| | | | |
|---|---|---|---|
| Document Reference: | EPIRP - 1 | Effective Date: | 10 May 2024 |
| Document Name: | Elevation of Privilege Playbook | Expiry Date: | 10 May 2025 |

# Elevation of Privilege Incident Response Playbook

*Redback Operations*

| | | | |
|---|---|---|---|
| Document Owner: | Pari | Last Modified By: | Pari |
| Next Review Date: | 15 July 2024 | Last Modified on: | 10 May 2024 |

| Version | Modified By | Approver | Date | Changes made |
|---|---|---|---|---|
| 1.0 | Pari | | | Initial Draft |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

# Table of Contents

# 1 Introduction

## 1.1 Overview

In today's digitally interconnected landscape, organizations face an ever-growing array of cyber threats, with elevation of privilege attacks standing out as particularly insidious. The Elevation of Privilege Incident Response Playbook serves as a vital tool to equip organizations with the means to effectively counter such threats. By offering a structured approach to incident response, this playbook is designed to fortify organizational resilience against security breaches and safeguard critical assets. Through proactive measures and clear response protocols, it empowers security teams to swiftly detect, contain, and remediate incidents, thereby minimizing potential damage and disruption. Moreover, the playbook serves as a proactive strategy to bolster the organization's overall security posture and readiness in the face of evolving cyber threats.

## 1.2 Purpose

The primary purpose of the Elevation of Privilege Incident Response Playbook is to empower organizations to respond swiftly and decisively to elevation of privilege attacks. By providing clear guidelines and procedures, the playbook enables security teams to detect, contain, and remediate incidents in a timely manner, thereby minimizing the potential damage and disruption caused. Additionally, the playbook serves as a proactive measure to enhance the organization's overall security posture and readiness to combat evolving cyber threats.

## 1.3 Attack definition

An elevation of privilege attack occurs when a malicious actor gains unauthorized access to privileged accounts, systems, or resources within an organization's network. This type of attack typically involves exploiting vulnerabilities in software, misconfigurations, or weaknesses in authentication mechanisms to escalate their level of access beyond what is intended. Examples of elevation of privilege attacks include privilege escalation exploits, credential theft, and lateral movement within the network. By clearly defining these attack vectors, the playbook equips responders with the knowledge to identify and mitigate such threats effectively.

## 1.4 Scope

The Elevation of Privilege Incident Response Playbook covers a wide range of elevation of privilege incidents that may occur within the organization's infrastructure. This includes attacks targeting servers, workstations, cloud environments, and other critical assets. The playbook applies to incidents involving both internal and external threats, encompassing malicious activities perpetrated by insiders, external adversaries, or third-party actors.

Clarifying the scope ensures that responders understand the playbook's applicability and can effectively execute response procedures within their designated domain of responsibility.

# 2 Attack Types

## 2.1 Vertical Privilege Escalation

In this , an attacker seeks to elevate their privileges within the same system or application. This typically involves escalating from a lower privilege level (e.g., a standard user) to a higher privilege level (e.g., an administrator or root user) on the same system. Attackers often exploit vulnerabilities in the operating system, applications, or configuration settings to gain elevated privileges.

Common techniques for vertical privilege escalation include:

- **Exploiting Software Vulnerabilities:** Attackers exploit vulnerabilities in operating systems, applications, or services to gain unauthorized access to higher privilege levels. This can include buffer overflow attacks, input validation vulnerabilities, or insecure configurations that allow attackers to execute arbitrary code with elevated privileges.
- **Kernel Exploitation:** Exploiting vulnerabilities in the operating system kernel to gain root/administrator privileges on the same system. This typically involves exploiting vulnerabilities in kernel-level components such as device drivers or system calls to escalate privileges within the same system.
- **DLL Hijacking (Windows):** Exploiting insecure DLL loading mechanisms in Windows applications running on the same system to execute arbitrary code with elevated privileges. This involves planting malicious DLLs in directories searched by vulnerable applications on the same system.
- **File System Manipulation:** Manipulating file system permissions, symbolic links, or file attributes within the same system to gain higher privilege levels. This includes modifying file permissions or creating symbolic links to gain unauthorized access to sensitive files or directories within the same system.

## 2.2 Horizontal Privilege Escalation

Horizontal privilege escalation involves gaining access to the same level of privileges but on a different system or application within the same network environment. This is often referred to as an account takeover. Instead of escalating to a higher privilege level, attackers aim to access resources or data that they are not authorized to access within their current privilege level. This type of attack is often associated with lateral movement within a network, where

attackers exploit vulnerabilities or weaknesses in interconnected systems to move laterally and gain access to additional resources.

