CS-006 · Foundations

Threat Actors

Who attacks, what motivates them, and how their goals shape the defenses you need.

Executive Summary

Threat actors are the people and groups that attempt to compromise systems and data. They range from opportunistic criminals and organized ransomware crews to insiders, hacktivists, and well-resourced nation-state groups. Understanding who is likely to target an organization, and why, helps teams prioritize the right defenses.

What It Is

A threat actor is any individual or group that carries out or intends to carry out malicious cyber activity. Common categories include cybercriminals motivated by money, nation-state groups pursuing espionage or disruption, hacktivists driven by a cause, insiders who misuse legitimate access, and unskilled attackers who rely on tools built by others. Actors differ widely in skill, funding, patience, and goals. The most capable groups, sometimes described as advanced persistent threats, can stay hidden inside a network for a long time. Threat intelligence is the practice of studying these actors, their motives, and their methods.

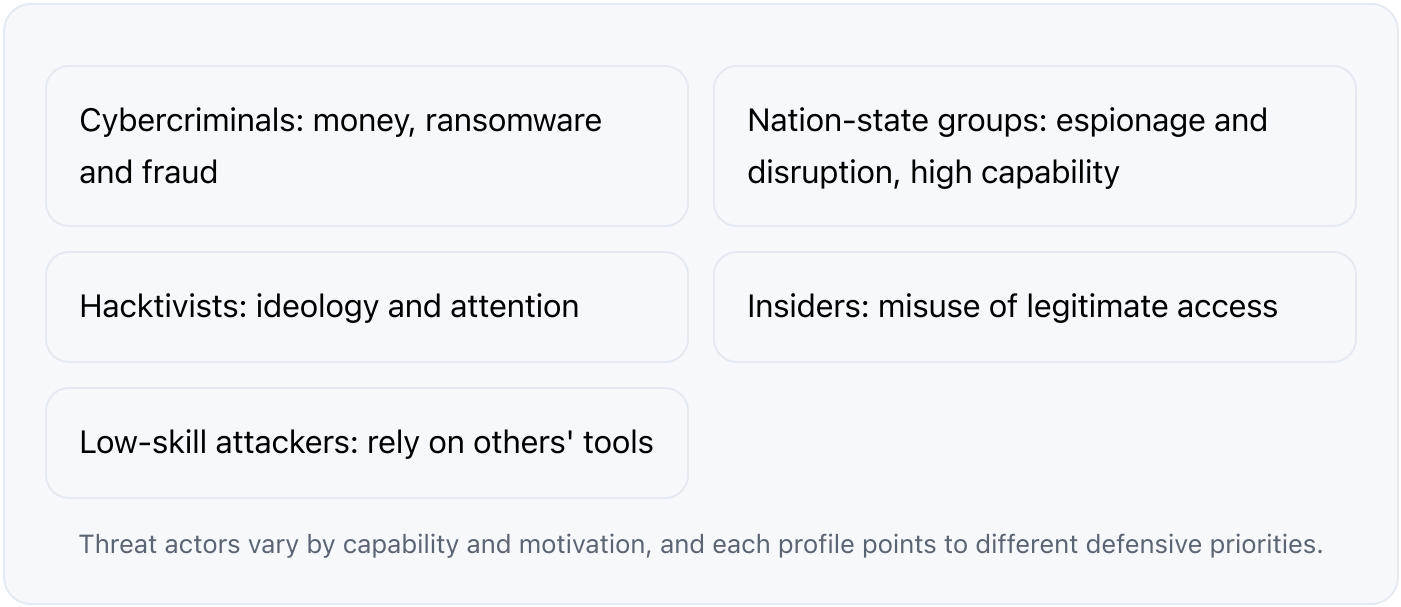
Why It Matters

Defense is not one size fits all. A small business worried about opportunistic ransomware faces different risks than a defense contractor targeted by a nation-state group. Knowing the likely adversary shapes where to invest, what to monitor, and how to respond. It also helps teams communicate risk to leadership in concrete terms rather than vague fear. For professionals, the ability to describe threat actors and map them to realistic scenarios is expected in security operations, threat intelligence, and risk roles, and it makes an incident response far more focused.

How It Works

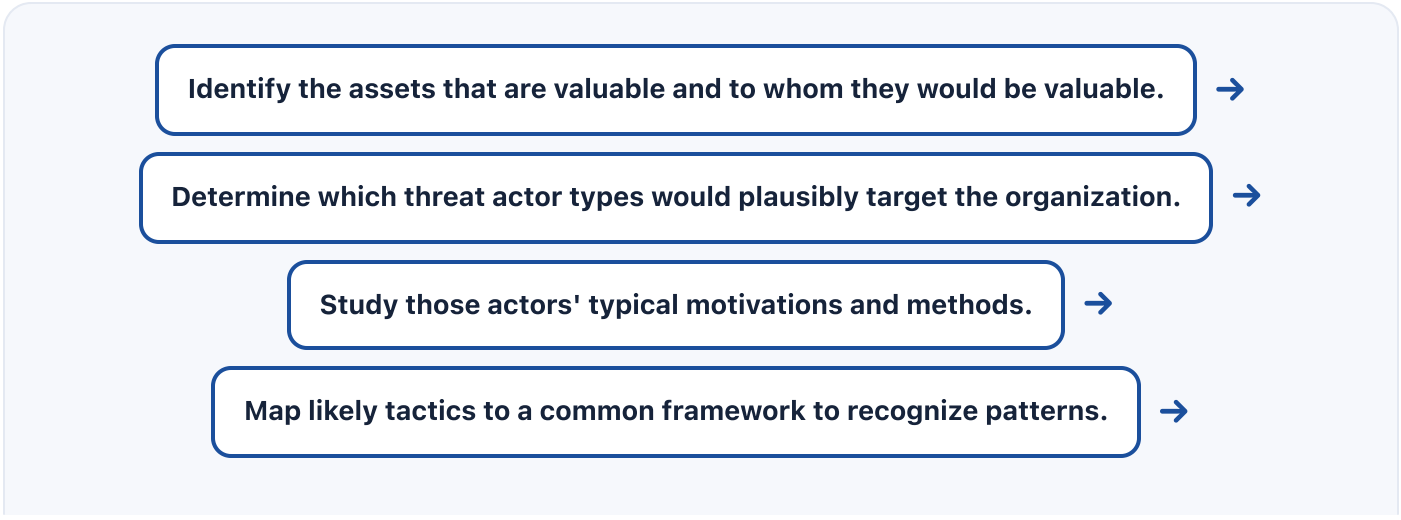
Analysts profile threat actors by capability, motivation, and typical behavior. They study the tactics, techniques, and procedures an actor uses, often mapping them to a common framework so patterns can be recognized across incidents. This profiling feeds into threat modeling, where teams ask which actors would want their assets and how those actors tend to operate. The output guides prioritization: an organization likely to face financially motivated ransomware focuses on backups, segmentation, and email defense, while one facing espionage invests more in detection of stealthy, long-term intrusions. Threat intelligence keeps these profiles current as actors evolve.

