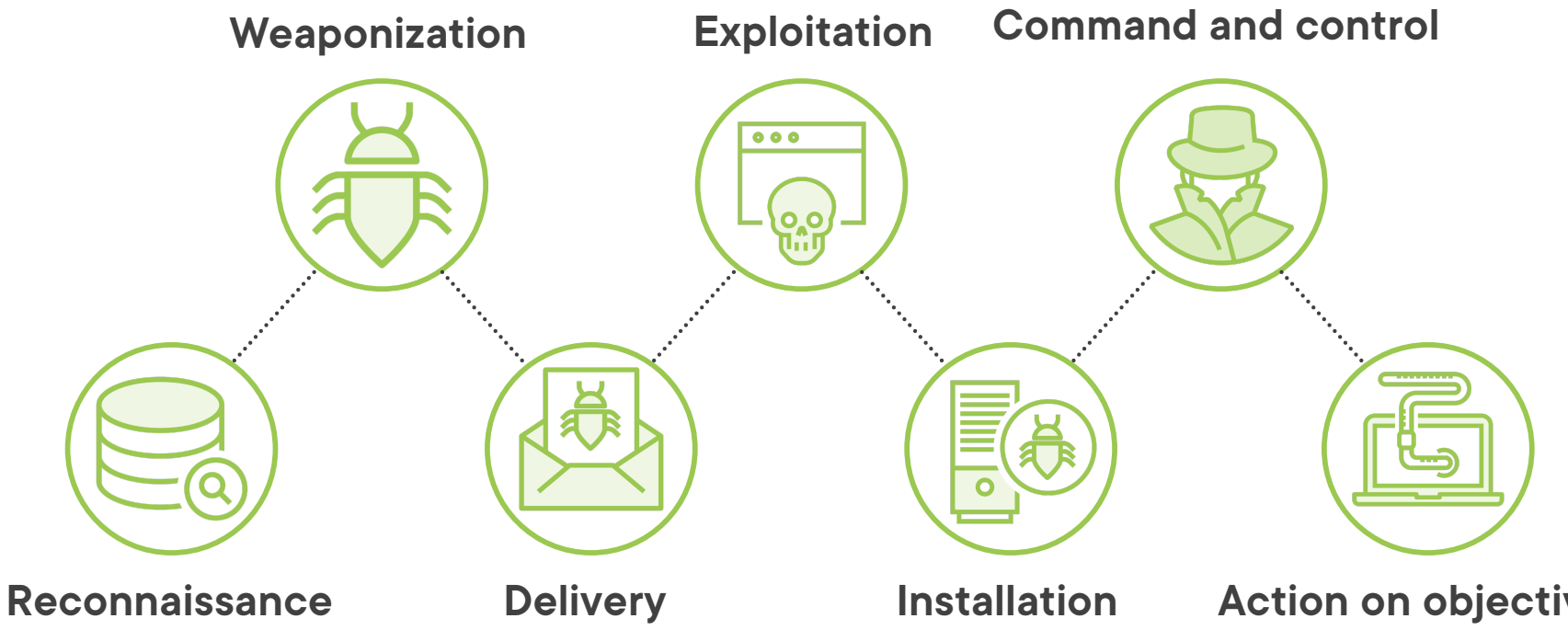
Understanding the Attackers and Their Methods

Dale Meredith
MCT | CEI | CEH | MCSA | MCSE
Cyber Security Expert

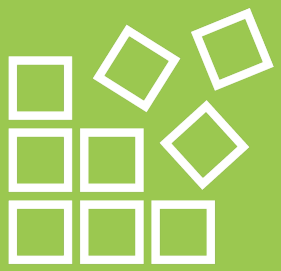
dalemeredith.com | Twitter: @dalemeredith | Linkedin: dalemeredith|

