**Incident Response Playbook: Suspicious Network Activities (System Intrusion)**

**Phase 1: Initial Detection and Triage**

Alert: The security operations center (SOC) or monitoring tools generate an alert regarding suspicious network activities indicating a possible system intrusion.

Triage: The incident response team reviews the alert and assesses the severity and criticality of the incident based on the information available, including the type of activity, affected systems, and potential impact.

**Phase 2: Incident Notification and Escalation**

Notification: The incident response team notifies the relevant stakeholders, including IT management, security team, legal team, and executive leadership, about the incident.

Escalation: Depending on the severity of the incident, the incident response team escalates the incident to higher levels of management or other specialized teams for further investigation and response.

**Phase 3: Investigation and Containment**

Investigation: The incident response team conducts a detailed investigation to determine the scope, cause, and impact of the suspicious network activities. This may involve reviewing logs, analyzing network traffic, examining system configurations, and conducting forensic analysis.

Containment: The incident response team takes immediate steps to contain the incident, such as isolating affected systems from the network, disabling compromised accounts, or blocking malicious IP addresses to prevent further damage or data exfiltration.

**Phase 4: Mitigation and Remediation**

Mitigation: The incident response team identifies and implements temporary or permanent measures to mitigate the risks associated with the incident, such as patching vulnerabilities, updating access controls, or deploying additional security controls.

Remediation: The incident response team works with the IT team to restore affected systems to their normal operation and ensure that all traces of the intrusion are removed, including backdoors, malware, or other unauthorized access points.

**Phase 5: Communication and Reporting**

Communication: The incident response team maintains regular communication with relevant stakeholders, providing updates on the incident investigation, containment efforts, and mitigation measures.

Reporting: The incident response team prepares a detailed incident report, including a timeline of events, findings from the investigation, and recommendations for improving the security posture to prevent similar incidents in the future. This report is shared with management, security team, and other relevant parties.

**Phase 6:** **Post-Incident Review**

Review: After the incident is resolved, the incident response team conducts a post-incident review to analyze the effectiveness of the response process and identify areas for improvement. Lessons learned from the incident are documented, and recommendations for refining the incident response playbook or enhancing security controls are incorporated into the organization's security practices.

**Phase 7: Follow-up and Monitoring**

Follow-up: The incident response team continues to monitor the network for any signs of recurring suspicious activities or potential system intrusions and takes appropriate action to investigate and respond to any new incidents.

Monitoring: The incident response team also reviews and updates the incident response playbook periodically to reflect changes in the threat landscape, technology environment, or organizational processes, and conducts regular drills and exercises to ensure preparedness for future incidents.

**Please Note:** The above playbook is a general guideline and may need to be tailored to the specific requirements and policies of an organization. It is important to involve legal, compliance, and other relevant teams as appropriate during the incident response process to ensure compliance with regulations and laws.

**Second option**

Per <https://github.com/certsocietegenerale/IRM/blob/main/EN/IRM-5-MaliciousNetworkBehaviour.pdf>

1. Preparations: get ready to handle the incident
2. Identification: detect the incident
3. Containment: limit the impact of the incident
4. Remediation: Remove the threat
5. Recovery: recover to a normal stage
6. Lessons learned: draw up and improve the process.

**Preparations: Get Ready to Handle the Incident**

1. Establish an incident response team with designated roles and responsibilities.
2. Define and document the incident response process, including escalation procedures and communication channels.
3. Create a centralized incident management system to log and track incidents.
4. Develop and regularly update an inventory of critical systems, network devices, and data assets.
5. Ensure that all team members are trained and have access to necessary tools and resources for incident response.
6. Review and update security controls, such as firewalls, intrusion detection/prevention systems, and anti-malware software, to be prepared for potential incidents.
7. Have a backup and recovery plan in place, including offsite backups, to quickly restore systems in case of a successful intrusion.

**Identification: Detect the Incident**

1. Monitor network traffic and system logs for signs of suspicious activity, such as unusual access patterns, unauthorized logins, or unexpected system behavior.
2. Deploy security monitoring tools, such as Security Information and Event Management (SIEM) systems, to collect and analyze security logs from various sources.
3. Regularly review and analyze security alerts and reports from security solutions to identify potential incidents.
4. Conduct regular vulnerability assessments and penetration testing to proactively identify potential vulnerabilities that could be exploited by intruders.
5. Train employees to report any suspicious network activities they observe to the incident response team.

**Containment: Limit the Impact of the Incident**

1. As soon as a suspicious network activity is detected, isolate the affected system or network segment from the rest of the network to prevent further spread of the threat.
2. Change all affected credentials, including passwords, access keys, and certificates, to prevent further unauthorized access.
3. Disable any compromised accounts or services to prevent further misuse.
4. Apply security patches or updates to affected systems to remediate vulnerabilities that may have been exploited.
5. Block suspicious IP addresses or domains at the firewall or other security devices to prevent further communication with malicious entities.
6. Collect and preserve evidence for forensic analysis and potential legal actions.

