TELESOFT

AI CYBER THREAT DETECTION

TDAC PLATFORM

STAY AHEAD OF CYBER ATTACKERS

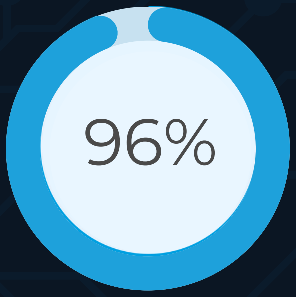
OVERVIEW

The explosive progression of Artificial Intelligence (AI) and Machine Learning (ML) in recent years has unfortunately enabled cyber attackers to scale the sophistication and frequency of their malicious campaigns. AI enhanced attacks can be seen to help adversaries automate attacks, evade detection through ML, and more. At Telesoft, we are constantly working to stay ahead of cyber attackers and have utilised AI and ML to enhance our powerful Telesoft Data Analytics Capability (TDAC) Platform; the complete network visibility, threat detection, and data retention solution.

DETECT THREATS FASTER

RAPIDLY BLOCK DGAs & PHISHING ATTEMPTS

Our expert team have developed AI modules which rapidly & autonomously detect phishing attempts and domain generation algorithms (DGAs). DGAs allow attackers to rapidly generate new domains. Once one domain is blocked, the attacker can quickly pivot to another to continue with their attack, ultimately leading to a game of whack-a-mole for a cyber analyst. However, with TDAC's AI-powered DGA detection module, analysts can rapidly identify and block these DGA domains before any malicious activity can be conducted, thereby stopping the attacker and preventing a breach from escalating.



Telesoft's DGA Detection Module has already achieved 96% accuracy.

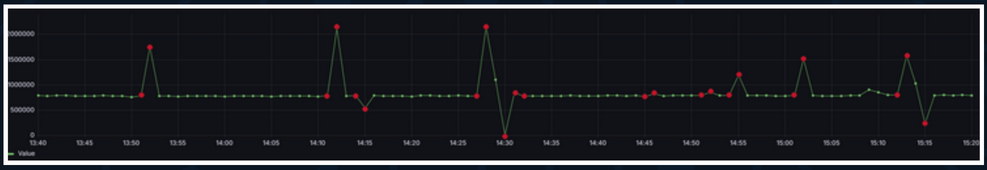
AI POWERED ANOMALY DETECTION

Telesoft's AI and ML models rapidly alert users to potentially malicious activity such as:

- Suspicious Outliers
- Unusual Lateral Movement
- Suspicious Logins such as Time Travel Logins
- Unauthorised Privilege Escalation

Trained on the relevant data, Telesoft also possess models to detect anomalous spikes/dips in the following:

- Network Traffic
- Failed Login Attempts
- TCP Flags
- And more...



TELESOFT

sales@telesoft-technologies.com

telesoft-technologies.com

TELESOFT

AI CYBER THREAT DETECTION

TDAC PLATFORM

Telesoft's AI & ML models can be deployed to detect and alert on:

- DGA Domains
- Spikes/Dips in Network Telemetry
- Outlier Activity
- DNS Exfiltration
- Anomalies in Network Telemetry
- Domain Risk
- Port Scanning
- Beacon Detection

Rapidly identify suspicious outlier activity.

OPTIMISE EFFICIENCY

REDUCE MEAN TIME TO RESPONSE (MTTR)

Through the increased threat detection speeds provided by the efficacy and efficiency of our powerful AI modules, SOC & NOC teams are able to respond to threats faster and with greater precision, freeing time and resource to carry out other critical tasks.

ENHANCE YOUR CYBER SECURITY TODAY

WITH AI CYBER THREAT DETECTION

Discover the complete network visibility, threat detection, and data retention solution with the AI-Enhanced TDAC Platform.

CONTACT US AT:

SALES@TELESOFT-TECHNOLOGIES.COM

TRUSTED GLOBALLY

TELESOFT

sales@telesoft-technologies.com

telesoft-technologies.com