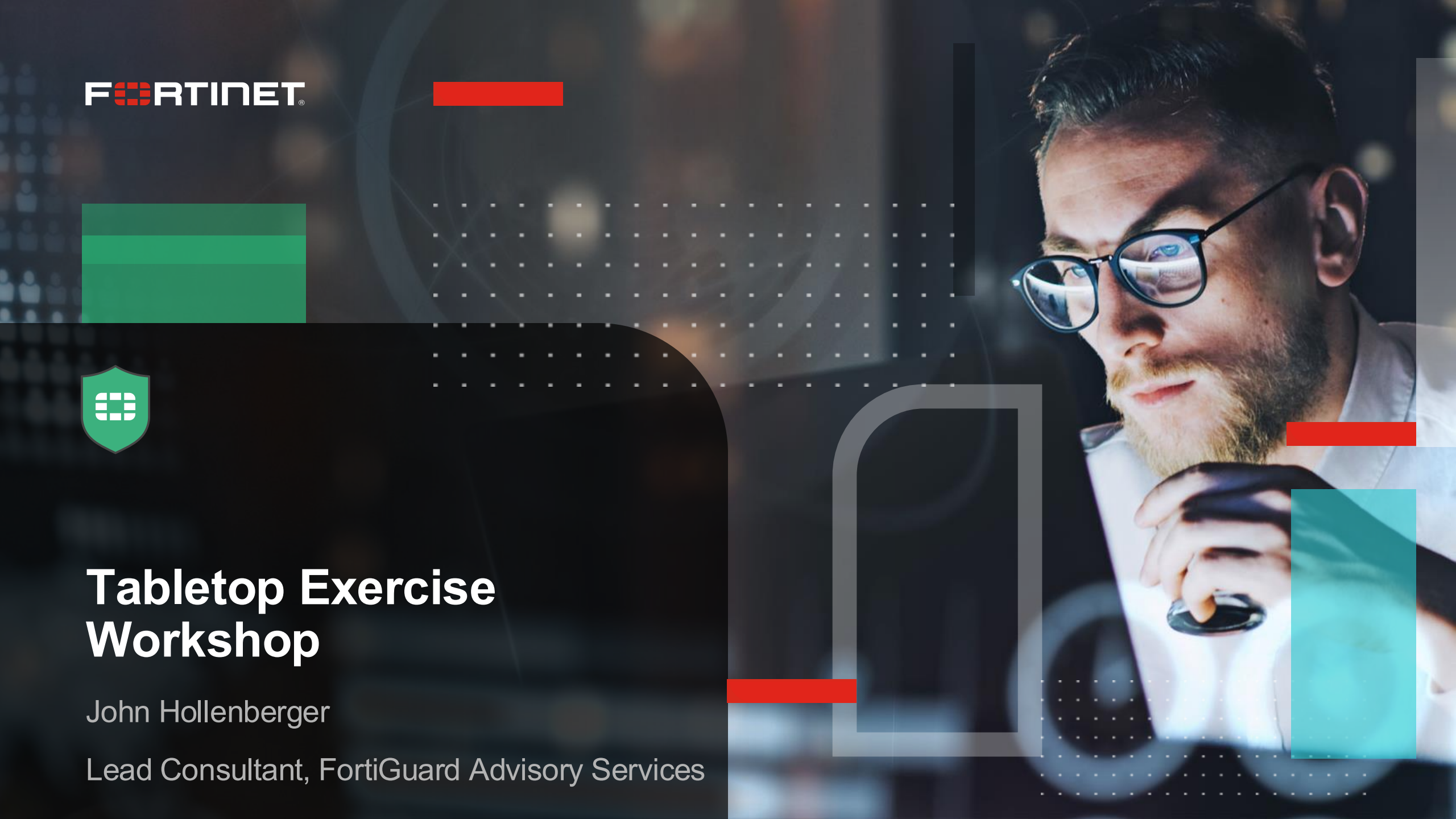


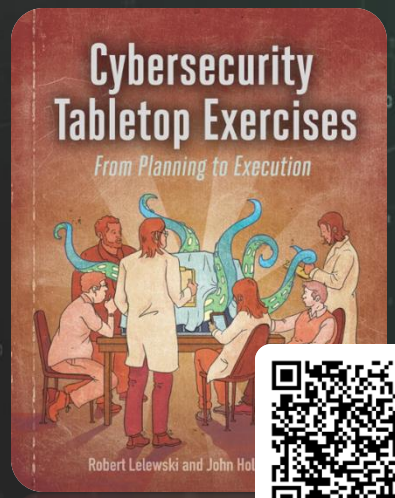
Tabletop Exercise Workshop

John Hollenberger

Lead Consultant, FortiGuard Advisory Services

John Hollenberger

Lead Consultant
FortiGuard Proactive Services



- Over 18 years of experience in cyber security and IT Operations, including four years as the Director of IT for a non-profit organization.
- Previous focus areas include web- and host-based vulnerability assessments, incident response, PCI compliance and Data Loss Prevention.
- Presented, trained and mentored on proactive Incident Response services for large corporations, small businesses, and non-profit organizations. Presented at a number of international, national, and regional conferences.
- Co-author of *Cybersecurity Tabletop Exercises: From Planning to Execution*

