GUIDE TO SECURITY PLAYBOOKS AND RUNBOOKS WITH EXAMPLES AND SIMULATIONS

BY IZZMIER IZZUDDIN

ABNASIA.ORG

PLAYBOOK VS RUNBOOK

SECURITY PLAYBOOK

A security playbook is a structured, step-by-step guide that outlines the procedures and protocols an organisation should follow when responding to specific cybersecurity incidents or threats. It serves as a blueprint for incident response teams, ensuring a consistent and effective approach to managing and mitigating security events.

Key Components of a Security Playbook

1. **Objective**
    - **Definition**: Clearly states the purpose of the playbook, specifying the type of incident or threat it addresses.
    - **Example**: "To detect, analyse, and respond to phishing incidents to mitigate the impact on the organisation."
2. **Scope**
    - **Definition**: Defines the boundaries of the playbook, detailing which systems, departments, or scenarios it applies to.
    - **Example**: "Applicable to all email communications within the organisation and covers all forms of phishing attempts."
3. **Roles and Responsibilities**
    - **Definition**: Enumerates the team members involved in the incident response process and delineates their specific duties.
    - **Key Roles**:
        - **Incident Response Lead**: Oversees the entire response process.
        - **Security Analyst**: Conducts the technical analysis and initial triage.
        - **SOC Engineer**: Implements technical controls and containment measures.
        - **Communications Team**: Manages internal and external communications.
        - **Legal and Compliance Team**: Ensures adherence to legal and regulatory standards.
4. **Incident Identification and Triage**
    - **Definition**: Processes for detecting potential security incidents and determining their validity and severity.
    - **Components**:
        - **Detection Mechanisms**: SIEM alerts, user reports, automated monitoring tools.
        - **Triage Procedures**: Steps to verify the incident, assess impact, and prioritise response.
5. **Response Procedures**
    - **Definition**: Detailed, step-by-step actions to be taken once an incident is confirmed.
    - **Phases**:

        - **Containment**: Immediate actions to limit the spread or impact of the incident.
        - **Eradication**: Removing the threat from the environment.
        - **Recovery**: Restoring affected systems and services to normal operation.
        - **Post-Incident Activities**: Lessons learned, reporting, and playbook updates.
6. **Communication Plan**
    - **Definition**: Outlines how information about the incident will be communicated internally and externally.
    - **Components**:
        - **Stakeholder Notifications**: Identifying who needs to be informed and at what stages.
        - **Public Relations**: Managing external communications, especially if the incident becomes public.
        - **Employee Guidance**: Instructions and information provided to staff to prevent panic and misinformation.
7. **Documentation and Reporting**
    - **Definition**: Procedures for recording all aspects of the incident and response actions.
    - **Components**:
        - **Incident Reports**: Detailed logs of the incident, actions taken, and outcomes.
        - **Compliance Reporting**: Ensuring reports meet regulatory requirements.
        - **Record Keeping**: Maintaining records for future reference and audits.
8. **Review and Update Mechanisms**
    - **Definition**: Processes to evaluate the effectiveness of the playbook post-incident and make necessary adjustments.
    - **Components**:
        - **Post-Incident Review Meetings**: Gathering the response team to discuss what went well and areas for improvement.
        - **Playbook Revisions**: Updating procedures based on lessons learned and changing threat landscapes.
        - **Training and Drills**: Ensuring the team is familiar with updates through regular training sessions and simulated exercises.
9. **Appendices and Supporting Documents**
    - **Definition**: Supplementary materials that support the playbook's procedures.
    - **Examples**:
        - **Contact Lists**: Up-to-date information for all stakeholders and team members.
        - **Checklists**: Quick-reference guides for response actions.
        - **Flowcharts**: Visual representations of response processes.

Importance of a Security Playbook

- **Consistency**: Ensures that all incidents are handled uniformly, reducing the likelihood of oversight.
- **Efficiency**: Provides a ready-made plan, allowing teams to respond swiftly without deliberation.
- **Compliance**: Helps in adhering to legal and regulatory standards by embedding necessary compliance steps.
- **Training**: Serves as a training tool for new team members, familiarising them with response protocols.
- **Continuous Improvement**: Facilitates learning from past incidents, enabling the organisation to refine its security posture.

Example

Phishing Incident Response Playbook

Objective: To detect, analyse, and respond to phishing incidents to mitigate the impact on the organisation.

