PROJECT
ENG
PRO

CYBER SECURITY FOR INDUSTRIAL CONTROL SYSTEMS

By Project ENG PRO

What is Cyber Security?

Welcome to this lesson dedicated to the study of cyber security. In this lesson, we will explore the fundamental concepts of cyber security and gain a clear understanding of its purpose and significance.

Anatomy of a Cyber Attack

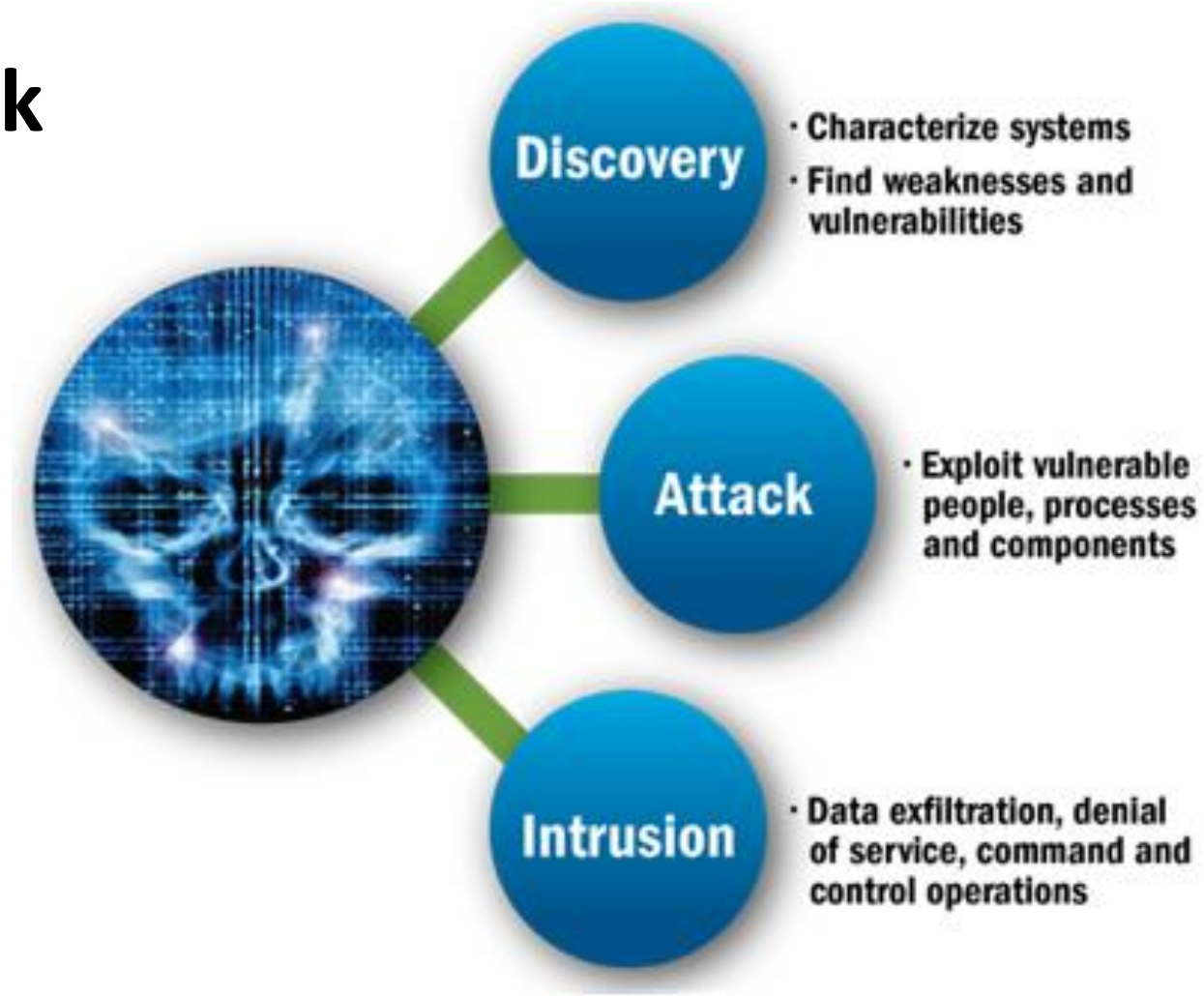
Understanding Cybersecurity:

Grasp cyber-attack concept for comprehensive defence.