**Remediation: Remove the Threat**

1. Conduct a thorough investigation to determine the root cause of the incident, the extent of the damage, and the scope of the intrusion.
2. Identify and remove all malicious files, scripts, or other artifacts left by the intruders.
3. Close all known vulnerabilities and implement additional security measures, such as hardening system configurations and updating security policies.
4. Restore affected systems and services to their normal state, ensuring that they are fully patched and up to date.
5. Conduct a post-incident review to identify any gaps in the security posture that may have allowed the incident to occur and take corrective actions to prevent similar incidents in the future.

**Recovery: Recover to a Normal Stage**

1. Gradually restore access to affected systems and services in a controlled and monitored manner, ensuring that they are fully patched and updated.
2. Verify that all security controls and monitoring tools are functioning correctly and are configured according to best practices.
3. Conduct thorough testing to ensure that the systems and services are operating as expected and that all data and configurations have been fully restored.
4. Monitor the network and systems for any residual signs of malicious activity to ensure that the threat has been completely eradicated.
5. Update incident reports and notify relevant stakeholders, including senior management, legal, and regulatory authorities, as required.

**Lessons Learned: Draw Up and Improve the Process**

1. Conduct a thorough review of the incident response process to identify any areas for improvement.
2. Update the incident response plan based on lessons learned from the incident.
3. Provide additional training and awareness programs to educate employees on how to detect and report suspicious network activities.
4. Review and update security controls, policies, and procedures based on the findings of the incident.
5. Regularly

**Incidence Response playbook: Data Theft**

**Phase 1: Initial Detection and Assessment**

1. Upon detecting a potential data theft incident, the incident response team should be notified immediately through established communication channels, such as a dedicated incident response hotline or email.
2. The team should assess the nature and scope of the incident, including the type of data that may have been stolen, the potential impact, and the affected systems or applications.
3. The team should gather relevant information, such as timestamps, logs, and other forensic data, to support the investigation and response.

**Phase 2: Containment and Mitigation**

1. The incident response team should take immediate steps to contain the incident and prevent further data loss. This may involve isolating affected systems or networks, disabling user accounts, or implementing temporary security measures.
2. The team should change all relevant passwords, revoke access to compromised accounts or systems, and update security controls to prevent further unauthorized access.
3. Backups of affected systems or data should be checked for integrity and used to restore any lost data or systems, if available.
4. The team should work closely with internal IT and security teams, as well as external stakeholders, such as law enforcement or legal counsel, to ensure proper handling and mitigation of the incident.

**Phase 3: Investigation and Analysis**

1. The incident response team should conduct a thorough investigation to determine the cause and extent of the data theft incident. This may involve analyzing logs, examining network traffic, and reviewing system configurations.
2. The team should identify the entry point, the methods used by the attackers, and any indicators of compromise (IOCs) to understand the attack vector and the scope of the incident.
3. Forensic analysis should be conducted to collect evidence, preserve chain of custody, and document findings for potential legal or regulatory purposes.
4. The team should coordinate with internal or external resources, such as a digital forensics team or a threat intelligence provider, to gain additional expertise and insights.

**Phase 4: Notification and Communication**

1. The incident response team should communicate the details of the data theft incident to relevant stakeholders, including senior management, legal counsel, public relations, and affected parties, as required by law or company policy.
2. Communication should be timely, accurate, and coordinated to ensure a consistent message and to manage potential reputational, legal, or regulatory risks.
3. The team should prepare and distribute internal and external notifications, including data breach notifications, incident reports, or media statements, based on established procedures and legal requirements.

**Phase 5: Recovery and Remediation**

1. The incident response team should work with relevant teams to implement necessary controls, patches, or updates to prevent similar incidents in the future.
2. The team should conduct a comprehensive review of security controls, policies, and procedures to identify any gaps or weaknesses that may have contributed to the data theft incident.
3. Lessons learned from the incident should be documented and used to update the incident response playbook, as well as to improve security practices and awareness across the organization.
4. The team should conduct post-incident monitoring and follow-up to ensure that all security measures are effectively implemented, and the incident is fully resolved.

**Phase 6: Post-Incident Analysis**

1. After the incident is resolved, the incident response team should conduct a post-incident analysis to assess the effectiveness of the response efforts and identify any areas for improvement.
2. The team should review the timeline of events, actions taken, and outcomes to identify any deviations from the incident response playbook and to identify potential improvements.
3. The team should document the findings and recommendations for future incidents and share the analysis with relevant stakeholders for further action or awareness.

**Please Note:** The above incident response playbook is a general outline and should be customized to fit the specific needs and requirements of each organization. It should be reviewed and updated regularly to reflect changes in the threat landscape, technology, and business processes. Additionally, it's important to involve.

Incidence Response playbook: Policy Violation