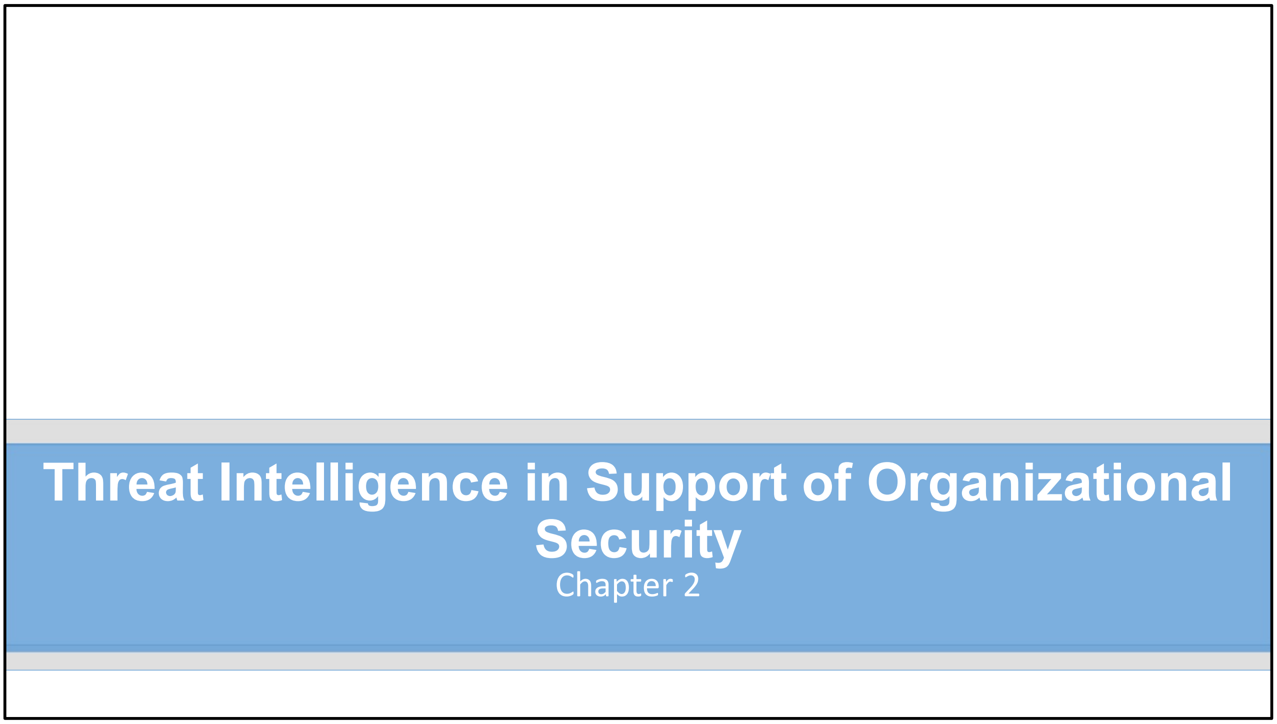


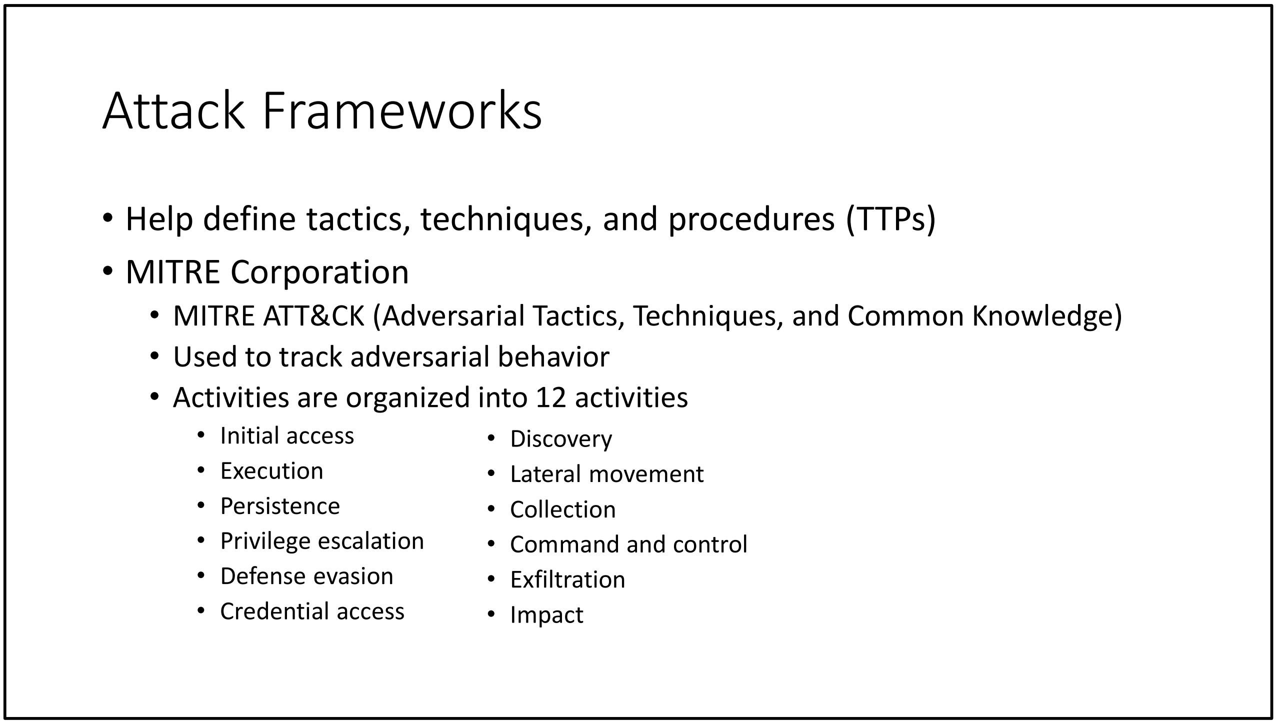
Threat Intelligence in Support of Organizational Security