Cyber Kill Chain Methodology

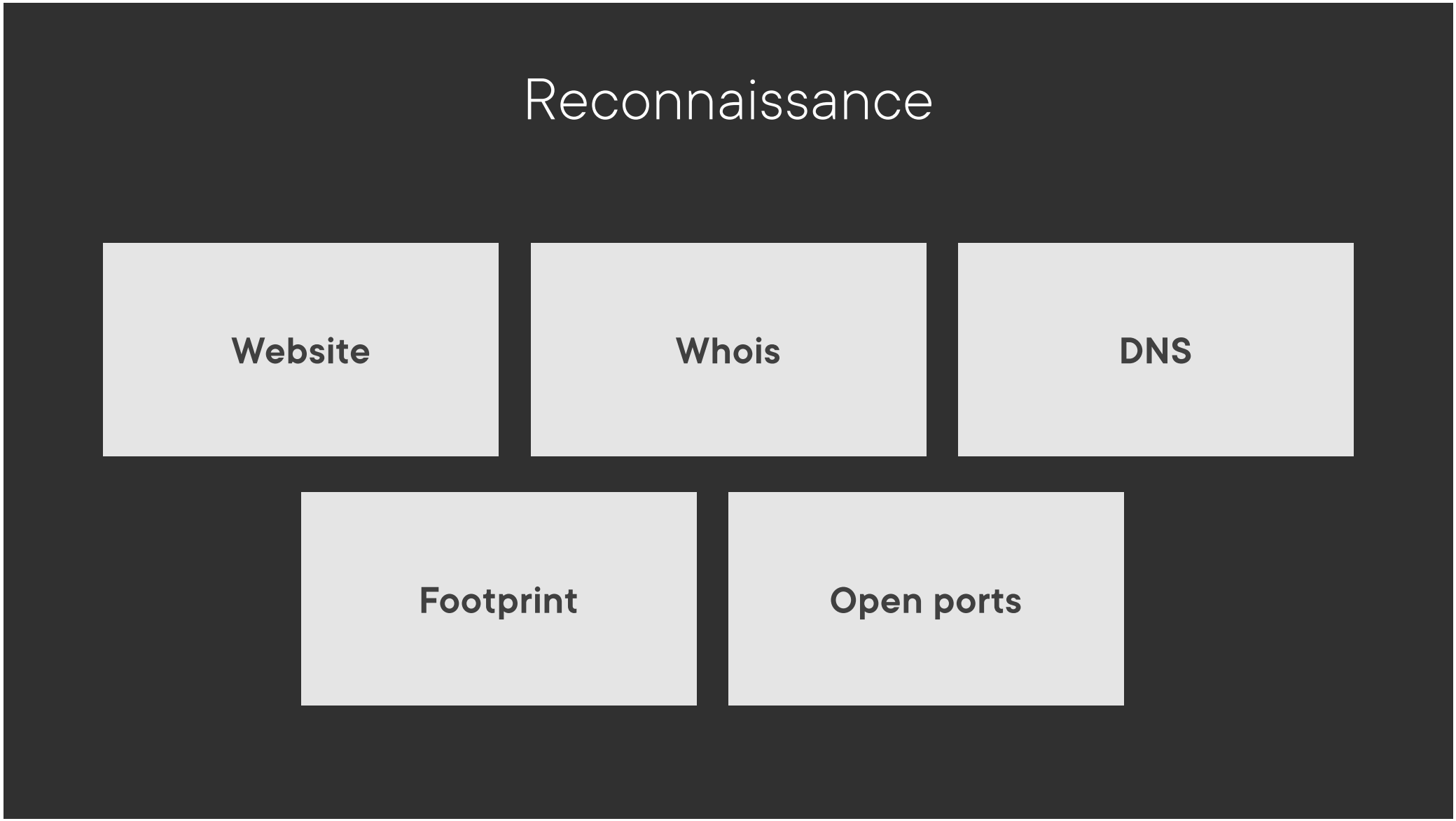
Cyber Kill Chain Methodology



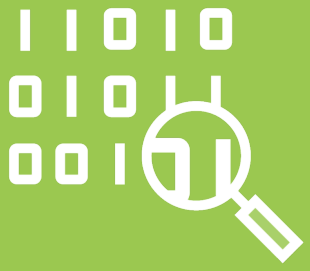
Reconnaissance

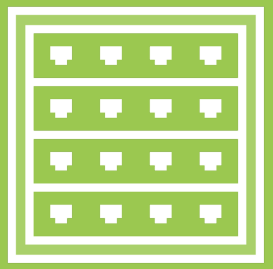




