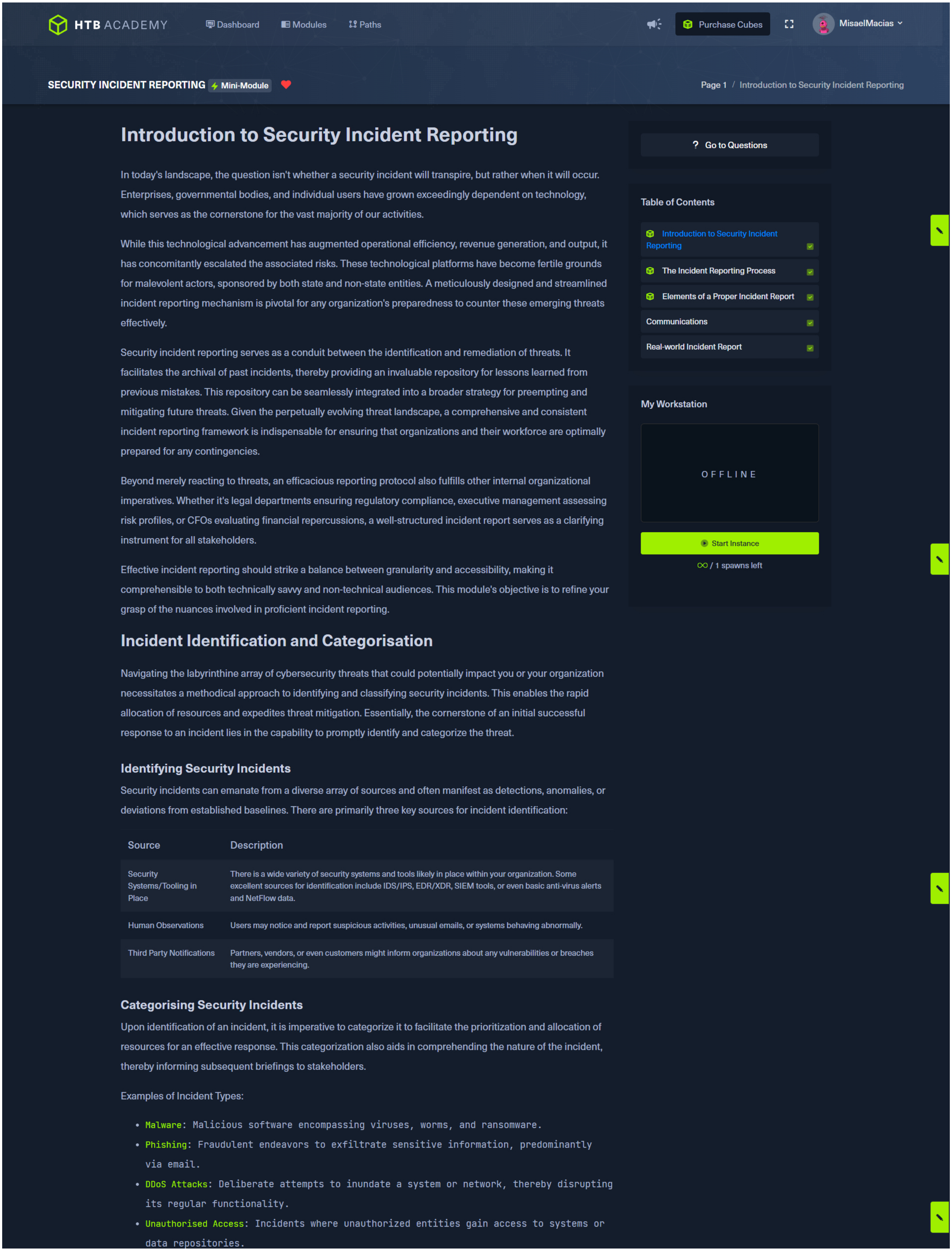


Introduction to Security Incident Reporting

In today's landscape, the question isn't whether a security incident will transpire, but rather when it will occur. Enterprises, governmental bodies, and individual users have grown exceedingly dependent on technology, which serves as the cornerstone for the vast majority of our activities.

