Document Reference: IUIRP-2 Effective Date: 03 August 2024
Document Name: Improper usage Playbook Expiry Date: 03 August 2025

Improper Usage Incident Response Playbook

Redback Operations

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

Version	Modified By	Approver	Date	Changes made
1.0	Priyanshu		20 April 2024	First draft
1.1	Devika Sivakumar		10-May-2024	Changed the flowchart mentioned the stages, updated the incident response stages in part-5 and arranged the document with correct format. Added correct page number. Added the content table. Gave correct font size and theme
2.0	Devika Sivakumar		03 August 2024	A comprehensive update has been carried out throughout the playbook. Case studies have been added to each attack. The stakeholder's section has been revised, and a RACI chart has been included. 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.

Contents

1. Introduction

1.1 Overview

Redback Operations is at the forefront of innovation and technological improvement in the ever-changing field of cybersecurity. However, these innovations also bring with them new challenges, such as improper usage incidents. These occurrences encompass a broad spectrum of improper or unauthorized use of Redback's systems, data, or resources, posing serious risks to Redback's data security, operational continuity, and industry reputation. These risks can stem from employee errors resulting in accidental data exposure, insiders purposefully abusing their access privileges, or malicious actors coordinating sophisticated external attacks.

1.2 Purpose

This incident response plan provides Redback Operations with a methodical and comprehensive way to address improper usage issues. The playbook seeks to enable Redback to react quickly and decisively to improper usage issues, minimizing their impact on data security, operational continuity, and the company's reputation by outlining clear principles, protocols, and best practices.

1.3 Attack Definition

At Redback Operations, incidents involving improper usage can take many different forms, each with unique challenges and consequences. Insider threats involve staff members abusing their access rights for improper reasons, such as sabotage or personal gain. External attacks are planned by hostile organizations aiming to compromise systems, steal data, or interfere with business operations. These can include sophisticated hacks like malware infections, denial-of-service attacks, or hacking.

1.4 Scope

This playbook covers all types of improper or unauthorized use of Redback Operations' resources, systems, or data. It offers instructions for handling different kinds of improper usage issues, whether they stem from internal negligence or malicious external intent. The playbook includes practical insights and tactics for managing risks, controlling incidents, and minimizing their impact on Redback's operations.

2. Attack Types

2.1 Insider Threat

The security and integrity of Redback Operations' data are seriously threatened by insider threats. These threats entail members of the organisation abusing their access rights for improper intent, which may result in data breaches, sabotage, or the unlawful publication of private information. Insider risks might arise from disgruntled employees, careless behaviour, or unintentional activities. As such, they are challenging to identify and prevent in the absence of effective monitoring and reaction processes.

Case Study: Tesla Insider Sabotage (2020)

- **Overview:** A disgruntled employee at Tesla attempted to sabotage the company's manufacturing systems by making unauthorized changes to the code of the manufacturing operating system.
- **Impact:** The incident could have disrupted Tesla's operations, but the attack was detected and contained before significant damage occurred.
- **Response:** Tesla conducted a thorough investigation, terminated the employee, and implemented additional security measures to prevent future insider threats.

2.2 External Attack

External assaults use a variety of strategies and techniques to infiltrate systems, steal data, or interfere with operations to target Redback Operations from outside the company. Cybercriminals, nation-state actors, or other hostile organisations may be the source of these assaults if they are attempting to take advantage of holes in Redback's networks, applications, or infrastructure. Advanced cyberattacks, such as phishing, malware infections, or denial-of-service assaults, are frequently used in external attacks with the intention of breaching Redback's defences and taking advantage of flaws for illicit financial gain or other goals.

Case Study: Equifax Data Breach (2017)

- **Overview:** Attackers exploited a vulnerability in Equifax's web application framework to gain access to sensitive information.
- **Impact:** The breach exposed personal information of approximately 147 million individuals.
- **Response:** Equifax enhanced its cybersecurity practices, implemented stronger access controls, and paid a settlement of up to $700 million.

2.3 Data Breaches

The security and confidentiality of Redback Operations' data are seriously threatened by data breaches. These instances happen when private or sensitive data is obtained, revealed, or taken without permission, putting Redback at risk of loss of money, legal repercussions, and harm to its reputation. Internal threats, external attacks, and other weaknesses in Redback's systems or procedures can lead to data breaches, which emphasises the significance of strong data protection measures and incident response procedures in reducing the risks and repercussions of such incidents.

