12.1.4 Incident Response Frameworks and Management Facts

This lesson covers the following topics:

- Attack frameworks
- Stakeholder management
- Internal policies

Attack Frameworks

There are a few frameworks you can utilize for incident response. The table below describes three.

Framework	Description
MITRE ATT@CK	MITRE ATT@CK is a universally accessible database. This database contains techniques, tactics and other operational information about malicious actors. This data has been gathered and aggregated using empirical observations. All of this data are available to anyone for free.
Diamond Model of Intrusion Analysis	The Diamond Model has four points; adversary, victim, capabilities and infrastructure. There is always a direct connection between adversary and victim. There is also a direct connection between capabilities and infrastructure. The way this model is used is very much up to the security analyst. Normally the analysts and first responders use these points (called meta or core features) to find and predict attacks. For example, by identifying the types of victims and why they were attacked, the analyst/first responder can make an educated guess as to who is behind the attack and who are potential victims. This information can then be used to compare information in the MITRE ATT@CK database. Since there are always unknowns, the database helps to fill in some of the unknowns.
Cyber Kill Chain	The Cyber Kill Chain was developed by Lockheed Martin to identify and provide visibility of the hurdles a malicious actor must overcome to achieve the objective to exploit or attack. This makes the malicious actor's moves highly visible to a first responder or security analyst and is valuable in the defense of assets. The following seven steps of an attack help a security analyst to identify the phases of an attack in progress. ▪ Reconnaissance ▪ Weaponization delivery ▪ Delivery ▪ Exploitation ▪ Installation ▪ Command and control ▪ Action on objectives

Stakeholder Management

You might use a table to organize communication pathways with stakeholders. The table should use the proper html class attributes. The header row of the table should use class=header. At least one paragraph should be included before the table.

Communication	Description

Target	
Internal stakeholders	Maintain an open dialogue with all internal departments about development, implementation, testing, etc., of incident response.
C level executives	Keep incident response awareness a priority with C level executives. Their support will help to garner support from other employees.
Communicate with business unit managers	Keep open lines of communication with unit managers. Be willing to accept their input. These are the people you will work with the most.

Internal Policies

Your company should have internal policies in place to handle incidents and respond to them appropriately. The following table describes a few of these policies.

Policy	Description
Communication plan	A plan to effectively communicate important company information in the case of an emergency.
Disaster recovery plan	A documented plan of policies and procedures that are executed in the event of a disruption of business.
Business continuity plan	More detailed and longer than the disaster recover plan, the business continuity plan has procedures and policies for each business unit. The policies and procedures are written by each business unit with guidelines from corporate management. This document includes organization charts, phone lists, order of restore, and vendor contact information.
Incident response team charter	A document that describes the creation and function of a specialized team trained to identify malicious actions against a network. The charter documents the funding, reporting hierarchy, authority, and responsibility of the team designated to stop an attack, investigate incidents, and collect evidence.