While this technological advancement has augmented operational efficiency, revenue generation, and output, it has concomitantly escalated the associated risks. These technological platforms have become fertile grounds for malevolent actors, sponsored by both state and non-state entities. A meticulously designed and streamlined incident reporting mechanism is pivotal for any organization's preparedness to counter these emerging threats effectively.

Security incident reporting serves as a conduit between the identification and remediation of threats. It facilitates the archival of past incidents, thereby providing an invaluable repository for lessons learned from previous mistakes. This repository can be seamlessly integrated into a broader strategy for preempting and mitigating future threats. Given the perpetually evolving threat landscape, a comprehensive and consistent incident reporting framework is indispensable for ensuring that organizations and their workforce are optimally prepared for any contingencies.

Beyond merely reacting to threats, an efficacious reporting protocol also fulfills other internal organizational imperatives. Whether it's legal departments ensuring regulatory compliance, executive management assessing risk profiles, or CFOs evaluating financial repercussions, a well-structured incident report serves as a clarifying instrument for all stakeholders.

Effective incident reporting should strike a balance between granularity and accessibility, making it comprehensible to both technically savvy and non-technical audiences. This module's objective is to refine your grasp of the nuances involved in proficient incident reporting.

Incident Identification and Categorisation

Navigating the labyrinthine array of cybersecurity threats that could potentially impact you or your organization necessitates a methodical approach to identifying and classifying security incidents. This enables the rapid allocation of resources and expedites threat mitigation. Essentially, the cornerstone of an initial successful response to an incident lies in the capability to promptly identify and categorize the threat.

Identifying Security Incidents

Security incidents can emanate from a diverse array of sources and often manifest as detections, anomalies, or deviations from established baselines. There are primarily three key sources for incident identification:

Source	Description
Security Systems/Tooling in Place	There is a wide variety of security systems and tools likely in place within your organization. Some excellent sources for identification include IDS/IPS, EDR/XDR, SIEM tools, or even basic anti-virus alerts and NetFlow data.
Human Observations	Users may notice and report suspicious activities, unusual emails, or systems behaving abnormally.
Third Party Notifications	Partners, vendors, or even customers might inform organizations about any vulnerabilities or breaches they are experiencing.

Categorising Security Incidents

Upon identification of an incident, it is imperative to categorize it to facilitate the prioritization and allocation of resources for an effective response. This categorization also aids in comprehending the nature of the incident, thereby informing subsequent briefings to stakeholders.

Examples of Incident Types:

- `Malware`: Malicious software encompassing viruses, worms, and ransomware.
- `Phishing`: Fraudulent endeavors to exfiltrate sensitive information, predominantly via email.
- `DDoS Attacks`: Deliberate attempts to inundate a system or network, thereby disrupting its regular functionality.
- `Unauthorised Access`: Incidents where unauthorized entities gain access to systems or data repositories.