Chapter 2

Episode 2.01

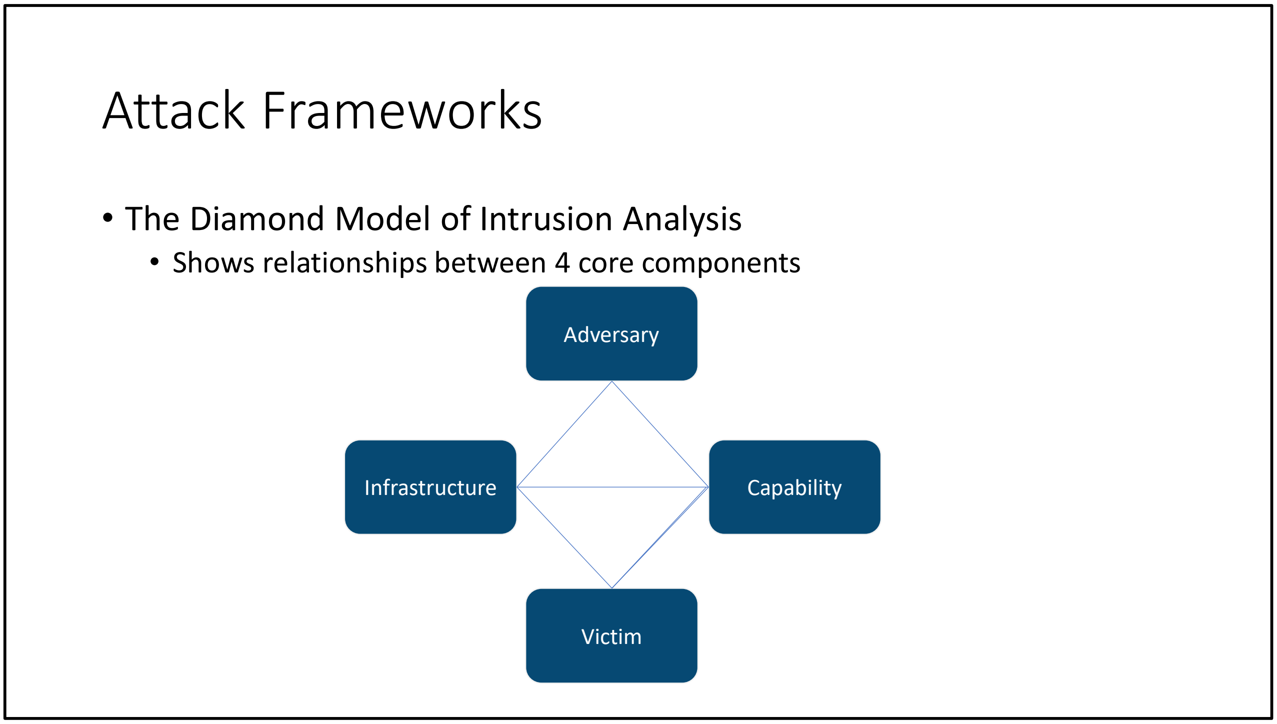
Attack Frameworks

Objective 1.2 Given a scenario, utilize threat intelligence to support organizational security.
• Attack frameworks
- MITRE ATT&CK
- The Diamond Model of Intrusion Analysis
- Kill chain