Douglas Jose Pereira dos Santos

Director
Advanced Threat Intelligence

- Over 25 years experience, including more than a decade at Fortinet.
- Extensive experience, spanning the development and implementation of advanced cybersecurity strategies, with a current focus on revolutionizing threat intelligence tools, standards, and methodologies.
- As the lead researcher collaborating with MITRE's Center for Threat-Informed Defense (CTID), Douglas is spearheading innovative projects to enhance the understanding of threat intelligence and incident response within the cybersecurity landscape

Agenda

- Tabletop Exercise Fundamentals
- Planning and Preparation
- Keeping it Simple
- Tabletop Exercise Simulation
- Debrief
- Q & A

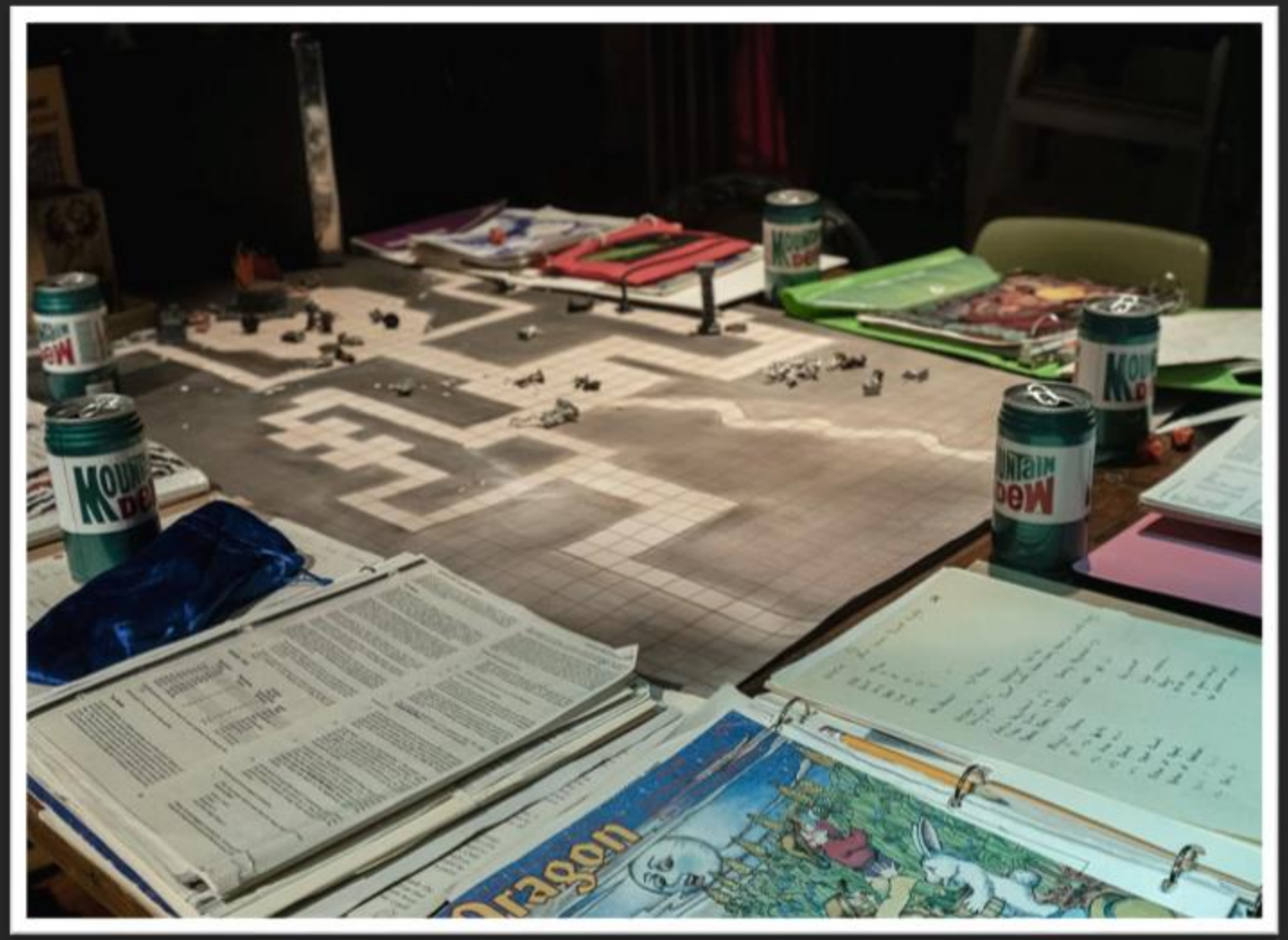
Tabletop Exercise Fundamentals

What is a Tabletop Exercise?

"A discussion-based exercise in response to a scenario, intended to generate a dialogue of various issues to facilitate a conceptual understanding, identify strengths and areas for improvement, and/or achieve changes in perceptions about plans, policies, or procedures."

