TYCHON

USE CASE: AUTOMATED CONTINUOUS ENDPOINT MONITORING

CONTACT US
web: tychon.io
email: info@tychon.io

TYCHON is an advanced endpoint security and management 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 Enterprise Endpoint Management Platform provides robust endpoint situational awareness with rapid response.

TYCHON is a software company that develops advanced enterprise endpoint management technology that enables commercial and government organizations to bridge the gap between security and IT operations. TYCHON participates in McAfee's Security Innovation Alliance and the TYCHON Enterprise Endpoint Management Platform is engineered using the software development kits for McAfee ePO and leverages the Data Exchange Layer (DXL) and other messaging fabrics.

CAPABILITIES

Automated Scorecard

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

Endpoint Security Solutions

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

Remediation

Enable quick remediation and investigation via the Cyber Hygiene dashboard.

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

TYCHON

KEY FEATURES

REAL-TIME INCIDENT RESPONSE

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.

- Efficient IOC Searches
- One-Click Response Actions
- Two Person Integrity
- Target Endpoint by System Tree
- Netflow
- Trace

CYBER HYGIENE 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.

- Strong Authentication
- Zero Trust
- Device Hardening
- Reducing Attack Surface
- Improved Detection and Response to Attacks

END USER ENGAGEMENT - TYCHON COMMUNICATOR

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. Send custom messages to one, some or all users (e.g. inform users that their machines are temporarily quarantined.)

- Displays Persistent Banner
- Send Custom Messages to any Endpoint

TYCHON ENDPOINT 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.

- FIPS 140-2 Compliance
- Historical Data
- Compressed Messaging to Reduce Bandwidth
- Fuzzy Hash
- Netflow

API INTEGRATION

TYCHON's robust set of APIs makes integration with other endpoint or network capabilities straightforward and rapid via custom content creation, expanding data recording fields, and more.

- External Server Feeds
- DXL, Open DXL, Kafka
- SIEM Feeds
- API/SDK

ARCHITECTURAL FEATURES

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 Framework
- Embedded Micro Services
- Client-Server Model
- Data Roll-up
- No Scans required
- Targeting System Efficiencies

TECHNICAL PARTNERS

TYCHON partners with the best in class industry leaders and service providers to provide enriched endpoint data that is visible, accessible, understandable, trusted, interoperable, and secure.

- McAfee
- Elastic
- Palo Alto
- ThreatQ and more