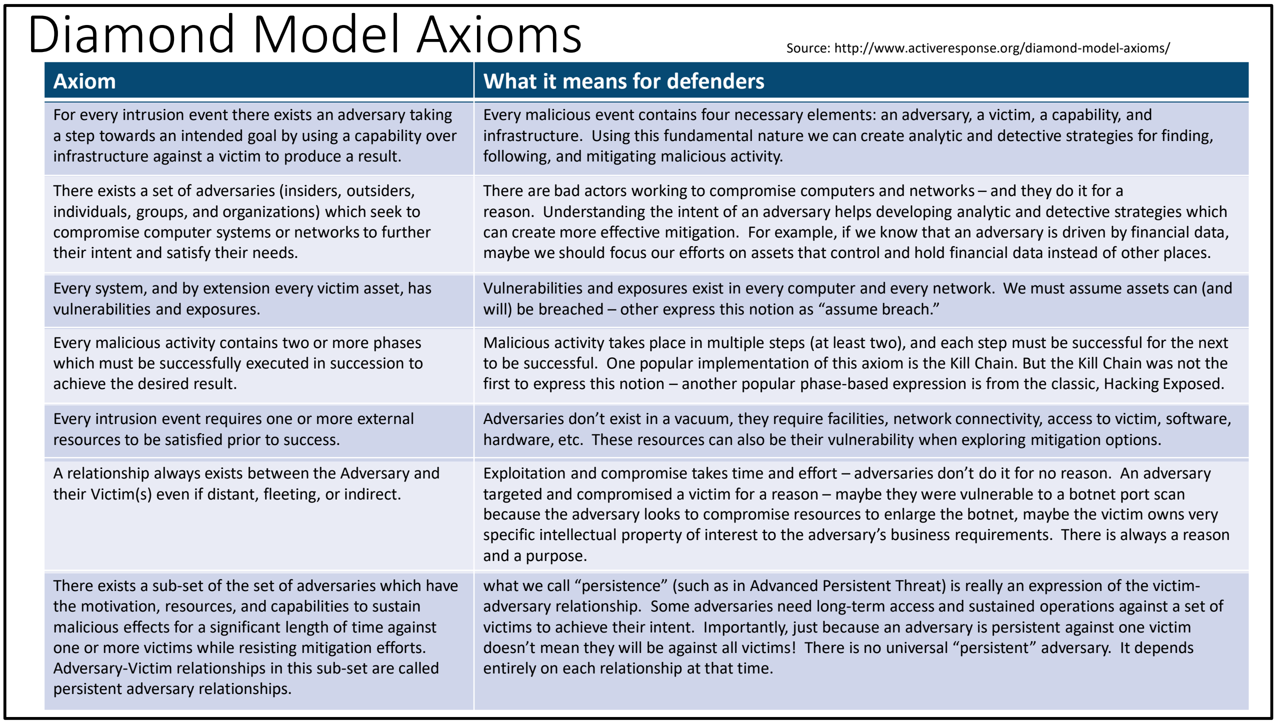
Attack Frameworks

- Help define tactics, techniques, and procedures (TTPs)
- MITRE Corporation
  - MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge)
  - Used to track adversarial behavior
  - Activities are organized into 12 activities
    - Initial access
    - Execution
    - Persistence
    - Privilege escalation
    - Defense evasion
    - Credential access
    - Discovery
    - Lateral movement
    - Collection
    - Command and control
    - Exfiltration
    - Impact



Attack Frameworks

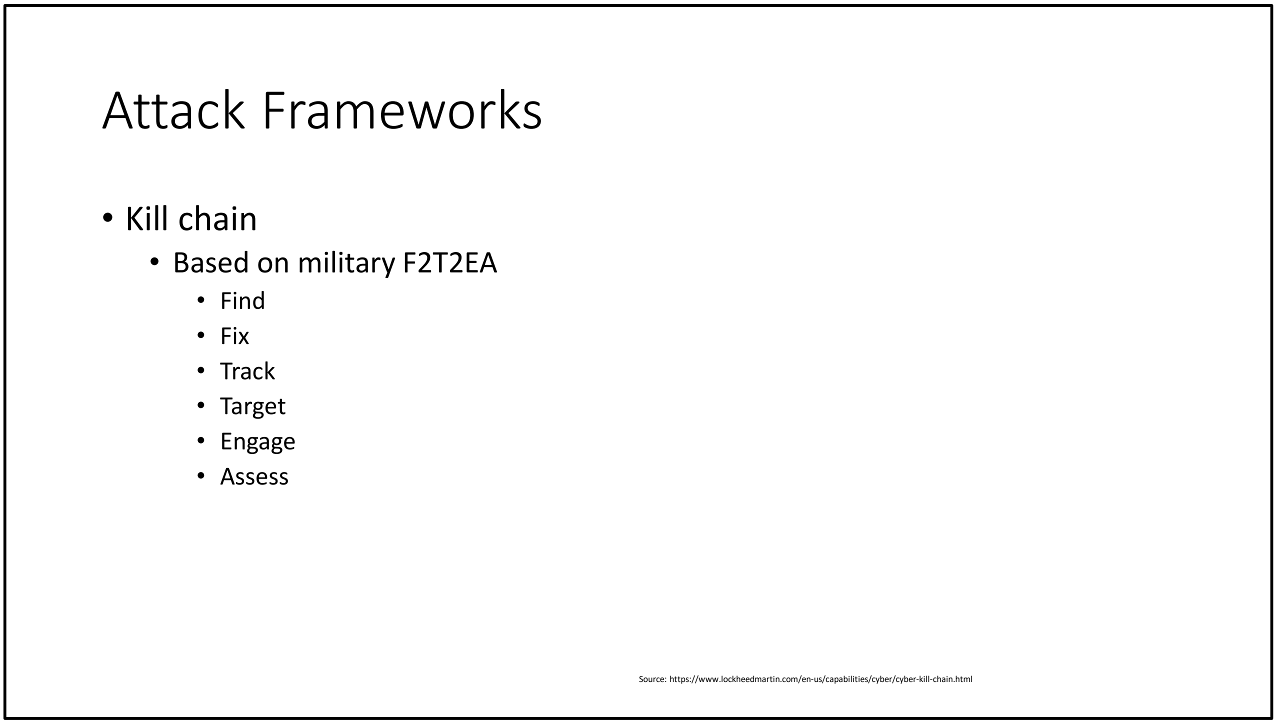
- The Diamond Model of Intrusion Analysis
  - Shows relationships between 4 core components



