Case Study

SEdesk™

The importance of connected data in Threat Intelligence

Background

The stark reality is that cyber-attacks are now commonplace. The adversaries are smart, highly-organised and adept at making changes to side-step attempts to stop them. Security professionals are expected to plan and prepare not only for existing threats but also ones that may emerge in the future.

Challenge

By harnessing the power of cyber threat intelligence, governments and enterprises are able to cut across the noise and discern the most relevant threats to them. With a Threat Intelligence Platform (TIP) analysts are able to generate actionable intelligence. Precise and accurate threat intelligence helps drive better informed strategic, tactical and operational decisions, ensuring the most effective remedial action is implemented. The result is that the impact of breaches on the organisation is minimised.

Industry

Cyber Security
Threat Intelligence

Challenges

- Consuming Cyber Threat Intelligence from a variety of un/structured sources
- Processing, normalising and enriching CTI data
- Producing timely, actionable and relevant CTI products for the organisation
- Dissemination of CTI to various stakeholders, including integration with other systems
- Privacy and legal implications in data sharing

Goals

- Turn CTI data into relevant and actionable intelligence across all stakeholders and partners to take proactive measures to protect their networks

Solution

SE*desk*™ is a unified workspace providing on-device isolation for a controlled access to whitelisted resources, protecting and securing access to EclecticIQ Platform

Solution

EclecticIQ Platform is the analyst-centric TIP, it ingests intelligence data from open sources, commercial suppliers and industry partnerships into a single collaborative analyst workbench. EclecticIQ Platform eliminates the manual and repetitive work involved with processing multiple intelligence feeds, allowing analysts to identify the most critical threats, take timely action, advise the organisation on how to respond, and collaborate with industry peers. EclecticIQ Platform is based on industry best practice, compatible with STIX & TAXII, and developed with CTI workflows and tradecraft at its core.

SE*desk*™ is the perfect combination of application and network layer protection through isolation. By defining a controlled perimeter, SE*desk*™ provides authenticated service isolation and data protection through delivery and storage. Leveraging SE*desk*™ technology data sharing is anonymised and protected. A multi-layer approach applied at network and endpoint level.

SE*desk*™ is used alongside EclecticIQ Platform to secure access to the platform in a zero-trust environment. Zero Trust is a security concept centred on the belief that organisations should not automatically trust anything inside or outside its perimeters and instead must verify anything and everything trying to connect to its systems before granting access.

SE*desk*™ enables secure access to EclecticIQ Platform by providing Encryption, Multi Factor Authentication and detailed audit logging at the management layer.

Benefits

- **Complete isolation** of data and applications on devices
- **Fine-grained access control** to the central network through context-based policies and User-Device-Server multi-factor authentication
- **VPN-free secure connection** between the dashboard at the SoC and the endpoints
- **Strong encryption mechanisms** for data integrity and protection
- **Application whitelisting**
- **Zero configuration** on endpoint devices for easy deployment

> “SE*desk*™ provides easy and secure access to our Cyber Threat Intelligence platform through an isolated digital workspace
>
> Karen Sundermann
> VP Government Sector WW
> EclecticIQ BV”

EclecticIQ

EclecticIQ enables intelligence-powered cybersecurity for government organisations and commercial enterprises. We develop analyst-centric products that align our clients' cybersecurity focus with their threat reality. And we tightly integrate our solutions with our customers' IT security controls and systems. The result is intelligence-led security, improved detection, prevention, and response. More: https://www.eclecticiq.com