TYCHON

Vulnerability Management Use Case

TYCHON Enterprise 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 unpatched vulnerabilities. This efficient method significantly reduces endpoint and network resource use. At any point in time, a TYCHON user can see the state of a CVE by 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.

Benefits

Detect

Identify attack surface exposures to detect system vulnerabilities.

Monitor

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

Customize

Target a full array of vulnerabilities to address critical issues earlier.

Visualize

Maintain complete visibility using dashboards to assess vulnerabilities.

Enforce

Remediate issues from a single tool using TYCHON Patch Management.

Risk Analysis

Assess you network with TYCHON's risk analysis to identify exposures.

Identify Exposures to *make better decisions.*

725 Jackson Street, Suite 101 I Fredericksburg, VA 22401

tychon.io | info@tychon.io

TYCHON

Key Features

1 TYCHON SENSOR

Lightweight agent built on a micro service engine framework to optimize integrations and provide superior data quality to fulfill use cases.

- Logins, Permissions, & Users
- File Meta Data & Integrity
- Digital Signatures & Certificates

2 MESH MODEL

Instantly query up to a million endpoints. Unique architecture components built for scalability and fast response.

- Deploy Patches
- Update OVAL / CVE Definitions
- Device Hardening

3 OPEN ARCHITECTURE

Built on an open, flexible framework with embedded micro services built using a Client-Server Model with an integrated journal.

- Cloud / Hybrid / On Premise
- Low Bandwidth / Disconnected
- Best In Class Technical Partners

4 INCIDENT RESPONSE

Instantly respond to threats by executing a cleanup, AV update, and services status check across endpoints in a matter of seconds.

- Flexible Endpoint Targeting
- One-Click Response Actions
- IOC Searches

5 TYCHON JOURNAL

Fully indexed record from every endpoint. Monitor and record endpoint and server activity for near-instant identification of threats.

- Master Endpoint Record
- FIPS 140-2 Compliance
- Netflow & DNS History

6 DYNAMIC DASHBOARDS

Interactive dashboards, which display real-time enterprise compliance metrics for up-to-date situational awareness of network risk.

- Continuous Comply 2 Connect
- Cyber Hygiene
- Zero Trust

7 END USER ENGAGEMENT

A direct line of communication from the incident responder to the desktop of end users.

- Custom Banner & Messages
- Outlook Searching
- User Created/Connected Shares