Diamond Model Axioms

Source: http://www.activeresponse.org/diamond-model-axioms/

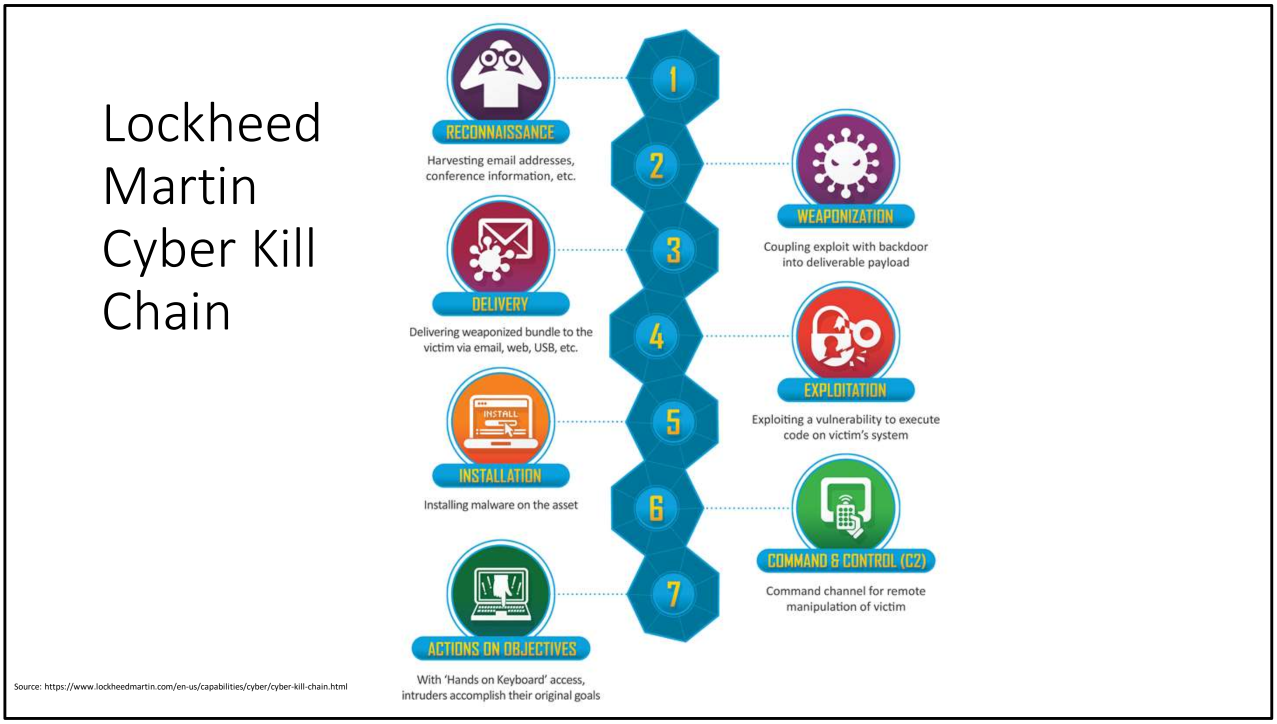
Axiom	What it means for defenders
For every intrusion event there exists an adversary taking a step towards an intended goal by using a capability over infrastructure against a victim to produce a result.	Every malicious event contains four necessary elements: an adversary, a victim, a capability, and infrastructure. Using this fundamental nature we can create analytic and detective strategies for finding, following, and mitigating malicious activity.
There exists a set of adversaries (insiders, outsiders, individuals, groups, and organizations) which seek to compromise computer systems or networks to further their intent and satisfy their needs.	There are bad actors working to compromise computers and networks – and they do it for a reason. Understanding the intent of an adversary helps developing analytic and detective strategies which can create more effective mitigation. For example, if we know that an adversary is driven by financial data, maybe we should focus our efforts on assets that control and hold financial data instead of other places.
Every system, and by extension every victim asset, has vulnerabilities and exposures.	Vulnerabilities and exposures exist in every computer and every network. We must assume assets can (and will) be breached – other express this notion as "assume breach."
Every malicious activity contains two or more phases which must be successfully executed in succession to achieve the desired result.	Malicious activity takes place in multiple steps (at least two), and each step must be successful for the next to be successful. One popular implementation of this axiom is the Kill Chain. But the Kill Chain was not the first to express this notion – another popular phase-based expression is from the classic, Hacking Exposed.
Every intrusion event requires one or more external resources to be satisfied prior to success.	Adversaries don't exist in a vacuum, they require facilities, network connectivity, access to victim, software, hardware, etc. These resources can also be their vulnerability when exploring mitigation options.
A relationship always exists between the Adversary and their Victim(s) even if distant, fleeting, or indirect.	Exploitation and compromise takes time and effort – adversaries don't do it for no reason. An adversary targeted and compromised a victim for a reason – maybe they were vulnerable to a botnet port scan because the adversary looks to compromise resources to enlarge the botnet, maybe the victim owns very specific intellectual property of interest to the adversary's business requirements. There is always a reason and a purpose.
There exists a sub-set of the set of adversaries which have the motivation, resources, and capabilities to sustain malicious effects for a significant length of time against one or more victims while resisting mitigation efforts. Adversary-Victim relationships in this sub-set are called persistent adversary relationships.	what we call "persistence" (such as in Advanced Persistent Threat) is really an expression of the victim-adversary relationship. Some adversaries need long-term access and sustained operations against a set of victims to achieve their intent. Importantly, just because an adversary is persistent against one victim doesn't mean they will be against all victims! There is no universal "persistent" adversary. It depends entirely on each relationship at that time.



