FERTINET
Training Institute

FERTINET
CERTIFIED
SOLUTION
SPECIALIST

Security
Operations

Security Operations Analyst

SOC Concepts and Security Frameworks

FortiAnalyzer 7.4

Last Modified: 21 January 2025

Lesson Overview

- SOC Main Functions and Roles
- Fortinet SOC Environment Benefits
- Attack Frameworks Overview

SOC Main Functions and Roles

Objectives

- Describe the main functions and roles within a SOC
- Describe the main challenges within a SOC

FORTINET
Training Institute

What Is a SOC?

Security
Operations
Center

Threat Monitoring
Continuous monitoring for security events and compromise indicators

Threat Detection
Analyzing data for patterns and anomalies, and identifying malicious activities

Incident Response
Swiftly responding, investigating, containing, and restoring from security incidents

Threat Hunting
Proactively searching for hidden threats using advanced techniques

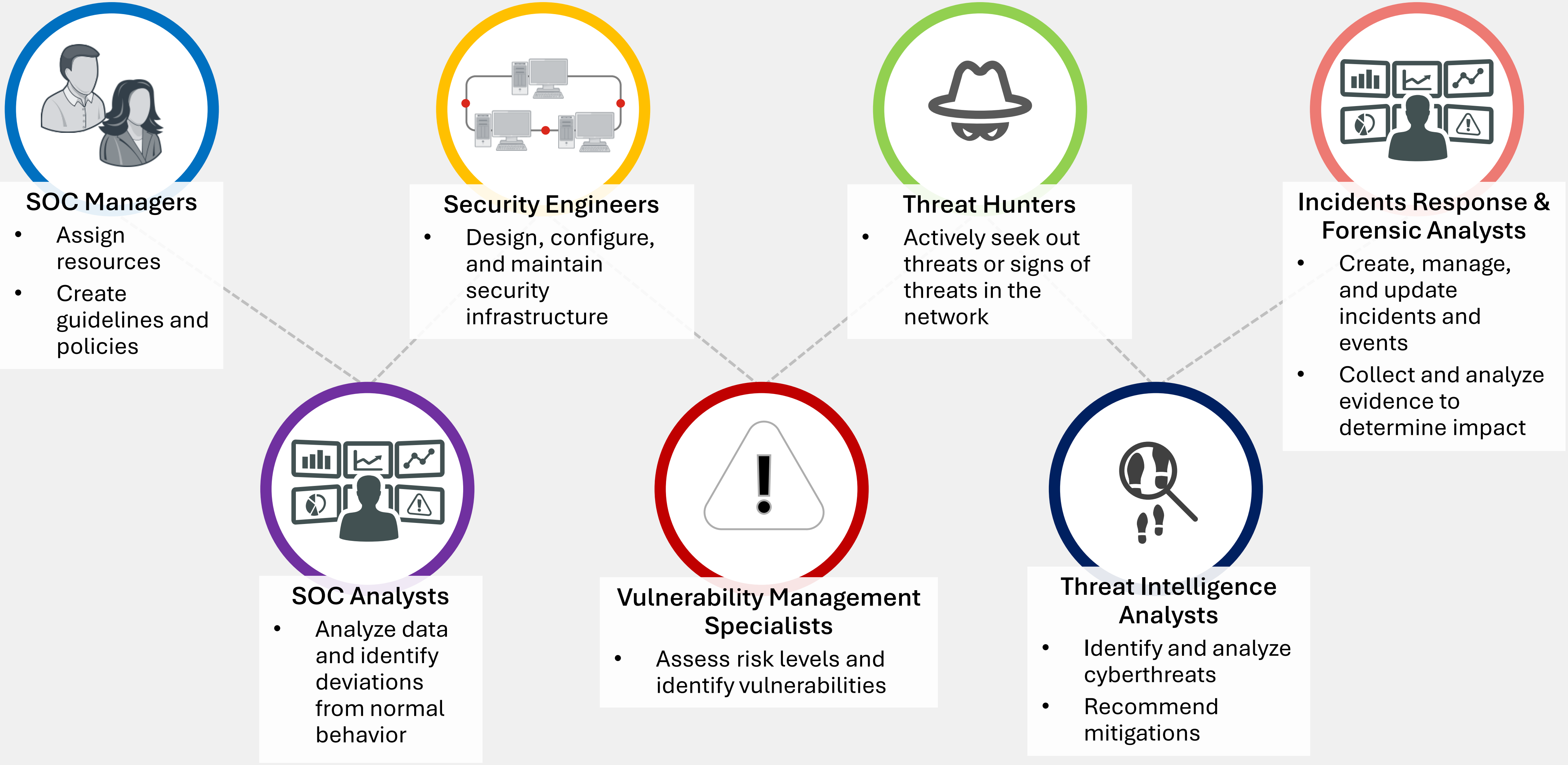
Vulnerability Management
Identifying and prioritizing vulnerabilities, patching, and configuration

Threat Intelligence
Gathering, analyzing, and sharing emerging threat information

Reporting and Documentation
Documenting incidents, preparing reports, and tracking metrics

Compliance and Regulations
Ensuring adherence to industry-specific regulations

SOC Roles



SOC Managers

- Assign resources
- Create guidelines and policies

Security Engineers

- Design, configure, and maintain security infrastructure

Threat Hunters

- Actively seek out threats or signs of threats in the network

Incidents Response & Forensic Analysts

- Create, manage, and update incidents and events
- Collect and analyze evidence to determine impact

SOC Analysts

- Analyze data and identify deviations from normal behavior

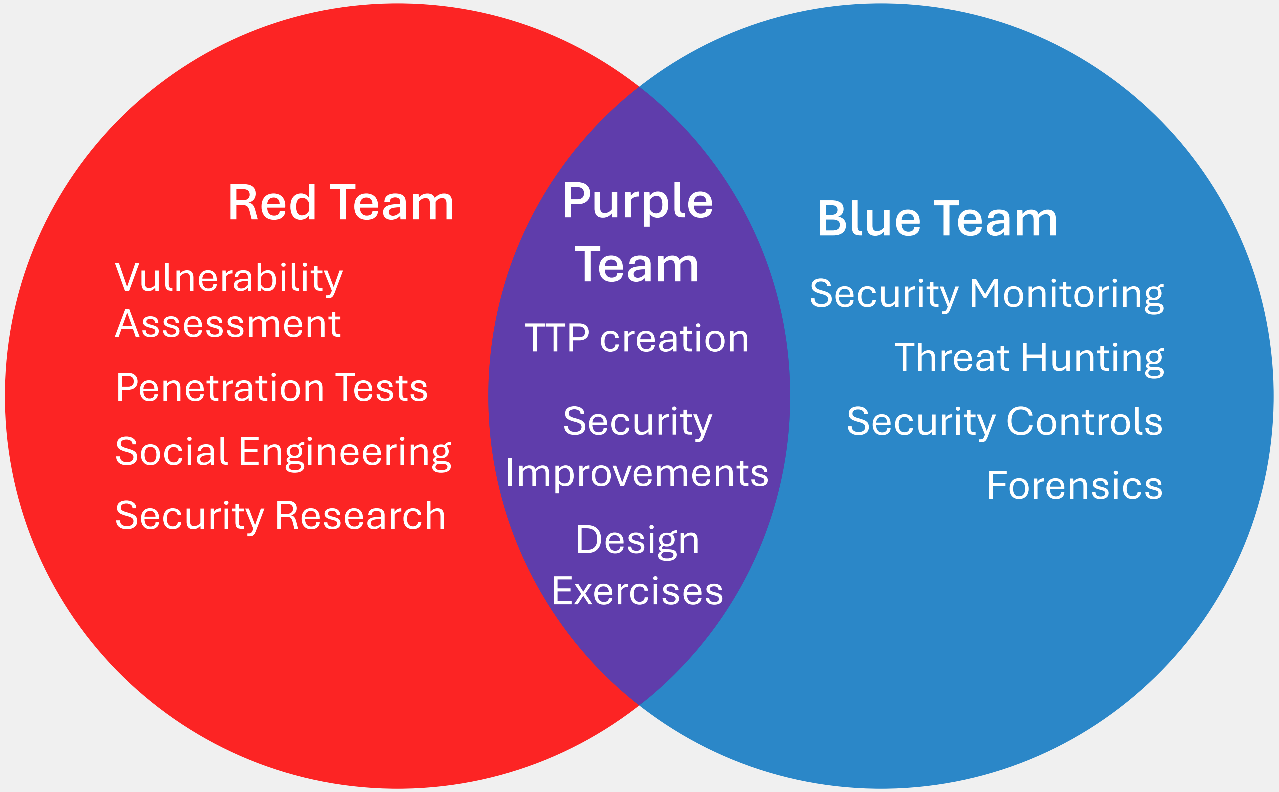
Vulnerability Management Specialists

- Assess risk levels and identify vulnerabilities

Threat Intelligence Analysts

- Identify and analyze cyberthreats
- Recommend mitigations

Teams Within a SOC



Red team *simulates* adversaries

- Attempts to exploit vulnerabilities
- Conducts penetration tests and vulnerability assessments
- Performs security research

