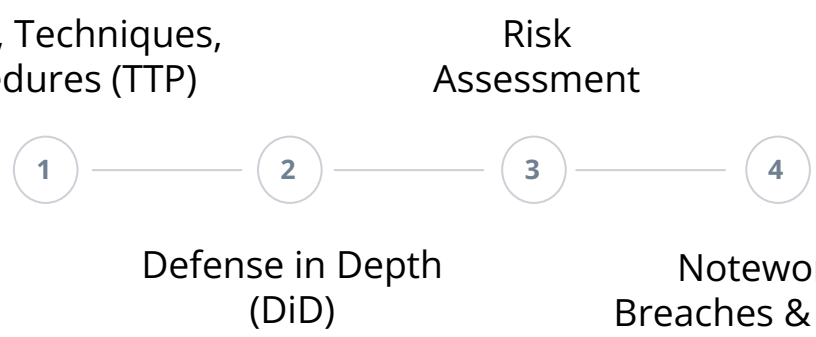
CYBERSECURITY PROFESSIONAL PROGRAM

Introductory Course

Threats & Threat Actors

Threats & Threat Actors

Module Path



Module Objectives

By the end of the lesson, you will have the opportunity to learn and develop the following skills:

- Identify key components of a threat modeling process.
- Assess different angles and perspectives of possible cyber security breaches.
- Apply the threat modeling process against noteworthy breaches.

Threats & Threat Actors

Tactics, Techniques, Procedures (TTP)

By the end of the lesson, you will have the opportunity to learn and develop the following skills:

1. Identify a threat.
2. Outline blue team and red team mitigation within the context of previously discussed frameworks.
3. Explain mitigation and strengthen cybersecurity posture based on outcomes.

What Is Threat Modeling (TM)?

- A set of activities for improving security
- Uncovers design flaws in the context of security

> NIST (n.d.) defines threat modeling as a form of risk assessment that simulates aspects of the attack and defense sides of a logical entity, such as a piece of data, an application, a host, a system, a network, or an environment.

Threat Actors

- **Cybercriminals**: These threat actors intend to steal data or use ransomware to make data inaccessible.
- **Insider Threat**: Employees, contractors, or partners may compromise an organization's data or key processes.
- **Nation-States**: Countries who target companies or institutions to steal data or impede a government function.

Threat Classification via STRIDE

Type	Description	Security Control
Spoofing	Threat action aimed at accessing and using another user's credentials, such as username and password	Authentication
Tampering	Threat action intending to maliciously change or modify persistent data, such as records in a database, and the alteration of data in transit between two computers over an open network, such as the internet	Integrity
Repudiation	Threat action intends to perform an illegal or malicious action in a system and denies involvement.	Non-Repudiation

(Conklin, Drake, n.d.)

Threat Classification via STRIDE

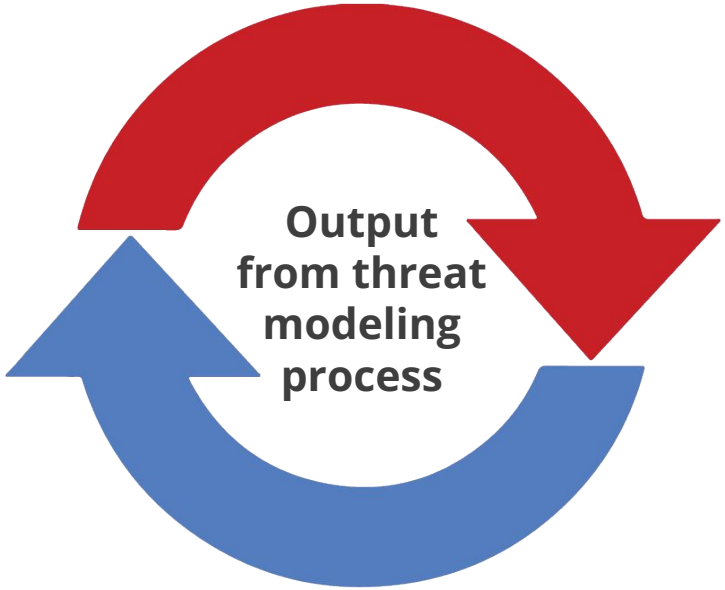
Type	Description	Security Control
Information Disclosure	Threat action intending to read a file that one was not granted access to, or to read data in transit.	Confidentiality
Denial of Service	Threat action attempts to deny access to valid users, such as by making a web server temporarily unavailable or unusable.	Availability
Elevation of Privilege	Threat action intending to gain privileged access to resources to gain unauthorized access to information or to compromise a system.	Authorization

(Conklin, Drake, n.d.)