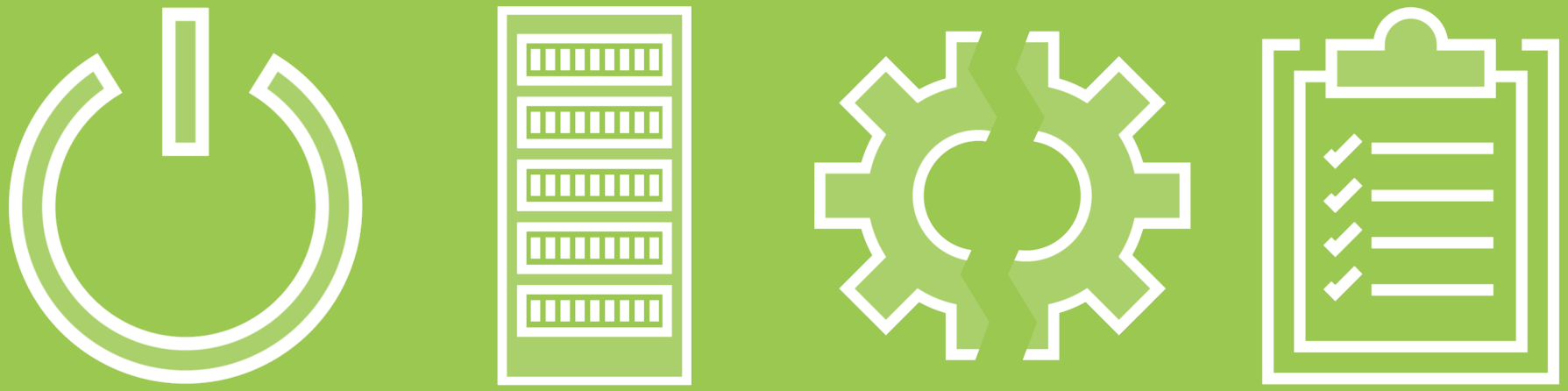



Weaponization





Exploitation



Installation

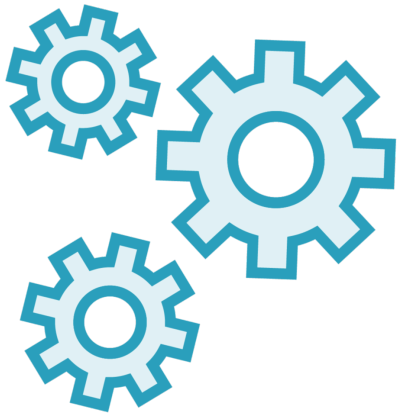
Command and Control (C&C)

