Chapter 14 - Key Terms

Term	Page	Description
Diamond Model of Intrusion	580	A model representing the steps taken by an adversary to accomplish an intrusion.
security incident	587	A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.
adversary	577	An attacker, hacktivist, disgruntled employee, and so on.
metadata	584	Data about data, such as who created a file and the last time it was opened.
Cyber Kill Chain Model	580	A model representing the steps taken by an adversary to accomplish an intrusion.
reconnaissance	586	Research on a target, such as available network ports, data on social media sources, learning about people at an organization, and so on.
weaponization	589	The process of developing and testing how an attack will be executed.
delivery	580	The stage in the cyber kill chain where an attacker sends a malicious payload through email, transferring across a network, or physically plugging in a device on the affected system.
exploitation	581	A process that involves attacking a weakness or vulnerability within a system, application, network, and so on.
installation	583	In terms of the kill chain, what is delivered by a successful exploitation. Examples might be ransomware and remote-access tools.
command & control (C2 or CnC)	579	Software that an attacker could use to manipulate (control) a compromised system by sending commands to perform different actions, such as performing denial of service (DoS) attacks, compromising other systems, exfiltrating data, and more.
incident response	583	The process and tools that defenders use to respond to a cybersecurity incident.

Term	Page	Description
ATT&CK	578	A framework developed and maintained by MITRE that provides a collection of matrices of adversarial tactics and techniques.
PRE-ATT&CK	586	An elemental part of the ATT&CK framework developed and maintained by MITRE. PRE-ATT&CK is used to document the tactics and techniques used by real-world adversaries before they compromise a system or a network. You can obtain information about the MITRE ATT&CK framework and PRE-ATT&CK at https://attack.mitre.org.
Untitled		