TYCHON

USE CASE: CYBER HYGIENE

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

TYCHON's Enterprise Endpoint Management Platform enhances operational resiliency by allowing you to manage your system health, reduce vulnerabilities and improve online security with real-time endpoint visibility, proactive monitoring and validation through its automated cyber hygiene scorecard. Through interactive dashboards, TYCHON decreases your enterprises cyber security risk by allowing organizations to validate security settings at the endpoint in real-time and query specific system(s) to remediate vulnerabilities, add/remove software, quarantine systems, update patches and more all from a single console. TYCHON's proactive compliance validation expands your organization's defense-in-depth.

TYCHON is a software engineering 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 the Data Exchange Layer (DXL).

CAPABILITIES

Strong Authentication

Protect high-value assets and degrade an adversary's ability to access the network by enforcing your organization's authentication standards.

Reduce Attack Service

Mitigate the threat of Internet -based adversaries and reduce external attack vectors by auditing all Internet Facing, DMZ, and PKI based authentication on web servers to ensure compliance

Device Hardening

Reduce internal and external attacks and prevent an adversary's ability to escalate privileges by ensuring all asset have proper computer configurations, computer patches are applied, and all Internet Facing webservers are within the DMZ.

Detection and Response

Prevent and respond to adversary activity by taking action to remove or quarantine internet facing webservers, systems with CAT 1 findings, expired RMF packages, 120+ days IAVAs, obsolete office assets, and unauthorized user accounts.

TYCHON COMPLIANCE ENFORCEMENT

- Enforce accountability, prevent unauthorized access, and avoid network compromise.
- Identify vulnerabilities on your network to proactively address security issues through a centrally controlled management solution.
- Prevent exploitation and increase your cybersecurity readiness with real-time visibility.
- Ensure situational awareness of network threats and mitigations with interactive, easy to use dashboards.

McAfee COMPATIBLE

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

AUTOMATED DOD CYBER HYGIENE SCORECARD

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 PKI and DMZ, asset inventory, system authorization, HBSS/ESS Services, patching and overall organization software compliance.

- Strong Authentication
- 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

PARTNER 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 and Open DXL
- SIEM/ESM Feeds
- API/SDK

ARCHITECTURAL FEATURES

The TYCHON architecture was built using a Client-Server Model with a 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.

- Client-Server Model
- CSC and Data Roll-up
- No Scans required
- Targeting System Efficiencies

MCAFEE INTEGRATION

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 the Data Exchange Layer (DXL).

- ePO: Single Pane of Glass, Centralized Control, Data Roll-up Support, Policy Enforcement, Access Control
- DXL: Sharing Information with other Vendors

McAfee COMPATIBLE