

1. Which three (3) of these were among the top 5 security drivers in 2019? (Select 3)

1 point

☒ Factors such as cloud migration and IT complexity act as cost multipliers making new breaches increasingly expensive

☐ New security and privacy laws that went into effect in 2019

☒ A significant skills gap exists with more new cybersecurity professional needed the total number currently working in this field

☒ IOT device attacks moving from targeting consumer electronics to targeting enterprise devices
2. What was the average time to identify and contain a breach in 2019?

1 point

☐ 12 hours

☐ 7 days

☐ 46 days

☒ 279 days
3. Which industry had the highest average cost per breach in 2019 at \$6.45M

1 point

☐ Manufacturing

☐ Finance

☐ Government

☐ Technology

☒ Healthcare

☐ Retail
4. Breaches caused by which source resulted in the highest cost per incident in 2019?

1 point

☐ Employee or contractor negligence

☐ Criminal insider

☐ Politically motivated hactivists

☒ Credentials theft
5. According to the Threat Intelligence Strategy Map, The threat intelligence process can be broken down into 4 steps: Collect, Process, Analyze, and Share. Which step would contain activities such as normalize, correlate, confirm and enrich the data?

1 point

☐ Collect

☒ Process

☐ Analyze

☐ Share
6. According to the Threat Intelligence Strategy Map, The threat intelligence process can be broken down into 4 steps: Collect, Process, Analyze, and Share. Which step would contain activities such as investigate, contain, remediate and prioritize?

1 point

☐ Collect

☐ Process

☒ Analyze

☐ Share
7. According to the Crowdstrike model, threat hunters, vulnerability management and incident response belong in which intelligence area?

1 point

☐ Tactical

☐ Control

☒ Operational

☐ Strategic
8. Which three (3) sources are recommended reading for any cybersecurity professional? (Select 3)

1 point

☒ X-Force Exchange

☐ Der CyberSpiegel

☒ InfoSecurity Magazine

☒ Krebs on Security
9. Which two (2) of these were among the 4 threat intelligence platforms covered in the Threat Intelligence Platforms video? (Select 2)

1 point

☒ IBM X-Force Exchange

☒ TruSTAR

☐ BigFix

☐ AVG Ultimate
10. Which threat intelligence framework is divided into 3 levels. Level 1 is getting to know your adversaries. Level 2 involves mapping intelligence yourself and level 3 where you map more information and use that to plan your defense?

1 point

☐ Diamond Model of Intrusion Analysis

☐ Lockheed Martin Cyber Kill Chain

☒ Mitre Att&ck Knowledgebase

☐ Cyber Threat Framework
11. True or False. An organization's security immune system should be isolated from outside organizations, including vendors and other third-parties to keep it from being compromised.

1 point

☐ True

☒ False
12. Activities performed as a part of security intelligence can be divided into pre-exploit and post-exploit activities. Which two (2) of these are pre-exploit activities? (Select 2)

1 point

☐ Perform forensic investigation

☐ Gather full situational awareness through advanced security analytics


☒ Prioritize vulnerabilities to optimize remediation processes and close critical exposures

☒ Detect deviations from the norm that indicate early warnings of APTs
13. True or False. According to the FireEye Mandiant's Security Effectiveness Report 2020, more that 50% of successful attacks are able to infiltrate without detection.

1 point

☒ True

☐ False

Coursera Honor Code [Learn more](#) 

☒ I, **Giang Pham**, understand that submitting work that isn't my own may result in permanent failure of this course or deactivation of my Coursera account.

Submit

Save draft