



Document Reference: EPIRP - 2

Effective Date: 03 August 2024

Document Name: Elevation of Privilege Playbook

Expiry Date: 03 March 2025

Elevation of Privilege Incident Response Playbook

Redback Operations

Document Owner: Blue Team
Next Review Date: 03 March 2025

Last Modified By: Devika Sivakumar
Last Modified on: 03 August 2024



Document Reference: EPIRP - 2

Effective Date: 03 August 2024

Document Name: Elevation of Privilege Playbook

Expiry Date: 03 March 2025

Version	Modified By	Approver	Date	Changes made
1.0	Pari			Initial Draft
2.0	Devika Sivakumar		03 August 2024	A comprehensive update has been carried out throughout the playbook. Several new attack types and case studies have been added. The stakeholder's section has been revised, and a RACI chart has been included. The incident response stage has been updated, with steps for monitoring threats now included. New terminology has been introduced. The overall format of the playbook has been adjusted to align with other playbooks. The table has also been updated.

Document Owner: Blue Team
Next Review Date: 03 March 2025

Last Modified By: Devika Sivakumar
Last Modified on: 03 August 2024



Document Reference: EPIRP - 2 Effective Date: 03 August 2024
Document Name: Elevation of Privilege Playbook Expiry Date: 03 March 2025

Table of Contents

1 Introduction	5
1.1 Overview	5
1.2 Purpose	5
1.3 Attack definition	5
1.4 Scope.....	5
2 Attack Types	6
2.1 Vertical Privilege Escalation	6
2.2 Horizontal Privilege Escalation	7
2.3 Credential Theft.....	8
2.4 Lateral Movement.....	8
2.5 Insecure API Usage	9
3 Stakeholders.....	10
4 Flow Diagram	14
5 Incident Response Stages.....	17
5.1 Preparation	17
5.2 Detection	17
5.3 Analysis.....	17
5.4 Containment	18
5.5 Eradication	18
5.6 Recovery	18
5.7 Post-Incident Review.....	19
6. Steps for Monitoring Threats	20
6.1 Establish a Monitoring Strategy.....	20
6.2 Deploy Monitoring Solutions.....	20
6.3 Continuous Monitoring and Analysis	21
6.4 Alerting and Notification.....	21
6.5 Investigate and Respond.....	21
6.6 Post-Incident Review.....	22

Document Owner: Blue Team Last Modified By: Devika Sivakumar
Next Review Date: 03 March 2025 Last Modified on: 03 August 2024



Document Reference: EPIRP - 2

Effective Date: 03 August 2024

Document Name: Elevation of Privilege Playbook

Expiry Date: 03 March 2025

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.

Document Owner: Blue Team
Next Review Date: 03 March 2025

Last Modified By: Devika Sivakumar
Last Modified on: 03 August 2024



Document Reference: EPIRP - 2

Effective Date: 03 August 2024

Document Name: Elevation of Privilege Playbook

Expiry Date: 03 March 2025

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.

Case Study: Microsoft Exchange Server Exploit (2021)

- **Overview:** Attackers exploited vulnerabilities in Microsoft Exchange Server, allowing them to elevate privileges and gain access to email accounts and install additional malware.
- **Impact:** Hundreds of thousands of servers were compromised worldwide, affecting both private and public sector organizations.
- **Response:** Microsoft released patches to address the vulnerabilities, and organizations were urged to apply these patches immediately and review their systems for signs of compromise.

Document Owner: Blue Team
Next Review Date: 03 March 2025

Last Modified By: Devika Sivakumar
Last Modified on: 03 August 2024



Document Reference:	EPIRP - 2	Effective Date:	03 August 2024
Document Name:	Elevation of Privilege Playbook	Expiry Date:	03 March 2025

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.

Case Study: SolarWinds Cyberattack (2020)

- **Overview:** Attackers inserted malicious code into the SolarWinds Orion platform, enabling them to move laterally within networks and gain access to sensitive information.
- **Impact:** The breach affected numerous organizations, including government agencies and private companies, leading to significant data breaches and security concerns.
- **Response:** SolarWinds released updates to secure their platform, and affected organizations conducted thorough investigations and applied security measures to prevent further unauthorized access.

Document Owner:	Blue Team	Last Modified By:	Devika Sivakumar
Next Review Date:	03 March 2025	Last Modified on:	03 August 2024



Document Reference: EPIRP - 2

Effective Date: 03 August 2024

Document Name: Elevation of Privilege Playbook

Expiry Date: 03 March 2025

2.3 Credential Theft

Description: Attackers steal user credentials such as usernames and passwords, often using techniques like phishing, keylogging, or exploiting weak password policies. These stolen credentials are then used to access systems and escalate privileges.