Attack Frameworks

- Kill chain
  - Based on military F2T2EA
    - Find
    - Fix
    - Track
    - Target
    - Engage
    - Assess

Source: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html



Lockheed Martin Cyber Kill Chain

1. RECONNAISSANCE
   Harvesting email addresses, conference information, etc.
2. WEAPONIZATION
   Coupling exploit with backdoor into deliverable payload
3. DELIVERY
   Delivering weaponized bundle to the victim via email, web, USB, etc.
4. EXPLOITATION
   Exploiting a vulnerability to execute code on victim's system
5. INSTALLATION
   Installing malware on the asset
6. COMMAND & CONTROL (C2)
   Command channel for remote manipulation of victim
7. ACTIONS ON OBJECTIVES
   With 'Hands on Keyboard' access, intruders accomplish their original goals

Source: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Episode 2.02

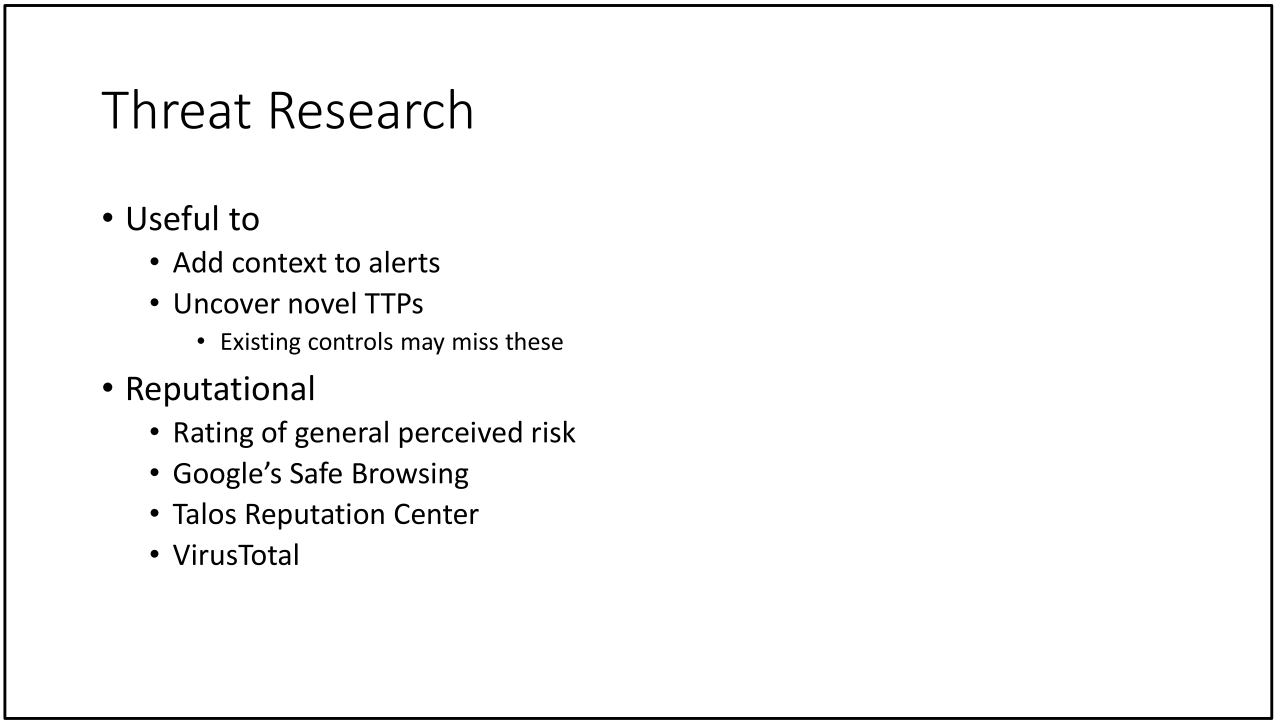
Threat Research

Objective 1.2 Given a scenario, utilize threat intelligence to support organizational security.

- Threat research
- Reputational
- Behavioral
- Indicator of compromise (IoC)
- Common vulnerability scoring system (CVSS)

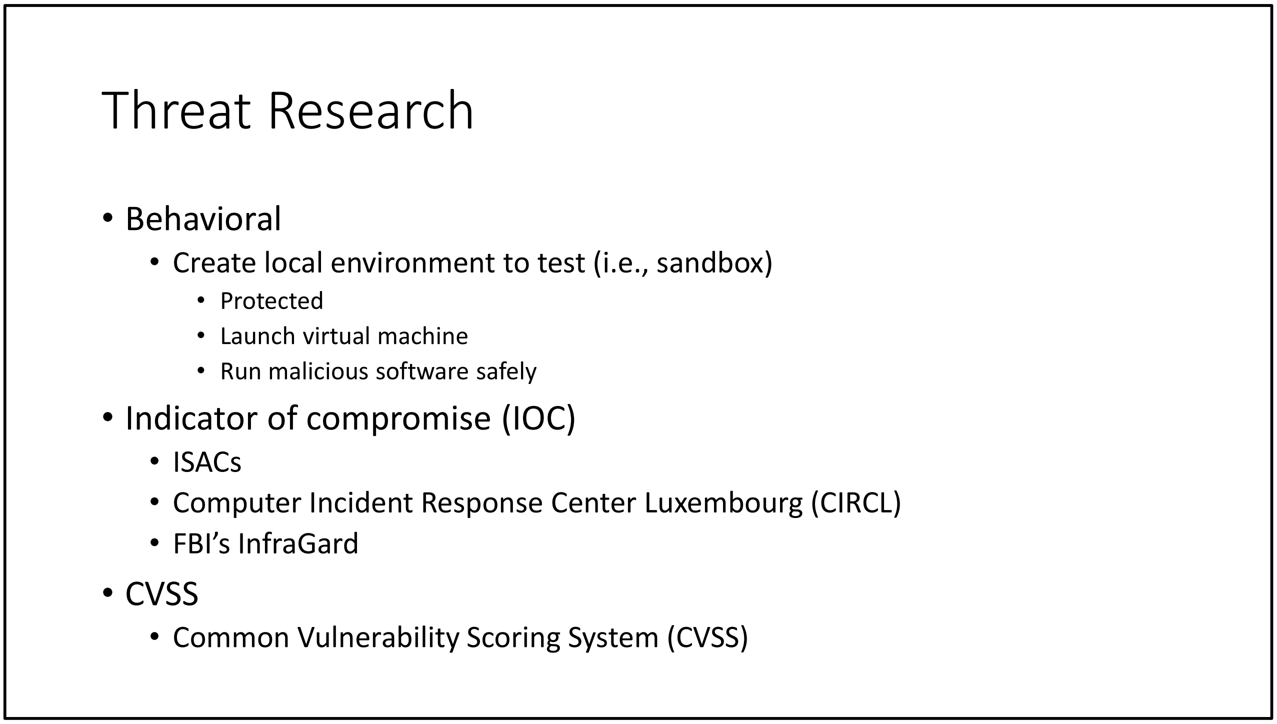
Objective 3.2 Given a scenario, implement configuration changes to existing controls to improve security.

