Simulation: "Salt Typhoon" CyberSecurity Breach
User Manual and Guidelines

Overview:

The "Salt Typhoon" Cybersecurity Breach simulation is an immersive exercise designed to evaluate and strengthen an organization's ability to respond to a cyber attack. The scenario simulates a sophisticated cyber breach, enabling participants to react in real-time and experience the dynamics pf managing a high-stakes cyber incident. The primary focus is to help cybersecurity teams, and other relevant departments, practice their response skills, uncover weaknesses, and improve overall preparedness for real-world cyber threats.

Objectives:

1. **Assess Reaction Strategies:** The primary aim is to examine how effectively the organization reacts to a cyberattack. This includes testing communication flows, decision-making capabilities, and the execution of response protocols.
2. **Uncover Security Gaps:** The exercise provides a controlled environment where organizations can discover weaknesses in their cybersecurity infrastructure, policies, and procedures that could be exploited by attackers.
3. **Simulate Progressive Threats:** Cyber threats are often unpredictable and continuously changing. This simulation is designed to reflect that dynamic nature, requiring participants to adjust their strategies as the breach evolves and new challenges arise.
4. **Strengthen Interdepartmental Cooperation:** The simulation encourages collaboration between various teams, including IT, legal, and communications, ensuring that the organization responds to the breach in a coordinated and efficient manner.
5. **Refine Crisis Response Capabilities:** The exercise emphasizes enhancing participants' ability to manage high-pressure situations, make informed decisions rapidly, and maintain a calm and effective response throughout the crisis.

Expected Outcomes:

1. **Optimized Incident Management Plans:** Through the simulation, participants will gain a clearer understanding of their existing incident response plans' effectiveness, leading to necessary revisions and improvements.
2. **Improved Cybersecurity Defenses:** By identifying vulnerabilities and testing their security infrastructure, organizations can strengthen their overall cybersecurity posture and enhance resilience against future attacks.

3. **Better Team Collaboration:** The simulation fosters stronger communication and coordination across departments, ensuring a unified approach to handling cybersecurity threats.
4. **Greater Understanding of Emerging Threats:** Participants will gain insights into current and evolving cyber threats, such as sophisticated hacking techniques, social engineering, and persistent cyber espionage, helping them stay ahead of potential risks.

Roles and Responsibilities:

The "Salt Typhoon" Cybersecurity Breach simulation involves various participants who take on specialized roles, each with their own set of responsibilities and objectives. These roles are designed to mimic real-world organizational functions and ensure a comprehensive, collaborative response to the cyberattack. Below is a condensed list of roles, highlighting their responsibilities and perspectives within the simulation:

1. Incident Response Coordinator

- **Role Description:** The Incident Response Coordinator is responsible for overseeing the overall incident management process. This individual ensures that all teams are working together effectively and that the response is progressing according to the defined strategy.
- **Objectives:**
  - Oversee the implementation of the response plan and monitor progress.
  - Act as a liaison between internal teams and executive leadership to provide timely updates.
  - Ensure that all response activities are documented for post-incident analysis.
- **Point of View:** The Coordinator is focused on maintaining order throughout the incident, ensuring that the response stays aligned with organizational priorities and timelines. They focus on both tactical and strategic oversight of the breach response.

2. Network Security Specialist

- **Role Description:** The Network Security Specialist is tasked with protecting the organization's network infrastructure. They work to prevent the spread of the attack, identify network entry points, and secure critical systems.
- **Objectives:**
  - Identify and neutralize any network-based threats, such as DDoS attacks or data exfiltration.
  - Work closely with other technical teams to isolate affected segments of the network.

    - Implement additional monitoring tools and network defenses to block further intrusion.
- **Point of View:** The Network Security Specialist’s primary concern is to contain the breach within the network and prevent further infiltration. Their role is critical in ensuring the organization’s infrastructure remains intact and secure during the attack.

3. Malware Analyst

- **Role Description:** The Malware Analyst is responsible for dissecting malicious software and understanding its behavior. They play a key role in identifying the nature of the breach and developing strategies for neutralizing malware.
- **Objectives:**
    - Analyze infected systems and determine the type and scope of malware involved.
    - Identify the origin and potential objectives of the attackers.
    - Develop strategies for eradicating malware and preventing future infections.
- **Point of View:** The Malware Analyst’s focus is on understanding the technical specifics of the attack. They work to eliminate the threat at the source and provide critical intelligence to other teams working on containment and recovery.

4. Data Privacy Officer

- **Role Description:** The Data Privacy Officer ensures that the organization complies with data protection laws and regulations. They are responsible for assessing the impact of the breach on sensitive data and guiding legal actions concerning data exposure.
- **Objectives:**
    - Identify any personal or sensitive data that may have been compromised.
    - Advise on legal obligations related to data breaches, including notification timelines.
    - Work with the legal team to ensure compliance with data protection regulations.
- **Point of View:** The Data Privacy Officer’s priority is to protect individuals' privacy rights. They need to ensure that the organization handles data breaches appropriately to mitigate potential legal consequences and public backlash.