? Go to Questions

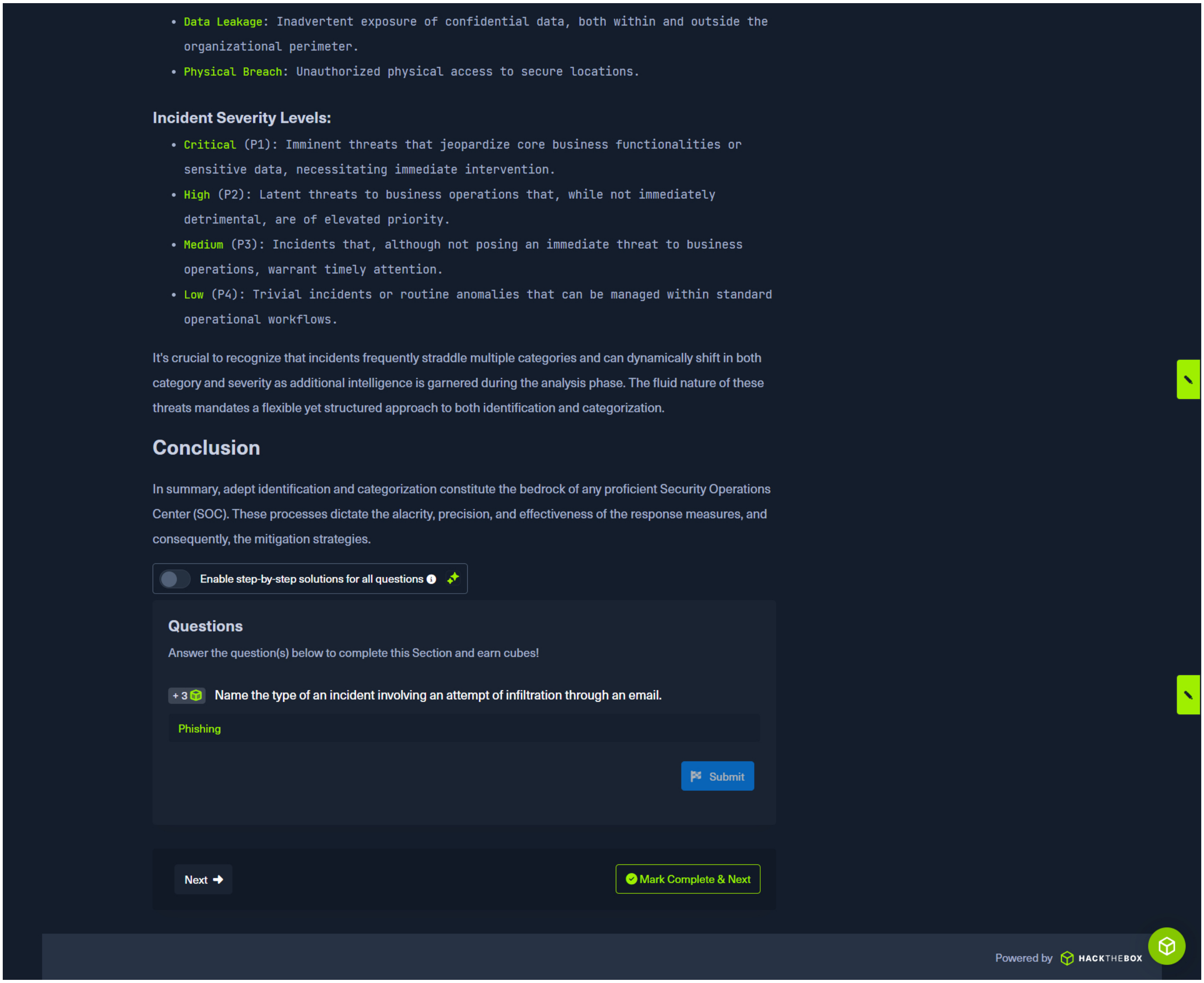
Table of Contents

My Workstation

OFFLINE

Start Instance

∞ / 1 spawns left



- Data Leakage: Inadvertent exposure of confidential data, both within and outside the organizational perimeter.
- Physical Breach: Unauthorized physical access to secure locations.

Incident Severity Levels:

- Critical (P1): Imminent threats that jeopardize core business functionalities or sensitive data, necessitating immediate intervention.
- High (P2): Latent threats to business operations that, while not immediately detrimental, are of elevated priority.
- Medium (P3): Incidents that, although not posing an immediate threat to business operations, warrant timely attention.
- Low (P4): Trivial incidents or routine anomalies that can be managed within standard operational workflows.

It's crucial to recognize that incidents frequently straddle multiple categories and can dynamically shift in both category and severity as additional intelligence is garnered during the analysis phase. The fluid nature of these threats mandates a flexible yet structured approach to both identification and categorization.

Conclusion

In summary, adept identification and categorization constitute the bedrock of any proficient Security Operations Center (SOC). These processes dictate the alacrity, precision, and effectiveness of the response measures, and consequently, the mitigation strategies.

Questions

Answer the question(s) below to complete this Section and earn cubes!

+ 3 Name the type of an incident involving an attempt of infiltration through an email.

Phishing