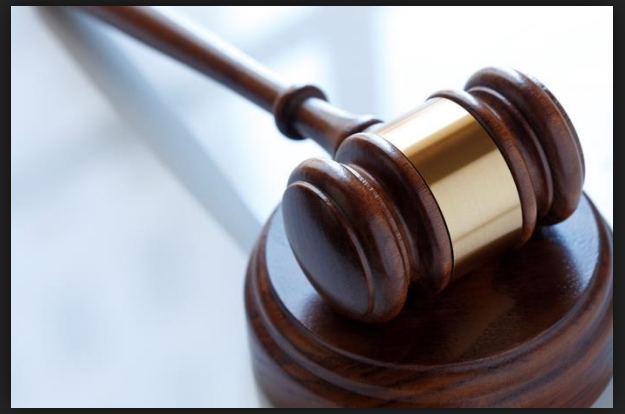
-Homeland Security Exercise and Evaluation Program (HSEEP)

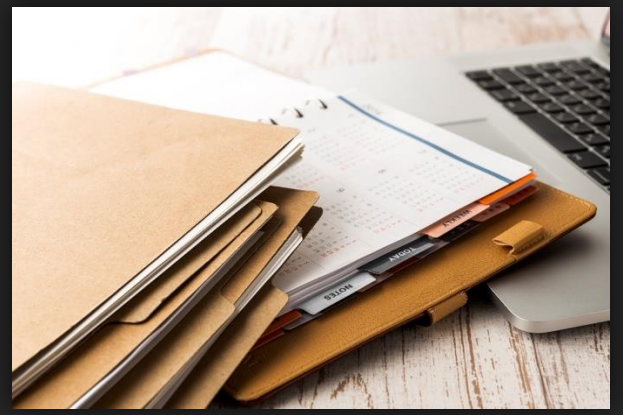
Can you Simplify That?

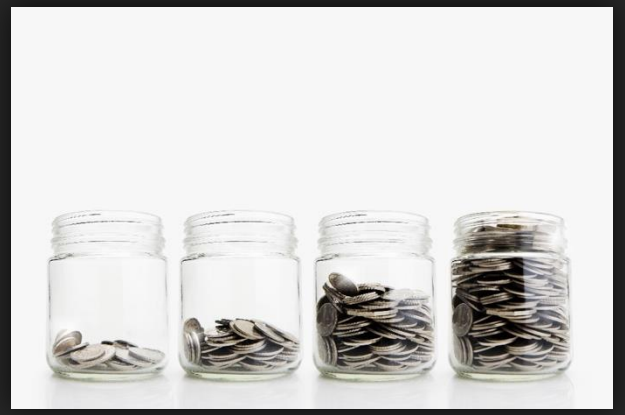


- Discussion-based exercise
- Low(er)-stress, controlled environment
- Walk-through of a realistic cybersecurity scenario
- Scenario is realistic and relevant for the audience at hand
- Identify gaps in our people, processes, and technologies

Why Perform Cybersecurity Exercises?