5. Risk Management Officer

- **Role Description:** The Risk Management Officer is responsible for assessing the potential risks associated with the breach and advising on mitigation strategies. They evaluate the breach's impact on business operations and overall security posture.

- **Objectives:**
    - Conduct a risk assessment to understand the short- and long-term impact of the breach on the organization.
    - Advise on the allocation of resources for risk mitigation and prioritize actions to reduce potential damage.
    - Work with senior leadership to implement strategies that strengthen the organization's overall risk management framework.
- **Point of View:** The Risk Management Officer focuses on understanding the broader implications of the attack. They balance business continuity with risk reduction, ensuring that the organization minimizes the potential damage from the breach.
    - Ensure that department functions are maintained as much as possible, despite the ongoing breach.
    - Support the recovery of business operations and systems within their unit.
- **Point of View:** Business Unit Leaders focus on minimizing the impact of the breach on their specific departments. They work to ensure that their teams have the necessary resources and guidance to continue functioning and recover quickly.

These roles focus on critical areas like managing the incident, securing infrastructure, protecting sensitive data, and minimizing organizational risks.

Step-By-Step Simulation Guide:

Timeline:

Phase 1: Initial Compromise and Discovery (Days 1-5)

- **Early Warning Signs, Detection, Internal Alerts**
    - *Key Events:* Suspicious activity is detected. CISA alert is issued. Early Media leaks occur.
    - *Group Deadline:* Threat Assessment

Phase 2: Breach Confirmation and Escalation Tactics (Days 6-10)

- **Confirmed Breach, Attribution debates focused on early containment**
    - *Key Events:* Breach is confirmed. Containment of the breach is necessary as rumors of who is responsible begin to spread.
    - *Group Deadline: Containment Plan*

Phase 3: Public Crisis and Attribution (Days 11-16)

- **Full Public Disclosure and International Fallout**

    - *Key Events:* Salt Typhoon is found to be responsible for the attack. Full media attention has started as lawsuits begin to emerge.
    - *Group Deadline:* Crisis Communication Plan for the public

Phase 4: Recovery, Regulation, and Policy Reform (Days 17-20)

- **Long-term recovery plans, regulatory changes, and strategic reform.**
    - *Key Events:* Policy responses are needed. The Telecom industry proposes reform strategies.
    - *Group Deadline: A* Resilience Strategy is needed to prevent future attacks.

Facilitator Instructions:

The facilitator will be tasked with organizing and administering the simulation by providing an introduction, handling participant questions, and will provide and/or inject additional information as the simulation evolves.

Introducing the Simulation

- When **introducing** the simulation, the facilitator will provide an overview of the "Salt Typhoon" Cybersecurity Breach, ensuring that participants are familiar with the purpose and objectives of the simulation (Assess Reaction Strategies, Uncover Security Gaps, Simulate Progressive Threats, Strengthen Interdepartmental Cooperation, Refine Crisis Response Capabilities)
- **The facilitator will assign roles** (Incident Response Coordinator, Network Security Specialist, Malware Analyst, Data Privacy Officer) to each group member, ensuring that each participant is aware of the individual responsibilities, objectives, and areas of concern associated with their role.
- **The simulation will be introduced in phases.** The facilitator will provide all relevant details and information pertaining to each phase as the simulation unfolds and will ensure that deliverables for each phase are produced (Threat Assessment, Containment Plan, Crisis Communication Plan, Resilience Strategy).
- **The facilitator will track group progress** using defined evaluation metrics as the scenario unfolds.

Handling Participant Questions

- The facilitator should act as a neutral party that guides the organization, structure, and administration of the simulation. They should avoid directly providing solutions and should rather guide participants through the process and encourage internal problem-solving amongst group members.

Providing and Injecting Additional Information

- The facilitator can inject additional information that may disrupt or change the simulation to mimic real-world developments, pressure, or ambiguity that challenges participants decision-making and problem-solving skills.
- Injects should simulate real-world developments (e.g., media leaks, policy updates, technical discoveries) to mirror the unpredictability of actual cyber incidents and keep the scenario dynamic.
- Injects guide the simulation toward key goals and objectives, uncover possibleblind spots, and ensure group engagement with all aspects of cyber crisis management (technical, legal, ethical, and strategic).

Evaluation Metrics:

The Evaluation Metrics section of the User Manual provides the criteria for evaluating the participants' performance. The metrics are designed to measure the group's performance in terms of simulation success and aspects of teamwork within the group. Listed are detailed guidelines for measuring a group's success in the simulation and measuring the best practices for a cyber crisis simulation.

There are four distinct categories of measurement for a group's performance.