- Sandboxing



Threat Research

- Useful to
  - Add context to alerts
  - Uncover novel TTPs
    - Existing controls may miss these
- Reputational
  - Rating of general perceived risk
  - Google’s Safe Browsing
  - Talos Reputation Center
  - VirusTotal



Threat Research

- Behavioral
  - Create local environment to test (i.e., sandbox)
    - Protected
    - Launch virtual machine
    - Run malicious software safely
- Indicator of compromise (IOC)
  - ISACs
  - Computer Incident Response Center Luxembourg (CIRCL)
  - FBI’s InfraGard
- CVSS
  - Common Vulnerability Scoring System (CVSS)

Episode 2.03

Threat Modeling and Intelligence Sharing

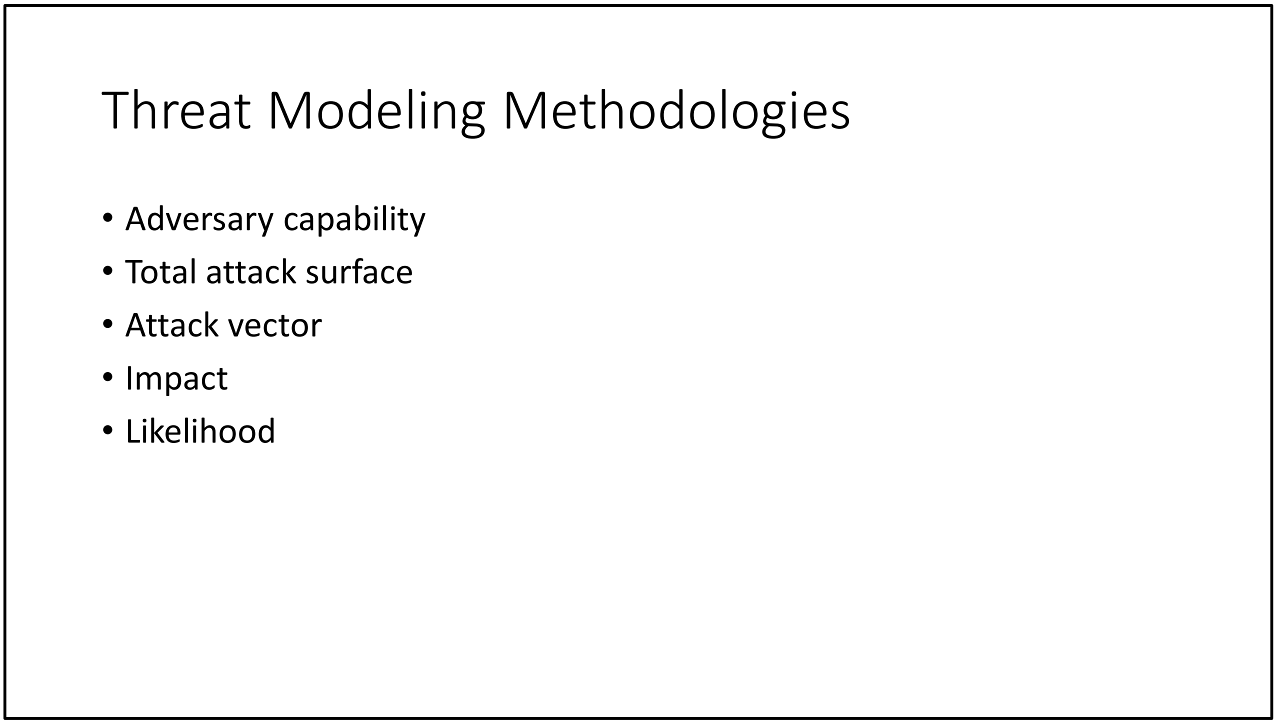
Objective 1.2 Given a scenario, utilize threat intelligence to support organizational security.