Threat Modeling: Blue & Red Team Uses

BLUE TEAM

Selecting appropriate controls

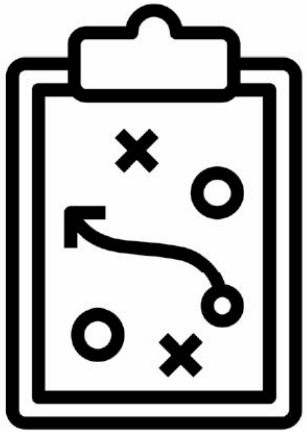


RED TEAM

Replicating attack to understand impact

Tactics, Techniques, and Procedures

Tactics, techniques, and procedures used by threat actors to compromise a target



Tactics, Techniques, and Procedures

- **TACTICS**

Represent the *why* of a technique and describe what an adversary is trying to accomplish

- **TECHNIQUES**

Represent *how* the threat actor achieves a tactical objective; actions that lead up to the tactic

- **PROCEDURES**

Represent the detailed steps or how the technique is applied to execute the attack

(NIST Special Publication 800-150, 2016)

Lab IC-08-L1

Colonial Pipeline Breach| 10–15 minutes

Mission

In this practice, you are required to conduct research and answer questions regarding the Colonial Pipeline information security breach.

Steps

- Follow lab prompts in TDX Arena.
- Participate in the follow-up discussion.

ACCESSING THE LAB

- TDX-Arena Colonial Pipeline Breach Lab Link
- Note: The lab module in Canvas also contains a link that will direct you to TDX Arena.

RELATED FILE

- Lab Document IC-08-L1

Defense in Depth (DiD)

By the end of the lesson, you will have the opportunity to learn and develop the following skills:

1. Discuss the importance of security.
2. Assess the different angles and perspectives of possible attacks.

Why Is Defense Important?

- Prevents unauthorized access
- Keeps personal information safe
- Keeps organizational information safe
- Prevents data loss and leakage

From: Freepik on Flaticon (accessed 3/2022)

Personal Defense and Cyber Hygiene

- Many people save valuable data in digital format.
- Data can be saved on computers, phones, and many other devices.
- Any device that is left alone or that is connected to a network can be hacked.

From: Freepik on Flaticon (accessed 3/2022)

Organizational Defense

- Every organization stores data in various ways.
- Encrypted, stolen, or leaked data can lead to significant damage.
- Organizations may also store sensitive client information.

From: Flaticon (accessed 3/2022)

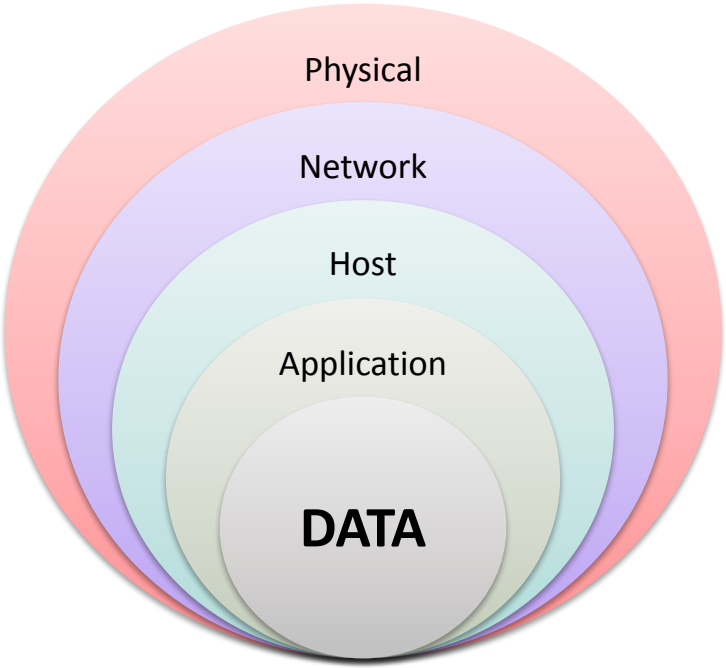
Defense Best Practices

Guidelines
Many manufacturers of systems and devices provide best practices for security.

