Introduction

Environment

Welcome Student

1. This scenario takes place on a hypothetical company.

2. The company's information is described in the file titled "brief-company". The download button is placed below these instructions.

3. Before you continue, it is required to download and read carefully this document which contains critical information to complete the activities.

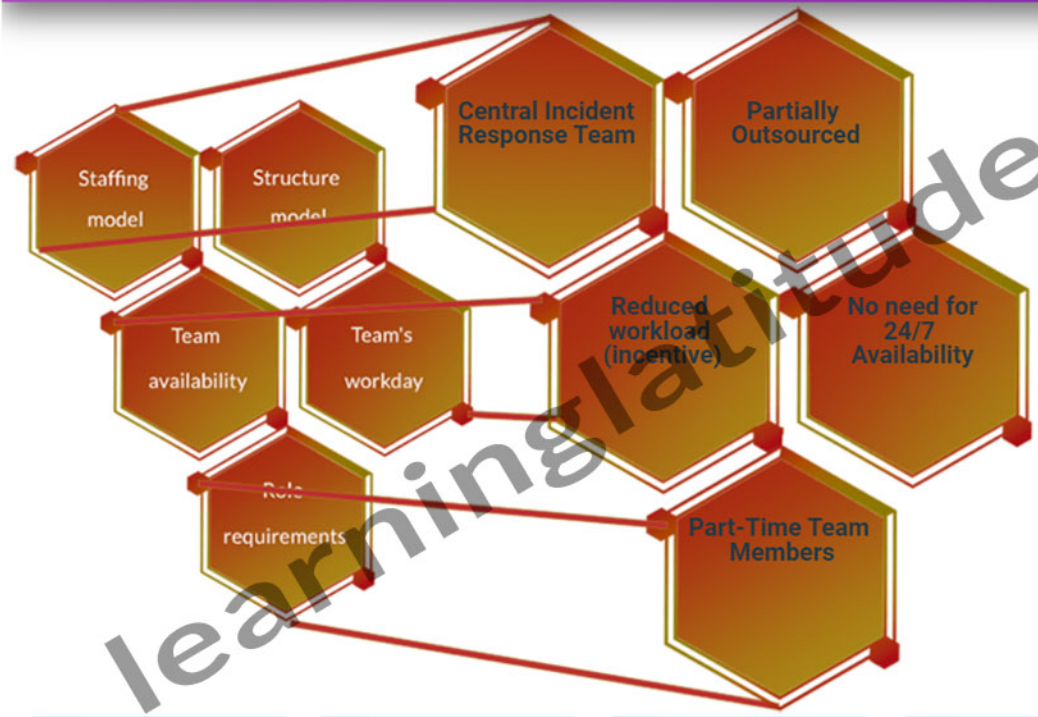
Glossary

brief-company

Continue

Complete

Incident Response Team



Print/Save Analysis

Continue

Once you click on the "Continue" button you will not be able to change the team's choice.

If you need to make a change use the buttons at the bottom.

Update Staffing Model

Update Structure Model

Update Team availability

Update Team's workday

Update Role requirements

I SCENARIO

1. The network admin detected an abnormal traffic
2. Three of the six Huawei routers in the company are trying to reach out an IP address

   217.110.254.18

   The affected routers are in the network of the ISP **M-net**

3. After a daunting task, the network administrator sends to the IRT the indicator of compromise (md5)

   cf203ca2c8d8411b7c7cfb1baf0f51c2

Alert Student

1- Please go to the following site https://otx.alienvault.com/.... (link is shown below - blue circle)
In the search bar of this site enter the string of characters provided in the scenario document - (see item # 3 of the scenario).

2. Read the information shown in the page, after the search is completed. Identify the type of attack.

3- Please go to the link (below) whatismyipaddress.com (link is shown below - blue circle) ...and enter the IP address provided in the scenario document - (see item # 2 of the scenario).
Identify who is affected / targeted in this attack.

