Storyboard – FIRST 2025 Example 2

Exercise Date	June 24, 2025
Executive Sponsor	Dave Murray, Vice President of Information Technology
Development Team	Julie O'Conner, Lead Analyst (Facilitator) Michelle Kane, CIO
Location	Executive Conference Room
Goals	Perform a tabletop exercise aimed at ensuring the CSIRT can respond to an APT attack effecting the organization security operations.
Objectives	1. Perform a tabletop exercise focused on the compromise of the organization's social media accounts. 2. Examine the organization's security posture and response to a security incident pertaining to social media accounts. 3. Educate participating business staff on the importance of not reusing passwords.
Scenario	The National Cyber Security Incident Response Team (CSIRT) plays a crucial role in defending the country against cyber threats. However, it becomes the primary target of a sophisticated cyberattack launched by an Advanced Persistent Threat (APT) group, suspected to be state-sponsored. This attack aims to disrupt national cybersecurity operations, compromise sensitive threat intelligence, and erode public trust in the CSIRT's capabilities.
Inject #1 **Tuesday, 9:15am**	• The CSIRT's internal Security Operations Center (SOC) detects an unusual spike in outbound network traffic from its internal systems, suggesting possible data exfiltration. • Analysts notice suspicious login attempts from multiple global IP addresses, resembling a brute-force attack on privileged accounts. • A senior incident responder reports being locked out of their account, with their credentials seemingly used to access sensitive threat intelligence databases. • The SOC identifies an unauthorized command-and-control (C2) connection from a previously unknown system.
Inject #1 **Key Issues**	• What initial actions should be taken to validate and investigate this activity? • What logging and monitoring tools can help determine the scope of the intrusion? • Should external partners be alerted at this stage?
Inject #2 **Tuesday, 12;00 PM**	• Ransomware spreads across CSIRT's internal network, encrypting critical response tools and incident logs. • The CSIRT's public-facing threat intelligence portal is defaced, replacing security alerts with disinformation aimed at undermining trust in national cyber defense. • A ransomware note appears on compromised systems, demanding payment for decryption keys and threatening to leak classified cybersecurity incident reports. • Several CSIRT analysts report phishing emails containing malware, indicating that the attack may have originated from a spear-phishing campaign.
Inject #2 **Key Issues**	• What measures can be taken to contain the spread of ransomware and prevent reinfection?

	• Should the CSIRT engage with ransomware negotiation specialists, or is paying the ransom completely off the table? • How can the team validate the integrity of remaining unaffected systems to ensure they are not compromised?
Inject #3 **Wednesday, 1:45pm**	• Government agencies, private sector partners, and international allies express concerns as the CSIRT struggles to coordinate national cybersecurity operations. • Threat intelligence sharing platforms are temporarily suspended to prevent further data leaks. • The CSIRT's ability to analyze ongoing cyber threats is crippled, leaving national critical infrastructure operators without guidance on emerging threats. • The attack gains media attention, fueling panic over national cybersecurity readiness.
Inject #3 **Key Issues**	• How should the government and CSIRT manage public communication to maintain trust while mitigating the impact of disinformation? • What alternative mechanisms can be put in place to continue cybersecurity monitoring while CSIRT systems are offline? • Should international partners be informed or engaged to assist in the investigation and containment efforts? • How should intelligence-sharing frameworks be adapted to continue secure collaboration without compromising sensitive data?
Inject #4 **Thursday, 3:45pm**	• The CSIRT's incident response team isolates infected systems and initiates recovery procedures using offline backups. • The investigation leads to the identification of attack indicators, linking the incident to a known APT group. • Threat hunting teams work to identify and remove persistent threats, including backdoors planted by attackers.
Inject #4 **Key Issues**	• How can the CSIRT ensure complete eradication of threats while minimizing operational downtime? • What countermeasures can be implemented to prevent the attackers from regaining access to the network? • How should the CSIRT prioritize restoring services while ensuring forensic investigations are not compromised?
Inject #5 **Monday, 10:00am**	• The CSIRT gradually restores critical services, ensuring that compromised systems are clean before reconnecting. • A detailed forensic investigation reveals that the initial compromise occurred through a zero-day vulnerability in the CSIRT's internal document management system. • The CSIRT issues an official response, attributing the attack to a foreign nation-state actor and considering diplomatic and legal countermeasures.
Inject #5 **Key Issues**	• How can the CSIRT rebuild national and international confidence in its ability to handle cyber threats? • What is the processes to restores systems and determines which services take priority?