Common Techniques:

1. **Phishing:** Deceptive emails or messages trick users into disclosing their credentials.
2. **Keylogging:** Malicious software records keystrokes to capture login information.
3. **Brute Force Attacks:** Automated attempts to guess passwords by trying numerous combinations.

Case Study: Uber Data Breach (2016)

- **Overview:** Attackers used stolen credentials to access Uber's GitHub repository and obtain sensitive data, including personal information of drivers and riders.
- **Impact:** Personal information of 57 million drivers and riders was exposed.
- **Response:** Uber implemented stronger access controls, enhanced monitoring, and improved security practices to prevent future breaches.

2.4 Lateral Movement

Description: After gaining initial access, attackers move laterally within the network to access additional systems and data. This is often done to maintain persistence and escalate privileges further.

Common Techniques:

1. **Pass-the-Hash:** Using hashed credentials to authenticate without knowing the actual password.
2. **Exploiting Trust Relationships:** Leveraging legitimate network connections to move between systems.
3. **Using Exploited Accounts:** Compromising additional user accounts to access more resources.

Case Study: NotPetya Ransomware Attack (2017)

- **Overview:** The NotPetya ransomware spread laterally within networks, encrypting data and disrupting operations.
- **Impact:** The attack caused extensive damage to various organizations, including Maersk and Merck, leading to billions of dollars in losses.

Document Owner: Blue Team
Next Review Date: 03 March 2025

Last Modified By: Devika Sivakumar
Last Modified on: 03 August 2024



Document Reference: EPIRP - 2

Effective Date: 03 August 2024

Document Name: Elevation of Privilege Playbook

Expiry Date: 03 March 2025

- **Response:** Organizations improved their network segmentation, applied patches, and enhanced their incident response capabilities to mitigate the effects of similar attacks in the future.

2.5 Insecure API Usage

Description: Attackers exploit vulnerabilities or misconfigurations in application programming interfaces (APIs) to gain elevated privileges. APIs that are not properly secured can be used to access sensitive data or perform unauthorized actions.

Common Techniques:

1. **Parameter Tampering:** Manipulating parameters sent to APIs to bypass authentication or authorization controls.
2. **Injection Attacks:** Exploiting injection vulnerabilities in API endpoints to execute malicious code.
3. **Excessive Data Exposure:** Accessing sensitive data that is inadvertently exposed through poorly designed APIs.

Case Study: Facebook API Exploit (2018)

- **Overview:** Attackers exploited vulnerabilities in Facebook's APIs, allowing them to gain access to user accounts and steal personal data.
- **Impact:** The breach affected millions of users, exposing their personal information.
- **Response:** Facebook patched the vulnerabilities, conducted a thorough security review, and improved their API security practices.

Document Owner: Blue Team
Next Review Date: 03 March 2025

Last Modified By: Devika Sivakumar
Last Modified on: 03 August 2024



Document Reference: EPIRP - 2 Effective Date: 03 August 2024
Document Name: Elevation of Privilege Playbook Expiry Date: 03 March 2025

3 Stakeholders

Effective elevation of privilege incident response requires collaboration among key stakeholders within and outside Redback Operations.

3.1 IT Security Team

Lead: Daniel McAulay (Senior Project Leader)

Responsibilities:

- Identifying, researching, and preventing elevation of privilege attacks.
- Leading technical response tasks such as privilege escalation analysis and vulnerability patching.

3.2 Incident Response Team

Lead: Devika Sivakumar (Blue Team Leader)

Responsibilities:

- Coordinating response efforts and communicating with relevant parties.
- Implementing incident response protocols and conducting post-incident analysis.

3.3 Communication Team

Lead: Kaleb Bowen (Company Lead)

Responsibilities:

- Managing internal and external communications regarding the incident.
- Informing staff, clients, and other relevant parties about the response activities.

3.4 Customers

Responsibilities:

- Reporting suspicious activity.
- Following organizational guidelines to protect personal information.

3.5 Third-Party Vendors and Partners

Responsibilities:

- Providing specialized knowledge and assistance during the response process.
- Complying with data security and privacy requirements.