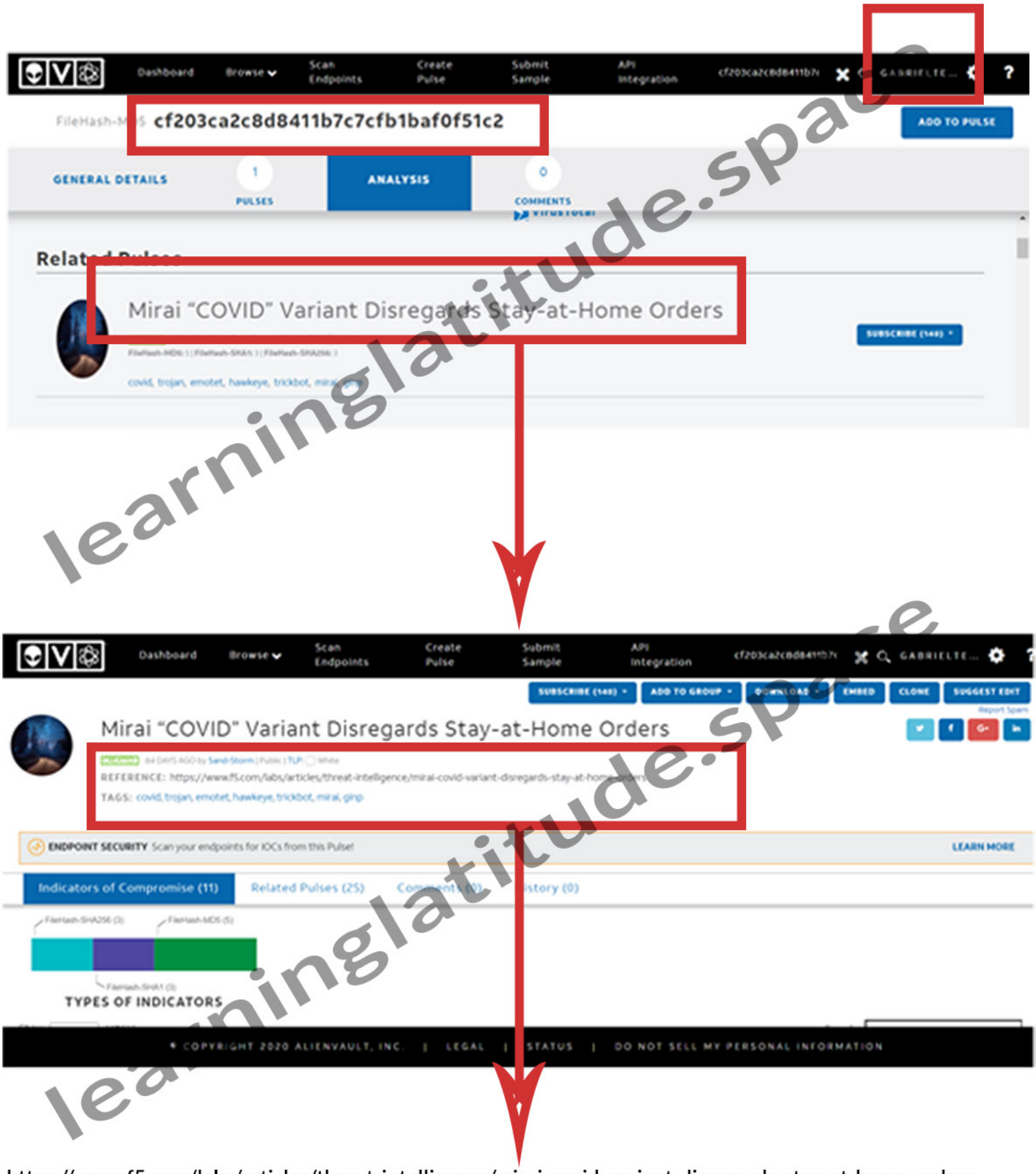
4. Identify the Host name of the affected /targeted party - Refer to the image to the right as example.

learninglatitude.space

whatismyipaddress.com

otx.alienvault.com

scenario



https://www.f5.com/labs/articles/threat-intelligence/mirai-covid-variant-disregards-stay-at-home-orders