- Threat modeling methodologies

- Adversary capability
- Total attack surface
- Attack vector
- Impact
- Likelihood

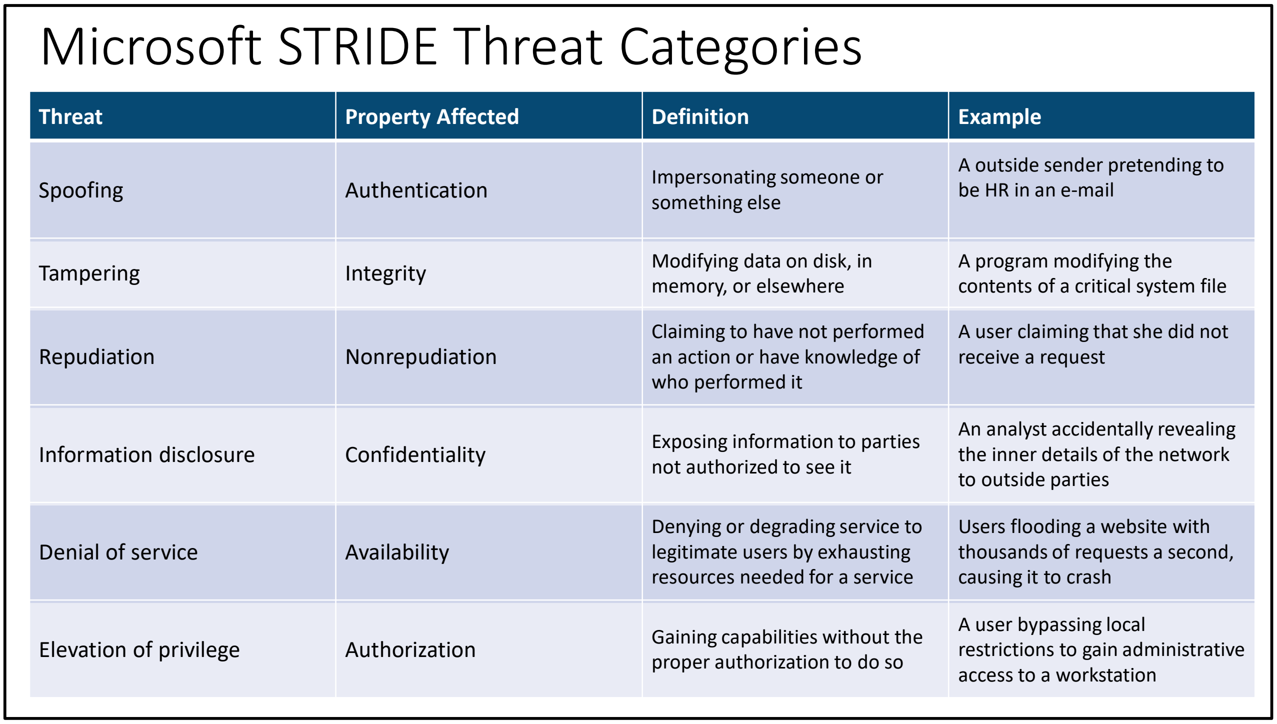
- Threat intelligence sharing with supported functions

- Incident response
- Vulnerability management
- Risk management
- Security engineering
- Detection and monitoring



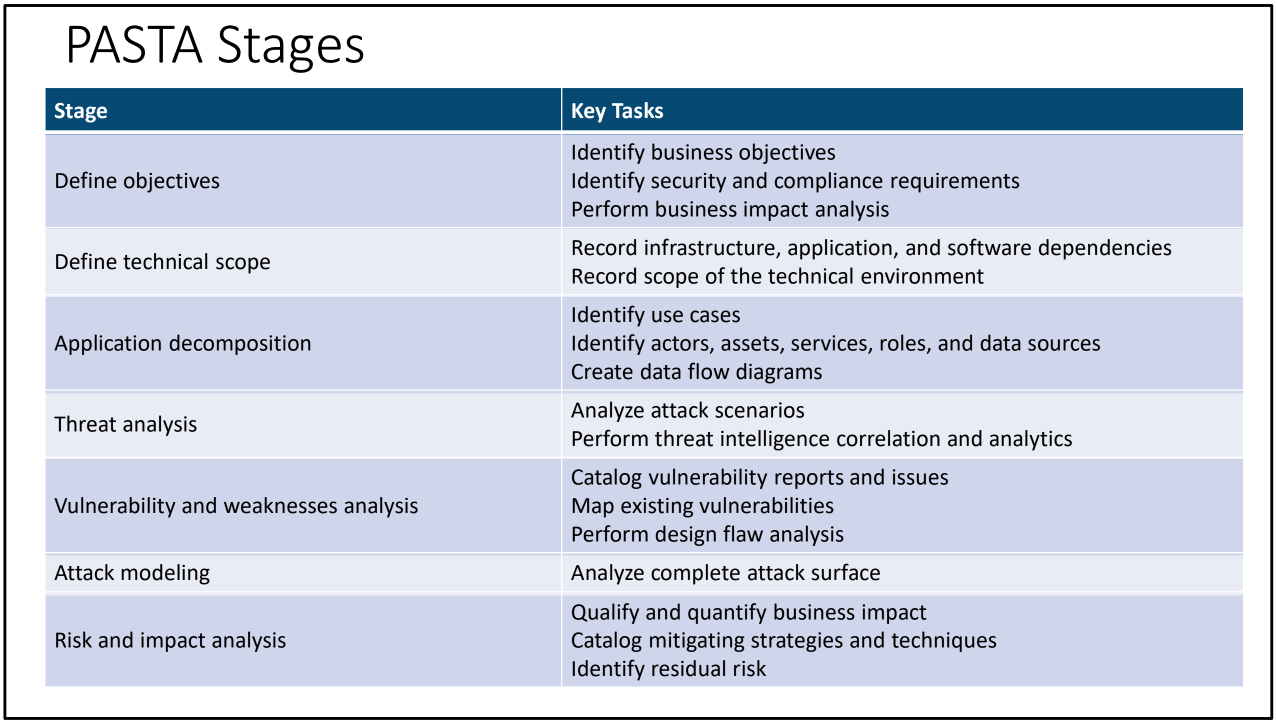
Threat Modeling Methodologies

- Adversary capability
- Total attack surface
- Attack vector
- Impact
- Likelihood