Blue team *defends* against adversaries

- Identifies, responds to, and mitigates security incidents
- Performs security monitoring, threat hunting, and forensics
- Detects, responds to and recovers from incidents

Purple team *orchestrates* knowledge sharing

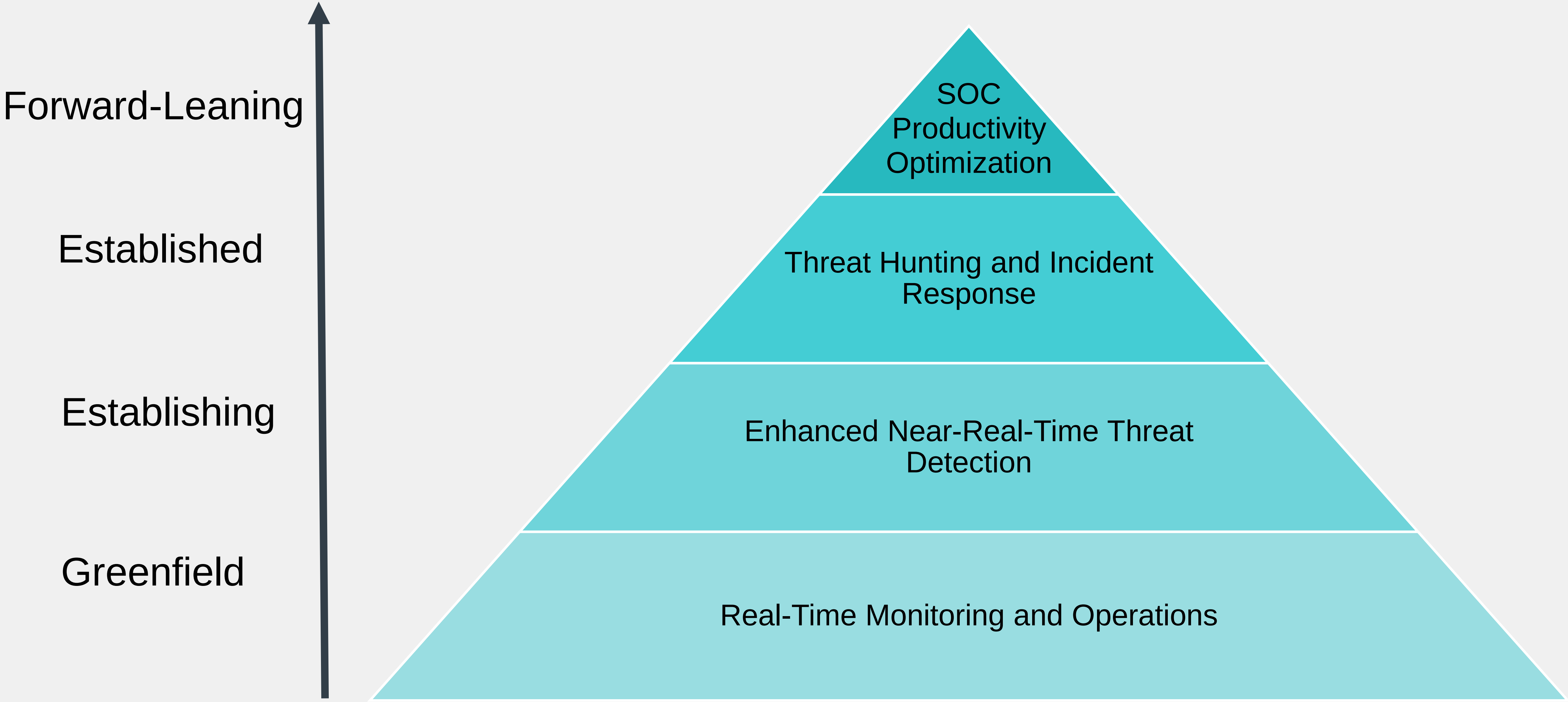
- Bridges the gap between red and blue teams
- Facilitates knowledge transfer
- Designs exercises
- Improves organizational security posture
- Creates TTP mapping

FORTINET
Training Institute

Reasons Why SOCs Fail or Succeed

	Scope	Technology	Implementation
Success	- Focused requirements and use cases - Realistic expectations - Appropriate application (current and future) - Compliant with regulations	- Strong understanding of the market and technology - Meets current and future requirements, and in-scope processes - High-fidelity outputs	- Resources allocated - Required skills identified and planned for - Impact on SOC playbooks understood
Failure	- Shallow and narrow coverage - Unrealistic expectations - Wrong focus (threat vector) - Non-compliance with regulations	- Lack of understanding of how tools work - Too many events (poor sources or poor tech) - Solution didn’t deliver	- Too small—no team - Lacking key skills - No playbook—no process - Inconsistent responses

SOC Maturity


Forward-Leaning
Established
Establishing
Greenfield
SOC Productivity Optimization
Threat Hunting and Incident Response
Enhanced Near-Real-Time Threat Detection
Real-Time Monitoring and Operations

Knowledge Check

1. Which SOC role is responsible for investigating logs to identify problems?

   ✓ A. SOC analyst

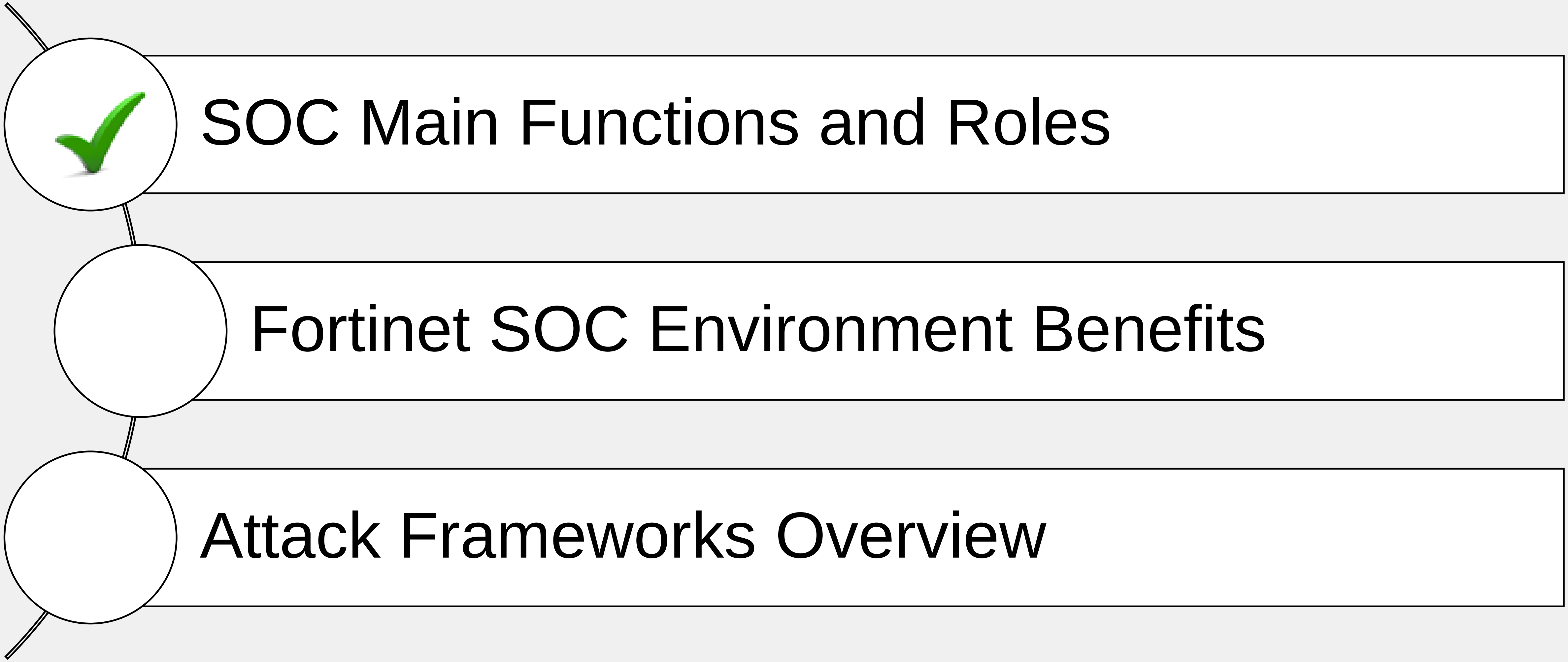
   B. Threat hunter

2. What is the role of the red team in a SOC?

   A. To gather and analyze evidence, and determine scope of impact

   ✓ B. To assess and exploit vulnerabilities

Lesson Progress



- ✓ SOC Main Functions and Roles
- Fortinet SOC Environment Benefits
- Attack Frameworks Overview