Case Study: Marriott Data Breach (2018)

- **Overview:** Attackers gained unauthorized access to Marriott's Starwood guest reservation database.
- **Impact:** Personal information of approximately 500 million guests was exposed.
- **Response:** Marriott notified affected individuals, offered free identity theft monitoring, and enhanced its security measures.

2.4 Phishing Incidents

Phishing attacks use phoney emails, messages, or websites to target Redback Operations' stakeholders and employees with the intention of tricking them into divulging private information, including login passwords or financial information. These assaults can be challenging to identify and stop without the right knowledge and training since they frequently pose as authentic messages from reliable sources. Phishing attacks have the potential to cause financial fraud, data breaches, or unauthorised access to Redback's systems, which emphasises the significance of preventative steps like email filtering and security awareness training in reducing the dangers associated with these occurrences.

Case Study: Google and Facebook Phishing Scam (2013-2015)

- **Overview:** Attackers sent fraudulent invoices and other documents to employees at Google and Facebook, tricking them into wiring over $100 million to the attackers.
- **Impact:** Significant financial loss for both companies.
- **Response:** The companies cooperated with law enforcement to investigate the scam, recover funds, and implement stronger email security measures.

2.5 Ransomware Attacks

The data security and operational continuity of Redback Operations are seriously threatened by ransomware assaults. To encrypt data or prevent users from accessing computers, malicious software is deployed in these attacks. The attackers then demand a ransom to unlock the encrypted data or to get access back. Attacks using ransomware have the potential to cause data loss, financial extortion, and operational interruptions. This emphasises the significance of having strong backup and recovery procedures in place, as well as proactive steps to stop and lessen the effects of such situations.

Case Study: WannaCry Ransomware Attack (2017)

- **Overview:** The WannaCry ransomware spread rapidly across the globe, encrypting data on infected systems and demanding ransom payments in Bitcoin.
- **Impact:** Over 200,000 computers in 150 countries were affected, causing significant disruptions to businesses and public services.
- **Response:** Organizations applied patches, restored systems from backups, and enhanced their cybersecurity practices to prevent future ransomware attacks.

2.6 Credential Theft

One popular strategy used by attackers to obtain unauthorised access to Redback Operations' systems or networks is credential theft. Phishing attacks, social engineering, and other techniques could be used in these incidents to trick employees or stakeholders into giving over their login credentials or authentication tokens. It is crucial to have robust authentication procedures, user awareness, and monitoring in place to identify and lessen the risks associated with credential theft incidents because, with compromised credentials, attackers can evade authentication mechanisms, obtain privileged access to confidential data, or engage in unauthorised activities within Redback's infrastructure.

Case Study: Dropbox Data Breach (2012)

- **Overview:** Attackers gained access to Dropbox user credentials, which were later leaked online.
- **Impact:** Approximately 68 million user accounts were compromised.
- **Response:** Dropbox prompted affected users to change their passwords, implemented two-factor authentication, and enhanced its security measures.

3. Stakeholders

The proficient handling and settlement of incidents require the coordinated endeavours and cooperation of a heterogeneous group of stakeholders, each possessing distinct knowledge, viewpoints, and roles. The following parties are essential to the incident response process, from frontline responders entrusted with containment and mitigation to senior leadership tasked with making strategic decisions:

3.1 IT Security Team

Lead: Daniel McAulay (Senior Project Leader)

Responsibilities:

- Leading technical efforts to identify, examine, and address improper usage incidents.
- Monitoring system and network logs, conducting forensic analysis, and implementing security controls to prevent future incidents.

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 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.

