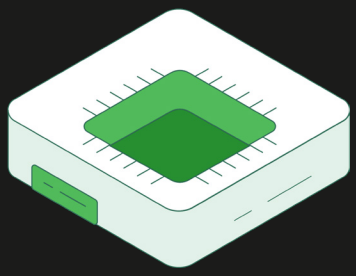
7 USER PORTAL

The User Portal is provided to query, visualise, and investigate the data the TDAC Platform has passively captured. Allowing for teams such as Digital Forensics, SecOps and Threat Hunting to quickly discover and be alerted on the latest network threats and anomalies.



ARCHITECTURE

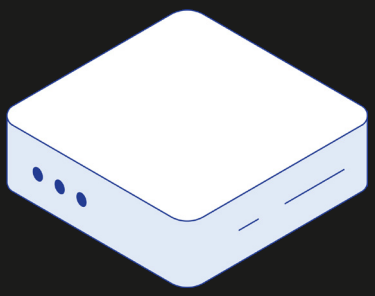
PROBES & SENSORS



FLOWPROBE

Utilising ATCO-TELESOFT's in-house designed and manufactured PCIe boards and the latest Intel FPGA technology, the 800Gbps FlowProbe provides unsampled, enriched, real-time flow records for network visibility within a 1U form-factor.

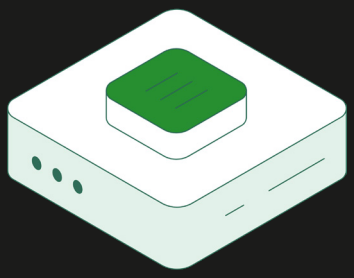
- Encrypted Traffic Analysis
- Layer 6 & 7 telemetry extraction including HTTP, TLS, SIP, and more
- Automated detection of tunnelled traffic, including GRE, GTP, MPLS, and IP-in-IP for visibility of encapsulated flows
- Flow direction detection and bi-flow handling for reduced record generation



CERNE

Supporting 200Gbps, the CERNE performs signature based intrusion detection using 3rd party cyber intelligence data. In addition to alerting on suspicious activity, the CERNE can be triggered to record all flow packets related to an event; and with the capability to buffer the full 200G stream, even packets prior to the potential threat can be captured, providing a SOC analyst or incident responder additional details to investigate and remediate the threat.

- 1 million signatures
- Automated alerting
- 2.5 second back in time buffer
- Triggered full packet recording of attack

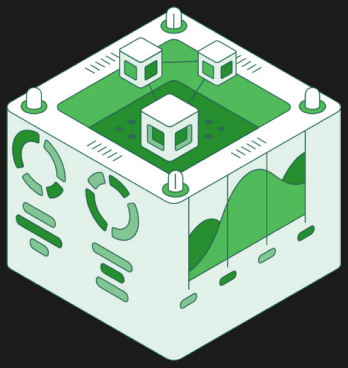


MOBILE SIGNALLING PROBE

The Mobile Signalling Probe provides deep packet inspection of signalling messages within 2G, 3G, 4G, and 5G networks to support detection and alerting of malicious signalling events that could result in network disruption, data violation or exfiltration.

- Automated alert based on GSMA FS rules
- Full signalling decode for storage and comprehensive investigation
- Supported protocols such as; SS7, Diameter, and GTP-C

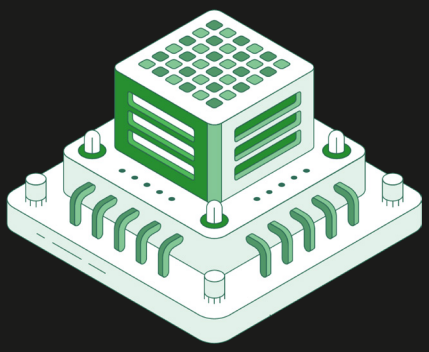
DATA INTELLIGENCE



INTELLIGENCE GATEWAY

TDAC Platform utilises its own Intelligence Gateway, its job is to manage, aggregate, and poll 3rd party threat intelligence sources to be applied by the CyberEngine, in real-time.

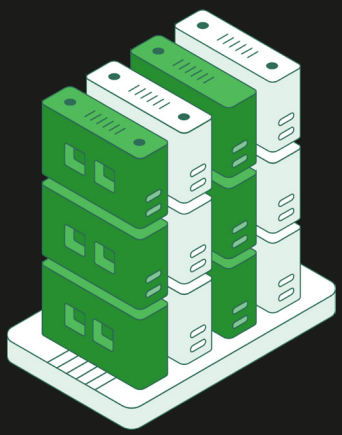
- MISP integration
- Advanced 3rd party integration
- Applies severity and classifications
- Built in TDAC Platform co-operation



CYBERENGINE

The CyberEngine acts as the central hub of the TDAC Platform, it's responsible for a number of data enhancement features including:

- Machine Learning Anomaly Detection using Statistical Analysis
- User-Defined Anomaly Detection
- Data Enrichment to enable further clarity of unsampled traffic flows enabling enhanced network visibility and detection of malicious or suspicious events
- Intelligence distribution



DATA LAKE

The data lake is responsible for intelligently storing flow records provided by the CyberEngine, utilising Hot - Warm architecture the data lake enables ultra-fast querying.

- Petabyte data storage capability
- High scalability
- Ultra-fast querying
- 12+ month data retention

USER PORTAL

QUERY

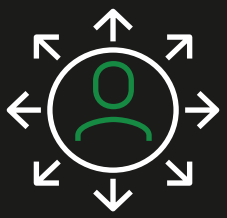
Build simple & complex queries to gather important information on the network. Supported by the in-house built frontend query framework, the TDAC Platform enables all types of users to gather key network records at incredible speeds, increasing productivity when investigating data.

VISUALISE

Visualise relevant data within the TDAC Platform. The User Portal enables users to utilise the built in visualisations to display a wealth of information. Dashboards are used to collate multiple visualisations together and be displayed in one screen, allowing users to display and query common visualisations without having to run each one on its own.

USER MANAGEMENT

Manage user permissions across the platform by creating custom roles and permissions to each and every user. The TDAC Platform has strict security policies in place to make sure that a user can only see and manage data they're permitted to see.



USER DEFINED

TDAC Platform users have the ability to customise and set their own rules for anomaly detection, allowing the end user to define exactly what an anomaly is. Alongside the anomaly detection, the user is able to define their assets and query against those specific assets within the user interface.

ALERT & REPORT

Instantly be updated on the network security posture. The TDAC Platform actively delivers network alerts based on threats and anomalies seen. Alongside alerts, reports are periodically sent to enable complete understanding of the networks attack surface.

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

SAUDI ARABIA
Telesoft Arabia
ATCO Building
P.O. Box 718 - Dammam 31421
Kingdom of Saudi Arabia
+966 13 833 5588
salesindia@telesoft-technologies.com

LONDON
5 Cheapside
London
EC2V 6AA
+44 (0)1258 480880
+44 (0)1258 486598
sales@telesoft-technologies.com

AMERICAS
Telesoft Technologies Inc
125 Townpark Drive
Suite 300, Kennesaw
GA 30144
USA
salesusa@telesoft-technologies.com

SAUDI MADE

صناعة سعودية

telesoft-technologies.com