Suggestions
Password strength, security feature implementations, backups, and more

From: Flaticon (accessed 10/6/22)

Defense in Depth (DiD)



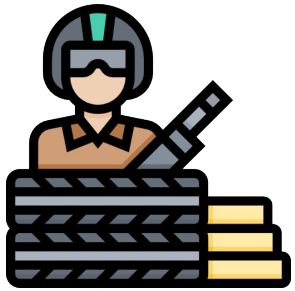
From: ThriveDX

Physical Controls

- Implement physical security measures, such as fences, CCTV, doors, security guards, etc.
- Prevent physical, unrestricted access to important systems.

From: Flaticon (accessed 3/2022)

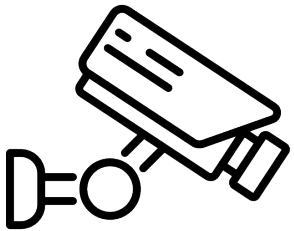
Security Guards



- Manage access points and verify the identity of individuals
- Managing visitor registration and escorting guests to designated areas
- Respond to security incidents, minimizing the impact and providing immediate assistance

From Flaticon.com (accessed 10/7/22)

CCTV



- Visible CCTV cameras acts as a deterrent for potential intruders.
- CCTV footage can be reviewed in case of security incidents
- Utilize advanced technology to enable real-time remote monitoring

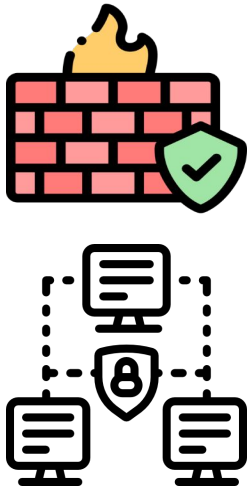
From: Flaticon.com (accessed 10/7/22)

Technical Controls

- Implement software and hardware protection, including firewalls, antivirus software, and others
- Prevent unauthorized network access

From: Flaticon (accessed 3/2022)

Firewalls



- A hardware appliance or software implementation designed to protect one network from another
- Secures traffic between trusted internal networks and untrusted external networks
- Used to filter specific traffic between trusted networks
- Can be in the form of software or a physical device

From Flaticon.com (accessed 10/7/22)

Antivirus

- Protects against malware
- Can detect, remove, and prevent malware
- Implements identification based on multiple parameters
- Signature-based, heuristics, and real-time

From: Flaticon.com (accessed 10/7/22)

IDS and IPS

Intrusion Detection System (IDS)
Monitors activity on a network or system and reports any suspicious behavior or violation

Intrusion Prevention System (IPS)
In addition to IDS features, IPS also prevents malicious activity.

From: Flaticon (accessed 4/29/23)

Administrative Controls

- Implement policies and security awareness
- Configure access permissions and guidelines
- Prevent human errors that may lead to breaches

From: Flaticon (accessed 3/2022)

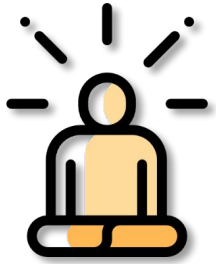
Security Policies

- Configure rules for permitted user activity
- Define permissions and restrictions
- Can be configured to log user activity
- A common use of policies is for device control, which restricts the use of CDs, USBs, etc

From: Flaticon.com (accessed 10/7/22)

Security Awareness

- Getting users to pay attention to possible cyber threats
- Demonstrate what a threat looks like and what actions can be taken against it.
- Minimize the chances for human error