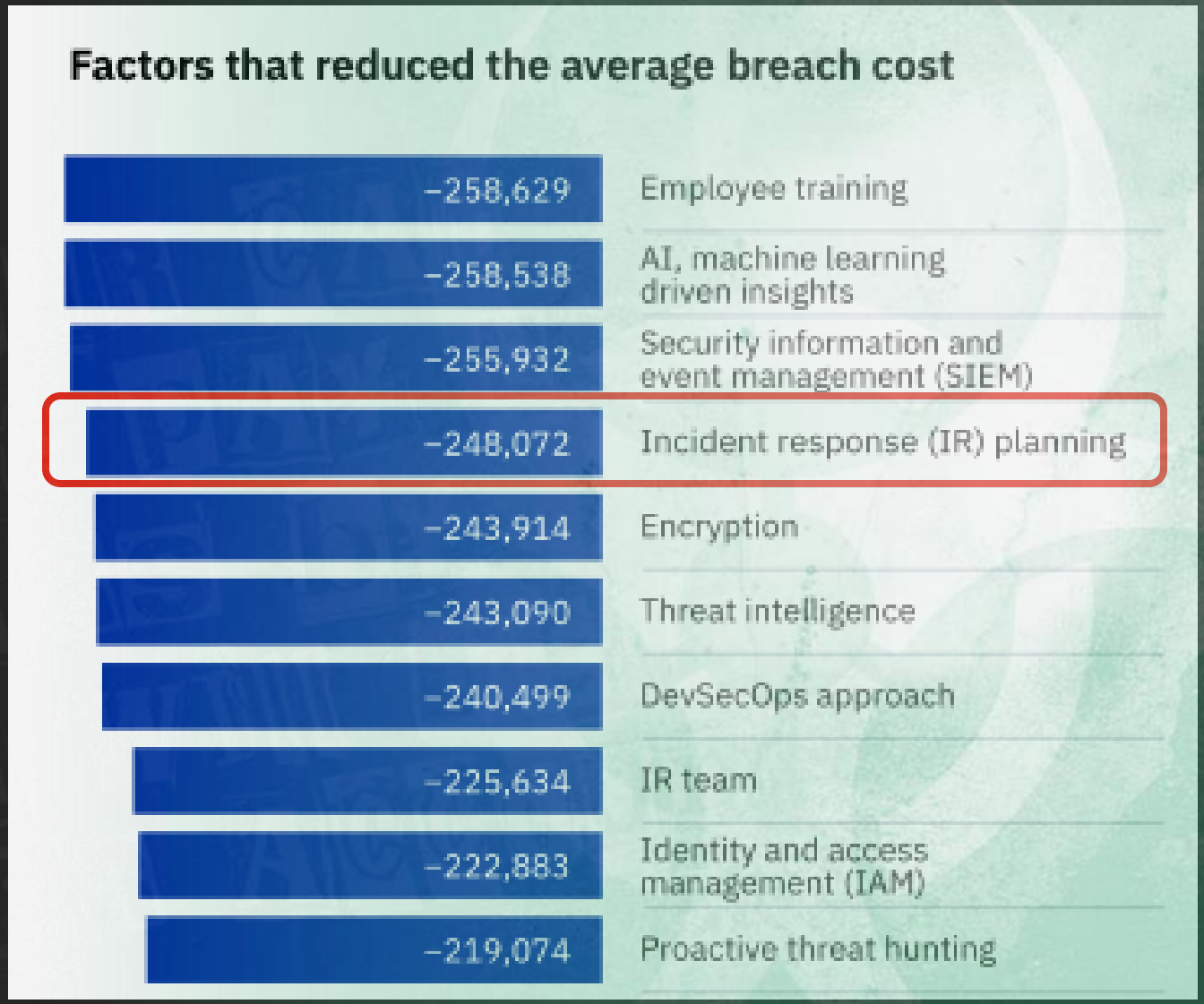




Financial Impact of Data Breaches

Organizations with Incident Response (IR) Planning resulted in an average of $248,072 less in data breach costs.

*Cost difference based on the average cost of $4.88M.

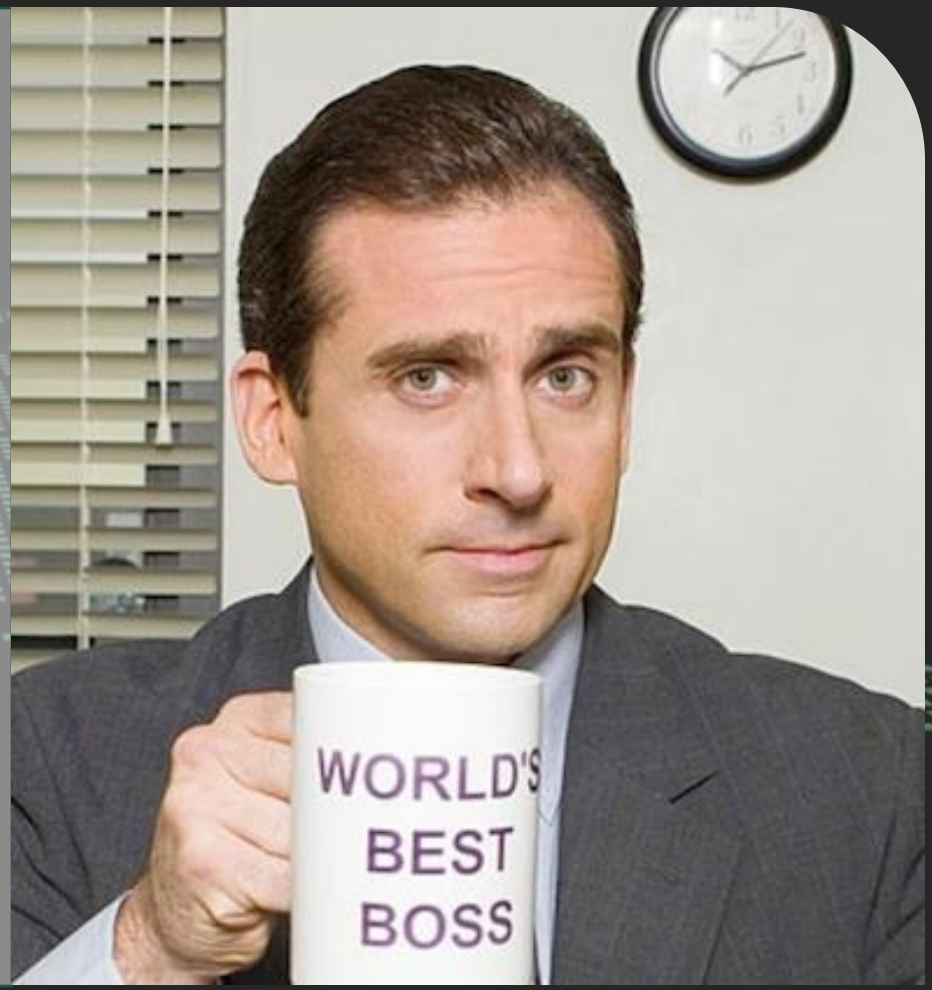


Used with permission. Research sponsored by IBM Security and conducted by Ponemon Institute.

Planning and Preparation

Executive Support

Executive / Leadership Support is crucial...



Select the Audience

Technical Exercise

Executive Exercise

Include Outside Participation?