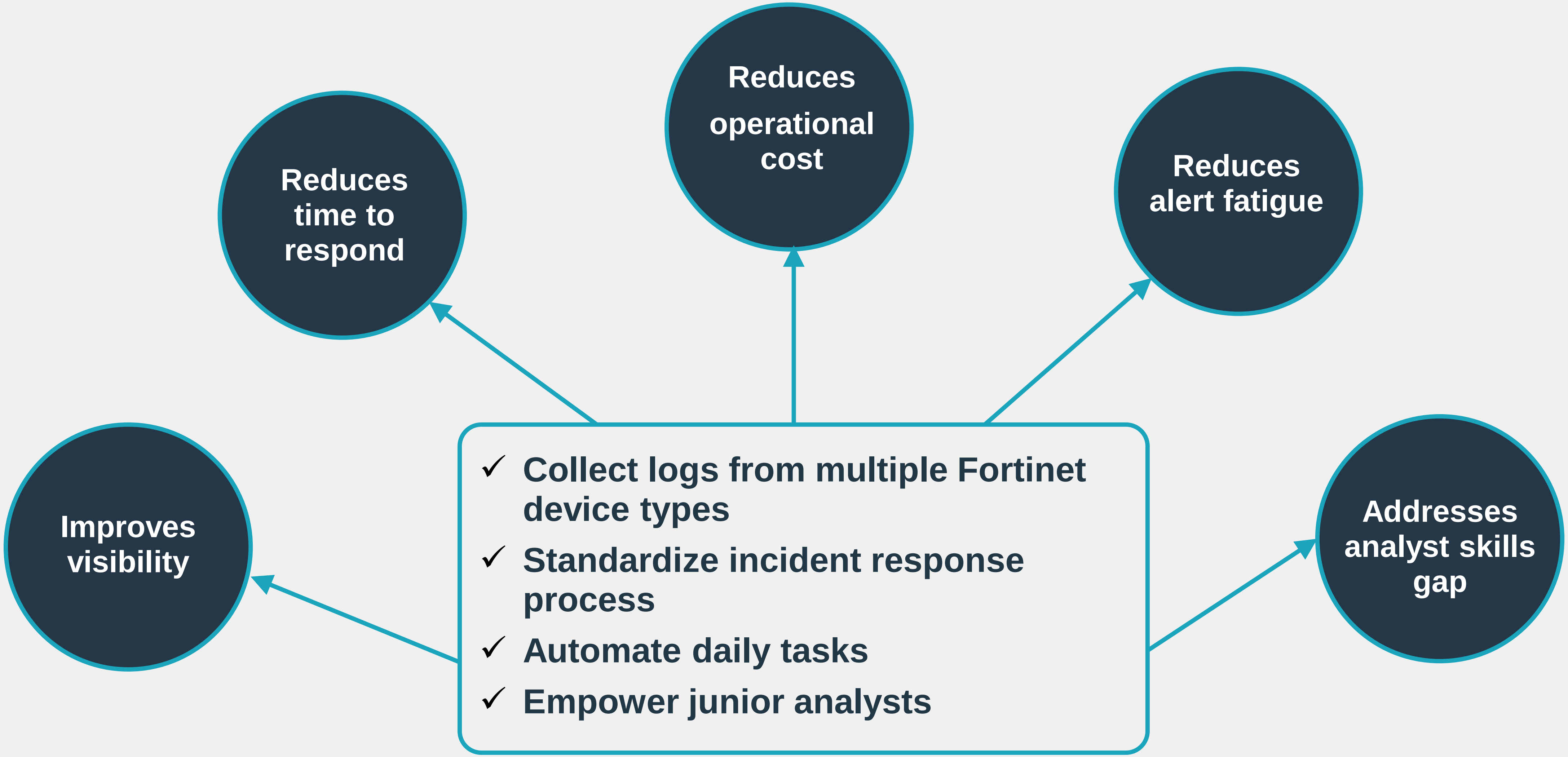
FORTINET Training Institute

Fortinet SOC Environment Benefits

Objectives

- Identify the challenges that can be solved by the Fortinet SOC
- Describe the Fortinet SOC solution workflow

Benefits of the Fortinet SOC Environment



Reduces time to respond

Reduces operational cost

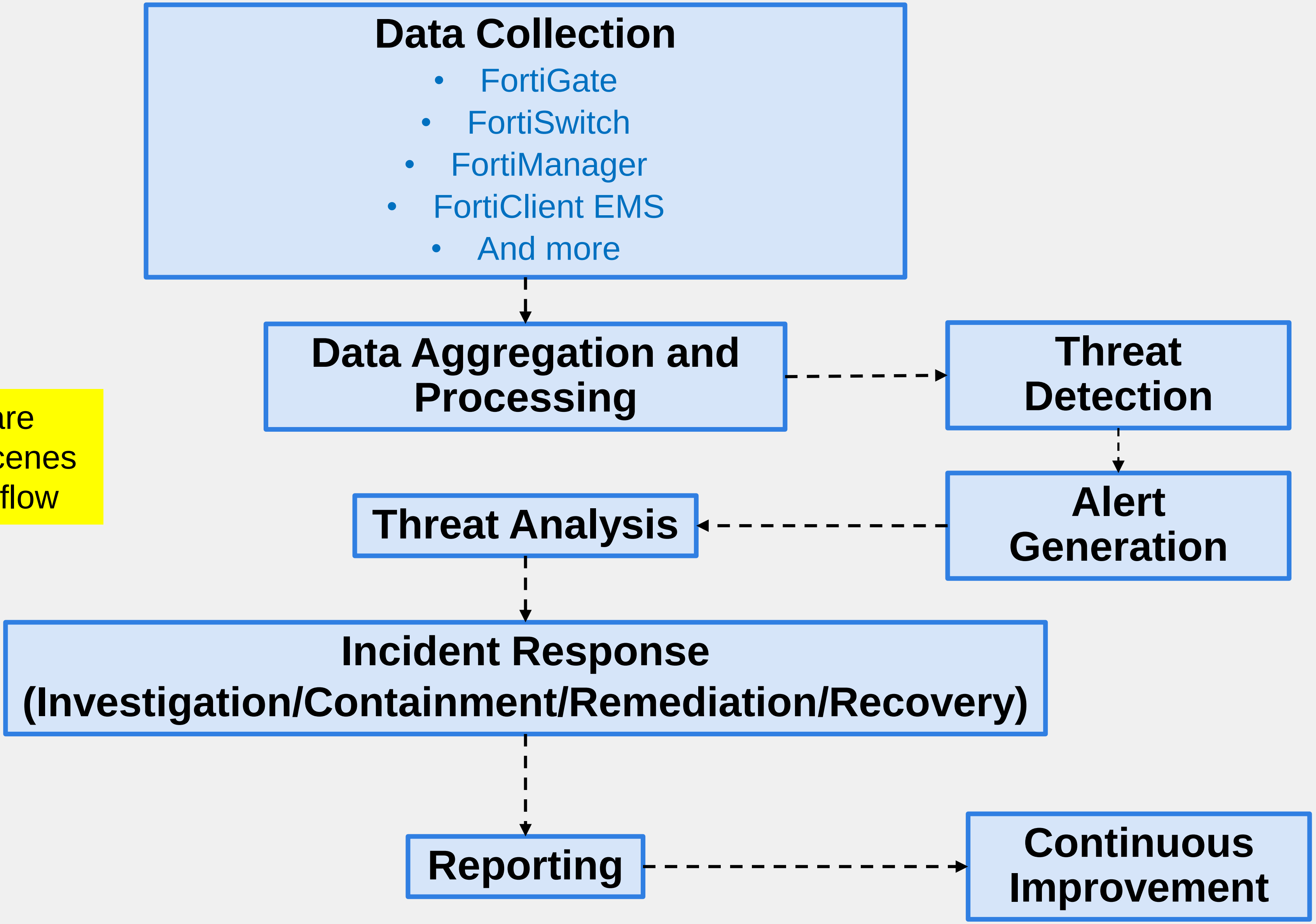
Reduces alert fatigue

Improves visibility

Addresses analyst skills gap

- ✓ Collect logs from multiple Fortinet device types
- ✓ Standardize incident response process
- ✓ Automate daily tasks
- ✓ Empower junior analysts

Fortinet SOC Solution Workflow

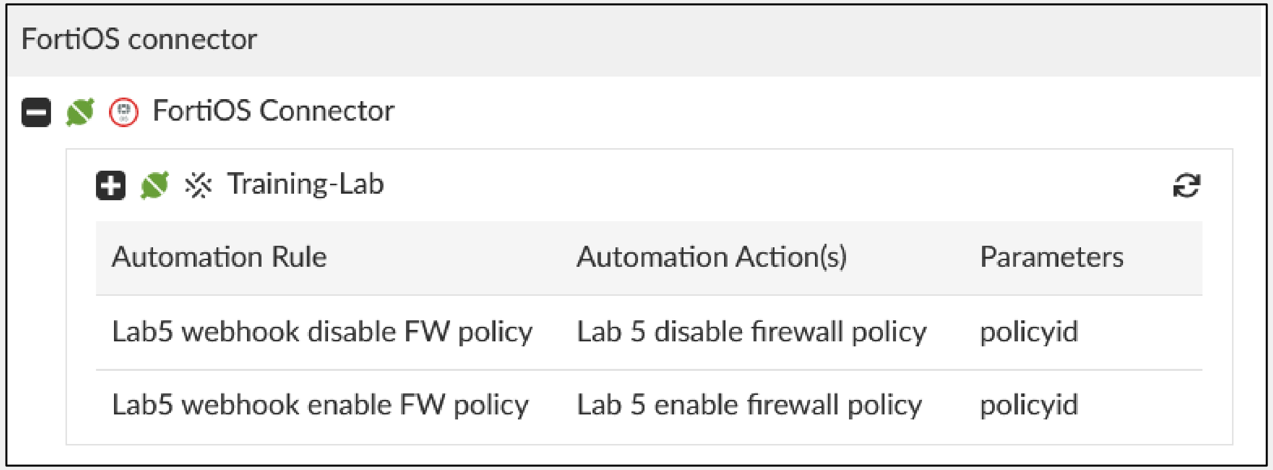


Note: Playbooks are running behind the scenes throughout the workflow

Training Institute

Integration Examples

- Connectors allow playbooks to interact with devices in the Security Fabric and standalone devices
  - They determine which actions can be performed by playbook tasks