From: Flaticon (accessed 3/2022)

Controls Summary

Control	Example	Use Case
Physical	Fences	Deters access
Physical	Door	Controls access
Physical	Security guard	Reporting and responding
Technical	Antivirus	Detects and prevents malware
Technical	Web filtering	Prevents website access
Administrative	Security policy	Informs behavior

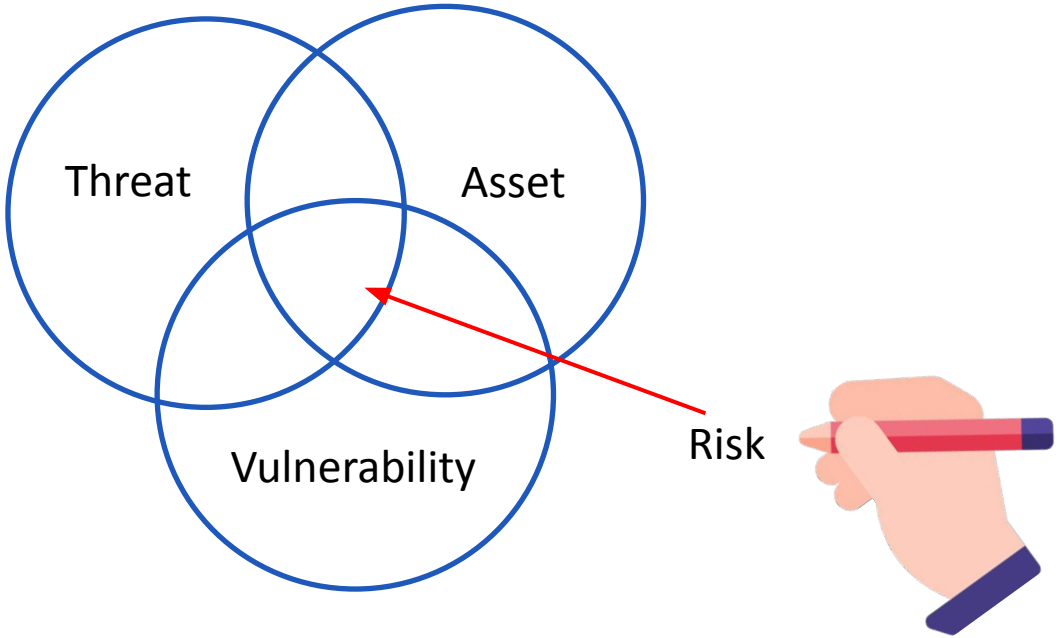
Risk Assessment

By the end of the lesson, you will have the opportunity to learn and develop the following skills:

1. Understand risk assessment terminology.

Risk Determination

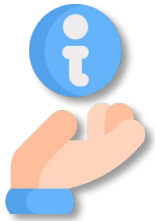
- Affected by the asset, vulnerability, and threat
- Its level is determined with the combined calculation of the three terms.



From: ThriveDX

Assets

Physical Assets



Information Assets

Human Assets

Reputation Assets

From: Flaticon (accessed 8/22/22)

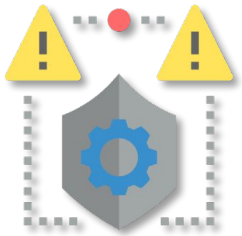
Vulnerability

- Possible security flaw
- Can be in software or hardware
- Can be exploited by an attacker
- Can lead to unauthorized network, system, and application access

From: Flaticon (accessed 3/2022)

Vulnerabilities vs. Mitigation

Vulnerabilities
Flaws in a system that could be potentially exploited by an attacker



Mitigation
Processes on a system that try to identify potential vulnerabilities and fix them

From: Flaticon (accessed 4/29/23)

Discussion

Who is threatening the assets?

Why are they a threat?

How can they impact vulnerabilities in assets?

