Cyber Threat Intelligence BY P3NGU1N

CTI Lifecycle

🎯 At what stage is big data created in cyber threat intelligence?

ANSWER: information gathering

🎯 Which of the following is not among the questions that the organization should ask itself during the Planning and Direction phase?

- A- Does the organization have a SOC team?
- B- Has the organization been attacked before?
- C- Do the attacks target the organization or the individuals?
- D- Which EDR product is used in the organization?

ANSWER: d

🎯 Tom, the cyber security analyst in the SOC team, wants to collect data from the major intelligence sources for his organization. Tom wants to use decoy systems to detect potential attackers. Which intelligence source is Tom trying to bring in?

ANSWER: honeypot

Types of Cyber Threat Intelligence

🎯 What type of intelligence is appropriate for a threat hunter in the organization?

ANSWER: operational cyber threat intelligence

🎯 What type of threat intelligence is appropriate for an employee working as an L1 analyst in the organization?

ANSWER: technical cyber threat intelligence

Determining the Attack Surface

🎯 How many subdomains does "blueteam.training" have?

ANSWER: 0

🎯 What is the service of the page builder on letsdefend.io/blog/ ?

ANSWER: webflow

🎯 Which of the following is not one of the subdomain discovery tools?

- Aquatone
- Httpx
- Sublist3r
- SecurityTrails

ANSWER: httpx

🎯 Shodan can be used to detect IP blocks. (True or False)

ANSWER: true

Gathering Threat Intelligence

🎯 What is the name of the data that identifies a threat, threat actor, malicious files, and plays an important role in threat intelligence?

ANSWER: ioc

🎯 What is the filter that allows us to search the name of an organization on Shodan?

ANSWER: org

🎯 Which of the following is not among the messaging applications that threat actors frequently use?

- Telegram
- ICQ
- IRC
- Instagram DM

ANSWER: Instagram DM

🎯 Practice question – Tom is a SOC analyst at “LetsDefend” organization. Tom received a notification stating that malware containing the name of his organization was uploaded to AnyRun. Find the IP address the malware is connecting to?

File MD5 Hash: f6517b0a49bb245e1983d77d2f5b2f98

ANSWER: 192.168.50.104

🎯 How many processes does the malware with the MD5 Hash value "f6517b0a49bb245e1983d77d2f5b2f98" create?

ANSWER: 2

Threat Intelligence Data Interpretation

🎯 What is the first data collected in threat intelligence called?

ANSWER: big data

Using Threat Intelligence

🎯 What part of extended threat intelligence contains vulnerability management?

ANSWER: easm

🎯 If we receive an alarm from the threat intelligence product we use indicating that an IP address of our organization has been blacklisted. Which of the following actions would be incorrect to apply in this situation?

A- The reason why the IP address is blacklisted should be determined.

B- The reputation should be corrected by contacting the vendor whose IP address is blacklisted.

C- The IP address should be disabled.

D- A search should be made for the server to which the IP address points.

ANSWER: c

🎯 Mike is a SOC analyst at LetsDefend. The organization received intelligence indicating that the "fac941eefc8571e51aef69289b5903c4" MD5 value of one of its systems was found in malicious data. Mike needs to isolate the device from the network. Can you help us, what is the hostname of this endpoint?

(go to endpoint security section in lets defend)

ANSWER: temphost

Threat Intelligence and SOC Integration

🎯 Which network security tool should be integrated to the threat intelligence products in order to prevent malicious inbound traffic coming into our organization in the fastest way?

ANSWER: firewall

🎯 Which of the following cannot be integrated with threat intelligence?

- EDR
- SIEM
- SOAR
- Nmap

ANSWER: Nmap

QUIZ:

🎯 **Which of the followings is not one of the stages in the CTI Lifecycle?**

ANSWER: **External Attack Surface Management**

🎯 **How many types of cyber threat intelligence are there?**

ANSWER: 4

🎯 **Which of the following is one of the tools used to create the domain structure while creating the attack surface?**

ANSWER: Aquatone

🎯 **Which tab in the developer console should we use to display the header of incoming requests within the outgoing and incoming request structures to detect web technologies?**

ANSWER: Network

🎯 **Which of the followings is not a tool used to detect the e-mail addresses of C-Level employees?**

ANSWER: **SecurityTrails**

🎯 **Which of the followings is not one of the sources where threat intelligence is collected?**

ANSWER: **E-Commerce Website Comments**

🎯 **Which of the following alerts is considered within the External Attack Surface Management area?**

ANSWER: **DNS Zone Transfer Detected**

🎯 **Which of the following alarms is considered within the Digital Risk Protection field?**

ANSWER: **Botnet Detected at Black Market**

🎯 **If a cybersecurity analyst receives an alert indicating that there is another domain mimicking his organization's website, which of the following actions should he take?**

ANSWER: **The domain should be taken down**

🎯 **Which of the following security tools cannot be integrated with threat intelligence products?**

ANSWER: Nuclei