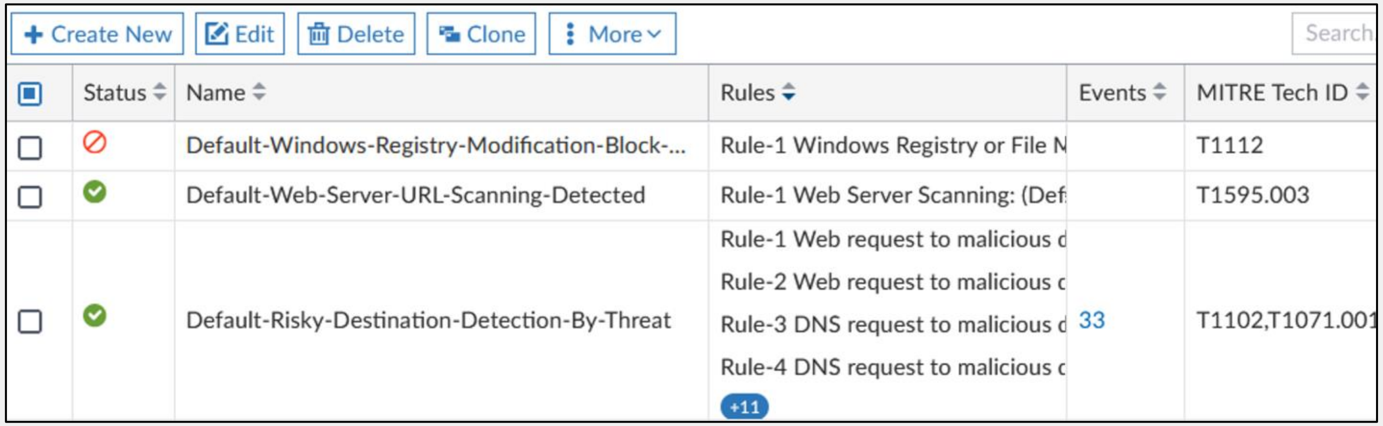
FortiOS connector

⊟ FortiOS Connector

⊞ Training-Lab

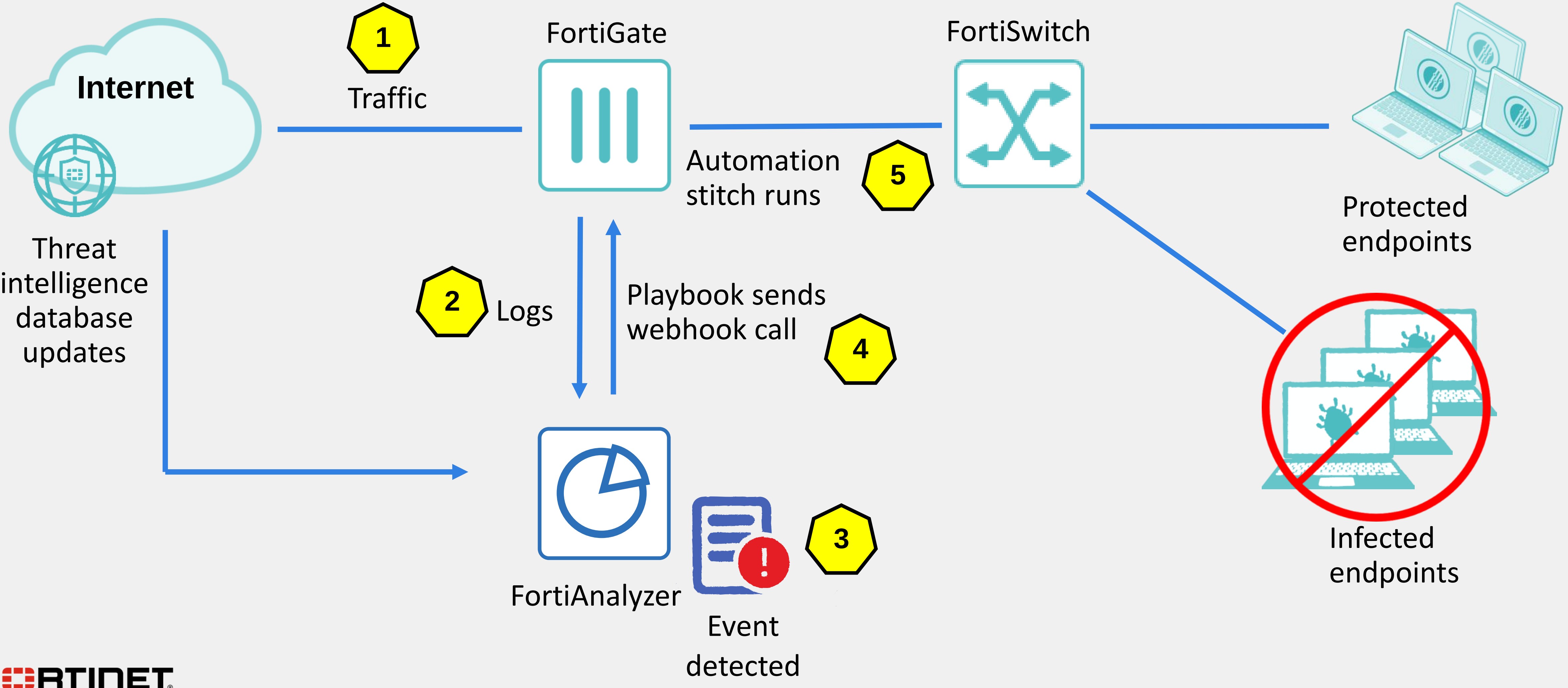
Automation Rule	Automation Action(s)	Parameters
Lab5 webhook disable FW policy	Lab 5 disable firewall policy	policyid
Lab5 webhook enable FW policy	Lab 5 enable firewall policy	policyid

- Event handlers generate events when a rule is matched
  - FortiAnalyzer contains many predefined (default) event handlers for many Fortinet devices
  - You can also create your own event handlers



☐	Status	Name	Rules	Events	MITRE Tech ID
☐	⊘	Default-Windows-Registry-Modification-Block-...	Rule-1 Windows Registry or File N		T1112
☐	✓	Default-Web-Server-URL-Scanning-Detected	Rule-1 Web Server Scanning: (Def		T1595.003
☐	✓	Default-Risky-Destination-Detection-By-Threat	Rule-1 Web request to malicious d Rule-2 Web request to malicious c Rule-3 DNS request to malicious d Rule-4 DNS request to malicious c +11	33	T1102,T1071.001