Know methods malicious actors use to exploit vulnerabilities.

Similarity to techniques security pros use for testing.

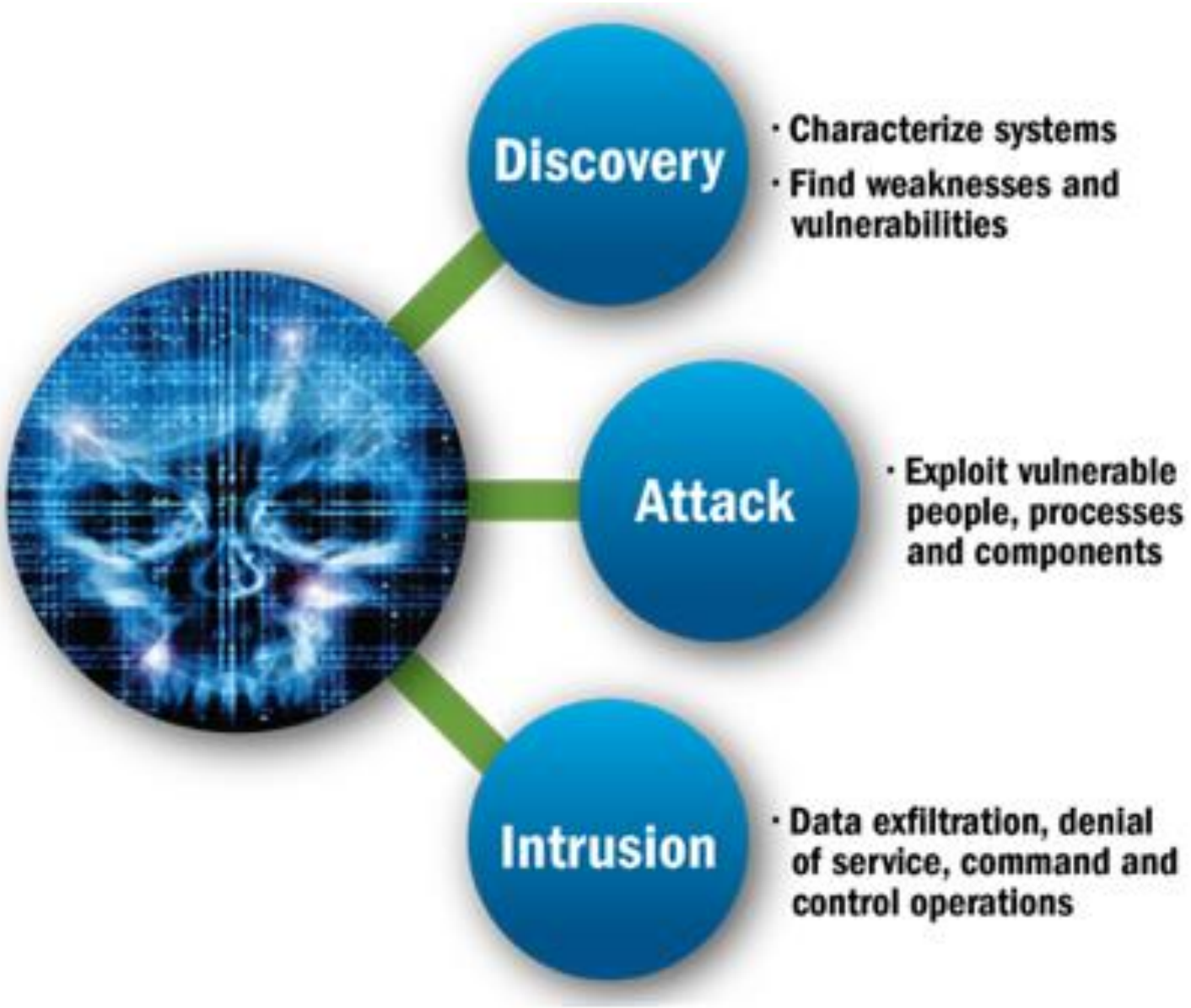
Insight into approaches helps implement effective defence strategies.



