TALENTO TECH

REGIÓN 3

CAUCA - NARIÑO

LESSON 2 -UNIT 2

TIC

Universidad Tecnológica de Pereira

faceIT

Lesson 2 Reading

INCIDENT RESPONSE FUNDAMENTALS

A computer security incident is any real or suspected adverse event related to the security of your system or computer networks (Choi, 2020). One of the strong dimensions of security is resilience, which allows us to identify, detect, prevent, and react to technological or process failure with the purpose of avoiding or minimizing the damage originating from service failure (Nogueira et al., 2009).

A security incident can be defined as the result of a network or host activity that threatens the security of an existing computer system. Each organization will need to define what a computer security incident represents for their site and its structure.

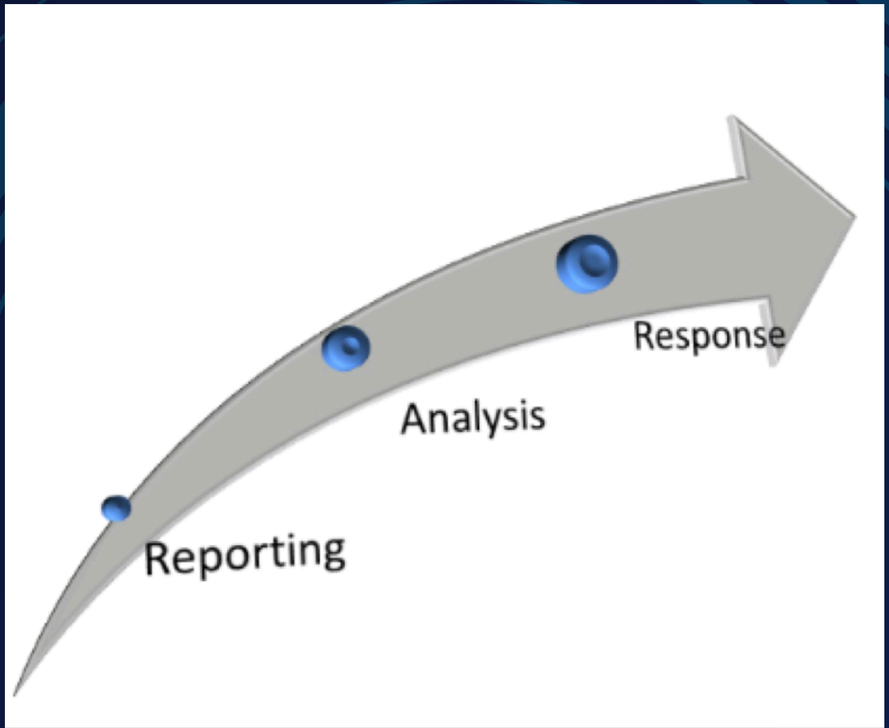
Examples of incidents include the following activities:

- Attempts to gain unauthorized access to a system or to data from this system (Shulman & Waidner, 2014);
- Unwanted disruption or refusal of service (Hacks, Katsikeas, Ling et al., 2020);

Unauthorized use of the system to process some data changes to system hardware, or software features without the knowledge of the owner of this system (Morikawa & Yamaoka, 2011);

• When a security incident is reported to an organization's customer site, the organization must handle the incident responsibly (Noel etal., 2009).
Signs of an incident can fall into one of two categories:
• Precursors;
• Indicators.

A precursor is considered to be a sign that an incident regarding the system may occur in the future. An indicator is considered to be a sign that an incident has occurred or may occur on the system at this time.
Most possible attacks that can be realized do not have identifiable or detectable signs or precursors from a target perspective. If some precursors are detected in time, the organization may have the opportunity to organize and to prevent the incident by changing its security position to save an attack target (Paja, Dalpiaz, & Giorgini, 2015).
At the very least, the organization could monitor more closely the activity involving the target (Ferrillo, 2015).



Incident handling includes three functions:

- incident reporting;
- incident analysis;
- incident response.

The incident reporting feature allows a CERT to serve as a central point of contact for reporting local issues.

This allows all incident reports and activity to be collected at the location where the information can be reviewed and correlated within the parent organization or constituency.

This information can then be used to determine intruder activity trends and patterns and to recommend appropriate prevention strategies for the entire constituency.

The other part of the incident analysis involves a detailed analysis of the incident report or activity to determine the purpose, priority and threat of the incident, as well as research into possible response and mitigation strategies.

A CERT may send recommendations for recovery, retention, and prevention to constituents or systems and network administrators on sites that then perform the response steps themselves.
A CERT can also perform these steps on the affected systems.
The response may also involve the exchange of information and lessons learned with other response teams and other appropriate organizations and sites.

TIC

TALENTO TECH

Universidad Tecnológica de Pereira

faceIT