Threat Analysis

Table of Contents

Threat Analysis

Threat Analysis

29

**029 Threat analysis is another component of the cyber intelligence conceptual framework.

Threat Analysis

- The assessment of technical telemetry (network and machine generated data) and non-technical data pertaining to specific threats to your organization and industry to inform cybersecurity operations/actions and Strategic Analysis.

- Threat Analysis tends to consist of:
  - **Tactical Analysis:** Analysis of specific threats, attacks, incidents, vulnerabilities, or unusual network activity that enhances decision making for network defenders, incident responders, and machines pertaining to cybersecurity and incident response
  - **Operational Analysis:** Analysis of specific **threats, threat actors,** and **threat actor campaigns, intentions, and capabilities** against an organization and its industry.

30

**030 In other words, data gathering usually leads to some form of analysis, where an analyst seeks to evaluate and estimate how a cyber threat impacts its target, based on the threat's technical complexities or characteristics. Threat analysis is the assessment of technical telemetry. In other words, that is network and machine-generated data, and non-technical data pertaining to specific threats to your organization and industry to inform cybersecurity operations or actions such as network defense, cyber hygiene, incident response, and also informs strategic analysis. Threat analysis is built on operational and tactical analysis and enhances a CSO or CISO in other mid- to senior-level decisionmakers' ability to make decisions.

Tactical analysis is analysis of specific threats, attacks, incidents, vulnerabilities, and unusual activity, network activity, that enhances decision making for network defenders, incident responders, and machines pertaining to cybersecurity and incident response.

The information analyzed is usually technical telemetry such as network and endpoint activity, atomic and behavioral and computed indicators such as malware samples, hash values, domains, IPs, logs, and email header information. Tactical analysis tends to answer specific intelligence requirements and immediate daily and weekly questions about what, where, when how regarding threats to your organization.

Operational analysis is analysis of specific threats, threat actors and threat actor campaigns. Their intentions and capabilities against an organization and its industry. Operational analysis tends to answer priority and specific requirements to enhance a CSO or CISOs and other mid- to senior-level decisionmakers' leadership decisions regarding non-immediate, but also near-term threats to business processes and cybersecurity decisions. These might be more weekly or quarterly type threat and questions that decisionmakers could be aware of.

Evaluating in Terms of Threat Analysis

- In evaluating the state of the practice of cyber intelligence in terms of Threat Analysis, we considered the following factors:

1. Threat Analysis Workflow
2. Timeliness and Accuracy of Threat Analysis
3. Diversity in Technical Disciplines
4. Traits, Core Competencies, and Skills
5. Threat Analysis Tools

31

**031 In evaluating in a state of practice of cyber intelligence in terms of threat analysis, we considered the following factors. Does an organization have a threat analysis workflow to understand, evaluate and assess threats and report that out to a decisionmaker? Is there a timeliness, an accuracy of that threat analysis? Does the organization have a diversity in technical disciplines of analysts that are looking at these threats? And what are the traits, core competencies and skills of these threat analysts? And lastly, does an organization have the right tools to be able to assist it with the type of threat analysis that it needs in order to do effective analysis on such threats?

Notices

This material is based upon work funded and supported by the Department of Homeland Security under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

DM20-0262