Threat Intelligence Program

Threat Intelligence Overview

Threat intelligence provides context about threats, adversaries, and attack techniques. Enables proactive defense and informed decision-making.

Sources: Commercial feeds, open source intelligence (OSINT), information sharing groups, internal telemetry.

Intelligence Collection

Collect indicators of compromise (IOCs): Malicious IPs, domains, file hashes, URLs. Tactics, techniques, and procedures (TTPs) of threat actors.

Vulnerability intelligence: New vulnerabilities, exploits, patches. Industry-specific threats and trends.

Intelligence Analysis

Analyze intelligence for relevance to our environment. Prioritize based on likelihood and potential impact.

Correlate intelligence with internal security data. Identify gaps in defenses. Provide actionable recommendations.

Threat Actor Profiling

Track known threat actors targeting our industry. Understand their motivations, capabilities, and TTPs.

Attribution helps predict future attacks and tailor defenses. Share profiles with SOC and incident response teams.

Indicator Management

Ingest IOCs into security tools (SIEM, firewall, endpoint protection). Automate blocking of known malicious indicators.

Regularly update and expire old indicators. Track indicator effectiveness and false positive rates.

Threat Intelligence Sharing

Participate in industry information sharing groups (ISACs). Share anonymized threat data with community.

Receive early warnings of threats targeting our sector. Collaborate on threat research and mitigation strategies.

Intelligence Dissemination

Distribute intelligence to relevant stakeholders: SOC, incident response, IT, management.

Tailor intelligence to audience: Technical details for SOC, strategic overview for executives. Use standardized formats (STIX, TAXII).

Threat Modeling

Identify likely threats to our assets and operations. Model attack scenarios and potential impacts.

Use threat intelligence to validate and update threat models. Prioritize security investments based on threat landscape.

Vulnerability Intelligence

Monitor vulnerability disclosures relevant to our technology stack. Assess exploitability and potential impact.

Prioritize patching based on threat intelligence. Track if vulnerabilities are being actively exploited.

Dark Web Monitoring

Monitor dark web for mentions of company, leaked credentials, or planned attacks.

Track sale of access to our systems or data. Alert relevant teams to take protective actions.

Threat Intelligence Platforms

Use threat intelligence platform (TIP) to aggregate, analyze, and disseminate intelligence.

Integrate TIP with security tools for automated response. Track intelligence workflow and effectiveness.

Metrics and Reporting

Track: Intelligence sources used, IOCs ingested, threats detected, incidents prevented.

Report threat landscape trends to management quarterly. Demonstrate value of threat intelligence program.