Armaan Shamsaasef

Threat Actors

# Threat Actors - SY0-701 - 2.1

Definition: An individual or group that performs malicious actions against a target.

## Key Attributes for Profiling a Threat Actor

1. Internal vs. External:
    - Internal: An actor within the organization (e.g., employee, contractor, trusted partner). They have authorized access.
    - External: An actor outside the organization with no authorized access.
2. Level of Sophistication/Capability:
    - Unskilled (Script Kiddies): Use pre-made tools and scripts.
    - Skilled: Develop their own exploits and methodologies.
    - Highly Sophisticated (Nation-State): Have significant resources, funding, and advanced skills.
3. Resources/Funding:
    - Ranges from an individual with a single computer to a well-funded nation-state with a massive budget.
4. Intent/Motivation: *This is a primary differentiator.*

## Types of Threat Actors

### 1. Nation-State

- Motivation: Cyberwarfare, espionage (stealing IP or state secrets), political disruption, sabotage.
- Attributes:
    - Highest level of funding/sophistication.
    - Extensive resources and time.
    - Often have a political or military agenda.
- Example: The video implies groups like those from China, Russia, North Korea, or Iran that target government and critical infrastructure.

**2. Unorganized Hackers**

- Motivation: Personal challenge, fame, entertainment, or curiosity.
- Attributes:
    - Low sophistication (e.g., script kiddies).
    - Use tools and exploits they didn't create.
- Example: Someone using a pre-built tool to deface a website "for fun" or to see if they can do it.

**3. Organized Crime**

- Motivation: Financial gain.
- Attributes:
    - Highly skilled and well-organized.
    - Run like a business, focusing on profit.
    - Heavily involved in ransomware, data theft, and fraud.
- Example: A ransomware-as-a-service (RaaS) group that systematically attacks businesses to extort money.

**4. Hacktivists**

- Motivation: Political or social ideology.
- Attributes:
    - Goal is to draw attention to a cause, create disruption, or shame a target.
    - May use website defacement, denial-of-service attacks, or doxing.
- Example: The group Anonymous targeting organizations they perceive as unjust.

**5. Insider Threats**

- Who: Current or former employees, contractors, or partners.
- Types:
    - Malicious Insider: Intentionally causes harm (e.g., stealing data before leaving for a competitor).
    - Unintentional Insider: Accidentally causes a security breach (e.g., falling for a phishing scam).
- Attributes: They are especially dangerous because they have trusted access and knowledge of internal systems.

**6. Shadow IT**

- Definition: When individuals or departments use unauthorized hardware or software without the knowledge or approval of the IT/Security team.
- Why it's a Threat Actor "Vector": It creates unmanaged and insecure systems that can be easily compromised, effectively becoming a threat actor's entry point.
- Example: A marketing team using an unapproved cloud storage service to share large files, bypassing corporate security controls.

---

## Summary

- Threat actors are characterized by their location (internal/external), resources, sophistication, and intent.
- Key motivations include financial gain (Organized Crime), ideology (Hacktivists), espionage/sabotage (Nation-State), and personal reasons (Insider Threats).
- Shadow IT is not a person, but an organizational practice that creates significant vulnerability for other threat actors to exploit.