An Example of Automation With a Playbook

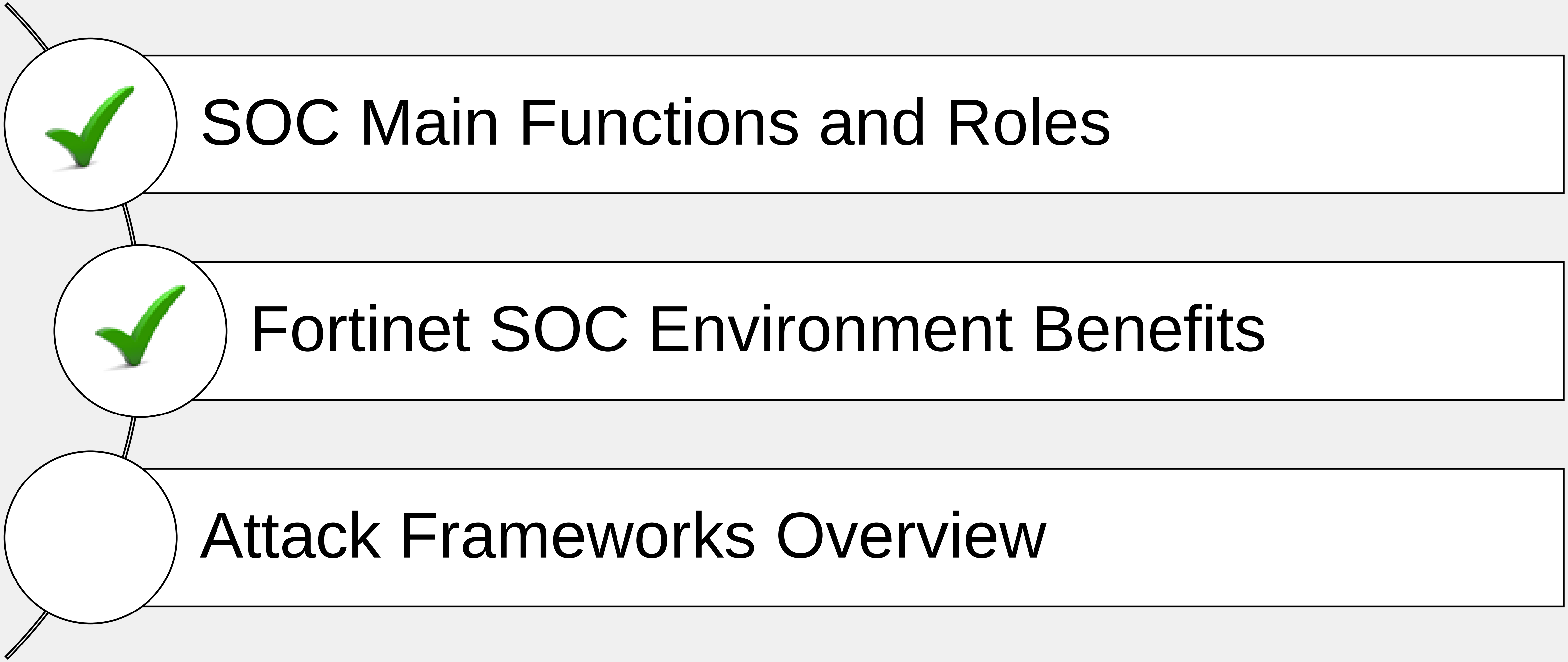


FORTINET Training Institute

Knowledge Check

1. What determines the possible actions a playbook task can perform?
   A. The event handler
   ✓ B. The connector

Lesson Progress



- ✓ SOC Main Functions and Roles
- ✓ Fortinet SOC Environment Benefits
- Attack Frameworks Overview

Attack Frameworks Overview

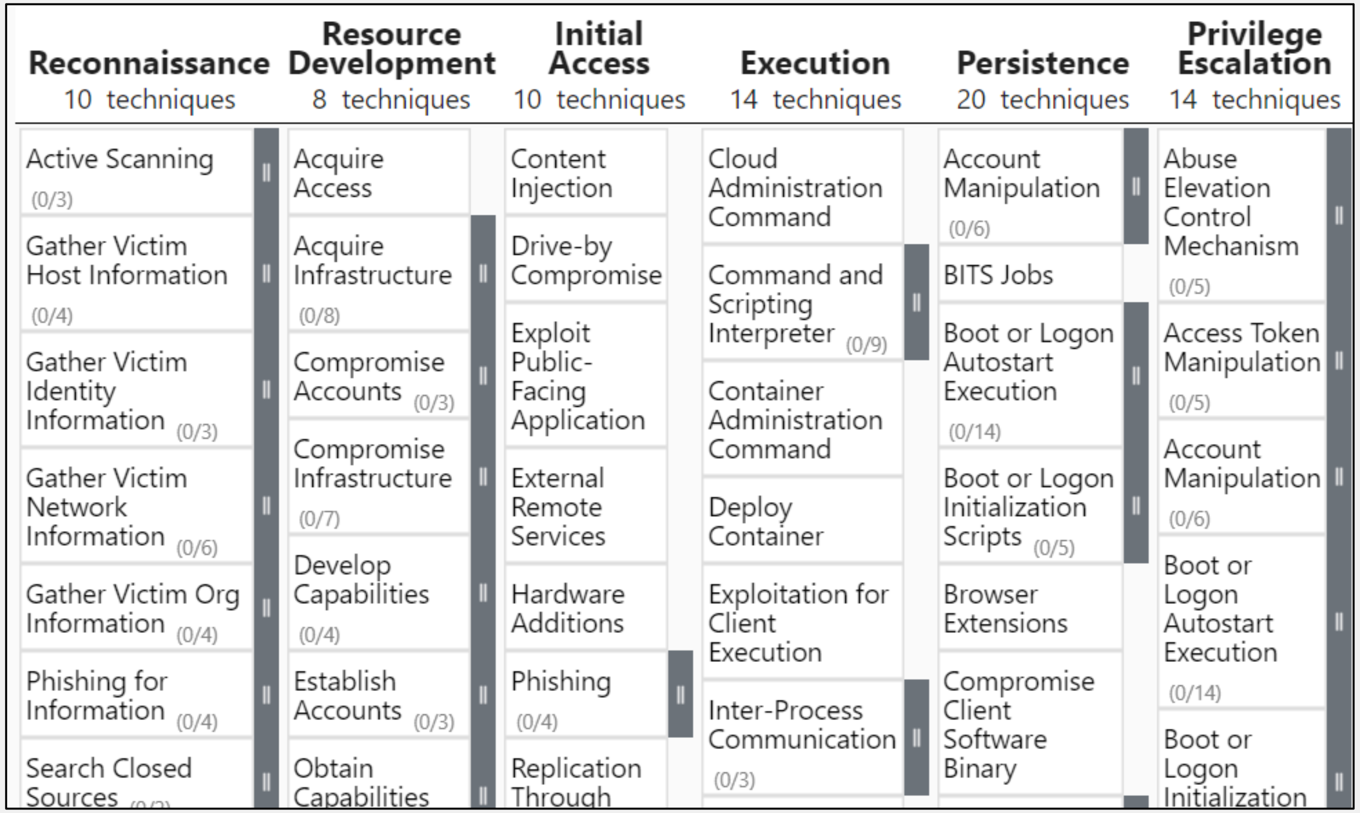
Objectives

- Describe the MITRE ATT&CK Matrix for Enterprise
- Describe the Cyber Kill Chain

MITRE ATT&CK Overview

ATT&CK = Adversarial Tactics, Techniques, and Common Knowledge

- Detailed mapping of adversary behavior framework
- Threat intelligence and adversary emulation use cases
- Guidelines for classifying and describing cyberattacks and intrusions
- 14 tactics categories consisting of "technical objectives" of an adversary
- Categories broken down further into specific techniques and subtechniques
- Created by the MITRE Corporation in 2013



Reconnaissance 10 techniques	**Resource Development** 8 techniques	**Initial Access** 10 techniques	**Execution** 14 techniques	**Persistence** 20 techniques	**Privilege Escalation** 14 techniques
Active Scanning (0/3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (0/6)	Abuse Elevation Control Mechanism (0/5)
Gather Victim Host Information (0/4)	Acquire Infrastructure (0/8)	Drive-by Compromise	Command and Scripting Interpreter (0/9)	BITS Jobs	Access Token Manipulation (0/5)
Gather Victim Identity Information (0/3)	Compromise Accounts (0/3)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (0/14)	Account Manipulation (0/6)
Gather Victim Network Information (0/6)	Compromise Infrastructure (0/7)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Autostart Execution (0/14)
Gather Victim Org Information (0/4)	Develop Capabilities (0/4)	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Boot or Logon Initialization
Phishing for Information (0/4)	Establish Accounts (0/3)	Phishing (0/4)	Inter-Process Communication (0/3)	Compromise Client Software Binary	
Search Closed Sources (0/2)	Obtain Capabilities	Replication Through			

