

## PQC Management Module

In 2022, the White House signed into law the Quantum Computing Cybersecurity Preparedness Act. This law requires agencies to prepare now to implement Post-Quantum Cryptography. Specifically, government agencies must maintain an inventory of all information technology in use that is vulnerable to Post-Quantum Cryptography. The TYCHON Post-Quantum Cryptographic (PQC) Management Module is an add-on module for TYCHON's Enterprise Endpoint Analytics & Remediation Platform designed specifically to help agencies meet the requirements of this law. The module delivers 1) a comprehensive inventory of cryptographic systems and 2) a prioritized inventory of vulnerable information systems.

### PQC MANAGEMENT DASHBOARD



- ▶ Track certificates by algorithm type.
- ▶ Identify countries of origin for certificates.
- ▶ Quickly detect expired certificates.
- ▶ Calculate certificate ages to identify your most vulnerable certs.
- ▶ Filter and search based on host, keywords, file types, and more.

### CRYPTOGRAPHIC RISK MANAGEMENT

Take advantage of TYCHON's multiple data sources to collect valuable cryptographic system datasets.



Signing  
Certificates



Certificate  
Files



Encryption  
Libraries



Listening  
Services



Web  
Services



Root  
Certificates



User  
Certificates

- ▶ Track all Certificates in the Certificate Store
- ▶ Identify Soft Certs on Drives
- ▶ Identify Services hosting TLS/SSL Certificates
- ▶ Identify Web Service Encryption Methods

- ▶ Identify Software using Encryption Libraries
- ▶ Track External Connections using SSL/TLS
- ▶ Investigate the use of Web Browser Applications

## 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