CHECK POINT™

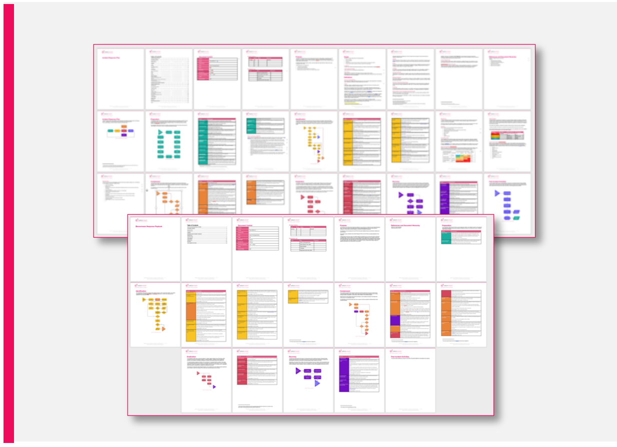
Incident Response Plan Development

An Incident Response Plan (IRP) is a dynamic, high-level framework/blueprint through which an organization defines and documents stakeholders and their responsibilities, critical systems and assets, communication channels, and technical and non-technical (legal, compliance, public relations) processes and procedures that should be followed to prepare, detect, and respond to cyber security incidents. The Check Point tailored IRP development considers the best practices from NIST 800-61 and 800-53, existing organization's internal guidelines, as well as any relevant industry constraints. The IRP is meant to be extended with additional detailed Playbooks for the required incident scenarios.

Aim: To prepare an organisation for a cyber security incident by having a well outlined Incident Response Plan, covering definitions, the stages of incident response, responsibilities, battle rhythm and decision/reporting points, referencing the specific playbooks for the identified incident scenarios.

Deliverables: Tailored Incident Response Plan

Methodology: Discussion & information gathering process through virtual meetings to understand the environment, current incident/crisis management followed by proposing a draft version based on internal template and gathered information throughout meetings, iterative process of adjusting, clarifying, validating



Benefits:

Effective Incident Management: An Incident Response (IR) plan ensures that an organisation is well-prepared to handle cyber security incidents. The plan outlines the necessary procedures, guidelines, and actions to be taken during different stages of incident response. By having a well-defined plan in place, organizations can respond promptly and effectively.

Consistent and Coordinated Response: An IR plan provides a framework for a consistent and coordinated response to cyber security incidents. It defines the roles and responsibilities of key personnel involved in the incident response process, ensuring that everyone knows their specific tasks and functions. This clarity and coordination enhance communication and collaboration among team members, enabling a more efficient response to incidents.

Reduced Response Time: With an established IR plan, organizations can respond to incidents more quickly. The plan outlines the necessary steps and actions to be taken, reducing the time required to make decisions and initiate a response. This swift response helps contain the incident and limit its impact, preventing further damage to systems, data, and reputation.

Compliance and Legal Requirements: Many industries and jurisdictions have specific compliance and legal requirements regarding incident response. Establishing an IR plan helps organizations meet these obligations and demonstrate their commitment to security and privacy. Compliance with regulations not only helps avoid penalties and legal consequences but also builds trust among customers, partners, and stakeholders.

Continuous Improvement: An IR plan serves as a living document that can be updated and improved based on lessons learned from previous Tabletop Exercises, incidents or the organisation's environment. By regularly reviewing and updating the plan, organisations can incorporate new technologies, methodologies, and best practices. This iterative approach allows for continuous improvement, ensuring that the IR plan remains relevant and effective.

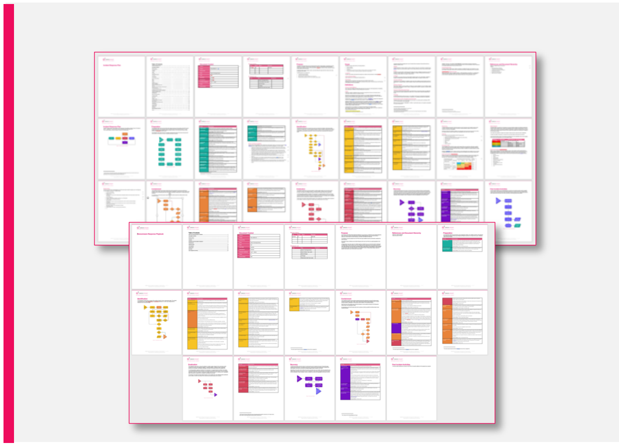
Playbook Development

Providing tailored Playbooks addressing specific incident scenarios. The Playbooks are tied to the overarching IR Plan. Currently, the following playbooks can be provided: Infected System Response Playbook, Ransomware Response Playbook, Data Loss Response Playbook, Data Breach Response Playbook, Media Response/Communications Playbook, Account Compromise Response Playbook.

Aim: To prepare an organisation for a specific cyber security incident type by having a well outlined Playbook that ties into the overarching IR Plan, detailing the stages of incident response and responsibilities for the incident scenario at hand.

Deliverables: Tailored Playbooks for the selected Incident Scenario's

Methodology: understanding the environment, current incident/crisis management, proposing draft based on internal template and gathered information throughout meetings, iterative process of adjusting, clarifying, validating



Benefits:

Standardized Response Procedures: Playbooks provide standardized and predefined procedures for specific incident scenarios. By establishing playbooks, organizations ensure that their response to each type of incident follows a consistent and structured approach. This consistency helps to minimize errors, improve efficiency, and reduce the time required to contain and mitigate the incident.

Rapid Incident Response: Playbooks outline the stages of incident response, including the necessary actions, decision points, and responsibilities for each stage. This predefined roadmap enables a faster response to incidents, as responders can quickly refer to the playbook for guidance on what steps to take. Rapid incident response is crucial for minimizing the impact of the incident and preventing it from escalating further.

Clear Roles and Responsibilities: Playbooks clearly define the roles and responsibilities of different individuals or teams involved in the incident response process. By assigning specific tasks and duties, playbooks ensure that each person knows their role and understands what is expected of them during an incident. This clarity helps to avoid confusion, facilitates collaboration, and ensures a coordinated response effort.

Effective Decision-Making: Playbooks include decision points and guidelines for making informed choices during an incident. By detailing the considerations and factors to be taken into account, playbooks assist responders in making effective decisions quickly and confidently. This helps prevent delays and ensures that the response actions align with the organisation's goals, policies, and regulatory requirements.

Continuous Improvement: Playbooks should be regularly reviewed and updated based on lessons learned from Tabletop Exercises, incidents, changes in the threat landscape or the organisation’s environment. By incorporating feedback and insights gained from simulated incidents, organisations can continuously improve their playbooks, making them more effective and responsive to emerging cyber threats. This iterative approach enhances the organisation's overall incident response capability over time.