Document Owner: Blue Team Last Modified By: Devika Sivakumar
Next Review Date: 03 March 2025 Last Modified on: 03 August 2024



Document Reference: EPIRP - 2

Effective Date: 03 August 2024

Document Name: Elevation of Privilege Playbook

Expiry Date: 03 March 2025

RACI Chart for Elevation of Privilege Incident Response

Task/Activity	IT Security Team	Incident Response Team	Communication Team	Customers	Third-Party Vendors
Preparation					
Establish incident response team	R, C	A, R	I	I	I
Develop response procedures	A, R	R, C	I	I	I
Conduct training sessions	A, R	R	I	I	I
Implement surveillance systems	A, R	R	I	I	I
Detection					
Monitor system logs and traffic	A, R	R	I	I	I
Use IDS and SIEM tools	A, R	R	I	I	I
Analyse alerts	A, R	R	I	I	I
Analysis					
Collect forensic data	A, R	R	I	I	I
Identify attack methods	A, R	R	I	I	I
Determine impact	A, R	R	I	I	I
Containment					
Isolate compromised systems	A, R	R	I	I	I

Document Owner: Blue Team
Next Review Date: 03 March 2025

Last Modified By: Devika Sivakumar
Last Modified on: 03 August 2024



Document Reference: EPIRP - 2

Effective Date: 03 August 2024

Document Name: Elevation of Privilege Playbook

Expiry Date: 03 March 2025

Implement access restrictions	A, R	R	I	I	I
Block malicious traffic	A, R	R	I	I	I
Eradication					
Remove malicious software	A, R	R	I	I	I
Patch vulnerabilities	A, R	R	I	I	I
Update security policies	A, R	R	I	I	I
Recovery					
Restore backups	A, R	R	I	I	I
Rebuild systems	A, R	R	I	I	I
Conduct user training	A, R	R	I	I	I
Post-Incident Review					
Review incident response	A, R	R	I	I	I
Document lessons learned	A, R	R	I	I	I
Update response procedures	A, R	R	I	I	I
Communication					
Create communication plans	C	C	A, R	I	I
Draft communication materials	C	C	A, R	I	I

Document Owner: Blue Team
Next Review Date: 03 March 2025

Last Modified By: Devika Sivakumar
Last Modified on: 03 August 2024



Document Reference: EPIRP - 2

Effective Date: 03 August 2024

Document Name: Elevation of Privilege Playbook

Expiry Date: 03 March 2025

Manage media relations	C	C	A, R	I	I
Provide updates	C	C	A, R	I	I

Key:

- **R:** Responsible (those who do the work)
- **A:** Accountable (those who are ultimately answerable)
- **C:** Consulted (those who provide input)
- **I:** Informed (those who are kept up to date)

Document Owner: Blue Team
Next Review Date: 03 March 2025

Last Modified By: Devika Sivakumar
Last Modified on: 03 August 2024



Document Reference: EPIRP - 2

Effective Date: 03 August 2024

Document Name: Elevation of Privilege Playbook

Expiry Date: 03 March 2025

4 Flow Diagram



Document Owner: Blue Team
Next Review Date: 03 March 2025

Last Modified By: Devika Sivakumar
Last Modified on: 03 August 2024



Document Reference: EPIRP - 2

Effective Date: 03 August 2024

Document Name: Elevation of Privilege Playbook

Expiry Date: 03 March 2025

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.

Document Owner: Blue Team
Next Review Date: 03 March 2025

Last Modified By: Devika Sivakumar
Last Modified on: 03 August 2024



Document Reference: EPIRP - 2

Effective Date: 03 August 2024

Document Name: Elevation of Privilege Playbook

Expiry Date: 03 March 2025

Post-Incident Review (Brown)

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

Document Owner: Blue Team
Next Review Date: 03 March 2025

Last Modified By: Devika Sivakumar
Last Modified on: 03 August 2024



Document Reference: EPIRP - 2

Effective Date: 03 August 2024

Document Name: Elevation of Privilege Playbook

Expiry Date: 03 March 2025

5 Incident Response Stages

5.1 Preparation

Objective: Establish the foundation for an effective elevation of privilege incident response.

Activities:

- 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.
- Reviewing and updating access control policies, privilege management practices, and security configurations to minimize the risk of privilege escalation.

Outcome: A fully prepared organization capable of responding quickly and effectively to elevation of privilege incidents.

5.2 Detection

Objective: Identify indications of elevation of privilege attacks or unauthorized access.

Activities:

- Implementing monitoring and detection mechanisms to identify suspicious activities, anomalies, or indicators of privilege escalation.
- Utilizing IDS, IPS, EDR solutions, and other security tools to monitor for signs of unauthorized access attempts, privilege escalation exploits, or abnormal behavior.
- Establishing thresholds and alerting mechanisms to notify incident responders of potential elevation of privilege incidents in real-time.
- Conducting regular security assessments, vulnerability scans, and penetration tests to identify weaknesses and vulnerabilities that could be exploited for privilege escalation.