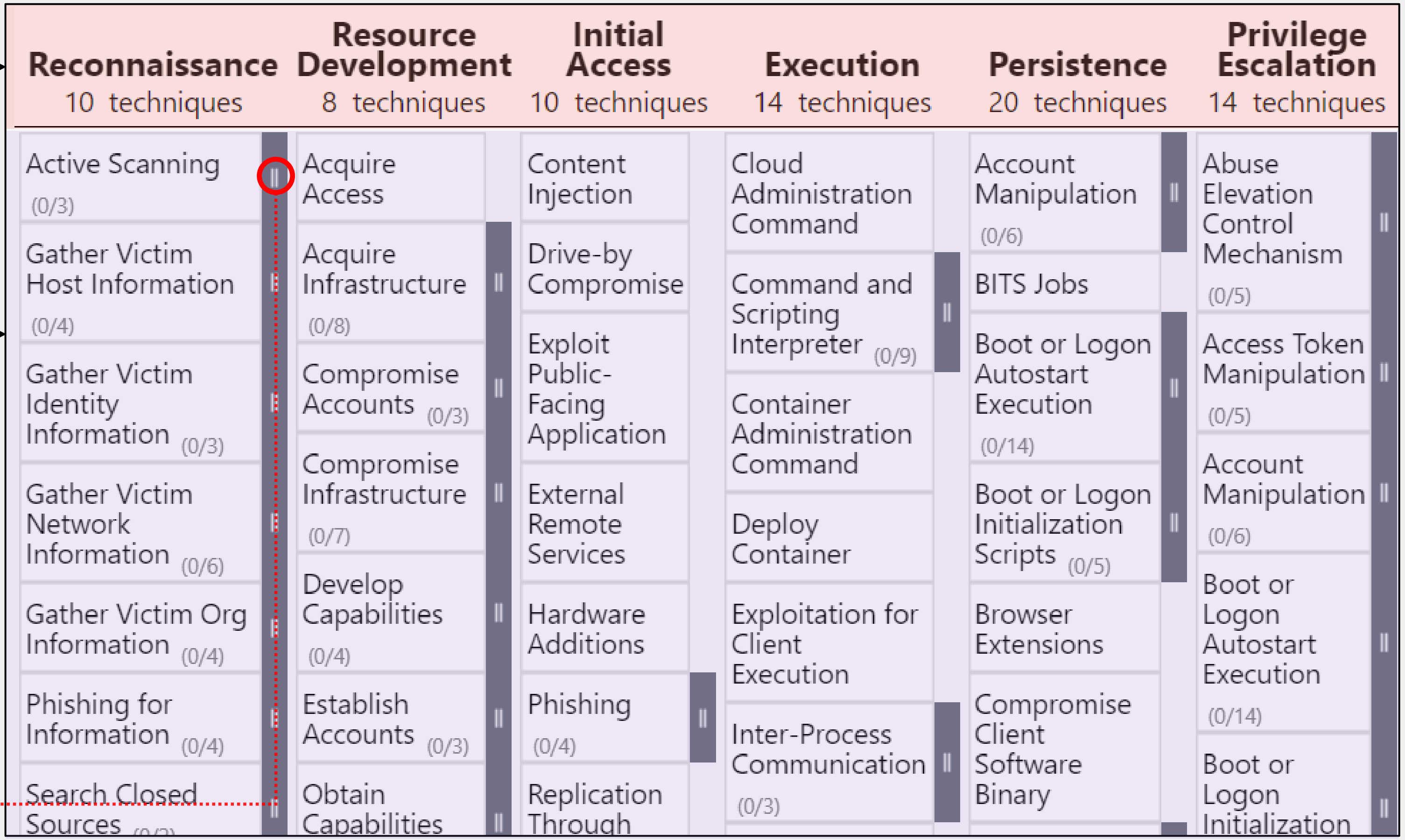
Note: Not all tactics and techniques are shown

FORTINET
Training Institute

MITRE ATT&CK Overview (Contd)

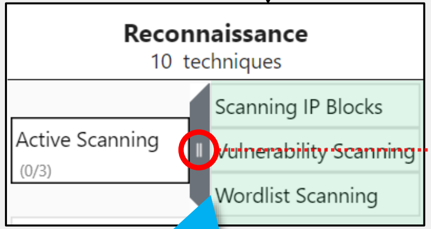
Tactics

Techniques



Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 10 techniques	Execution 14 techniques	Persistence 20 techniques	Privilege Escalation 14 techniques
Active Scanning (0/3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (0/6)	Abuse Elevation Control Mechanism (0/5)
Gather Victim Host Information (0/4)	Acquire Infrastructure (0/8)	Drive-by Compromise	Command and Scripting Interpreter (0/9)	BITS Jobs	Access Token Manipulation (0/5)
Gather Victim Identity Information (0/3)	Compromise Accounts (0/3)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (0/14)	Account Manipulation (0/6)
Gather Victim Network Information (0/6)	Compromise Infrastructure (0/7)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Autostart Execution (0/14)
Gather Victim Org Information (0/4)	Develop Capabilities (0/4)	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Boot or Logon Initialization
Phishing for Information (0/4)	Establish Accounts (0/3)	Phishing (0/4)	Inter-Process Communication (0/3)	Compromise Client Software Binary	
Search Closed Sources (0/2)	Obtain Capabilities	Replication Through			

Subtechniques



Reconnaissance
10 techniques

Active Scanning (0/3)	Scanning IP Blocks
	Vulnerability Scanning
	Wordlist Scanning

Expand to see subtechniques

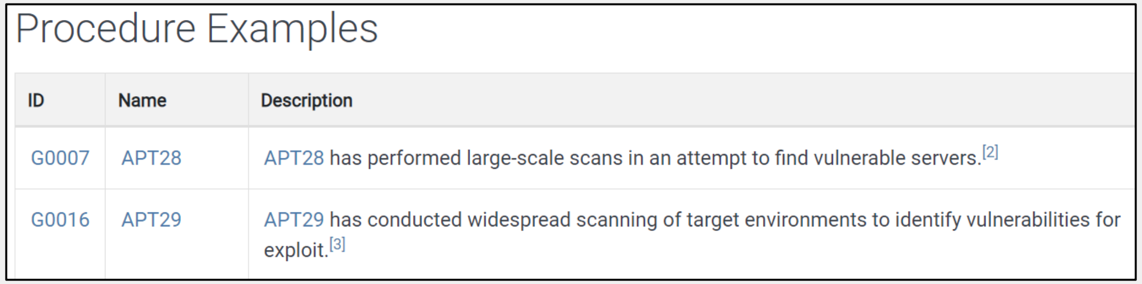
Note: To see all 14 tactics, access the ATT&CK Navigator: https://mitre-attack.github.io/attack-navigator/

MITRE ATT&CK Procedure, Mitigation, and Detection

- Procedure examples include information about known bad actors who use a technique

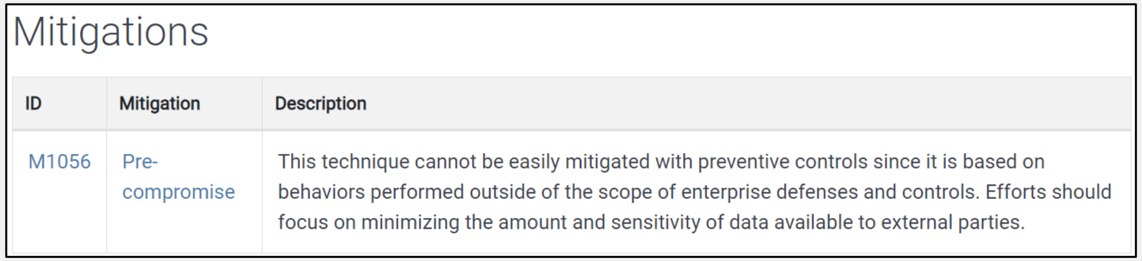
- Mitigations represent security concepts and classes of technology that may prevent the successful execution of a technique or subtechnique

- Detection covers high-level security concepts and classes of technology that can detect the execution of a technique or subtechnique



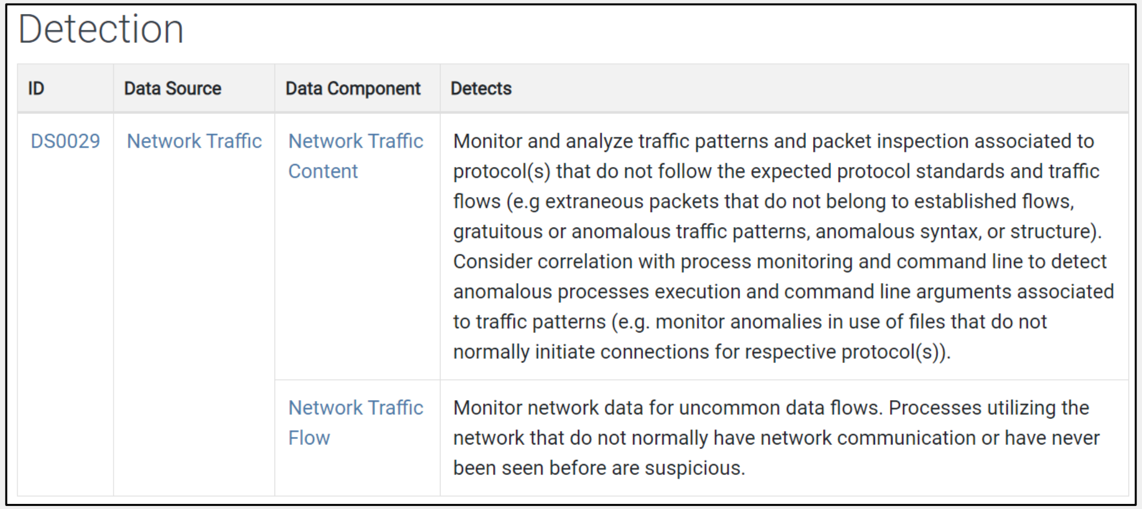
Procedure Examples

ID	Name	Description
G0007	APT28	APT28 has performed large-scale scans in an attempt to find vulnerable servers.[2]
G0016	APT29	APT29 has conducted widespread scanning of target environments to identify vulnerabilities for exploit.[3]



Mitigations

ID	Mitigation	Description
M1056	Pre-compromise	This technique cannot be easily mitigated with preventive controls since it is based on behaviors performed outside of the scope of enterprise defenses and controls. Efforts should focus on minimizing the amount and sensitivity of data available to external parties.