Threat Identification and Response

- This category measures the group's ability to detect cybersecurity threats quickly and accurately. It will also measure the group's ability to prioritize vulnerabilities based on their severity.
- Evaluation Guidelines: Groups will be scored from a scale of 1-5 based on the following guidelines per score.
    1. Poor: Group fails to identify critical threats or mismanages response priorities in full.
    2. Needs Improvement: Major threats were missed; responses were slow or improperly prioritized.
    3. Satisfactory: Some threats are missed, or the response prioritization is inconsistent.
    4. Good: Most threats are correctly identified on time, and the responses were appropriate but could have been better prioritized.
    5. Outstanding: Threats were identified quickly, and the responses were prioritized correctly and with clear justification. The group demonstrated proactive threat hunting.

Interdisciplinary Collaboration and Stakeholder Coordination

- This category measures the effectiveness of the communication between the roles in the simulation. It will also measure the integration between different stakeholder perspectives into the strategies.
- Evaluation Guidelines: Groups will be scored from a scale of 1-5 based on the following guidelines per score.
    1. Poor: Dysfunctional collaboration and role confusion
    2. Needs Improvement: Frequent miscommunication and major stakeholder views were ignored.
    3. Satisfactory: Some stakeholders take dominance with occasional breakdowns in collaboration.
    4. Good: Collaboration is smooth with some gaps when integrating stakeholder perspectives.
    5. Outstanding: Seamless and effective collaboration. All stakeholder perspectives were involved in decision-making.

Legal, Regulatory, and Policy Compliance

- This category measures the level of consideration taken by the group of national and international cyber laws and policies. It also measures if the group had a proper understanding of regulatory boundaries during decision-making.
- Evaluation Guidelines: Groups will be scored on a scale of 1-5 based on the following guidelines per score.
    1. Poor: Major noncompliance or illegal actions were performed during the simulation.
    2. Needs Improvement: Significant misunderstandings of legal obligations.
    3. Satisfactory: Basic legal awareness; however, important considerations were missed at times.
    4. Good: Most legal factors were addressed, and only minor oversights occurred in less critical areas.
    5. Outstanding: Legal and regulatory considerations were deeply integrated into every decision. The group also identified new compliance risks.

Ethical Reasoning and Decision-Making

- This category measures the balance between privacy, transparency, national security, and stakeholder interests. It will also measure the application of ethical frameworks in high-pressure situations.
- Evaluation Guidelines: Groups will be scored from a scale fo 1-5 based on the following guidelines per score.

1. Poor: Decisions are ethically problematic or reckless.
2. Needs Improvement: Ethical Concerns were overlooked.
3. Satisfactory: Ethical standards were inconsistently applied but present.
4. Good: Ethical reasons were evident, but small conflicts or trade-offs were not justified.
5. Outstanding: Ethical principles were consistently applied even under pressure situations. The group was able to balance competing interests.

FAQs and Troubleshooting:

Listed below are frequently asked questions pertaining to the simulation and any potential issues encountered over the course of the simulation.

1. What is the main objective of the "Salt Typhoon" simulation?

The simulation is designed to test and improve your organization's ability to respond to a major cybersecurity breach. It emphasizes real-time decision-making, cross-functional collaboration, and resilience under pressure.

2. How are roles assigned, and can participants switch roles?

Roles are assigned by the facilitator based on group size and expertise. While role-switching is not encouraged mid-simulation, accommodations can be made in smaller groups or due to participant absence.

3. What should I do if I don't understand my role or responsibilities?

Refer to the role descriptions in the manual. If clarification is needed, ask the facilitator — they can guide you without solving the problem for you.

4. What are "injects" and how do they affect the simulation?

Injects are surprise updates (e.g., news reports, new regulations, system failures) introduced by the facilitator to simulate the unpredictability of a real-world breach. They add complexity and challenge your team's adaptability and decision-making.

5. Can we ask the facilitator for advice during the simulation?

Yes, but facilitators will not give direct solutions. Instead, they will prompt you to think critically and guide your team through structured problem-solving.

6. How is our performance evaluated?

Performance is scored across four categories:

- Threat Identification and Response
- Interdisciplinary Collaboration and Stakeholder Coordination
- Legal, Regulatory, and Policy Compliance
- Ethical Reasoning and Decision-Making
- Each is rated on a 1–5 scale, with detailed rubrics provided in the manual.

7. What happens if we miss a phase deadline?

Missing a deadline will impact your evaluation. The simulation is structured to reflect time pressure in real-world scenarios, so staying on track is crucial for success.

8. What if there's a technical or logistical issue during the exercise?

Immediately notify the facilitator. They will resolve the issue or adapt the simulation timeline as needed to ensure continuity.

9. How realistic is the scenario?

The scenario is modeled after real-world cybersecurity threats and breaches. While fictional, it mirrors actual attack vectors, regulatory challenges, and public relations crises.