PROTECTING CRITICAL SUPPLY CHAINS

Cyber Threat Hunting—Changing the Game

OVERVIEW

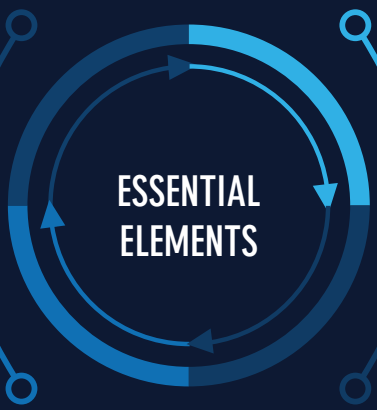
Nation-state actors are targeting U.S. critical infrastructure and its industrial base suppliers and vendors through obfuscated targeting of the cyber supply chain. Combating these sophisticated campaigns demands greater resources and attention. Enhancing third-party or value-chain threat detection and monitoring requires adopting proactive practices, including systemic threat hunting strategies.

Cyber threat hunting is designed to help counter contemporary cyber threats targeting connected software applications and services tied to business operations. Cyber threat hunting, whether in-house or outsourced, bolsters supply chain security and resilience by mitigating cyber risks to organizational operations and assets.

ESSENTIAL ELEMENTS

A structured cyber threat hunting program requires multiple tools and solutions that are integrated and designed to work in unison to achieve strategic cybersecurity outcomes. Threat hunting provides a continuous monitoring solution that identifies, investigates, and advises on threats to an organization's connected environment. Threat hunting professionals use foundational solutions such as security information and event management (SIEM), extended detection and response (XDR), and managed detection and response (MDR). Augmenting automated or manual processes with usage-data analysis, network scans, and commercially available technical data creates a strategic cyber threat hunting program. The essential cyber threat hunting program elements outlined below highlight how organizations can implement this capability to advance cyber supply chain security.

> **"China remains the most active and persistent cyber threat to U.S. Government, private sector, and critical infrastructure networks."**
>
> *– Annual Threat Assessment of the U.S. Intelligence Community (2024)*



MISSION

Identify your threat hunting mission, threat types, and hunt processes

DELIVERABLES

Define deliverables, use trend data; identify and prioritize risk equities

MATURITY MODEL

Build a maturity model, share findings across your supply chain

ADAPTION

Continually iterate your threat hunts; use results to augment gaps left by static correlation

MATURITY MODEL

The Cyber Threat Hunting Maturity Model (HMM) helps to identify the level of security controls in an organization. The HMM posture is aligned according to five levels:

INITIAL	MINIMAL	PROCEDURAL	INNOVATIVE	LEADING
Primarily reliant on automated alerting tools such as IDS, SIEM or antivirus to detect malicious activities against networks.	Routine collection of data through automated alerting tools & integrated into data lakes & SIEMs.	Hunt teams review large scale data sets & apply defined procedural activities to effect systematic changes.	Hunt teams integrate data collection with machine learning to reduce errors, abnormalities, & inconsistencies to improve data visualization.	Operationalizes successful hunt process; turns into automated detection; results in constant enhancement to the detection of highly skilled adversaries.

TAKEAWAY

Maturing your cyber threat hunting capability requires resource planning and a fully integrated supply chain risk management program. Threat hunting is an essential layer of cyber security that can augment traditional threat detection practices by actively identifying signs of intrusions, curtailing potential incidents, and sharing identified threats. Nation-state actors continue to innovate ways to defeat enterprise network security. Having a proactive cyber threat hunting capability is a force-multiplier to combat emerging threats, bolster cyber security, and enhance supply chain integrity and resiliency.

REFERENCES

Related controls in Security and Privacy Controls for Information Systems and Organizations (NIST SP 800-53 Rev. 5)

CA-2: Control Assessments
CA-7: Continuous Monitoring
CA-8: Penetration Testing
RA-3: Risk Assessment
RA-5: Vulnerability Monitoring and Scanning
RA-6: Technical Surveillance Countermeasures Survey
RA-10: Threat Hunting
SI-4: System Monitoring
NIST Special Publication 800-30
NIST Special Publication 800-172A

For more information on supply chain security, please visit ncsc.gov