TYCHON

AUTOMATED DOD CYBER HYGIENE SCORECARD

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

TYCHON offers interactive pivotable dashboards, which display enterprise metrics with data export capabilities to expand operational resilience and manage risk. This feature, known as the TYCHON Automated DoD Cyber Hygiene Scorecard, provides up-to-date situational awareness of risks to the network. The scorecard delivers instant visibility of critical cyber security policy violations. It encompasses vital security areas such as software patches, compliance, privileged users, and more as required by the DoD CIO. This centralized view of critical information enables operators to monitor endpoint compliance in near real-time.

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).

DASHBOARDS

Web Servers
Auditing on all Internet Facing (public), DMZ, and PKI-based authentication on web servers to ensure compliance.

↗ Disconnect non-approved web servers

HBSS / ESS
Service compliance visibility that includes running statuses, configuration, and version details.

↗ Deploy out-of-date services

Computer Configuration
Visibility of all CAT-1 Operating System STIG settings.

↗ Quarantine systems

System Authorization
Validation of expired or expiring RMF ATO packages.

↗ Quarantine systems

Users
Accounting for privileged, non-privileged, approved PKI, approved password, enabled vs disabled, local vs domain user accounts with logon details.

↗ Disable / delete accounts

Computer Patching
Provides critical IAVA compliance visibility for Server, Client, and infrastructure assets.

↗ Remove systems with high risk weakness

Asset Inventory Management
Accountability of all obsolete office and non-office operating system assets.

↗ Quarantine systems

Rogue System Detection
Provides visibility of un-managed systems.

↗ Enable management of rogue systems

↗ = One Click Action

725 Jackson Street, Suite 101 I Fredericksburg, VA 22401

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
- Trace

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