Action on Objectives

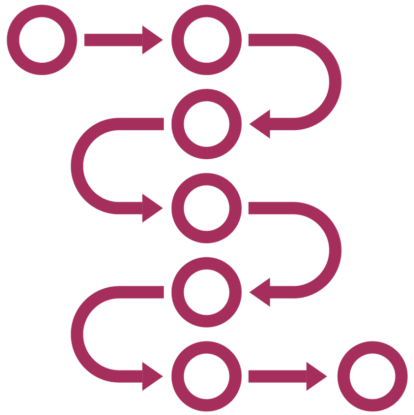
Tactics, Techniques and Procedures

Tactics, Techniques and Procedures

Tactics

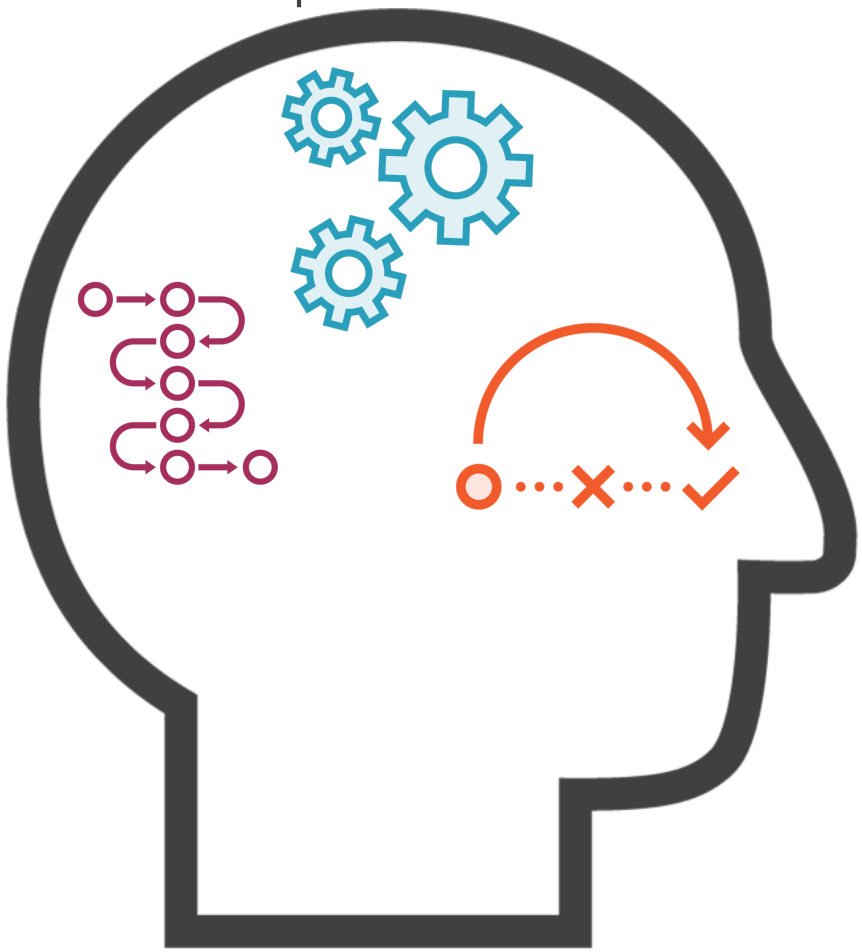


Techniques



Procedures

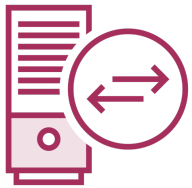
Tactics, Techniques and Procedures



Adversary Behavioral Identification

Adversary Behavioral Identification

Internal reconnaissance

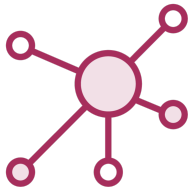


Suspicious proxy events

PowerShell

HTTP user agent

CLI processes



C&C servers

Internal Reconnaissance

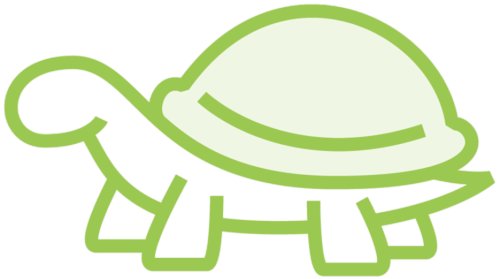
Enumeration

- **OS**
- **Services**
- **Apps and versions**
- **Hosts**
- **Processes**
- **User accounts**
- **IP addresses**
- **Host names**

Detect Compromised Hosts

Adversary Behavioral Identification

DNS Tunneling



Web-shells

Data staging

DNS Tunneling

- **Talk with C&C's**
- **Bypass security controls**
- **Monitor requests**
- **DNS Payloads**
- **Destinations**

Indicators of Compromise (IoC)

- Unauthorized software and files
- Suspicious emails
- Suspicious registry and file system changes
- Unknown ports and protocol usage
- Excessive bandwidth usage
- Rogue hardware
- Service disruption and defacement
- Suspicious or unauthorized account usage

Learning Check

Learning Check

- **Exploitation**
- **Action on Objectives**
- **Powershell**
- **DNS Tunneling**
- **Data Staging**

Key Terms

- **Tactics**
- **Techniques**
- **Procedures**

Up Next:
Comparing Hacking and Ethical Hacking