TYCHON

AUTOMATED DOD CYBER HYGIENE SCORECARD

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

TYCHON offers interactive dashboards, which display enterprise metrics 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 TYCHON Automated DoD Cyber Hygiene Scorecard is part of an interface with Kibana, an open source analytics and visualization platform. Through Kibana, users can manipulate TYCHON data to deliver instant visibility of critical cyber security policy violations. The scorecard 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 leverages the Data Exchange Layer (DXL) and other messaging fabrics.

DASHBOARDS

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

ESS Services
Service compliance visibility that includes running statuses

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

Audits
Visibility of all CAT-1 Operating System STIG settings

Patches
Provides critical IAVA compliance visibility for servers and workstations

Web Server PKI
Auditing on all internal and external web servers to ensure compliance

Cyber Hygiene Summary
Executive level view of major performance categories

DO MORE WITH TYCHON

- Automated cyber hygiene data via dynamic, customizable dashboards
- Accurate reporting on cybersecurity posture for manager and supervisors
- Executive level views for senior and executive leadership

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