- External Incident Response Team IT/Security Vendors
- Cyber Insurance
- External Legal
- Law Enforcement
- PR Firm
- Others?

Identifying a Topic

- Consult the Executive Sponsor
- An issue weighing on the IT staff
- Competitor or local business impacted by an incident
- Confer with the executive leadership on their concerns
- Consult with vendors on what they are seeing
- Check MITRE ATT&CK on TTPs targeting geographical region and industry
- Others?

Creating the Scenario

Choosing the Topic

Make it Relevant and Realistic

Realistic

- Affect organization software/ hardware
- What can happen to the organization / is more likely to happen?

Relevant

- Is there an issue weighing on leadership / the board?
- Is there an issue that affected a similar business in the industry or a nearby institution.

Logistical Considerations

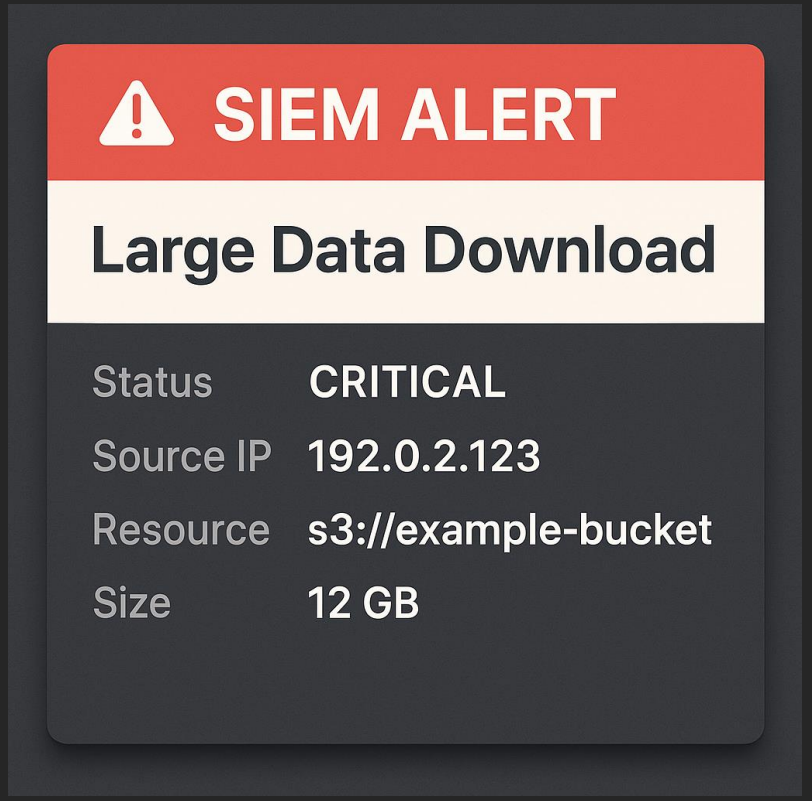
Tools and Tactics

Keep it Simple

Technical Focused Exercise

Objective: Evaluate the organization's ability to detect, assess, and respond to potential insider threats and credential compromise involving cloud resources.

- 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.



Technical Focused Exercise

Objective: Evaluate the organization's ability to detect, assess, and respond to potential insider threats and credential compromise involving cloud resources.

- 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.

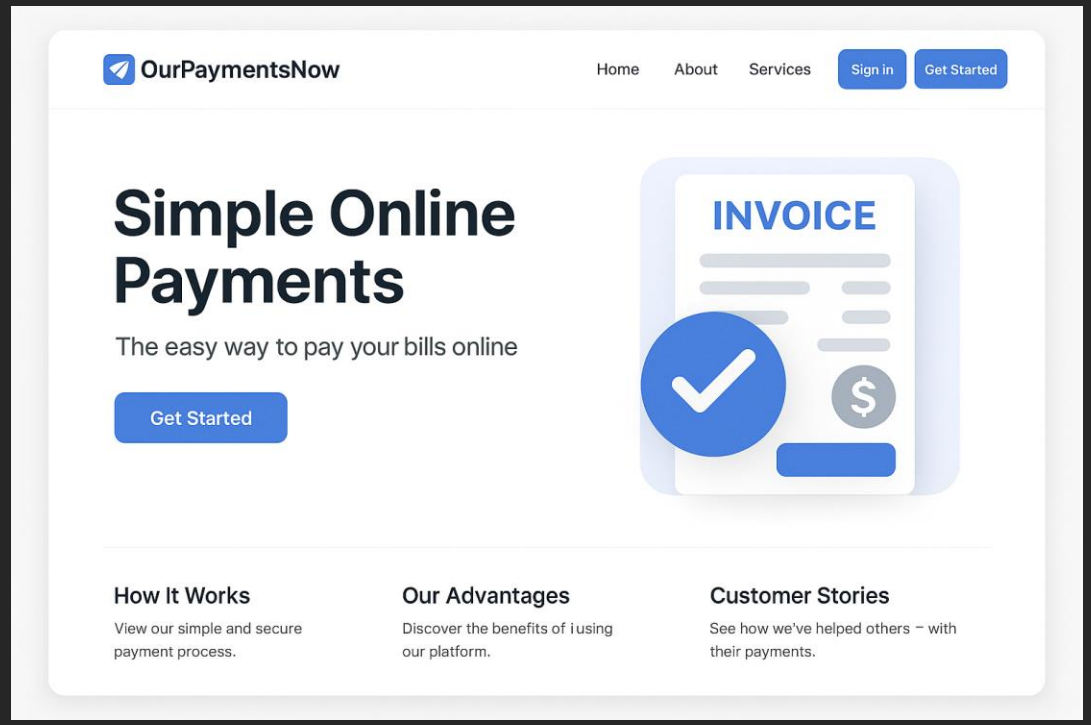
Discussion Points

- 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

Objective: Test our third-party risk response, contractual awareness, business continuity planning, and decision-making during an incident impacting our billing vendor.

