Tabletop Exercise Workshop: Single Inject Storyboards

Technical Focused Exercise

Exercise Date	June 24, 2025
Executive Sponsor	CISO
Development Team	John Hollenberger, Fortinet
Location	FIRST 2025
Goal	Run a technical focused tabletop exercise.
Objectives	Evaluate the organization's ability to detect, assess, and respond to potential insider threats and credential compromise involving cloud resources.
Inject #1	• At 09:14, the SIEM alerts on an internal user downloading 12 GB of data from a confidential S3 bucket over a short period. • An alert is also received for external access by an unrecognized IP in another country. • IAM logs show the user's credentials were used with elevated permissions.
Inject #1 Key Issues	• What immediate steps would be taken upon receiving this alert? • What can be done to determine if this is legitimate user activity vs. malicious? • What data sources are most critical to investigate this event? • What containment actions would be prioritized to stop further access or data exfiltration from the cloud environment?

Business Focused Exercise

Exercise Date	June 24, 2025
Executive Sponsor	CISO
Development Team	John Hollenberger, Fortinet
Location	FIRST 2025
Goal	Run a tabletop exercise with a focus on exercising business representatives and executives.
Objectives	Test our third-party risk response, contractual awareness, business continuity planning, and decision-making during an incident impacting our billing vendor.
Inject #1	• OurPaymentsNow (billing vendor) notifies legal of an incident impacting their cloud environment. • Customer PII processed on your behalf may be affected. • OurPaymentsNow cannot confirm whether data has been exfiltrated. • We have an SLA that requires notification of customers within 72 hours if PII is exposed.
Inject #1 Key Issues	• Who is activated in the response? • What contractual obligations apply? • Should the company notify affected customers preemptively? • How is continuity of billing and service ensured if the vendor is down? • What internal systems/processes depend on the third-party vendor?

Social Media Exercise

Exercise Date	June 24, 2025
Executive Sponsor	CISO
Development Team	John Hollenberger, Fortinet
Location	FIRST 2025
Goal	Continued adherence to the organization's incident response plan by performing a quarterly tabletop exercise.
Objectives	Test the organization's ability to identify, respond to, and recover from a public-facing social media compromise, with an emphasis on internal coordination, public communication, and account recovery.
Inject #1	• At 10:37, our official X account begins posting unusual and inappropriate content, including misleading information about company operations. • Multiple employees and external stakeholders report the activity. • Communications attempts to access the account but find login credentials have been changed. • Last known access appears to be from an IP outside the companies' geolocation range.
Inject #1 Key Issues	• What are the immediate steps to contain and investigate the incident? • Who is responsible for managing internal and external communications during the incident? • How do we assess reputational damage and respond to stakeholder and media inquiries? • What is the procedure for recovering the account?