TYCHON

USE CASE: ENDPOINT DETECTION & RESPONSE

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

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 McAfee's Security Suite®, offers a comprehensive and integrated EDR solution with automation, taking security to the next level.

TYCHON is a software company that develops advanced enterprise endpoint management technology that enables commercial and government organizations to bridge the gap between security and IT operations. TYCHON participates in McAfee's Security Innovation Alliance and the TYCHON Enterprise Endpoint Management Platform is engineered using the software development kits for McAfee ePO and the Data Exchange Layer (DXL).

CAPABILITIES

Two Party Authorization

Secure advanced features and actions by requiring two party approval

Roll Up Queries

Leverage TYCHON to quickly and easily generate roll up queries

Context Triggered Piecewise Hashing

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

Unify the Stack

Communicate with other OpenDXL partners to receive rapid responses

Remediation

Alleviate risk using a proactive vulnerability mitigation platform

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™, McAfee® ESM, TIE, and ATD in real time
  - Ingest data from third party databases and cloud services

McAfee® COMPATIBLE

TYCHON

KEY FEATURES

REAL-TIME INCIDENT RESPONSE

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.

- Efficient IOC Searches
- One-Click Response Actions
- Two Person Integrity
- Target Endpoint by System Tree
- Netlfow
- Trace

AUTOMATED DOD CYBER HYGIENE SCORECARD

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 PKI and DMZ, asset inventory, system authorization, HBSS/ESS Services, patching and overall organization software compliance.

- Strong Authentication
- Device Hardening
- Reducing Attack Surface
- Improved Detection and Response to Attacks

END USER ENGAGEMENT - TYCHON COMMUNICATOR

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. Send custom messages to one, some or all users (e.g. inform users that their machines are temporarily quarantined.)

- Displays Persistent Banner
- Send Custom Messages to any Endpoint

TYCHON ENDPOINT 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.

- FIPS 140-2 Compliance
- Historical Data
- Compressed Messaging to Reduce Bandwidth
- Fuzzy Hash
- Netflow

PARTNER INTEGRATION

TYCHON's robust set of APIs makes integration with other endpoint or network capabilities straightforward and rapid via custom content creation, expanding data recording fields, and more.

- External Server Feeds
- DXL and Open DXL
- SIEM/ESM Feeds
- API/SDK

ARCHITECTURAL FEATURES

The TYCHON architecture was built using a Client-Server Model with a 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.

- Client-Server Model
- CSC and Data Roll-up
- No Scans required
- Targeting System Efficiencies

MCAFEE INTEGRATION

TYCHON participates in McAfee's Security Innovation Alliance and the TYCHON Enterprise Endpoint Management Platform is engineered using the software development kits for McAfee ePO and the Data Exchange Layer (DXL).

- ePO: Single Pane of Glass, Centralized Control, Data Roll-up Support, Policy Enforcement, Access Control
- DXL: Sharing Information with other Vendors