- 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.



Business Focused Exercise

Objective: Test our third-party risk response, contractual awareness, business continuity planning, and decision-making during an incident impacting our billing vendor.

- 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.

Discussion Points

- 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

Objective: 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.

- 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.

Social Media Exercise

Objective: 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.

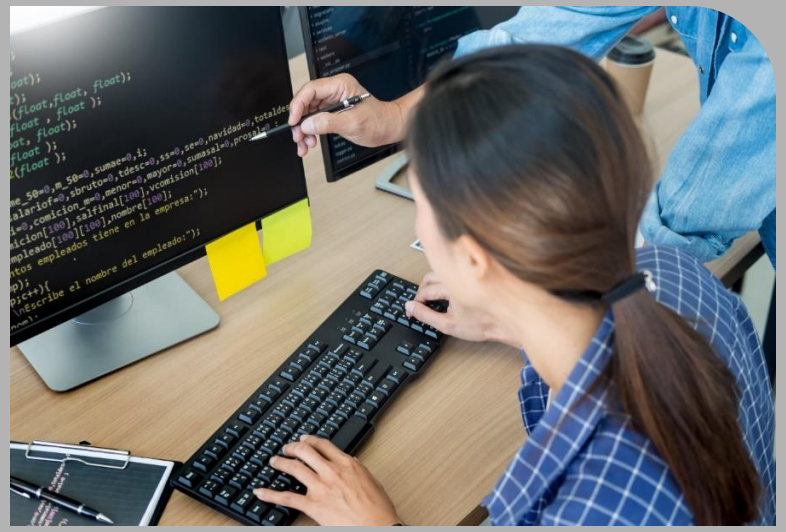
- At 10:37, our official X account begins posting unusual and inappropriate content, including misleading information about company operations.
- Multiple employees and external stakeholders report the activity.
- Communications attempts to access the account but find login credentials have been changed.
- Last known access appears to be from an IP outside the companies' geolocation range.

Discussion Points

- 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?

Tabletop Exercise Simulation

What to Expect



Injects

The scenario will be presented through a sequence of events, called “injects.”

Focused Questions

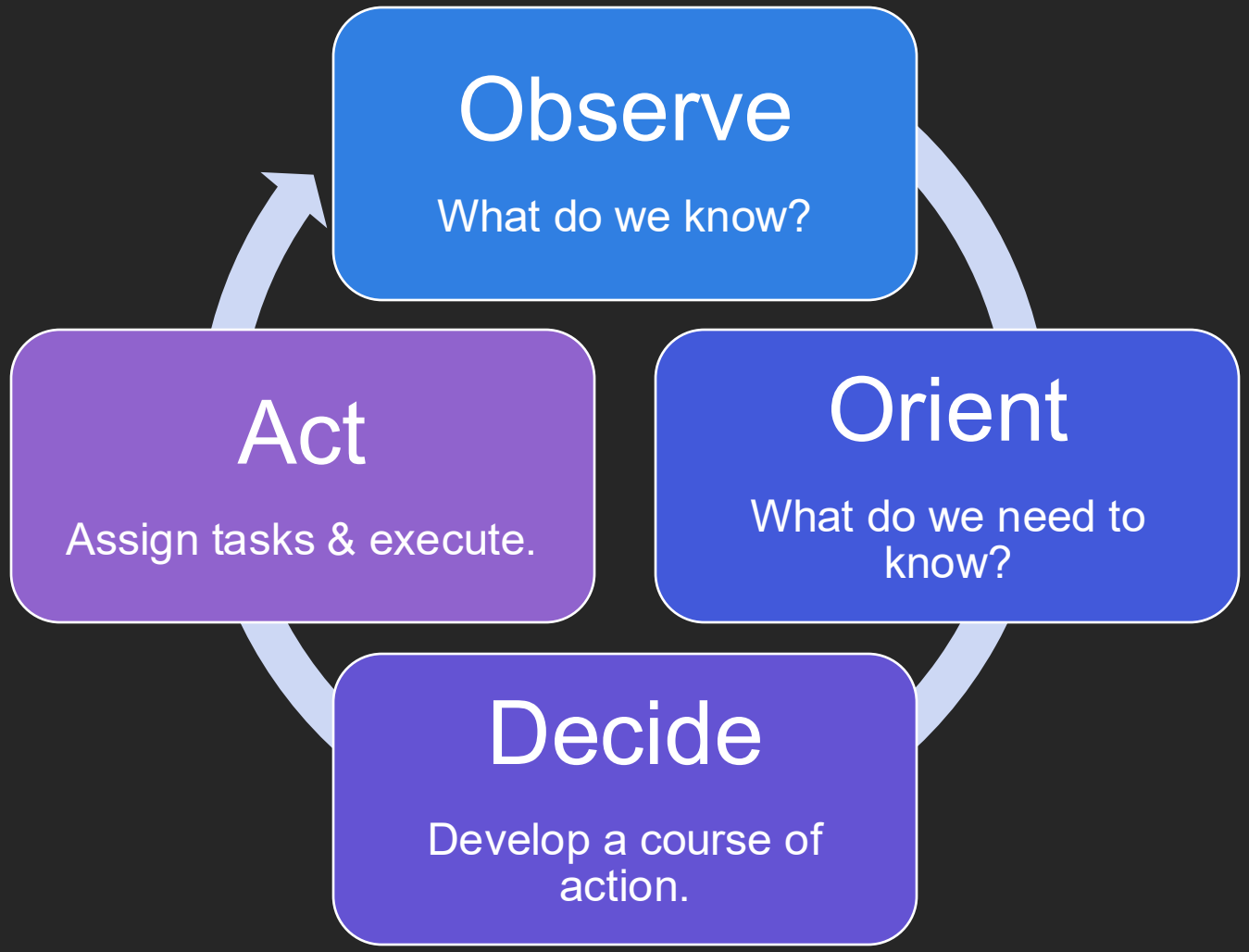
Each Inject will have focused questions that the facilitator will ask after the audience has a chance to bring up any items of discussion.

