TYCHON

TYCHON Use Cases Overview

TYCHON Enterprise is an endpoint analytics and remediation platform designed to be the 'gold source' for enterprise endpoint data.

- Visibility, monitoring, and query and response at unparalleled speed and scale
- Automated dashboards for instant visibility and situational awareness
- Track privileged users, Web PKI and DMZ, inventory, system authorization, security, patching, and overall compliance



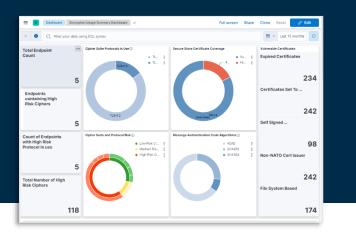
Comprehensive & Customizable Endpoint Datasets to *make better decisions.*



TYCHON

TYCHON Enterprise Use Cases

Get near real-time visibility into every endpoint across your enterprise, while minimizing network usage and leveraging existing investments.



©

Attack Surface Management

Achieve continuous discovery, monitoring, evaluation, and remediation of attack surfaces with built in analytics, reports, and dashboards.



Enterprise Endpoint Management

Retrieve intelligence from endpoints at speed and scale using natural language questions and PowerShell scripts for comprehensive real-time visibility.



Vulnerability & Patch Management

Monitor all vulnerabilities with a CVE number using OVAL and XCCDF. Use delta based checks to reduce scan time and risk analysis to eliminate exposures and uncertainty.



•

Comply to Connect

Record, index, and monitor endpoints in real-time, quarantine outdated OSs, identify patch vulnerabilities, and more to validate C2C compliance.



Incident Response & Hunt Operations

Proactively identify suspicious activities, providing more robust anomaly detection and endpoint visibility to remove security blind spots on your network.



Cyber Hygiene

Manage system health, reduce vulnerabilities, and improve online security with real-time endpoint visibility, proactive monitoring, and validation.



Quantum Readiness

Rapidly gather, inventory, and prioritize cryptographic systems. Customize, manage, and enforce policies to address your most vulnerable assets first.

Configure Targets	Select Question	Inspect Res							
 Current Target Configuration 		Endpoints 📧 Realms 🚺	Groups	a					
Select Question				-	(without data)				
Any OS Windows	Linux All Question Types	en Types Execute Scripts Simple Filters Basic Tooks Patch Detections			Q Kibana Query Language 1 field			Submit	0
What are all the local groups on Windows assets?			0	~					100
Simple Filter					Hosts	group.name			
Local Groups		Outstion Documentation Data Acceptance Period No interacts			5	Access Control Assistance Operators			
mpact 🖻 🕓 🛞	Data Source(s) Operating System				5	Administrators			
· • •	R. Observed System				5	Backup Operators			
Get Answers					1	Certificate Service DCOM	Access		
				5	Cryptographic Operators				
			5	3	3	Device Owners			
		0	5	5	5	Distributed COM Users			
			9	5	5	Event Log Readers			
			5	5	5	Cuests			
			4	5	5	Hyper-V Administrators			
			9	5	5	IIS_IUSRS			
			4	5	5	Network Configuration Op	erators		