Detection

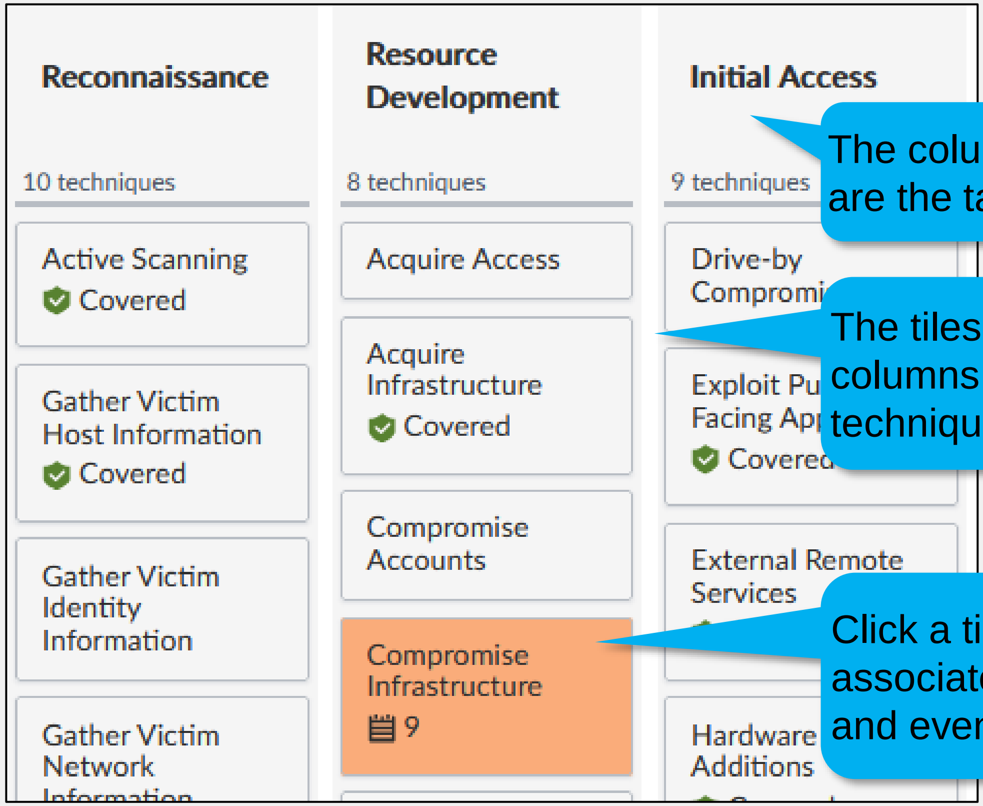
ID	Data Source	Data Component	Detects
DS0029	Network Traffic	Network Traffic Content	Monitor and analyze traffic patterns and packet inspection associated to protocol(s) that do not follow the expected protocol standards and traffic flows (e.g extraneous packets that do not belong to established flows, gratuitous or anomalous traffic patterns, anomalous syntax, or structure). Consider correlation with process monitoring and command line to detect anomalous processes execution and command line arguments associated to traffic patterns (e.g. monitor anomalies in use of files that do not normally initiate connections for respective protocol(s)).
		Network Traffic Flow	Monitor network data for uncommon data flows. Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious.

Note: Procedure, Mitigation, and Detection examples can be found at: https://attack.mitre.org/

MITRE ATT&CK Framework Matrices in FortiAnalyzer

- Cybersecurity tactics and techniques organized into matrices

Incidents & Events > MITRE ATT&CK > Attack



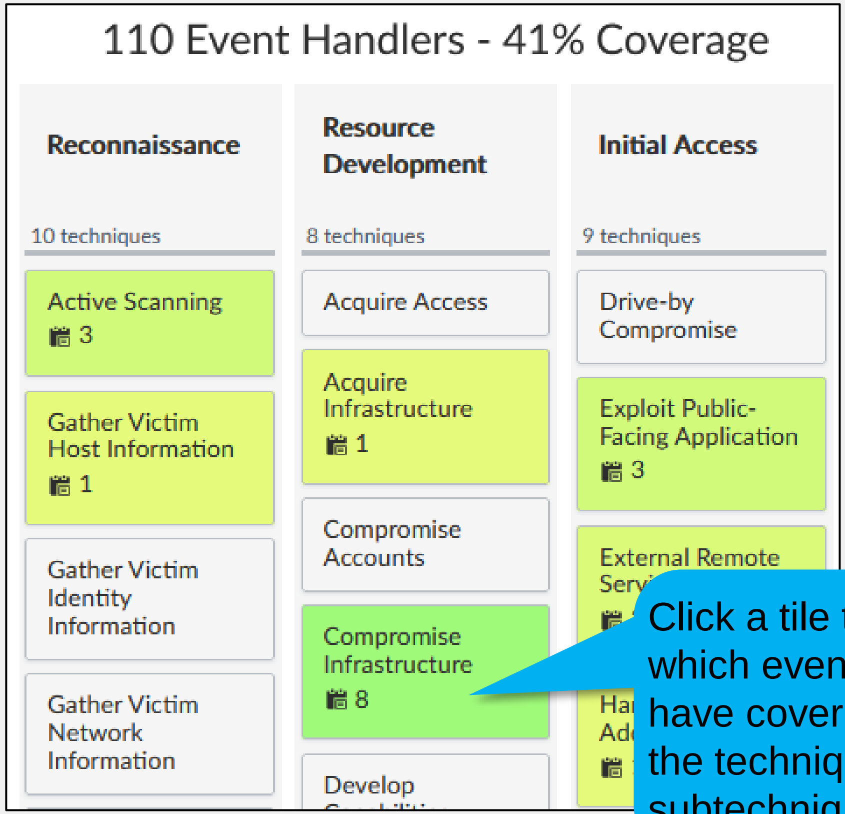
Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 9 techniques
Active Scanning ✓ Covered	Acquire Access	Drive-by Compromi
Gather Victim Host Information ✓ Covered	Acquire Infrastructure ✓ Covered	Exploit Pu Facing App ✓ Covered
Gather Victim Identity Information	Compromise Accounts	External Remote Services
Gather Victim Network Information	Compromise Infrastructure 9	Hardware Additions

The column headers are the tactics

The tiles under the columns are the techniques

Click a tile to see associated incidents and events

Incidents & Events > MITRE ATT&CK > Coverage



110 Event Handlers - 41% Coverage

Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 9 techniques
Active Scanning 3	Acquire Access	Drive-by Compromise
Gather Victim Host Information 1	Acquire Infrastructure 1	Exploit Public-Facing Application 3
Gather Victim Identity Information	Compromise Accounts	External Remote Servi
Gather Victim Network Information	Compromise Infrastructure 8	Ha Ad
	Develop	

Click a tile to see which event handlers have coverage against the technique or subtechnique

