INCIDENT RESPONSE SIMULATION

Ransomware Attack

Simulate a scenario where a ransomware attack has occurred, affecting critical systems and encrypting important data. Participants must respond by containing the attack, identifying the entry point, restoring systems, and implementing security measures.

Data Breach

Simulate a scenario where sensitive customer data has been compromised. Participants must investigate the breach, identify the vulnerabilities, mitigate further damage, notify affected parties, and implement measures to prevent future breaches.

Insider Threat

Simulate an incident where a trusted employee intentionally or unintentionally compromises data or systems. Participants must detect and investigate the insider threat, mitigate the damage, terminate unauthorized access, and improve monitoring and access controls.

Phishing Campaign

Simulate a widespread phishing campaign targeting employees, attempting to gain unauthorized access to systems or sensitive information. Participants must educate employees, identify compromised accounts, and implement additional security controls to prevent future phishing attempts.

https://www.linkedin.com/in/joas-antonio-dos-santos/

PS C:\Windows\System32\Pwned> .\PSRansom.ps1 -h

PSRANSOM

 # DEHASHED

Break Free - Network Exfiltration Tester

PyExfil
Stress Testing Detection
(and your creativity)

gophish
Open-Source Phishing Toolkit

evilginx.

PwnAuth