

What are Threat Assessments?

Objectives:

At the end of this episode, I will be able to:

Understand what a threat assessment is.

Explain the difference between threat correlation and threat contextualization.

Identify what threat intelligence is.

Define what threat attribution is.

External Resources:

Threat Assessment

What is a Threat Assessment?

The process of examining, filtering, transforming, and modeling of acquired threat data for extracting threat intelligence.

It is a process where the knowledge of internal and external threat information or vulnerabilities pertinent to a particular organization is matched to real-world attacks.

It enables the organization to predict, combat, and prevent possible threats to the organization.

Threat assessment allows the organizations to assess their current threat landscape by identifying flaws in their assets, the chances for exploitation using those flaws, and their origin.

Performing regular threat assessment to its infrastructure can allow an organization to protect its assets from evolving cyber threats.

What is Threat intelligence?

The collection and analysis of information about threats and adversaries and drawing patterns that provide an ability to make knowledgeable decisions for the preparedness, prevention, and response actions against various cyberattacks.

Helps an organization to identify and mitigate various business risks by converting unknown threats into known threats as well as focusing efforts on implementing various advanced and proactive defense strategies.

What is Threat contextualization?

The process of assessing the threats and their impacts in various conditions.

What is Threat correlation?

The process used by organizations to monitor, detect, and escalate various evolving threats from the organizational networks.

The main objective behind threat correlation is to reduce the false-positive alert rates and detect and escalate stealthy, complex attacks.

Threat correlation benefits the incident response teams, by helping them to focus on priority issues, reducing potential risk and corporate liabilities.

Commonly used correlation techniques:

- Relating multiple incident types and sources across multiple nodes
- Incident sequence
- Incident persistence
- Incident-directed data collection

What is Threat attribution?

The process of identifying the actors behind an attack, their goals and motives along with the sponsors, as well as analyzing the threats to identify the indicators of compromise (IoCs) and derive useful threat intelligence.