TYCHON

Automated Continuous Endpoint Monitoring

TYCHON is an advanced endpoint analytics and remediation platform specifically designed and developed to provide comprehensive enterprise endpoint asset visibility and automated continuous endpoint monitoring to the DoD. TYCHON fully automates 100% of the DoD Cyber Hygiene Scorecard in compliance with DoD OPORD 16-0080. TYCHON's Rapid Query (RQ) feature provides real-time visibility and control of every endpoint across the enterprise. Paired with TYCHON's other features, the TYCHON advanced endpoint analytics and remediation platform provides robust endpoint situational awareness with rapid response.

TYCHON helps clients search, visualize, remediate, and monitor every endpoint across their enterprise. From compliance monitoring to patch verification, the TYCHON platform manages every layer of endpoint security to keep analysts in control of their network.

BENEFITS

Automated Scorecard

Take advantage of an automated DoD Cyber Hygiene scorecard via dynamic dashboards with drill in and drill through capability.

Remediation

Enable quick remediation and investigation via the Cyber Hygiene dashboard.

Endpoint Security Solutions

Ensure HBSS/ESS modules are fully compliant and all assets are included in required patching and configuration reporting.

Executive Level Views

Produce accurate reporting on cybersecurity posture for managers and supervisors and executive level views for senior leadership.

TAKE ACTION WITH TYCHON

- TYCHON's Continuous Endpoint Monitoring / Cyber Hygiene Dashboard displays:
  - Managed and Unmanaged Assets
  - Installed Operating Systems
  - HBSS/ESS Installed Security Tools
  - User Activity and Logon Type
  - Risk Compliance (STIGs and IAVMs)
  - Web Servers (PKI/DMZ)
  - Installed Applications
  - Email Compliance Validation
  - Computer Configuration
  - System Authorization
  - Hardware Inventory

KEY FEATURES

TYCHON SENSOR

Lightweight agent built on a Micro Service engine framework designed to optimize integration with other third-party security vendors and provide superior data quality. Capture thousands of attributes per endpoint and fulfill use cases, such as systems management, cyber hygiene, and more.

- Logins, Permissions, & Users
- File Meta Data & Integrity
- Installed Software & Settings
- Digital Signatures & Certificates
- Licenses, Drivers, & Versions

MESH MODEL

Instantly query up to a million endpoints. Unique TYCHON components, such as Data Management Node (DMN), File Distribution Center (FDC), Dispatcher, and Orchestrator, are built for scalability and fast query response times.

- Deploy Patches
- Update OVAL / CVE Definitions
- Retrieve Files for Forensics
- Device Hardening
- Reducing Attack Surface

OPEN ARCHITECTURE

TYCHON is built on an open, flexible framework with embedded micro services built using a Client-Server Model with an integrated FIPS 140-2 compliant journal for endpoint data capture. Our custom designed compression algorithm allows data to be sent securely and quickly in any type of network condition, even with low bandwidth restrictions.

- Open, Flexible API Framework
- Embedded Micro Services
- Client-Server Model
- Data Roll-up
- Cloud / Hybrid / On Premise
- Low Bandwidth / Disconnected
- Best In Class Technical Partners

RAPID QUERY

Instantly respond to a new threat or IOC, from any vendor, by executing a cleanup, AV update, and services status check across all connected endpoints in a matter of seconds. Accepts both plain English text and full regular expression (REGEX) queries, and employs fail safe measures to guarantee fast and reliable content delivery.

- Flexible Endpoint Targeting
- One-Click Response Actions
- IOC Searches
- Trace
- Memory Analysis & Forensics
- Two Person Integrity

TYCHON JOURNAL

Fully indexed record from every endpoint. Continuously monitor and record endpoint and server activity for near-instant identification of threats – present or past – and the complete view of an incident, root cause analysis, and tracing of network propagation.

- Master Endpoint Record
- FIPS 140-2 Compliance
- Historical Data
- Historical Running Processes
- Fuzzy Hash
- Netflow & DNS History

DYNAMIC DASHBOARDS

Interactive dashboards, which display real-time enterprise compliance metrics for up-to-date situational awareness of network risk. Vital reports with details on privileged users, web server compliance, asset inventory, system authorization, required security services, patching, and overall organization software compliance.

- Continuous Comply 2 Connect
- Cyber Hygiene
- Compliance Validation
- Resource Utilization
- Strong Authentication
- Zero Trust

TYCHON COMMUNICATOR / END USER ENGAGEMENT

Close the gap between detection and response with a direct line of communication from the incident responder to the desktop of end users using the TYCHON Communicator platform.

- Displays Persistent Banner
- Send Custom Messages
- Outlook Searching
- User Created / Connected Shares