Architecture Diagram



Threat actors vary by capability and motivation, and each profile points to different defensive priorities.

Visual Workflow



Prioritize defenses and monitoring against the most likely actors. →

Update the picture as threat intelligence and the environment change.

Common Attacks

- Ransomware and extortion by financially motivated criminal groups
- Espionage and data theft by nation-state groups
- Website defacement and disruption by hacktivists
- Data theft or sabotage by malicious insiders
- Broad, automated attacks using tools sold as a service

Common Mistakes

- Assuming the organization is too small to be a target
- Defending against a generic threat rather than realistic actors
- Overlooking the insider threat while focusing only on outsiders
- Treating all attackers as equally skilled and patient
- Ignoring threat intelligence, so defenses lag behind actor behavior

Best Practices

- Base threat modeling on realistic actors, not worst-case fantasy alone
- Account for both external actors and insider risk
- Use threat intelligence to keep actor profiles current
- Map observed tactics to a common framework for consistency
- Prioritize controls against the most likely and most damaging actors
- Communicate threats to leadership in concrete, scenario-based terms

Quick Checklist

- [ ] Documented view of which threat actors are most relevant

- [x] Insider threat considered in access controls and monitoring
- [x] Threat intelligence source feeding current actor profiles
- [x] Defensive priorities mapped to the most likely actors
- [x] Detection tuned to the tactics those actors commonly use
- [x] Leadership briefed on the realistic threat picture

Recommended Tools

Threat intelligence platforms and feeds
Provide current information on actors and their methods

MITRE ATT&CK knowledge base
Common language for actor tactics and techniques

SIEM and detection tooling
Surfaces behavior consistent with known actor tactics

User and entity behavior analytics (UEBA)
Helps detect insider and anomalous account activity

Industry Standards

MITRE ATT&CK
Widely used taxonomy of adversary tactics and techniques

NIST SP 800-30
Guidance on risk assessment including threat sources

NIST Cybersecurity Framework (CSF) 2.0
Identify and Detect functions cover understanding threats

Career Relevance

Threat actor knowledge is core to threat intelligence analysts, SOC analysts, incident responders, and risk professionals. GRC analysts use it to justify controls and describe risk to

leadership. Penetration testers and red teams emulate specific actors to test defenses. Framing threats in terms of realistic adversaries is a skill valued across security and governance roles.

Interview Questions

- What are the main categories of threat actors, and how do they differ?
- How does knowing the likely threat actor change your defensive priorities?
- What is an advanced persistent threat, and why is it hard to detect?
- How should an insider threat change how you design access controls?
- How do frameworks like MITRE ATT&CK help in profiling actors?

Related Certifications

CompTIA Security+ | GIAC Cyber Threat Intelligence (GCTI) | ISC2 Certified in Cybersecurity (CC)

Further Reading

- MITRE ATT&CK
- CISA: Threats and Advisories
- NIST SP 800-30 Risk Assessment

Key Takeaways

- Threat actors range from opportunistic criminals to nation-state groups.
- They differ in skill, funding, patience, and motivation.
- Knowing the likely adversary shapes where to invest in defense.
- Insiders are a real and often underrated category of threat actor.
- Threat intelligence keeps actor profiles current as they evolve.

FAQ

▶ **Is a small organization really a target for threat actors?**

▶ **What is an advanced persistent threat?**

▶ **How do insiders fit into threat actors?**

Related Careers

RELATED ROLES

Soc Analyst | Grc Analyst | Penetration Tester

RELATED CERTIFICATIONS

CompTIA Security+

GIAC Cyber Threat Intelligence (GCTI)

ISC2 Certified in Cybersecurity (CC)

CURRENT OPENINGS

Live roles are on the job board.

Browse all jobs

GUIDES & SALARY

Career guides | Role roadmaps | Salary data | Career tools

SUGGESTED LEARNING PATH

1. Ground the basics with CS-001 Cybersecurity
2. Study this sheet: **Threat Actors**
3. Go deeper: Cybersecurity
4. Go deeper: Attack Surface
5. Validate it: work toward **CompTIA Security+**
6. Find the role: browse current openings

RELATED SHEETS

CS-001 Cybersecurity | CS-005 Attack Surface | CS-007 The Cyber Kill Chain | CS-008 MITRE ATT&CK | CS-010 Cyber Hygiene