Options to Proceed

The group will vote on how to ultimately proceed based on a vote with the majority being the choice selected.

Decision Cycle

OODA Loop



You'll get more out of the exercise if you…

- Speak up and share your interests and concerns.
- Participate.
- Ask questions.
- Be positive and respect other participants and their opinions.
- Cooperation and mutual interaction is essential.

Expectations

Please don’t fight the narrative.

- Scenarios are created with some creative liberties.
- When needed, clarification may be offered by the facilitator.

You cannot fail if there are no grades.

- There will be no grade for your participation. Your response will not be tested.
- A short debrief will occur at the conclusion of the exercise.

Please make every effort to work with the scenario as presented.


Questions?
Let’s Get Started

Scenario

Your company has fallen victim to a coordinated cyberattack that affects critical IT infrastructure and disrupts business operations. The exercise will test decision-making, technical incident response, and business continuity.

Inject 1: Initial Discovery (Day 0, 9:00 AM)

- A network monitoring tool detects unusual traffic patterns indicating potential data exfiltration from internal servers.
- Several employees report difficulty accessing key systems.
- Preliminary review shows possible unauthorized access to sensitive files.

A. Investigate Internally

B. Notify IR Vendor

C. Wait for More Info

Inject 1 - Slido

Inject 1: Initial Discovery (Day 0, 9:00 AM)

- A network monitoring tool detects unusual traffic patterns indicating potential data exfiltration from internal servers.
- Several employees report difficulty accessing key systems.
- Preliminary review shows possible unauthorized access to sensitive files.

A. Investigate Internally

B. Notify IR Vendor

C. Wait for More Info

A

Investigate Internally

Overall Impact on Incident

Internal investigation allowed for a rapid response; however, attack vectors were missed along with critical threat intelligence that would have helped to swiftly eradicate and recover from the incident. Initial costs were lower, but the resulting damage resulted in a higher financial impact.

Inject 2 →

B

Notify IR Vendor

Overall Impact on Incident

Utilizing the external incident response subscription service allowed for swift containment, however, there was a larger initial financial cost but overall, a lower overall cost on the business when impact is factored.

Inject 2 →

C

Wait for More Info

Overall Impact on Incident

The result was a delayed response and a rapid spread of the attack within the environment. This resulted in a large financial impact due to overall impact to the organization.

Inject 2 →

Inject 2: Threat Confirmation (Day 0, 1:00 PM)

- The security team confirms unauthorized access to sensitive customer data.
- Ongoing malicious network activity is detected.
- Affected systems include customer databases and critical operational servers.

A. Isolate the Network

B. Only Allow Mission-Critical Operations, Isolate Rest

C. Continue Monitoring Only

Inject 2 - Slido

Inject 2: Threat Confirmation (Day 0, 1:00 PM)

- The security team confirms unauthorized access to sensitive customer data.
- Ongoing malicious network activity is detected.
- Affected systems include customer databases and critical operational servers.

A. Isolate the Network

B. Only Allow Mission-Critical Operations, Isolate Rest

C. Continue Monitoring Only

A

Isolate the Network

Overall Impact on Incident

Isolation resulted in effective containment, but also caused immediate disruption to business operations and operational loss.

Inject 3 →

B Only Allow Mission-Critical Operations, Isolate Rest

Overall Impact on Incident

Resulted in a balance of containment and operations but allowed threat actor to maintain access for an extended period and gain access to critical servers.