Common techniques for horizontal privilege escalation include:

- **Exploiting Weak Authentication:** Leveraging weak or default credentials or authentication bypass vulnerabilities to gain unauthorized access to accounts or systems on other systems within the same network. For example, using compromised credentials to gain unauthorized access to accounts on other systems.
- **Abusing Misconfigured Permissions:** Exploiting misconfigured file system permissions or access control settings to gain unauthorized access to resources or data on other systems within the same network. This involves manipulating file permissions or access control settings to access sensitive resources on other systems.
- **Privilege Escalation via Services:** Exploiting vulnerabilities or misconfigurations in network services running on other systems within the same network to gain higher privilege levels. For instance, exploiting vulnerabilities in network services to gain administrative access to other systems.

Understanding the nuances between vertical and horizontal privilege escalation empowers organizations to customize the security defences and response strategies, effectively mitigating the distinct risks posed by each type of attack.

# 3 Stakeholders

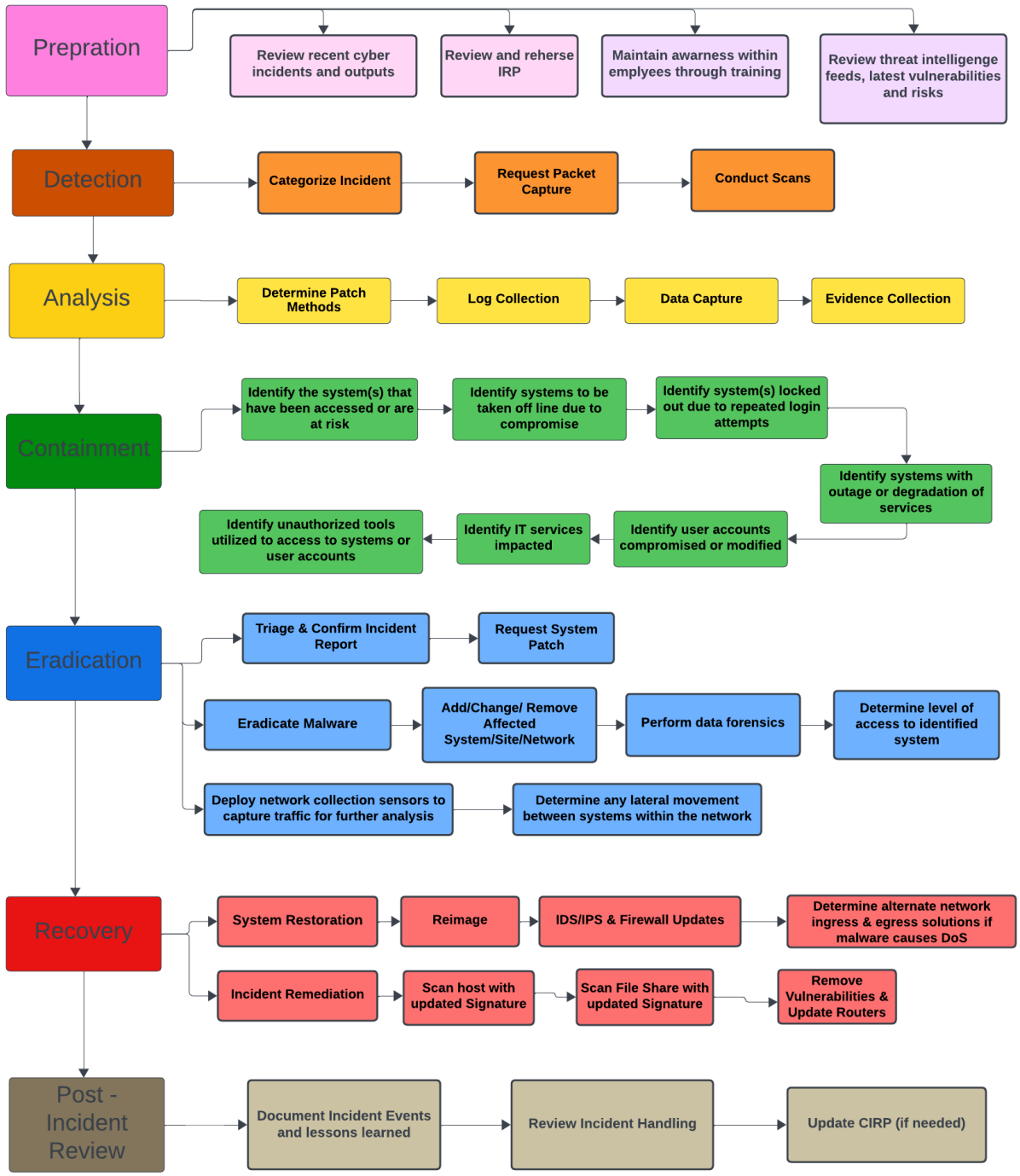
- **Security Team:** The security team comprises cybersecurity professionals responsible for monitoring, detecting, investigating, and responding to security incidents. This may include security analysts, incident responders, threat hunters, and forensic experts.
- **IT Operations Team:** The IT operations team manages the organization's IT infrastructure, including networks, servers, endpoints, and applications. They play a crucial role in implementing security controls, managing vulnerabilities, and coordinating incident response efforts.
- **Executive Leadership:** They are responsible for setting strategic direction, allocating resources, and making key decisions related to incident response and cybersecurity.
- **Board of Directors:** The board of directors provides oversight and governance of the organization's cybersecurity strategy and risk management practices. They may