Note: Not all tactics and techniques are shown

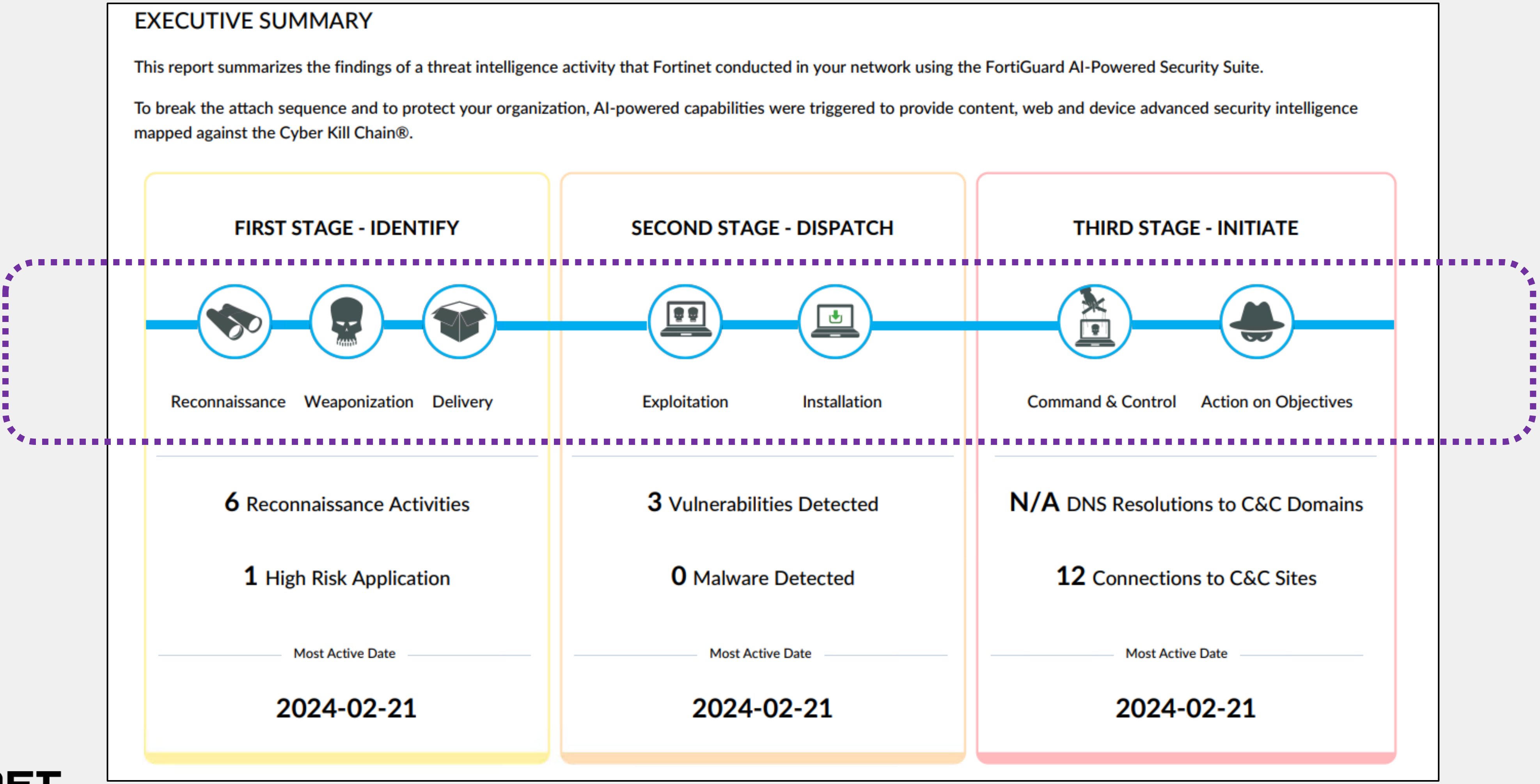
Cyber Kill Chain Overview

- Framework developed by Lockheed Martin
- Identifies what adversaries have to complete in order to achieve their objectives on a target
- Derived from a military concept called kill chain
- Provide visibility and understanding of sophisticated attacks and attacker’s tactics, techniques, and procedures
- Consists of seven steps that represent stages of advanced persistent threats (APT)

Reconnaissance	Gather information about the target
Weaponization	Use the gathered information to embed malware
Delivery	Transmission of the malware
Exploitation	Target system vulnerability
Installation	Malware is installed
Command & Control	Connection to an outside server is established
Actions on Objective	Attack on the network commences

Cyber Kill Chain in FortiAnalyzer

- In FortiAnalyzer, the predefined threat report is mapped to the Cyber Kill Chain stages for correlation and pattern identification



EXECUTIVE SUMMARY

This report summarizes the findings of a threat intelligence activity that Fortinet conducted in your network using the FortiGuard AI-Powered Security Suite.

To break the attach sequence and to protect your organization, AI-powered capabilities were triggered to provide content, web and device advanced security intelligence mapped against the Cyber Kill Chain®.

FIRST STAGE - IDENTIFY

Reconnaissance Weaponization Delivery

6 Reconnaissance Activities

1 High Risk Application

Most Active Date

2024-02-21

SECOND STAGE - DISPATCH

Exploitation Installation

3 Vulnerabilities Detected

0 Malware Detected

Most Active Date

2024-02-21

THIRD STAGE - INITIATE

Command & Control Action on Objectives

N/A DNS Resolutions to C&C Domains

12 Connections to C&C Sites

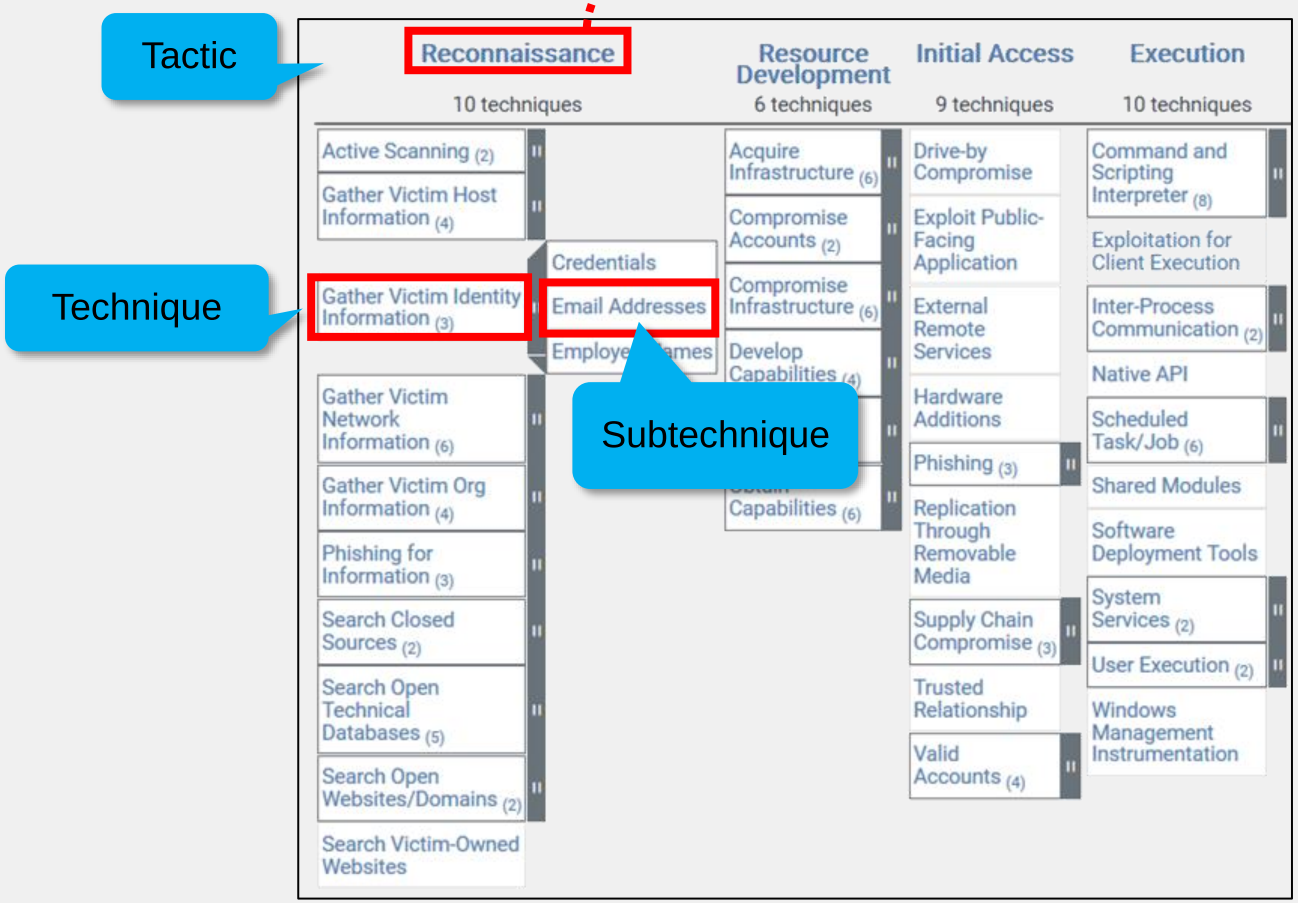
Most Active Date

2024-02-21

Adversary Behavior—MITRE ATT&CK vs. Cyber Kill Chain

Scenario: Group ABC initially *probes* the potential target's email systems in search of valid email accounts.

MITRE ATT&CK



Reconnaissance 10 techniques		Resource Development 6 techniques	Initial Access 9 techniques	Execution 10 techniques
Active Scanning (2)		Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (8)
Gather Victim Host Information (4)		Compromise Accounts (2)	Exploit Public-Facing Application	Exploitation for Client Execution
Gather Victim Identity Information (3)	Credentials Email Addresses Employee Names	Compromise Infrastructure (6)	External Remote Services	Inter-Process Communication (2)
Gather Victim Network Information (6)		Develop Capabilities (4)	Hardware Additions	Native API
Gather Victim Org Information (4)		Obtain Capabilities (6)	Phishing (3)	Scheduled Task/Job (6)
Phishing for Information (3)			Replication Through Removable Media	Shared Modules
Search Closed Sources (2)			Supply Chain Compromise (3)	Software Deployment Tools
Search Open Technical Databases (5)			Trusted Relationship	System Services (2)
Search Open Websites/Domains (2)			Valid Accounts (4)	User Execution (2)
Search Victim-Owned Websites				Windows Management Instrumentation

Cyber Kill Chain

Reconnaissance	Gather information about the target
Weaponization	Use the gathered information to embed malware
Delivery	Transmission of the malware
Exploitation	Target system vulnerability
Installation	Malware is installed
Command & Control	Connection to an outside server is established
Actions on Objective	Attack on the network commences

FORTINET
Training Institute

Knowledge Check

1. Which model or framework allows for a more detailed mapping of adversary behavior?

✓ A. MITRE ATT&CK

B. Lockheed Martin’s Cyber Kill Chain

2. Which one is a MITRE ATT&CK tactic?

✓ A. Initial access

B. Exploitation

Lesson Progress

- ✓ SOC Main Functions and Roles
- ✓ Fortinet SOC Environment Benefits
- ✓ Attack Frameworks Overview

Review

- ✓ Describe the main functions and roles within a SOC
- ✓ Identify the main challenges within a SOC
- ✓ Identify the challenges that can be solved by the Fortinet SOC
- ✓ Describe the MITRE ATT&CK Matrix for Enterprise
- ✓ Describe the Cyber Kill Chain