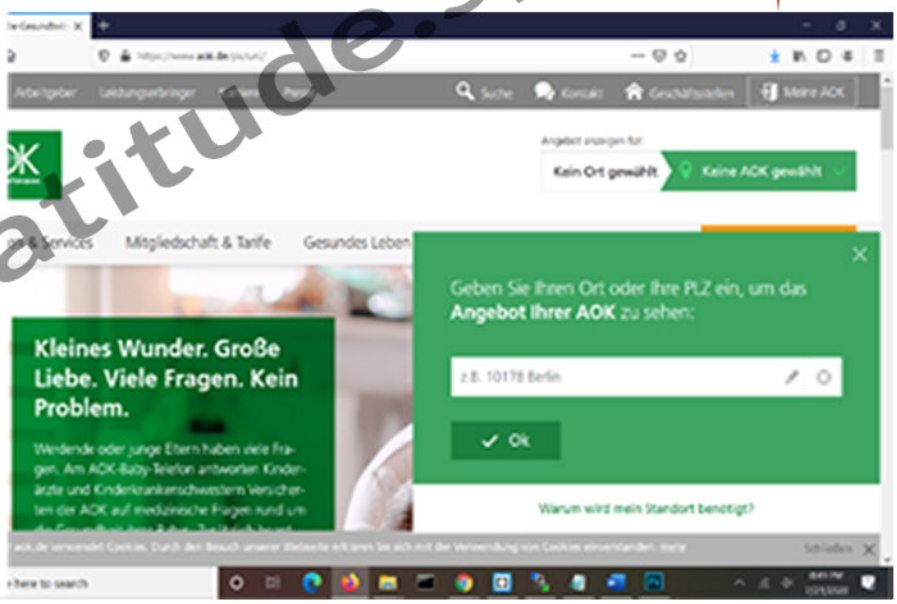
217.110.254.18 Lookup IP Address

Details for 217.110.254.18

IP: 217.110.254.18
Decimal: 3647929874
Hostname: ns2.aok.de
ASN: 8220
ISP: COLT Technology Services Group Limited
Organization: COLT Technology Services Group Limited
Services: None detected
Type: Corporate
Assignment: Likely Static IP
Blacklist: Click to Check Blacklist Status
Continent: Europe
Country: Germany
State/Region: Hesse
City: Frankfurt am Main
Latitude: 50.1188 (50° 7' 7.68" N)
Longitude: 8.6843 (8° 41' 3.48" E)
Postal Code: 60313

Hostname: ns2.aok.de

Geolocation Map



Decision-making

DETECTION

Write your comments

Malware name	Mirai "COVID" Variant Disregards Stay-at-Home Orders
Malware type	botnet (or thingbot)
Malware short description	Mirai is an IoT botnet (or thingbot) created to launch DDoS attacks. Mirai focuses TeamSpeak and Huawei devices because these systems have historically had vulnerabilities

Continue

Decision-making

DETECTION

Write your comments

Target affected	Company AOK Webpage www.aok.de
Target information	AOK is one of the oldest statutory health insurers Phone 0800 2650800 Company number (BNR): 90235319 Institutional number (IKNR): 109519005
Other third parties affected	ISP(M-net and Deutsche Telekom)

Continue

Print/Save Analysis

Decision-making

Web

Attack Vectors & Impact

Productivity	Less than 1% of systems; less than 1% of workforce	More than 1% workforce, but less than 10% of systems	More than 1% systems but less than 10% of workforce	More than 10% of systems; more than 10% of workforce	N/A
Widespread	Minimal	Moderate	High	None	N/A
Commonality	Commonly Seen	Occasionally happens	Rare	Never	N/A
Damage	Minimal	Moderate	High		N/A
Affected Parties	Less than 1% of systems; less than 1% of workforce	More than 1% workforce, but less than 10% of systems	More than 1% systems but less than 10% of workforce	More than 10% of systems; more than 10% of workforce	N/A
Business Impact	Minimal	Moderate	High		N/A

After you complete your selection of choices for this table, please click "continue" to advance to the next section. All decisions are final and you can Not go back to modify them, after advancing

Continue

Complete

Attack Vectors & Impact

Attrition	Severety	0
External/Removable Media	Severety	0
Web	Severety	11
Email	Severety	0
Impersonation	Severety	0
Improper usage	Severety	0
Loss or theft of equipment	Severety	0
Other	Severety	0

Priority Guideline	Score
Severity High: Loss of a major service	11

Initial action	Containment Goal
Immediately	<24 Hours

Print/Save Analysis

Continue

Analysis 1/3

Perform the next tasks.

1. **Propose three actions to improve security against this type of malware.**
2. Upload your proposal as a Word doc, into the virtual room, in the appropiate thread, for feedback and comments,
3. Once completed the previous steps click on the button "Continue".

Continue

1. Establish a policy to change periodically passwords**.
2. Avoid the use of default passwords in all devices.
3. Review and propose the replacement of network equipment that are known vulnerable.

**At least 8 characters

A combination of both, uppercase and lowercase letters

A combination of letters and numbers

Addition of at least one special character, e.g.,! @ # ?]

Analysis 2/3

SOP

Standard Operating Procedure

The IT department has developed some standard operation procedures (Playbooks) that your team has adopted.

Read the SOP's

Assign the SOP adequate to respond to the incident

Remote Access Trojan (RAT)

Phising

Denial-of-Service (DoS)

Denial-of-Service DoS — Assign

Phishing — No Assign

RAT — Assign

Print/Save Analysis

Continue