RACI Chart for Improper Usage Incident Response

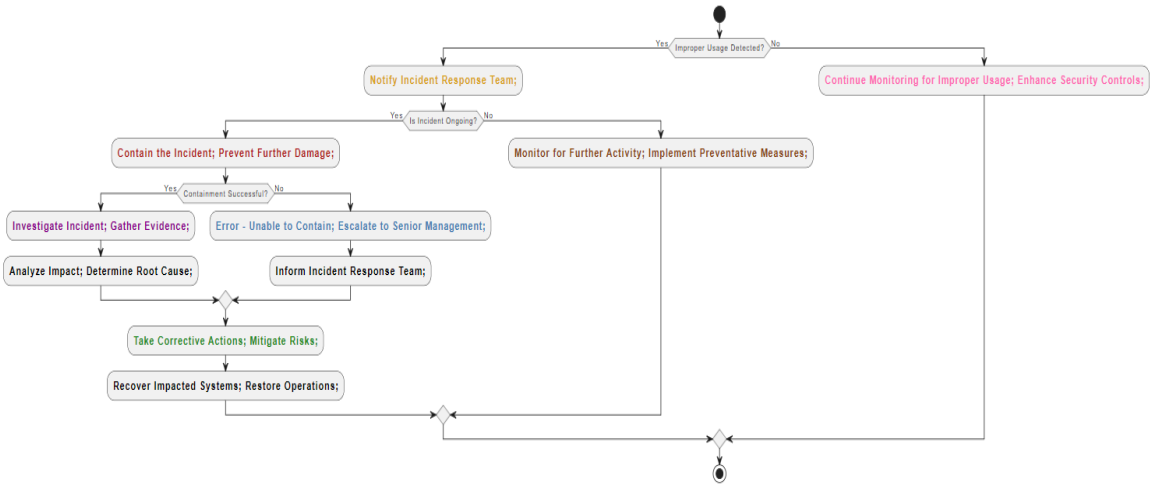
Task/Activity	IT Security Team	Incident Response Team	Communication Team	Customers	Third-Party Vendors
Preparation					
Establish incident response team	R, C	A, R	I	I	I
Develop response procedures	A, R	R, C	I	I	I
Conduct training sessions	A, R	R	I	I	I
Implement surveillance systems	A, R	R	I	I	I
Detection					
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
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
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)

4. Flow Chart



1. Preparation (Prep): Yellow
   - This phase denotes the start of the process of becoming ready to handle situations of inappropriate usage. An incorrect usage occurrence is immediately reported to the incident response team. The colour yellow represents the preparation character of this phase, which focuses on gathering the staff and resources required to handle the situation successfully.
2. Identification (Identify): Red
   - Identifying the incorrect usage incidence and containing it quickly are part of the identification step. Actions are done to stop the problem from spreading further and isolate the compromised systems. The important and urgent nature of this stage is shown by the colour red, underscoring the significance of acting quickly to stop more harm.
3. Notification (Notif): Violet
   - Stakeholders are informed at this phase, and preliminary mitigating actions are put into place. We take steps like modifying login credentials and running scans to find any illegal activity or access. Malicious activity is also examined, and parties are notified so they may organise a response. The colour violet denotes the incident's notice and first reaction attempts, emphasising the need for quick action and communication to lessen its effects.
4. Containment (Contain): Sky Blue
   - At this point, the main goals are to control the situation and stop more harm or illegal entry. Should containment tactics prove effective, more escalation might not be required. But higher management could be alerted for more assistance or a solution if containment proves difficult. The containment attempts to stop the incident's spread and lessen its effects on operations are symbolised by the colour sky blue.
5. Eradication (Erad): Light Green
   - The goal of the Eradication step is to restore system integrity and eradicate the incident's underlying cause. Procedures are implemented to eliminate malware, illegal

access, and other security risks. Details of the incident are recorded for review and analysis later. The activity of eliminating the event and guaranteeing the security of the organization's systems is symbolised by the light green colour.

6. Recovery (Recover): Brown

- At this point, attempts are being made to get past the event and resume regular business. Recovery operations begin, which might involve patching hacked systems, recovering data from backups, and adding further protection. Continuous observation is carried out to identify any lingering risks or weaknesses. The recovery phase, which aims to reinforce security measures and restore business continuity, is symbolised by the colour brown.

7. Post-Incident Actions (Post): Light Pink

- Conducting post-event activities to assess the response's efficacy and pinpoint areas in need of improvement is the last phase. In addition to doing a post-event evaluation to evaluate the organization's reaction and draw lessons from the occurrence, ongoing monitoring is carried out for instances of improper usage. The post-event efforts focused on introspection, education, and ongoing enhancement of incident response skills are represented by the light pink colour.