Threats & Threat Actors

Noteworthy Breaches & Attacks

By the end of this lesson, you will have the opportunity to learn and develop the following skills:

1. Identify the tactics, techniques, and procedures (TTPs) of specific notable breaches.

Activity

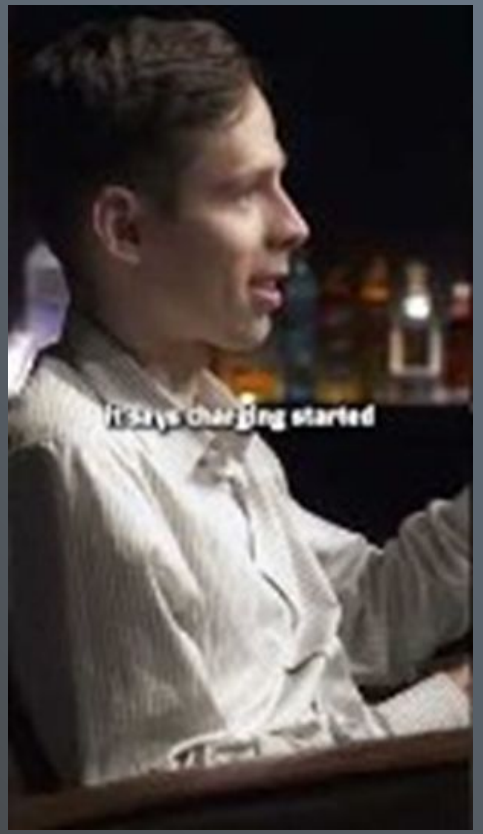
Ethical hacker "Spying through electronics" (Video) |1 minutes

Mission

Watch video titled “Spying through electronics.”

Learning Outcomes

Recognize the potential for privacy harm as private and sensitive information can inadvertently become exposed.



From: @elitecut(accessed 7/9/23)

Discussion

Do you also have such appliances at home?

Activity

Video: Target Stores Data Breach | 3 minutes

Mission

Watch the video titled Target Stores Data Breach.

Learning Outcomes

Gain insight into the Target security breach.

From: YouTube (accessed 03/30/ 2023)

Video with closed captions

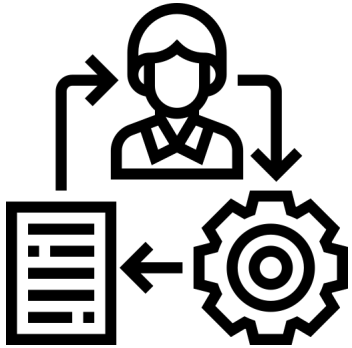
Target Breach TTPs

Tactics:

- Exfiltration, Tactic TA0010 - Enterprise | MITRE ATT&CK®
    - Gain access to Target's customers' PII.

Techniques:

- OS Credential Dumping: LSASS Memory, Sub-technique T1003.001 - Enterprise | MITRE ATT&CK®
- Additional techniques used throughout the breach:
    - Compromise a third-party vendor.
    - Access vendor portal.
    - Gain control of the servers.
    - Access point-of-sale systems.



From: Flaticon (accessed 4/29/22)

Target Breach TTPs

Procedures:

- Reconnaissance of Target, identifying vendor portal vulnerability and vendors likely to have poor cyber hygiene.
- Phishing campaign to HVAC vendor gets access credentials to vendor portal via Trojan.
- Pivot from portal to access Target's servers.
- Pivot from servers to access point-of-sale (POS) systems.
- Install malware.
- Perform memory scraping.
- Intercept cardholder information.

Target Breach TTPs: Mitigation

- **User account control and account use policies**
  - Implemented login lockouts, timeouts, multi-factor authentication
  - Implemented system configurations that restrict elevated process/application access
- **Password policies**
  - Began setting and enforcing secure password policies for user accounts
- **Network segmentation**
  - Designed network to isolate critical functions, systems, and resources
  - Limited public-facing applications' network access through a DMZ

