TYCHON

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

TACTICAL TYCHON

Tactical TYCHON (tTYCHON) is derivative implementation of TYCHON specifically developed for deployed forces and enables the HBSS/ESS infrastructure to operate in low, limited, or no bandwidth environments. TYCHON is a dynamic endpoint management and intelligence platform, built for the DoD and fully integrated into the McAfee security stack. TYCHON provides real-time endpoint visibility across the enterprise, provides customizable real-time data feeds, fully automates the DoD Cyber Scorecard and offers a flexible asset management query & response tool that gives incident responders complete control of their systems from any ePO server inside the DODIN.

TYCHON is a software security company that develops advanced enterprise endpoint management technology that enables commercial and government organizations to bridge the gap between security and IT operations. The TYCHON product suite is engineered in partnership with the McAfee® Security Innovation Alliance and is exclusively developed using the SDKs for McAfee® ePO and Data Exchange Layer (DXL).

CAPABILITIES

Deployable Incident Response

Data reduction and threat automation for deployed afloat assets

Reduced Events

Minimize the number of events by prioritizing and restricting criteria

Increase Efficiency

Reduce data size by removing non-essential data

Operate in Low Bandwidth

Launch agent level tasks over constrained bandwidth environments

Historical Data

Maintain historical data for later analysis, forensics, and reference

Flexibility

Benefit from customizable real-time data feeds and control over your system

TAKE ACTION WITH TYCHON

- Better understand and secure the environment of your enterprise with a single console.
- Automate day-to-day systems management processes and eliminate the human element.
- Take one-click actions to uninstall applications, quarantine machines, and find similar files.
- Do more with less. Streamline your internal operations by:
  - Identify and retire or eliminate outdated or unused software and tools, and orphaned or disconnected servers
  - Identify candidate servers for virtualization
  - Save money on audits, staffing, maintenance fees, training, and software licensing
  - Uninstall applications
  - Migrate with ease to new software applications or operating systems.

McAfee® COMPATIBLE

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

CYBER SCORECARD DASHBOARDS

Interactive dashboards, which display real-time enterprise compliance metrics for up-to-date situational awareness of network risk. Vital reports with scoring on Web Servers, User Logon, HBSS Services, STIGs, Windows and Linux Patches, 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 Journaling for Polymorphic Detection

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 is engineered in partnership with the McAfee Security Innovation Alliance and is exclusively developed using the SDKs for McAfee ePO and DXL. TYCHON is thoroughly tested, authorized and digitally signed by McAfee as 'McAfee Compatible'.

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