Outcome: Early identification of elevation of privilege threats enables rapid response.

5.3 Analysis

Objective: Determine the nature and scope of the elevation of privilege incident.

Document Owner: Blue Team

Last Modified By: Devika Sivakumar

Next Review Date: 03 March 2025

Last Modified on: 03 August 2024



Document Reference: EPIRP - 2

Effective Date: 03 August 2024

Document Name: Elevation of Privilege Playbook

Expiry Date: 03 March 2025

Activities:

- Restoring from backups or snapshots to recover data and configurations compromised during the incident.
- Rebuilding or re-imaging compromised systems to ensure they are free from malware or unauthorized access.
- Conducting system and network hardening activities to strengthen security posture and minimize the risk of recurrence.

Outcome: Full recovery of services with enhanced security measures.

5.7 Post-Incident Review

Objective: Evaluate the effectiveness of the response and identify improvements.

Activities:

- Documenting the incident response process, including timelines, actions taken, and outcomes.
- Reviewing the effectiveness of response activities and identifying gaps or deficiencies in protocols.
- Conducting a lesson learned meeting with the incident response team and relevant parties.
- Updating incident response documentation based on post-event evaluation findings.
- Sharing insights and recommendations with upper management to strengthen overall security posture.

Outcome: Enhanced incident response capabilities and preparedness for future elevation of privilege incidents.

Document Owner: Blue Team
Next Review Date: 03 March 2025

Last Modified By: Devika Sivakumar
Last Modified on: 03 August 2024



Document Reference:	EPIRP - 2	Effective Date:	03 August 2024
Document Name:	Elevation of Privilege Playbook	Expiry Date:	03 March 2025

6.3 Continuous Monitoring and Analysis

Objective: Maintain continuous monitoring and analysis to promptly detect and respond to elevation of privilege threats.

Activities:

- **Real-Time Monitoring:** Implement real-time monitoring to continuously observe user activities, system behavior, and network traffic, facilitating the immediate detection of elevation of privilege activities.
- **Anomaly Detection:** Utilize behavioral analytics and machine learning to identify anomalies and deviations from established baselines that may indicate elevation of privilege activities.
- **Correlate Events:** Correlate events from various sources to identify patterns that may indicate coordinated elevation of privilege attacks or persistent threats.

Outcome: Enhanced capability to detect elevation of privilege threats promptly, enabling swift response to mitigate potential impacts.

6.4 Alerting and Notification

Objective: Ensure timely and effective response to detected threats through a robust alerting system.

Activities:

- **Set Alert Thresholds:** Establish thresholds for different types of alerts based on severity and potential impact.
- **Automated Alerts:** Configure automated alerts to notify the security team of detected elevation of privilege threats. Ensure alerts provide sufficient context for prompt assessment and action.
- **Prioritize Alerts:** Implement a system to prioritize alerts based on their severity and potential impact, focusing on the most critical threats first.

Outcome: Timely and effective response to detected elevation of privilege threats, reducing the risk of significant damage.

6.5 Investigate and Respond

Objective: Conduct thorough investigations and implement appropriate actions to mitigate identified elevation of privilege threats.

Document Owner:	Blue Team	Last Modified By:	Devika Sivakumar
Next Review Date:	03 March 2025	Last Modified on:	03 August 2024



Document Reference:	EPIRP - 2	Effective Date:	03 August 2024
Document Name:	Elevation of Privilege Playbook	Expiry Date:	03 March 2025

Outcome: A proactive and adaptive threat monitoring strategy that evolves with the changing threat landscape.

Document Owner:	Blue Team	Last Modified By:	Devika Sivakumar
Next Review Date:	03 March 2025	Last Modified on:	03 August 2024



Document Reference: EPIRP - 2 Effective Date: 03 August 2024
Document Name: Elevation of Privilege Playbook Expiry Date: 03 March 2025

7 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.
- **Vertical Privilege Escalation:** The process of gaining higher levels of access within the same system or application, such as moving from user to administrator.
- **Horizontal Privilege Escalation:** The process of gaining access to the same level of privileges but on a different system or application within the same network environment.
- **Credential Theft:** The unauthorized acquisition of user credentials, such as usernames and passwords, often used to facilitate further attacks or unauthorized access.
- **Lateral Movement:** The process of moving within a network to access additional systems and data after gaining initial access.
- **Insecure API Usage:** Exploiting vulnerabilities or misconfigurations in APIs to gain unauthorized access or perform unauthorized actions.

Document Owner: Blue Team Last Modified By: Devika Sivakumar
Next Review Date: 03 March 2025 Last Modified on: 03 August 2024