Lab IC-08-L2

Data Center Attack | 30 minutes

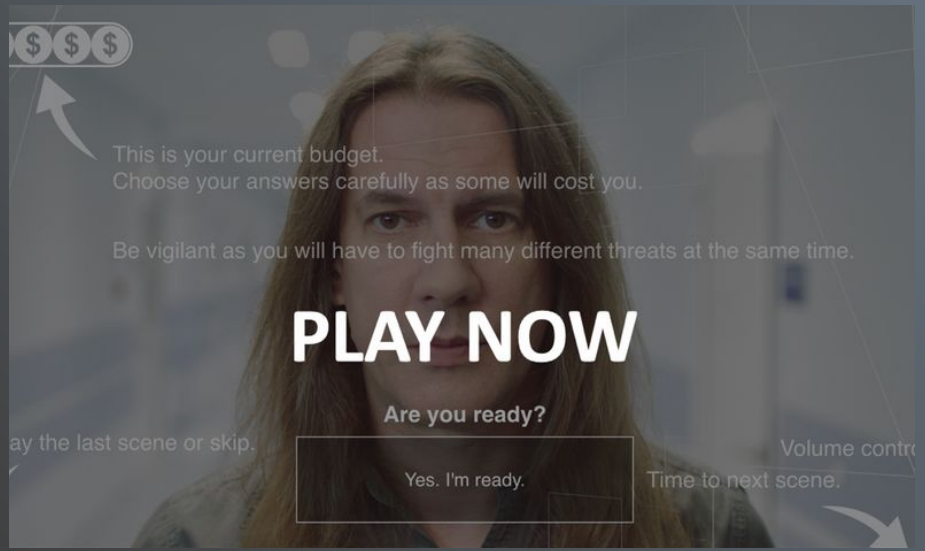
Mission
Access game and choose the most accurate answer base on the learned material.

Your goal is to go back in time and stop a crippling data centre attack.

Make the wrong choices and history repeats itself, but the right choices will show you the magic of DevSecOps and keep the hospital running smoothly.

ACCESSING THE LAB

- Access the link and press start.
- Chose the most accurate answer



Extra Practice

Cybersecurity Breach Research

Mission

Research a cyber-related breach and identify tactics, techniques, and procedures.

Learning Outcomes

Learn how to apply the threat modeling process to a cybersecurity breach.

ENVIRONMENT AND TOOLS

- IC-08 Cybersecurity Breach Research Practice document

Module Summary

In this module, the following topics were discussed:

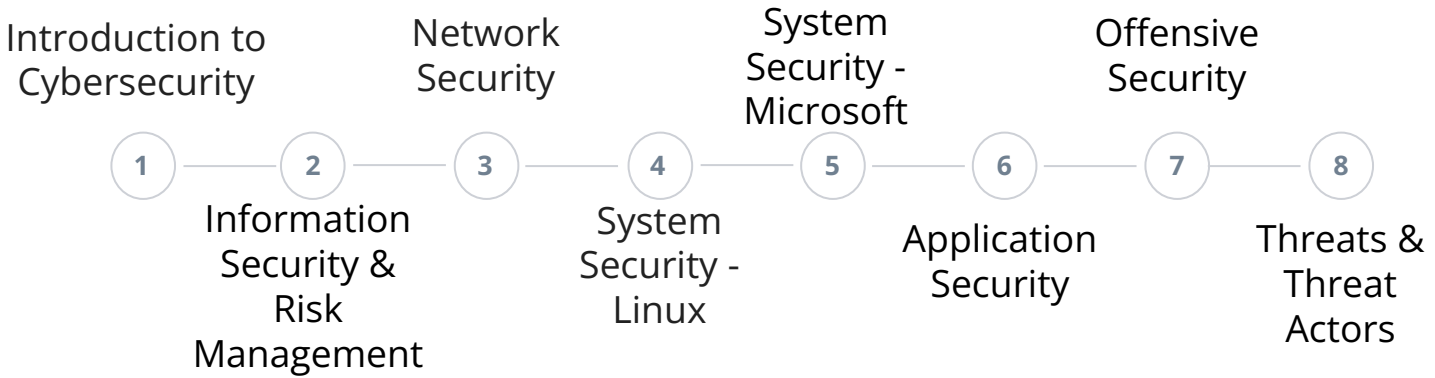
Key Takeaway #1

Identify key components of a threat modeling process.

Key Takeaway #2

Apply the threat modeling process against noteworthy breaches.

Before The End



THANK YOU

Questions? Thoughts? Concerns?