Roles and Responsibilities:

- **Incident Response Lead**: Coordinates the overall response, communicates with stakeholders, and ensures compliance with the incident response plan.
- **Security Analyst**: Performs initial triage, analysis of the phishing email, and identification of affected users.
- **SOC Engineer**: Executes containment actions, such as blocking malicious domains and isolating affected systems.
- **Communications Team**: Notifies employees and other stakeholders, providing guidance on actions to take.
- **Legal and Compliance Team**: Ensures all actions comply with legal and regulatory requirements, particularly regarding data breaches.

Scenario Overview:

On 13 August 2024, at 10:30 AM, the SOC received an alert from the email security gateway indicating that several employees received a suspicious email that appeared to be a phishing attempt.

Details of the Phishing Email:

- **Subject**: "URGENT: Update Your Account Information"
- **Sender**: info@secure-banking.com
- **Received By**: 25 employees across the finance and HR departments
- **Content**: The email claimed that the recipients' bank account information needed to be updated due to a security issue. It included a link to a fake banking website designed to steal login credentials.
- **Link**: http://securebanking-updates.com

Step-by-Step Procedures:

1. **Initial Triage**
    - **Security Analyst** reviews the alert and examines the email headers.
    - **Analysis**:
        - **Sender Address**: info@secure-banking.com (spoofed domain)
        - **URL in Email**: http://securebanking-updates.com (identified as malicious based on threat intelligence databases).
    - **Action**: Analyst confirms the email is a phishing attempt.
2. **Identification of Affected Users**
    - **Security Analyst** runs a query in the email gateway to identify all recipients.
    - **Results**:
        - 25 employees received the phishing email.
        - 5 employees clicked on the link, but none entered their credentials.
    - **Action**: Analyst adds affected users to an incident report.
3. **Containment**
    - **SOC Engineer**:
        - Blocks the malicious domain securebanking-updates.com at the network firewall.
        - Blacklists the sender email address on the email security gateway.
        - Isolates the systems of the 5 employees who clicked the link to prevent further spread.
    - **Action**: Containment actions are logged in the incident management system.
4. **User Notification**
    - **Communications Team**:
        - Sends an email to all employees warning them about the phishing attempt.
        - Provides instructions on how to recognise phishing emails and what to do if they suspect an email is malicious.
        - Directs affected users to reset their account passwords as a precaution.
    - **Action**: Notifications are recorded and sent to the Incident Response Lead.
5. **Analysis and Forensics**
    - **Security Analyst**:
        - Retrieves and analyses the clicked URLs to determine if any credentials were captured.
        - Uses forensic tools to examine the affected systems for signs of compromise.
    - **Results**:
        - No credentials were entered by the users who clicked the link.
        - Systems show no signs of malware or unauthorised access.
    - **Action**: The findings are documented in the incident report.
6. **Eradication and Recovery**
    - **SOC Engineer**:

        - Removes the isolation on the affected systems after verifying they are clean.
        - Ensures that all security patches are up-to-date.
    - **Action**: Systems are brought back online, and employees can resume work.
7. **Post-Incident Review**
    - **Incident Response Lead**:
        - Reviews the incident with the response team to identify any gaps in the process.
        - Updates the phishing playbook with lessons learned from this incident.
    - **Action**: A post-incident report is prepared, and any identified improvements are implemented.
8. **Reporting and Compliance**
    - **Legal and Compliance Team**:
        - Ensures that the incident response process complied with organisational policies and relevant regulations.
        - Reports the incident to regulatory bodies if required.
    - **Action**: Incident closure is documented, and a compliance report is filed.

Data:

- **Alert Data**:
    - Time: 10:30 AM
    - Trigger: Phishing email detected
    - Affected Users: 25 (names and emails can be simulated as needed)
    - Click-throughs: 5 (Izzmier, Iffah, etc.)
- **Malicious URL**: http://securebanking-updates.com
- **Incident Report ID**: 2024-08-13-001

SECURITY RUNBOOK

A security runbook is a detailed guide that provides the specific steps and commands needed to carry out routine operational tasks or incident responses in a cybersecurity context. Unlike a playbook, which provides a broader strategy and process for handling incidents, a runbook focuses on the exact, often technical, steps required to execute those processes.

