TYCHON

Security Optimization Use Case

TYCHON Enterprise secures organizations with a powerful customizable tool suite for advanced persistent threats (APT) and polymorphic-malware hunting, asset identification, file discovery, root cause analysis, and system forensics. Arming you with speed, scale, capacity, and performance at previously unattainable levels, TYCHON Enterprise continuously monitors and records client and server endpoint activity for real-time identification of threats. These tools provide a complete view of an incident (present or past), its cause, and the ability to trace network propagation, all from a single console.

Benefits

Security Optimization

Gain access io an array of insights about your enterprise endpoints.

Customization

Configure your environment and simplify the process to ensure compliance.

Endpoint Control

Gain control from a central console across multiple domains on or off network.

One-Click Remediation

Deploy patches, modify security settings, disable services all with a single click.

Comprehensive & Customizable Endpoint Datasets to *make better decisions.*

From compliance monitoring to patch verification, TYCHON Enterprise manages every layer of endpoint security to keep you in control of your network.

Key Features

1 TYCHON SENSOR

Lightweight agent built on a micro service engine framework to optimize integrations and provide superior data quality to fulfill use cases.

- Logins, Permissions, & Users
- File Meta Data & Integrity
- Digital Signatures & Certificates

2 MESH MODEL

Instantly query up to a million endpoints. Unique architecture components built for scalability and fast response.

- Deploy Patches
- Update OVAL / CVE Definitions
- Device Hardening

3 OPEN ARCHITECTURE

Built on an open, flexible framework with embedded micro services built using a Client-Server Model with an integrated journal.

- Cloud / Hybrid / On Premise
- Low Bandwidth / Disconnected
- Best In Class Technical Partners

4 INCIDENT RESPONSE

Instantly respond to threats by executing a cleanup, AV update, and services status check across endpoints in a matter of seconds.

- Flexible Endpoint Targeting
- One-Click Response Actions
- IOC Searches

5 TYCHON JOURNAL

Fully indexed record from every endpoint. Monitor and record endpoint and server activity for near-instant identification of threats.

- Master Endpoint Record
- FIPS 140-2 Compliance
- Netflow & DNS History

6 DYNAMIC DASHBOARDS

Interactive dashboards, which display real-time enterprise compliance metrics for up-to-date situational awareness of network risk.

- Continuous Comply 2 Connect
- Cyber Hygiene
- Zero Trust

7 END USER ENGAGEMENT

A direct line of communication from the incident responder to the desktop of end users.

- Custom Banner & Messages
- Outlook Searching
- User Created/Connected Shares