The Cat-and-Mouse Game

Cybersecurity Dynamic:

- Resembles Tom and Jerry rivalry.
- Defenders monitor, update to counter threats.
- Continuous challenge of protection vs. infiltration.
- Professionals build defenses, hackers seek compromise.



Cyber Attack Stages

Discovery Phase:

- Reconnaissance to find weaknesses.
- Identifying firewalls, servers, ports.

- Attack Execution:
  - Developing and launching the attack.
- Command and Control:
  - Establishing presence to achieve objectives.
- Sequential process from discovery to control for cyber attacks.

Attack Phase

Attack Phase Methods:

- Exploit weak authentication.
- Network scanning for vulnerabilities.
- Use of removable media for entry.
- Employ brute force tactics.
- Abuse access authority.
- Spear-phishing strategies.
- Exploit documented system weaknesses.
- Utilize device info for vulnerability identification.

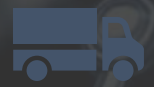
Attack Phase

- Post-Initial Access Actions:
  - Data Exfiltration, DoS attacks, Command and Control operations.
  - Manipulation of plant devices, feedback mechanisms, alarms, etc.
- Importance of Understanding:
  - Specific attack methods, discovery techniques, technologies.
  - Vital for effective defense, safeguard implementation.

ICS Cyber Attack Process

1. Reconnaissance Phase

2. Weaponization Phase



3. Delivery Phase

4. Exploitation Phase

5. Command and Control Phase

6. Actions on Objectives

1. Reconnaissance Phase

2. Weaponization Phase

3. Delivery Phase

4. Exploitation Phase

5. Command and Control Phase

6. Actions on Objectives

1. Reconnaissance Phase

- Initial Information Gathering: Attacker gathers data about the target ICS network, including IP addresses, network topology, and system details.
- Scanning and Enumeration: Attacker probes the ICS network for open ports, services, and vulnerabilities using tools like Nmap.
- Vulnerability Assessment: Identify weaknesses, misconfigurations, and potential entry points.

2. Weaponization Phase

- Malware Development: Attacker creates custom malware or exploits, tailored to the specific ICS environment and vulnerabilities.
- Payload Preparation: Malware is prepared to deliver its payload to the target system.

3. Delivery Phase

- Malware Distribution: Malicious payload is delivered to the ICS network through methods like phishing emails, infected files, or compromised external devices.
- Exploit Execution: Malware executes the exploit to gain access to the targeted ICS components.

4. Exploitation Phase

- Gaining Access: Attacker establishes a foothold in the ICS network, exploiting vulnerabilities to access critical systems.
- Privilege Escalation: Attacker elevates their privileges to gain control over ICS components.

5. Command and Control Phase

- Establishing Control: Attacker sets up communication channels to remotely control compromised systems.
- Remote Operations: Attacker uses command and control (C2) infrastructure to issue commands and manipulate ICS processes.

6. Actions on Objectives

- Data Exfiltration: Attacker extracts sensitive data or critical information from the compromised ICS environment.
- System Manipulation: Attacker can modify or disrupt ICS processes, causing physical damage or operational disruption.

Wrap Up

- Explored discovery and intrusion stages.
- Gained insights into ICS cyber attack process.
- Uncovered attack progression from discovery to intrusion.
- Equipped to comprehend cyber attack dynamics and ICS complexities.
- Empowered to bolster defenses against evolving threats.