Key Components of a Security Runbook

1. **Objective**
    - **Definition**: The specific purpose of the runbook, detailing the task or process it is designed to address.
    - **Example**: "To automate the containment of a malware infection on a compromised endpoint."
2. **Scope**
    - **Definition**: Defines the boundaries of what the runbook covers, including systems, scenarios, or tools it applies to.
    - **Example**: "Applicable to all Windows endpoints managed by the Security Operations Centre (SOC)."
3. **Pre-requisites**
    - **Definition**: Lists the requirements or conditions that must be met before executing the runbook.
    - **Examples**:
        - Access to the endpoint's administrative credentials.
        - Connection to the corporate network.
        - SIEM or EDR tool configured to detect relevant alerts.
4. **Roles and Responsibilities**
    - **Definition**: Outlines the specific individuals or teams responsible for executing the runbook.
    - **Key Roles**:
        - **SOC Analyst**: Executes the runbook steps and monitors outcomes.
        - **System Administrator**: Provides necessary access and support.
        - **Incident Response Lead**: Oversees the process and makes key decisions if issues arise.
5. **Tools Required**
    - **Definition**: Lists the software, tools, or scripts needed to perform the steps in the runbook.
    - **Examples**:
        - Endpoint Detection and Response (EDR) tool.
        - SIEM platform (e.g., QRadar).
        - PowerShell scripts for automation.
6. **Execution Steps**
    - **Definition**: The core of the runbook, providing a step-by-step guide on how to perform the task. This includes detailed commands, scripts, and expected outcomes.

- **Format**:
  - **Step Description**: A brief overview of what the step accomplishes.
  - **Command/Script**: The exact code or command to be executed.
  - **Expected Outcome**: What should happen after the step is performed.
- **Example**:
  - **Step 1: Isolate the Infected Endpoint**
    - **Description**: Disconnect the infected endpoint from the network to prevent malware spread.
    - **Command**:

      ```
      netsh interface set interface "Ethernet" admin=disable
      ```

    - **Expected Outcome**: The endpoint is disconnected from the network.

7. **Verification**
   - **Definition**: Steps to confirm that each action was successful and the desired outcome was achieved.
   - **Examples**:
     - Check network connectivity to ensure isolation.
     - Verify that malware processes are terminated.
     - Ensure backup files are successfully created and stored.
8. **Error Handling**
   - **Definition**: Procedures for addressing issues or errors that may occur during the execution of the runbook.
   - **Examples**:
     - If isolation fails, manually disable the network interface.
     - If a script fails, review logs to diagnose the issue and retry.
     - Escalate to the Incident Response Lead if the error persists.
9. **Post-Execution Actions**
   - **Definition**: Follow-up steps after the main task is completed to ensure everything is back to normal and no additional actions are required.
   - **Examples**:
     - Restore network connectivity to the endpoint once cleared.
     - Document the actions taken in the incident management system.
     - Notify relevant stakeholders of the completion of the runbook execution.
10. **Documentation and Reporting**
    - **Definition**: Details on how to document the steps taken during the runbook execution and report the outcomes.
    - **Components**:
      - **Runbook Execution Log**: A log of all actions performed, including timestamps and outcomes.
      - **Incident Report**: A summary report that captures the incident, the steps taken, and the final resolution.
      - **Audit Trail**: Ensures all steps are logged for future review and compliance purposes.

11. **Review and Update Mechanisms**
    - **Definition**: Processes for regularly reviewing and updating the runbook to ensure it remains effective and up-to-date with the latest tools and procedures.
    - **Components**:
        - **Periodic Reviews**: Scheduled reviews of the runbook by the SOC team.
        - **Feedback Loop**: Incorporate feedback from users to improve clarity and efficiency.
        - **Version Control**: Maintain a version history of the runbook for tracking changes.
12. **Appendices and References**
    - **Definition**: Supplementary materials that provide additional context or support for the runbook.
    - **Examples**:
        - **Command References**: A list of commands used in the runbook with explanations.
        - **Links to Vendor Documentation**: Access to official documentation for tools used in the runbook.
        - **Sample Logs**: Examples of logs that may be generated during the execution of the runbook.

Importance of a Security Runbook

- **Consistency**: Ensures that routine tasks and incident responses are performed uniformly across the organisation.
- **Efficiency**: Provides a clear and detailed guide, allowing tasks to be completed quickly and accurately without confusion.
- **Automation**: Enables the automation of repetitive tasks, reducing manual effort and the potential for human error.
- **Training**: Acts as a training tool for new SOC analysts or team members unfamiliar with specific tasks.
- **Continuous Improvement**: Allows for regular updates and refinements, ensuring the runbook evolves with the changing threat landscape and organisational needs.

Example

Ransomware Containment Runbook

Objective:

To automatically contain a ransomware attack by isolating affected systems, preserving critical data, and preventing the spread of the ransomware within the network.

Trigger:

The runbook is triggered when the SIEM system detects ransomware-related activities, such as unusual file encryption or a ransomware signature in the logs.

