Cyberthreat Hunting Summative Assessment

For each of the MITRE ATT&CK Framework Major Stages answer the following:

Describe/define the stage

What are at least 3 different techniques in this stage?

Where may you look to identify activity within this stage on your network? (i.e., what systems, log sources, etc.)

If you find activity within this stage, what would your next step be?

The major stages are:

Reconnaissance:

What are at least 3 different techniques in this stage?

Active Scanning

Gather Victim Host Info

Gather Victim Identityinfo

Where may you look to identify activity within this stage on your network? (i.e., what systems, log sources, etc.)

Scanning IP Blocks

Hardware Info of Victim

firewall logs

If you find activity within this stage, what would your next step be?

dont panic, find out where and who is trig to attack

Resource Development:

What are at least 3 different techniques in this stage?

Acquire Infrastructure

Compromise Accounts

Compromised Credentials

Where may you look to identify activity within this stage on your network? (i.e., what systems, log sources, etc.)

Domains log

Social Media Accounts

Virtual Private Server log

If you find activity within this stage, what would your next step be?

gain further info about attacker, try to identify the activity during resource development

Initial Access & Execution:

What are at least 3 different techniques in this stage?

Phishing

Supply Chain Compromise

Command Interpreter

Where may you look to identify activity within this stage on your network? (i.e., what systems, log sources, etc.)

antiMmalware logs

Firewallintrusion detection logs

email antiMalware logs

If you find activity within this stage, what would your next step be?

Gain more info aboutattacker and scope of attack. act fast to identfy and remove threat before they gain more of a foothold

Persistence:

What are at least 3 different techniques in this stage?

Account Manipulation

Boot Auto Start

Boot Initialization Scripts

Where may you look to identify activity within this stage on your network? (i.e., what systems, log sources, etc.)

Logon Script (Windows)

RegistryRun Keys

email logs from unknown source

If you find activity within this stage, what would your next step be?

Expand the search and resources to identify the threat and full scope of their access

Discovery and Lateral Movement:

What are at least 3 different techniques in this stage?

Remote Service Session

Account Discovery

Premission Groups Discovery

Where may you look to identify activity within this stage on your network? (i.e., what systems, log sources, etc.)

Domain Groups

SSH Hijacking

Email Accounts

If you find activity within this stage, what would your next step be?

Act Immediately to understand the threat and scopeof sccess

Command and Control:

What are at least 3 different techniques in this stage?

Application Layer Protocol

DataEncoding

Encrypted Channels

Where may you look to identify activity within this stage on your network? (i.e., what systems, log sources, etc.)

Firewall Logs

traffic bound for a known command and control channel

If you find activity within this stage, what would your next step be?

Take immediate action to first gsther info about the command and control network traffic, and than shut down the channel

Impact:

What are at least 3 different techniques in this stage?

Data destruction

Data exfiltration

denial of service

Where may you look to identify activity within this stage on your network? (i.e., what systems, log sources, etc.)

No need to go looking, it will be obvious

If you find activity within this stage, what would your next step be?

Begin incident response and recovery opertaions to minimize damage