TYCHON

Endpoint Detection & Response

TYCHON offers Endpoint Detection and Response (EDR) capabilities necessary to strengthen your endpoint security solution. Our EDR solution allows security analysts to proactively identify suspicious activities, providing more robust anomaly detection and endpoint visibility. When it comes to security, information is key and real-time information is critical for protecting your network. Remove security blind spots on your network by identifying high risk vulnerabilities and exploits using natural language queries and customizable content. TYCHON, with Trellix, offers a comprehensive and integrated EDR solution with automation, taking security to the next level.

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

Two Party Authorization

Secure advanced features and actions by requiring two party approval

Unify the Stack

Communicate with other OpenDXL partners to receive rapid responses

Roll Up Queries

Leverage TYCHON to generate roll up queries quickly and easily

Remediation

Alleviate risk using a proactive vulnerability mitigation platform

Context Triggered Piecewise Hashing

Generate, record, and index a fuzzy hash of all files on disk

Host Based Endpoint Journal

Benefit from always-on monitoring and indexing with DVR-like capability

TAKE ACTION WITH TYCHON

- Get the complete view of current security posture and stay up to date on the status of your endpoints.
- Deploy patches, modify security settings, and enable/disable services all with a single click.
- Take one-click action to:
  - Quarantine Machines
  - Kill Processes
  - Delete Files
  - Enforce Policy
  - Hunt for Threats
  - Uninstall Applications
  - Manage Asset Compliance
  - Monitor Event Logs
  - Feed data to Splunk ® ArcSight™, Trellix ESM, TIE, and ATD in real time
  - Ingest data from third party databases and cloud services

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