5. Incident Response Stages

5.1 Preparation

- **Objective:** Establishing in place the guidelines, practices, and tools required to handle instances of inappropriate usage.
- **Activities:**
  - Putting together a team for incident response with clear roles and duties.
  - Creating strategies and processes for crisis response, such as escalation routes and communication guidelines.
  - Holding practice sessions and exercises on a regular basis to guarantee readiness and rehearse incident response protocols.
  - Putting in place security measures and surveillance systems to find and stop instances of unauthorised usage.
- **Outcome:** A well-equipped company with the ability to react quickly and efficiently to instances of inappropriate use.

5.2 Detection

- **Objective:** Recognising warning signs of inappropriate use or illegal access to the systems and resources of the business.
- **Activities:**
  - Keeping an eye out for questionable activity, such strange access patterns or illicit data transfers.
  - Using security information and event management (SIEM) and intrusion detection systems (IDS) to find such problems.
  - Separating malicious from genuine activity by analysing anomalies and alarms.
- **Outcome:** Rapid reaction and mitigation efforts are made possible by early identification of inappropriate usage situations.

5.3 Analysis

- **Objective:** Recognising the kind and extent of the incident involving improper usage.
- **Activities:**
  - Gathering information and carrying out forensic investigation to Identify the extent and cause of the improper usage incidence.
  - Examining hacked networks and systems to find attack vectors and how they affect compromised data.
  - Recognising the tactics, methods, and procedures (TTPs) of threat actors and indicators of compromise (IOCs).

- **Outcome:** A comprehensive understanding of the improper usage incident, including its causes, effects, and attribution.

5.4 Containment

- **Objective:** Halting more illegal access or data leaks and lessening the effect and spread of the incident involving improper usage.
- **Activities:**
  - Dividing up susceptible networks and systems to stop intruders from moving laterally.
  - Putting safety measures and access restrictions in place to stop illegal access to sensitive data.
  - Limiting or preventing harmful data, software, or network flow to stop more damage.
- **Outcome:** Efficient handling of the improper usage event, reducing harm to the company's information and infrastructure.

5.5 Eradication

- **Objective:** Eliminating threats and any lingering vulnerabilities from the company's networks and IT systems.
- **Activities:**
  - Removing illegal software and data and returning hacked computers to a safe configuration.
  - Upgrading or patching susceptible systems and software to stop further exploitation.
  - Examining and revising security protocols and guidelines to fix flaws or vulnerabilities found.
- **Outcome:** Removal of all traces of the improper usage incident and reduction of vulnerabilities to prevent future occurrences.

5.6 Recovery

- **Objective:** Restarting company operations and returning impacted systems and data to normal functioning.
- **Activities:**
  - Restoring damaged systems and data backups to guarantee the integrity and accessibility of data.
  - Rebuilding or rearranging networks and systems to improve security and stop such incidents in the future.
  - Putting user awareness and education programmes into action to avert inappropriate usage events in the future.
- **Outcome:** Full restoration of operations and services, together with strengthened security measures to lessen the chance of recurrence.

5.7 Post-Incident Review

- **Objective:** Assessing the organization's reaction to the issue involving improper usage and determining what worked and what didn't.
- **Activities:**
  - Evaluating the incident response procedure in-depth to find its advantages, disadvantages, and potential areas for development.
  - Recording best practices and lessons discovered to improve incident response skills in the future.
  - Modifying security setups, rules, and incident response protocols considering review results.
- **Outcome:** Improved incident response capacities and preparedness for occurrences involving improper usage in the future.

6. Steps for Monitoring Threats

6.1 Establish a Monitoring Strategy

Objective: Establish and implement a comprehensive strategy for continuous threat monitoring specifically targeting improper usage incidents.
Activities:

- Objectives: Clearly define the objectives for threat monitoring, such as detecting unauthorized access attempts, identifying improper usage activities, and monitoring unusual network traffic indicative of improper usage incidents.
- Tools: Select appropriate security tools such as IDS/IPS (Intrusion Detection/Prevention Systems), SIEM (Security Information and Event Management) systems, EDR (Endpoint Detection and Response) solutions, and user behavior analytics software.
- Baselines: Establish baselines for normal user activity, system behavior, and network traffic patterns to identify deviations that may indicate improper usage activities.

Outcome: A well-defined monitoring strategy aligned with Redback Operations' goals, enhancing the ability to detect and respond to improper usage threats effectively.

