Threat Intelligence Program, Mitigation M1019 - Enterprise

Archived: 2026-04-05 17:28:42 UTC

A Threat Intelligence Program enables organizations to proactively identify, analyze, and act on cyber threats by leveraging internal and external data sources. The program supports decision-making processes, prioritizes defenses, and improves incident response by delivering actionable intelligence tailored to the organization's risk profile and operational environment. This mitigation can be implemented through the following measures:

Establish a Threat Intelligence Team:

- Form a dedicated team or assign responsibility to existing security personnel to collect, analyze, and act on threat intelligence.

Define Intelligence Requirements:

- Identify the organization’s critical assets and focus intelligence gathering efforts on threats targeting these assets.

Leverage Internal and External Data Sources:

- Collect intelligence from internal sources such as logs, incidents, and alerts.
  Subscribe to external threat intelligence feeds, participate in ISACs, and monitor open-source intelligence (OSINT).

Implement Tools for Automation:

- Use threat intelligence platforms (TIPs) to automate the collection, enrichment, and dissemination of threat data.
- Integrate threat intelligence with SIEMs to correlate IOCs with internal events.

Analyze and Act on Intelligence:

- Use frameworks like MITRE ATT&CK to map intelligence to adversary TTPs.
- Prioritize defensive measures, such as patching vulnerabilities or deploying IOCs, based on analyzed threats.

Share and Collaborate:

- Share intelligence with industry peers through ISACs or threat-sharing platforms to enhance collective defense.

Evaluate and Update the Program:

- Regularly assess the effectiveness of the threat intelligence program.
- Update intelligence priorities and capabilities as new threats emerge.

Tools for Implementation

Threat Intelligence Platforms (TIPs):

- OpenCTI: An open-source platform for structuring and sharing threat intelligence.
- MISP: A threat intelligence sharing platform for sharing structured threat data.

Threat Intelligence Feeds:

- Open Threat Exchange (OTX): Provides free access to a large repository of threat intelligence.
- CIRCL OSINT Feed: A free source for IOCs and threat information.

Automation and Enrichment Tools:

- TheHive: An open-source incident response platform with threat intelligence integration.
- Yeti: A platform for managing and structuring knowledge about threats.

Analysis Frameworks:

- MITRE ATT&CK Navigator: A tool for mapping threat intelligence to adversary behaviors.
- Cuckoo Sandbox: Analyzes malware to extract behavioral indicators.

Community and Collaboration Tools:

- ISAC Memberships: Join industry-specific ISACs for intelligence sharing.
- Slack/Discord Channels: Participate in threat intelligence communities for real-time collaboration.
