TYCHON

Incident Response & Hunt Operations Use Case

TYCHON Enterprise offers Incident Response and Threat Hunting capabilities necessary to strengthen your endpoint security solution. Our solution allows security analysts to proactively identify suspicious activities, providing more robust anomaly detection and endpoint visibility. When it comes to security, information is key and real-time information is critical for protecting your network. Remove security blind spots on your network by identifying high risk vulnerabilities and exploits using natural language queries and customizable content. TYCHON's comprehensive and integrated solution with automation takes security to the next level.

Benefits

Two Party Authorization

Secure advanced features and action by requiring two party approval.

Unify the Stack

Communicate with other partners to receive rapid responses.

Roll Up Queries

Generate roll up queries quickly and easily.

Context Triggered Hashing

Generate, record, and index a fuzzy hash of all files on disk.

Remediation

Alleviate risk using a proactive vulnerability mitigation platform.

Endpoint Journal

Benefit from always-on monitoring and indexing with DVR like capability.

Comprehensive Endpoint Datasets to *make better decisions.*

TYCHON Enterprise provides a complete view of your security posture to stay up to date on the status of your endpoints.

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