TYCHON

Capabilities: SECURITY OPTIMIZATION

Tychon secures enterprises with powerful customizable tool suite for advanced persistent threats (APT) and polymorphic-malware hunting, asset identification, file discovery, root cause analysis, and system forensics. Arming you with speed, scale, capacity, and performance at previously unattainable levels, Tychon continuously monitors and records client and server endpoint activity for near real-time identification of threats. These tools provide a complete view of an incident (present or past), its cause, and the ability to trace network propagation, all from a single console. Execute remediation of known vulnerabilities and patch out-of-date software in one click.

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 DXL. Products are tested, authorized, and digitally signed by McAfee as "McAfee Compatible" and have repeatedly earned this certification since 2012.

WHY TYCHON?

Tychon was created by former Cyber Defense Operators in the DoD responsible for Incident Response and Defensive Cyber Operations, similar to the role of today's CPT teams, to help address many of the operational and scalability challenges that are routinely faced with protecting DoD networks. There is currently a gap in the ability to rapidly perform event diagnosis and response at scale and across a global enterprise. Tychon was created to close that gap.

Gain speed and the ability to identify malware and vulnerabilities with precision and agility and act instantly with a one-click response. Near simultaneous discovery and remediation.

OVERVIEW

Asset Visibility through RapidQuery: Tychon records, indexes, and actively monitors endpoints locally in real-time. Endpoint events and data continuously recorded by Tychon are completely configurable and include:

- Running Processes
- Windows Registry
- Outlook Email
- Network Activity
- Installed Products
- Startup & Services
- Kernel Drivers
- Adapters
- Files & Hashes
- Event Logs
- User/Group Accounts
- Fuzzy Hash

Host Based Endpoint Journal: Tychon has a DVR like capability for your client or server, physical and virtual endpoints that provides an always-on endpoint monitoring, recording, and indexing capability.

Context Triggered Piecewise Hashing (Fuzzy Hash): Tychon generates, records, and indexes a fuzzy hash of all files on disk providing comprehensive searching and rapid termination for variants of IOCs and vulnerabilities yet to be discovered.

Remediation: Tychon provides a proactive vulnerability mitigation platform that alleviates risk by informing users with an actionable dashboard of the wellness of the enterprise.

TYCHON

CLEAR QUESTIONS. STRAIGHT ANSWERS. QUICK RESPONSE.

TAKE ACTION WITH TYCHON

- Get the complete view of an incident, root cause analysis, and tracing of network propagation.
- Contain suspect systems via host firewall or by integration with a Network Access Control (NAC) provider.
- Take one-click action to:
  - Quarantine Machines
  - Kill Processes
  - Delete Files
  - Perform First-Response Forensics
  - Find Similar (e.g. polymorphic malware or file types)
  - Uninstall Applications
  - Trace processes on a single machine, group of machines, or the entire enterprise
  - Feed data to Splunk®, ArcSight™, McAfee® ESM, TIE and ATD in real-time

PRODUCT FEATURES

Fully Indexed Record of Every Endpoint with Tychon Host Based Journal™	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. Fully indexed, FIPS 140-2 encrypted record of each endpoint (144 data points over 12 journal groups) requiring only 30mb yearly on average.
Automatic Response with Tychon RapidQuery™	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.
End User Engagement with 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).
Application Communication Whitelisting with Tychon Host Firewall Orchestrator™	Fully leverage McAfee HIPS and whitelist your entire application portfolio using the intelligent three-step wizard. Tychon simplifies HIPS administration and delivers defense-in-depth by minimizing the attack surface and mitigating data exfiltration.
Vulnerability and Patch Remediation	Includes full support for distributing software patches to Windows, Mac, and Linux machines and remediate known vulnerabilities enterprise-wide in seconds.
McAfee Data Exchange Layer (DXL) Integration	DXL has extended Tychon by providing a means for near-instantaneous global communication with endpoints and the ability to scale across enterprise wide deployments.
Third-Party Application Integration with DXL	Tychon broadcasts messages across DXL that can be picked up and acted on by third-party applications and appliances that also communicate across the DXL fabric. These can range from NAC appliances or firewalls to SIEM and beyond, opening a world of new possibilities for automation and autonomous action.