TYCHON

USE CASE:
CYBER HYGIENE

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

TYCHON is an endpoint analytics and remediation platform that 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 Cyber Hygiene Dashboards. Using 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. TYCHON's proactive compliance validation expands your organization's defense-in-depth.

Tychon LLC is a software engineering company that develops advanced enterprise endpoint management technology designed to provide asset visibility and automated continuous endpoint monitoring to the enterprise. TYCHON allows security operators the ability to quickly diagnose and take action against breaches and administrators the ability to manage cyber hygiene via dynamic Cyber Hygiene Dashboards.

BENEFITS

Strong Authentication

Protect high-value assets and degrade an adversary's ability to access the network by enforcing your organization's authentication standards to verify a user or device to secure access and information.

Device Hardening

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

Reduce Attack Service

Mitigate the threat of Internet based adversaries and reduce external attack vectors by auditing Internet facing, DMZ, and multi-factor based authenticated web servers to ensure compliance to policy and security controls.

Detection and Response

Prevent and respond to adversary activity by removing or quarantining Internet facing webservers and systems in violation of policy, hardening settings, and identifying obsolete 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.

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