Trigger Event Data:

- **Time of Detection**: 13 August 2024, 2:30 PM
- **Alert**: Ransomware signature detected in logs.
- **Affected Host**: HR-Workstation-07
- **Ransomware Detected**: Ryuk

Step-by-Step Procedures:

1. **Initiate Network Isolation**
    - **Action**: The runbook automatically isolates the affected host HR-Workstation-07 from the network.
    - **Command**: Execute a script that interacts with the network switch to disable the port associated with the affected machine.
    - **Verification**: Confirm that the host is no longer communicating with the network.
    - **Output**:
        - Log entry created: 2024-08-13 14:31: Host HR-Workstation-07 isolated from the network.
        - Alert notification sent to Incident Response Team.
2. **Initiate System Snapshot and Backup**
    - **Action**: The runbook triggers an automated backup of critical data from the affected system to a secure storage location.
    - **Command**:
        - Snapshot the current state of the system using a virtualisation platform.
        - Copy essential files to an off-network backup server.
    - **Verification**: Ensure that the backup completes successfully and the snapshot is intact.
    - **Output**:
        - Log entry created: 2024-08-13 14:40: Backup of critical data from HR-Workstation-07 completed successfully.
        - Backup completion alert sent to the Incident Response Team.
3. **Block Ransomware IPs and Domains**
    - **Action**: Automatically block known ransomware-related IP addresses and domains at the firewall level.
    - **Command**: Update the firewall rules to block outbound connections to known malicious IPs/domains associated with the Ryuk ransomware.
    - **Verification**: Verify that the firewall rules are updated and active.
    - **Output**:
        - Log entry created: 2024-08-13 14:45: Outbound connections to known Ryuk IPs/domains blocked.
        - Confirmation alert sent to the SOC Team.
4. **Initiate Malware Scan on Other Hosts**

    - **Action**: Launch an immediate malware scan across other systems in the same network segment as the affected host.
    - **Command**: Use endpoint detection and response (EDR) tools to initiate a full malware scan on all devices within the HR subnet.
    - **Verification**: Confirm that the scans are initiated and monitor for any other compromised systems.
    - **Output**:
        - Log entry created: 13-08-2024 15:00: Malware scan initiated on all devices within the HR subnet.
        - Scan results automatically reported to the SOC Team.
5. **Notify Incident Response Team**
    - **Action**: Send a detailed incident report to the Incident Response Lead and SOC Manager.
    - **Command**: Automatically generate an incident report with details of the ransomware detection, actions taken, and current status.
    - **Verification**: Ensure the report is accurate and includes all necessary details.
    - **Output**:
        - Incident report sent via email and logged in the incident management system.
        - Notification to stakeholders that containment actions are complete.
6. **Monitor and Escalate**
    - **Action**: Continuously monitor the network for any further signs of ransomware activity.
    - **Command**: Set up alerts for any new indicators of compromise (IOCs) related to Ryuk ransomware.
    - **Escalation**: If new activity is detected, automatically escalate to the Incident Response Lead for further action.
    - **Output**:
        - Continuous monitoring logs and real-time alerts sent to the Incident Response Team.
        - Escalation protocol triggered if further ransomware activity is detected.

Data:

- **Affected Host**: HR-Workstation-07 (IP: 192.168.1.27)
- **Ransomware Variant**: Ryuk
- **Malicious IPs Blocked**:
    - 185.141.25.242
    - 195.54.160.149
- **Backup Location**: \\secure-backup-server\HR-Workstation-07\
- **Incident Report ID**: 2024-08-13-002

HOW TO USE SECURITY PLAYBOOKS AND RUNBOOKS TOGETHER?

- **Playbook-driven runbooks:** A playbook can define the high-level strategy and procedure for handling a specific incident type or scenario, and a runbook can implement the low-level actions and tasks that are required to execute the playbook. For example, a playbook can outline the steps for responding to a phishing incident, such as verifying the source, analysing the email, identifying the targets, and notifying the users, and a runbook can automate and orchestrate the actions for each step, such as querying the email headers, extracting the URLs, checking the reputation, and sending the notifications.

- **Runbook-driven playbooks:** A runbook can trigger the execution of a playbook based on certain events or conditions, and a playbook can guide the human intervention and decision making that are required to complete the incident response process. For example, a runbook can detect and contain a ransomware attack, such as blocking the network traffic, isolating the infected machines, and taking the backups, and a playbook can instruct the human response team on how to eradicate the malware, restore the systems, and report the incident.

- **Hybrid playbooks and runbooks:** A playbook and a runbook can be combined into a single entity that provides both automation and orchestration capabilities, as well as human interaction and oversight. For example, a hybrid playbook and runbook can handle a denial-of-service attack, such as collecting and analysing the traffic data, mitigating the attack, and escalating the incident, and also allow the human response team to monitor, intervene, and approve the actions as needed.