require regular updates on security incidents, their impact on the organization, and the effectiveness of incident response efforts.

- **Third-Party Vendors and Partners:** Third-party vendors and partners who provide services or have access to the organization's systems and data may be affected by security incidents. Collaboration with these stakeholders is essential for coordinated incident response and mitigation efforts.

- **End Users:** Users of the organization's products or services may be impacted by security incidents, such as data breaches or service disruptions. Maintaining open communication with affected individuals and providing support and guidance are important aspects of incident response.

# 4 Flow Diagram



**Preparation (Pink)**

- Creating an incident response plan that outlines procedures, communication channels, and escalation paths.
- Train incident response teams and employees.
- Identifying critical assets and their associated risks.
- Ensuring that necessary tools and resources are available.

**Detection (Orange)**

- Implementing intrusion detection systems (IDS) and security monitoring tools.
- Analysing logs, alerts, and anomalies.
- Notifying the IRT when suspicious activity is detected.

**Analysis (Yellow)**

- Gathering information about affected systems, users, and potential attack vectors.
- Conducting forensics analysis.
- Assessing the severity and potential consequences.

**Containment (Green)**

- Blocking malicious traffic or isolating compromised hosts.
- Changing credentials and access controls.
- Implementing temporary workarounds.

**Eradication (Blue)**

- Identifying vulnerabilities or misconfigurations.
- Patching or updating affected systems.
- Removing malware or unauthorized accounts.

**Recovery (Red)**

- Verifying system integrity.
- Restoring data from backups.

**Post-Incident Review (Brown)**

- Conduct a thorough review.
- Learn from the incident.
- Update the CIRP.

# 5 Incident Response Stages

## 5.1 Preparation

The focus is on proactively preparing the organization to effectively respond to elevation of privilege incidents.

**Key actions:**

- Developing and maintaining an incident response plan specifically tailored for elevation of privilege incidents, outlining roles, responsibilities, and escalation procedures.
- Conducting regular training and awareness programs to educate employees about elevation of privilege risks and response procedures, emphasizing the importance of privilege management.
- Implementing security controls and measures to prevent, detect, and mitigate elevation of privilege attacks, such as implementing least privilege principles, robust authentication mechanisms, and monitoring solutions.
- Reviewing and updating access control policies, privilege management practices, and security configurations to minimize the risk of privilege escalation, including regular reviews of user permissions and access levels.

## 5.2 Detection

The Detection stage involves identifying potential elevation of privilege incidents as early as possible.

**Key actions:**

- Implementing monitoring and detection mechanisms to identify suspicious activities, anomalies, or indicators of privilege escalation, such as unauthorized access attempts or changes in user permissions.
- Utilizing intrusion detection systems (IDS), intrusion prevention systems (IPS), endpoint detection and response (EDR) solutions, and other security tools to monitor

for signs of unauthorized access attempts, privilege escalation exploits, or abnormal behaviour.

- Establishing thresholds and alerting mechanisms to notify incident responders of potential elevation of privilege incidents in real-time, enabling prompt investigation and response.
- Conducting regular security assessments, vulnerability scans, and penetration tests to identify weaknesses and vulnerabilities that could be exploited for privilege escalation, with a focus on identifying and remedying misconfigurations and vulnerabilities.

## 5.3 Analysis

In the Analysis stage, incident responders investigate and analyse suspected elevation of privilege incidents to determine their scope, impact, and root causes.