6.2 Deploy Monitoring Solutions

Objective: Deploy and configure monitoring tools across the organization’s infrastructure to detect improper usage threats.
Activities:

- Install and Configure Tools: Deploy the selected monitoring tools across networks, systems, and endpoints. Ensure they are configured to detect improper usage-related activities and collect relevant data.
- Integrate with Threat Intelligence: Integrate monitoring tools with threat intelligence feeds to enhance the detection of known and emerging improper usage threats.
- Enable Logging: Ensure logging is enabled on critical systems, networks, and applications. Centralize log collection for efficient analysis and correlation.

Outcome: Comprehensive deployment and integration of monitoring solutions providing detailed insights into potential improper usage threats.

6.3 Continuous Monitoring and Analysis

Objective: Maintain continuous monitoring and analysis to promptly detect and respond to improper usage threats.
Activities:

- Real-Time Monitoring: Implement real-time monitoring to continuously observe user activities, system behavior, and network traffic, facilitating the immediate detection of improper usage activities.
- Anomaly Detection: Utilize behavioral analytics and machine learning to identify anomalies and deviations from established baselines that may indicate improper usage activities.

- Correlate Events: Correlate events from various sources to identify patterns that may indicate coordinated improper usage attacks or persistent threats.

Outcome: Enhanced capability to detect improper usage 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 improper usage 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 improper usage threats, reducing the risk of significant damage.

6.5 Investigate and Respond

Objective: Conduct thorough investigations and implement appropriate actions to mitigate identified improper usage threats.
Activities:

- Initial Triage: Perform initial triage to verify the validity and potential impact of alerts. Determine the severity of the threat and whether the alert is a false positive.
- Detailed Analysis: Conduct in-depth analysis of confirmed alerts to understand the nature and extent of the improper usage threat. Use forensic tools and techniques to gather information and trace the source of the threat.
- Containment and Eradication: Initiate containment measures to prevent further damage if a threat is confirmed. Execute necessary eradication procedures to remove the improper usage threat from the environment.

Outcome: Effective investigation and mitigation of improper usage threats, ensuring minimal impact on the organization.

6.6 Post-Incident Review

Objective: Assess the effectiveness of the response and identify areas for improvement.
Activities:

- Document Findings: Record all details of the incident, including detection, analysis, and response actions taken.
- Review and Improve: Conduct a review of the monitoring and response processes post-incident to identify strengths, weaknesses, and lessons learned.
- Update Monitoring Tools: Update monitoring tools, configurations, and thresholds based on the findings to enhance future threat detection and response capabilities.

Outcome: Continuous improvement of incident response and threat monitoring processes, ensuring better preparedness for future improper usage incidents.

6.7 Continuous Improvement

Objective: Maintain and enhance the organization's threat monitoring strategy and tools.
Activities:

- Regular Audits: Conduct regular audits to ensure monitoring tools and strategies remain effective and up to date with the latest threats.
- Training and Awareness: Provide ongoing training to security personnel on the latest threats and best practices for monitoring and response.
- Adapt to New Threats: Continuously adapt the monitoring strategy to address emerging threats. Stay informed about the latest threat intelligence and incorporate it into monitoring processes.

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

7. Terminology

- **Intrusion Detection System (IDS):** Monitors network traffic for indications of malicious activity, unauthorized access, or security lapses. It analyses network packets and system logs to identify potential security risks.
- **Security Information and Event Management (SIEM):** Provides real-time visibility into security incidents by collecting, correlating, and analysing security event data from various sources. SIEM enhances overall security posture and resilience against improper usage incidents.
- **Vulnerability Assessment:** A preventive strategy to identify and fix security flaws in networks and systems. It involves regular scanning and analysis to find known vulnerabilities, misconfigurations, or weaknesses.
- **Zero-Day Vulnerabilities:** Security holes in software or systems that were previously undiscovered or revealed, making organizations vulnerable to exploitation. Proactive measures such as threat intelligence sharing, and patch management are essential to handle new threats.
- **Tactics, Techniques, and Procedures (TTPs):** Specific methods used by threat actors to achieve their objectives, including the tools and strategies employed during an attack.
- **Indicators of Compromise (IOCs):** Artifacts observed on a network or in an operating system that indicate a security breach, such as unusual file changes, network traffic, or system behaviors.