Inject 3 →

C

Continue Monitoring

Overall Impact on Incident

Resulted in better intelligence for containment and eradication; however, due to elongated threat actor access, increased data exfiltration was possible.

Inject 3 →

Inject 3: Data Impact Assessment (Day 1, 10:00 AM)

- Initial analysis indicates customer PII and financial records have been compromised.
- Key stakeholders are demanding immediate risk mitigation strategies.
- Regulatory compliance team flags potential legal reporting requirements.

A. Inform Affected Customers

B. Wait for Full Impact Assessment

C. Seek Legal Advice

Inject 3 - Slido

Inject 3: Data Impact Assessment (Day 1, 10:00 AM)

- Initial analysis indicates customer PII and financial records have been compromised.
- Key stakeholders are demanding immediate risk mitigation strategies.
- Regulatory compliance teams flag potential legal reporting requirements.

A. Inform Affected Customers

B. Wait for Full Impact Assessment

C. Seek Legal Advice

A

Inform Affected Customers

Overall Impact on Incident

This allows for the organization to build trust with customers; however without the full picture early notification risks misinformation being disseminated.

Inject 4 →

B

Wait for Full Impact Assessment

Overall Impact on Incident

Waiting allows for a full impact to be realized before informing customers and external parties, but this delay may damage the organization's reputation.

Inject 4 →

C

Seek Legal Advice

Overall Impact on Incident

Strong legal protection will be afforded the company; however, there may be a delay in stakeholder communication and thus a potential for reputational damage.

Inject 4 →

Inject 4: Business Continuity (Day 2, 12:00 PM)

- Critical systems remain offline, and production has halted.
- Financial losses are escalating.
- Customers are expressing dissatisfaction and exploring alternatives.

A. Implement Manual (Offline) Processes

B. Focus on System Restoration

C. Pivot to Cold Site and Backups

Inject 4 - Slido

Inject 4: Business Continuity (Day 2, 12:00 PM)

- Critical systems remain offline, and production has halted.
- Financial losses are escalating.
- Customers are expressing dissatisfaction and exploring alternatives.

A. Implement Manual (Offline) Processes

B. Focus on System Restoration

C. Pivot to Cold Site and Backups

A

Implement Manual Processes

Overall Impact on Incident

Results in immediate service restoration, however this is error-prone and resource-intensive.

Inject 5 →

B

Focus on System Restoration

Overall Impact on Incident

Results in long term stability, but results in prolonged business downtime.

Inject 5 →

C

Pivot to Cold Site and Backups

Overall Impact on Incident

Faster recovery then other available options, but there is a potential for synchronization issues and increased business costs.

Inject 5 →

Inject 5: Media and Reputation Management (Day 3, 8:00 AM)

- The incident becomes public through a media leak.
- Social media is flooded with negative comments from customers.
- Major news outlets are requesting comments from company leadership.

A. Hold a Press Conference

B. Release a Written Statement

C. Remain Silent

Inject 5 - Slido

Inject 5: Media and Reputation Management (Day 3, 8:00 AM)

- The incident becomes public through a media leak.
- Social media is flooded with negative comments from customers.
- Major news outlets are requesting comments from company leadership.

A. Hold a Press Conference

B. Release a Written Statement

C. Remain Silent

A

Hold a Press Conference

Overall Impact on Incident

High visibility and transparency for the organization but adds risk if the wrong thing is said or an untrained member of the staff delivers this address.

Inject 6 →

B

Release a Written Statement

Overall Impact on Incident

Controls messaging but is less personal. Can be vetted by internal personnel and public relations to ensure appropriate communications.

Inject 6 →

C

Remain Silent

Overall Impact on Incident

May be perceived as hiding information and further damage trust.

Inject 6 →

Inject 6: Post-Incident Review (Day 7, 3:00 PM)

- The immediate crisis has passed.
- The board demands a thorough post-incident review to strengthen future resilience.
- Departments are asked to provide lessons learned and suggest improvements.

A. Conduct Internal Review

B. Hire External Consultants

C. Focus on Quick Fixes

Inject 6 - Slido

Inject 6: Post-Incident Review (Day 7, 3:00 PM)

- The immediate crisis has passed.
- The board demands a thorough post-incident review to strengthen future resilience.
- Departments are asked to provide lessons learned and suggest improvements.

A. Conduct Internal Review

B. Hire External Consultants

C. Focus on Quick Fixes

A

Conduct Internal Review

Overall Impact on Incident

Cost-effective solution but can be biased if not conducted by a neutral party within the organization.

End →

B

Hire External Consultants

Overall Impact on Incident

Will provide a comprehensive assessment and may also provide root cause analysis but can be cost prohibitive.

End →

C

Focus on Quick Fixes

Overall Impact on Incident

May address immediate vulnerabilities but lacks long-term improvement for the organization.

End →

Debrief

Tabletop Exercise Keys to Success

- Keep it simple.
- Don’t overthink the exercise.
- Set clear goals.
- Practice often (quarterly – one facilitated, three internal)
- Have fun!

Questions

John Hollenberger

jhollenberger@fortinet.com

Douglas Jose Pereira dos Santos

dsantos@fortinet.com

←This is probably legitimate ☺

Thank you!


FORTINET