**Key actions:**

- Collecting and analysing evidence, logs, and artifacts related to the incident, including system logs, network traffic data, and forensic images, to understand the nature and extent of the privilege escalation.
- Correlating and contextualizing security events and alerts to reconstruct the attack chain and identify the techniques, tactics, and tools used by attackers to escalate privileges.
- Assessing the impact of the incident on affected systems, data, and users to prioritize response efforts and mitigate further damage, including identifying any data or systems compromised because of the privilege escalation.

## 5.4 Containment

The Containment stage focuses on preventing further unauthorized access or damage caused by the elevation of privilege incident.

**Key actions:**

- Isolating affected systems, networks, or resources to prevent the spread of malware or unauthorized access.
- Disabling compromised accounts, revoking unnecessary privileges, and resetting compromised credentials to prevent further exploitation.

- Implementing temporary security controls or mitigations to contain the incident while investigations are ongoing, such as implementing additional access controls or network segmentation to limit the attacker's ability to move laterally.
- Communicating with stakeholders and affected parties to notify them of containment measures and provide guidance on mitigating risks, such as resetting passwords or monitoring for suspicious activity.

## 5.5 Eradication

In the Eradication stage, incident responders work to remove the root cause of the elevation of privilege incident and eliminate any lingering threats or vulnerabilities.

**Key actions:**

- Patching or remediating vulnerabilities exploited by attackers to gain unauthorized access or escalate privileges, including applying security patches, updating software, and addressing misconfigurations identified during the incident response process.
- Removing malware, backdoors, or other malicious artifacts from compromised systems and networks, ensuring that the attacker no longer has access to compromised resources.
- Conducting thorough security hygiene checks and implementing security best practices to prevent similar incidents in the future, such as reviewing and updating security configurations and hardening systems against known attack vectors.

## 5.6 Recovery

The Recovery stage focuses on restoring affected systems, data, and services to normal operation following the elevation of privilege incident.

**Key actions:**

- Restoring from backups or snapshots to recover data and configurations compromised during the incident, ensuring that critical systems and data are restored to a known good state.
- Rebuilding or re-imaging compromised systems to ensure they are free from malware or unauthorized access, implementing additional security measures as necessary to prevent recurrence.
- Conducting system and network hardening activities to strengthen security posture and minimize the risk of recurrence, including implementing additional access controls, monitoring solutions, and security configurations.

- Communicating with stakeholders and users to provide updates on recovery efforts and restore confidence in the organization's security controls.

### 5.7 Post Incident Review

The Post-Incident Review stage involves conducting a comprehensive review and analysis of the elevation of privilege incident response process to identify lessons learned and areas for improvement.

**Key actions:**

- Evaluating the effectiveness of incident response procedures, tools, and communication protocols used during the incident, identifying any gaps or deficiencies that may have impacted the response effort.
- Documenting and analysing the root causes, contributing factors, and impacts of the incident to inform future prevention and response efforts, including identifying any systemic issues or recurring patterns that need to be addressed.
- Developing and implementing corrective actions, recommendations, or enhancements to strengthen incident response capabilities and prevent recurrence, such as updating incident response plans, improving training programs, or implementing additional security controls.

## 6 Terminology

- **Privilege Escalation:** The act of increasing the level of access or permissions granted to a user or application, typically to gain unauthorized control over system resources or sensitive data.
- **Least Privilege Principle:** The security principle that users, processes, and systems should be granted only the minimum level of access or permissions necessary to perform their intended tasks, reducing the risk of privilege escalation and unauthorized access.
- **Exploitation:** The process of taking advantage of vulnerabilities, misconfigurations, or weaknesses in software, systems, or networks to carry out malicious actions.
- **Security Controls:** Measures, mechanisms, or safeguards implemented to protect systems, networks, and data from security threats, such as access controls, authentication mechanisms, encryption, and monitoring solutions.
- **Root Cause Analysis (RCA):** A methodical investigation process used to determine the underlying cause or causes of a security incident, to address systemic issues, vulnerabilities, or weaknesses that contributed to the incident.

- **Post-Incident Review:** A structured review and analysis of the response to a security incident, including elevation of privilege incidents, to identify lessons learned, areas for improvement, and corrective actions to strengthen incident response capabilities and prevent future incidents.
- **Incident Response Team (IRT):** A dedicated team of professionals responsible for responding to security incidents, following the procedures outlined in the incident response plan to mitigate the impact and prevent further damage.