TYCHON

USE CASE: VULNERABILITY MANAGEMENT

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

TYCHON monitors all vulnerabilities with a corresponding Common Vulnerability and Exposures (CVE) number starting from Year 2012 up to the current day, using the Open Vulnerability and Assessment Language (OVAL). The TYCHON Security Content Automation Protocol (SCAP) scan engine runs checks on customizable days and times and feeds the results into the central database where it is analyzed.

The TYCHON scan engine leverages a **delta-based model** which reduces scan time by only monitoring vulnerabilities that have not been patched. Using this efficient method, endpoint and network resource utilization is significantly reduced. At any point in time, a TYCHON user can see the state of a CVE by a multitude of search types which include the CVE ID, IAVA, Severity, Risk Score and/or release date in the CVE dashboard. Analysts can also perform a CVE OVAL scan locally on endpoints by asking systems for their current CVE-ID status through TYCHON Rapid Query.

TYCHON is an endpoint analytics and remediation platform that helps clients search, visualize, remediate, and monitor every endpoint across their enterprise. From compliance monitoring to patch verification, the TYCHON platform manages every layer of endpoint security to keep analysts in control of their network.

BENEFITS

Detect

Identify attack surface exposures to detect system vulnerabilities.

Monitor

Focus on deltas to reduce required checks and minimize network impact.

Customize

Target a full array of vulnerabilities to address critical issues earlier not just after a CVE.

Enforce

Remediate issues from a single tool, using the TYCHON Patch Management feature when issues are identified.

Visualize

Maintain complete visibility using TYCHON Dashboards to monitor and assess vulnerabilities.

Risk Analysis

Assess your network vulnerability using TYCHON's risk analysis to identify exposures and eliminate uncertainty.

COMPLIANCE ENFORCEMENT

- Query your network in real time using Rapid Query and take action immediately with Patch Management.
- Take advantage of TYCHON's consistent running monitor of CVE compliance.
- Compliance with OVAL 5.11.

TYCHON

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