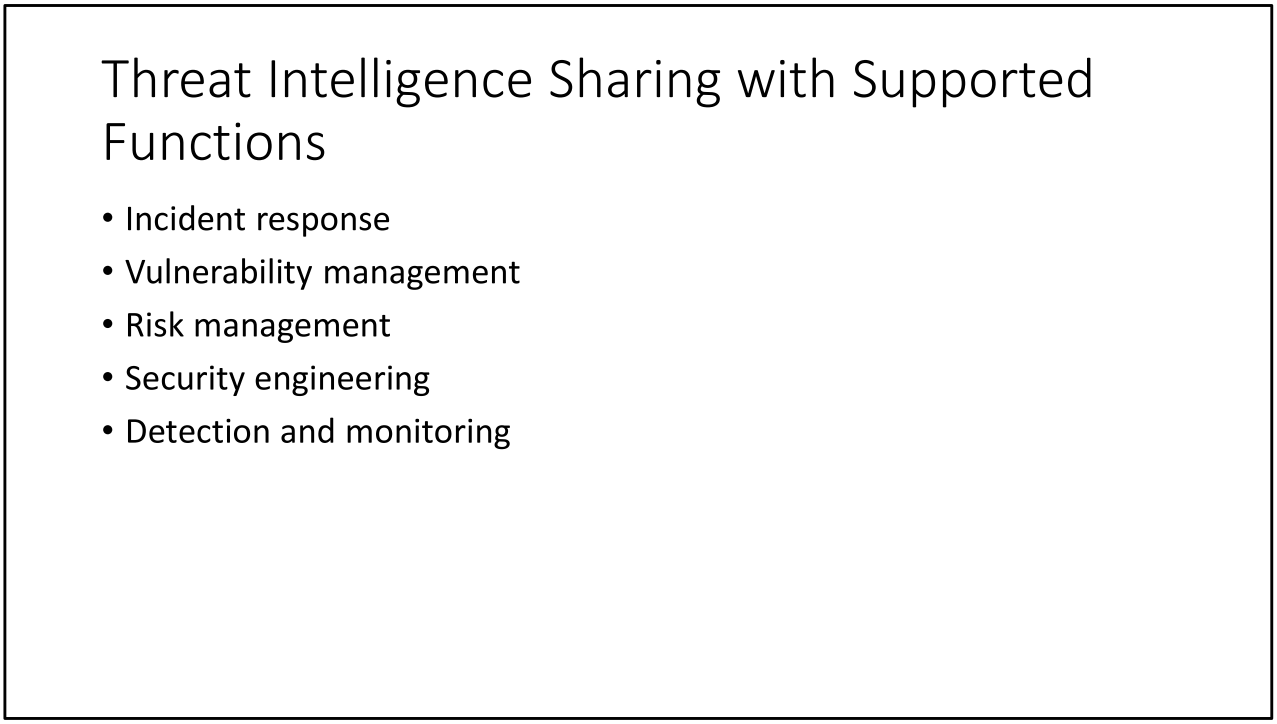
Microsoft STRIDE Threat Categories

Threat	Property Affected	Definition	Example
Spoofing	Authentication	Impersonating someone or something else	A outside sender pretending to be HR in an e-mail
Tampering	Integrity	Modifying data on disk, in memory, or elsewhere	A program modifying the contents of a critical system file
Repudiation	Nonrepudiation	Claiming to have not performed an action or have knowledge of who performed it	A user claiming that she did not receive a request
Information disclosure	Confidentiality	Exposing information to parties not authorized to see it	An analyst accidentally revealing the inner details of the network to outside parties
Denial of service	Availability	Denying or degrading service to legitimate users by exhausting resources needed for a service	Users flooding a website with thousands of requests a second, causing it to crash
Elevation of privilege	Authorization	Gaining capabilities without the proper authorization to do so	A user bypassing local restrictions to gain administrative access to a workstation



PASTA Stages

Stage	Key Tasks
Define objectives	Identify business objectives Identify security and compliance requirements Perform business impact analysis
Define technical scope	Record infrastructure, application, and software dependencies Record scope of the technical environment
Application decomposition	Identify use cases Identify actors, assets, services, roles, and data sources Create data flow diagrams
Threat analysis	Analyze attack scenarios Perform threat intelligence correlation and analytics
Vulnerability and weaknesses analysis	Catalog vulnerability reports and issues Map existing vulnerabilities Perform design flaw analysis
Attack modeling	Analyze complete attack surface
Risk and impact analysis	Qualify and quantify business impact Catalog mitigating strategies and techniques Identify residual risk



Threat Intelligence Sharing with Supported Functions

- Incident response
- Vulnerability management
- Risk management
- Security engineering
- Detection and monitoring