Document Reference: IUIRP-1 Effective Date: 12 May 2024
Document Name: Improper Usage Incident Response Playbook Expiry Date: 12 May 2025

Improper Usage Incident Response Playbook

Redback Operations

Document Owner: Purple Team Last Modified By: Priyanshu
Next Review Date: 17 June 2024 Last Modified on: 10 May 2024

Version	Modified By	Approver	Date	Changes made
0.1	Priyanshu		20 April 2024	First draft
0.2	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
1.0	Priyanshu, Devika Sivakumar	Joel Daniel	12 May 2024	Approved for Publishing

Contents

1. Introduction

1.1 Overview

Redback Operations is at the forefront of innovation and technological improvement in the always changing field of cybersecurity. But these innovations also bring with them a host of new difficulties, one of which is improper usage instances, which should worry us greatly. These occurrences include a broad spectrum of improper or unauthorised use of Redback's systems, data, or resources. Improper usage incidents pose serious risks to Redback's data security, operational continuity, and industry reputation. These risks can stem from employee error resulting in accidental data exposure, insiders purposefully abusing their access privileges, or malicious actors coordinating sophisticated external attacks.

Redback Operations is a member of its field and understands the value of prompt and efficient incident response procedures in reducing the risks associated with improper usage events. Redback can lessen the impact of these occurrences on its operations and guarantee the security and confidentiality of its data and systems by quickly discovering, evaluating, and mitigating them.

1.2 Purpose

This incident response plan is meant to give Redback Operations a methodical and all-inclusive way to deal with issues involving improper usage. The playbook seeks to enable Redback to react quickly and forcefully to improper usage issues, minimising their impact on data security, operational continuity, and the company's reputation. It does this by outlining clear principles, protocols, and best practices.

Fundamentally, the playbook is a proactive instrument that strengthens Redback's readiness and resilience to changing cybersecurity threats. Redback can enhance its response efficiency, better manage risks, and preserve the faith and confidence of its stakeholders, partners, and customers by instituting standardised incident response processes and standards.

1.3 Attack Definition

At Redback Operations, incidents involving improper usage can take many different forms, each with unique difficulties and consequences for incident response. Insider threats are internal threats that come from staff members abusing their access rights for improper reasons, such as sabotage, personal gain, or other nefarious motive. Insider threats can take many different forms, from unintentional data disclosure from carelessness to intentional acts of sabotage meant to compromise sensitive data or interfere with operations.

However, external attacks are planned by hostile organisations outside of Redback with the intention of compromising systems, stealing data, or interfering with business operations to obtain financial advantage or carry out other evil deeds. Targeting Redback's networks, applications, or infrastructure, these assaults could be sophisticated hacks like malware infections, denial-of-service attacks, or hacking.

1.4 Scope

This playbook covers all types of inappropriate or unauthorised use of Redback Operations' resources, systems, or data. It is intended to handle cases of improper usage. The playbook offers instructions for handling different kinds of improper usage issues, whether they are the result of malevolent external intent or internal carelessness. This guarantees a well-coordinated and efficient response that is in line with Redback's goals and priorities.

The playbook gives Redback the flexibility and adaptability required to effectively respond to changing threats and challenges by covering a broad range of attack types and situations. The playbook includes practical insights and tactics for managing risks, controlling incidents, and minimising their impact on Redback's operations, ranging from internal threats to external assaults, data breaches, phishing attempts, ransomware outbreaks, and credential theft.

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.

2.2 External Attack

External assaults use a variety of strategies and techniques to infiltrate systems, steal data, or interfere with operations in order 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.

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.

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.

2.5 Ransomware Attacks

The data security and operational continuity of Redback Operations are seriously threatened by ransomware assaults. In order 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.

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.

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:

1. **IT Security Team**: Leading the technical efforts to identify, examine, and address issues involving improper usage, Redback Operations' IT Security Team is a vital component of incident response. To stop similar incidents in the future, this team oversees keeping an eye on system and network logs, doing forensic analysis, and putting security controls in place. To ensure a coordinated and efficient reaction to situations of improper usage, they collaborate closely with other relevant parties, thereby reducing the impact on Redback's operations and data protection.

2. **Incident Response Team:** Members of Redback Operations' cross-functional incident response team come from the IT, security, legal, compliance, and management divisions. This team is in charge of organising incident response activities, liaising with relevant parties, and making crucial choices to contain and address occurrences involving improper usage. They guarantee that Redback's policies, processes, and regulatory requirements are met by incident response operations, promoting a unified and effective response.

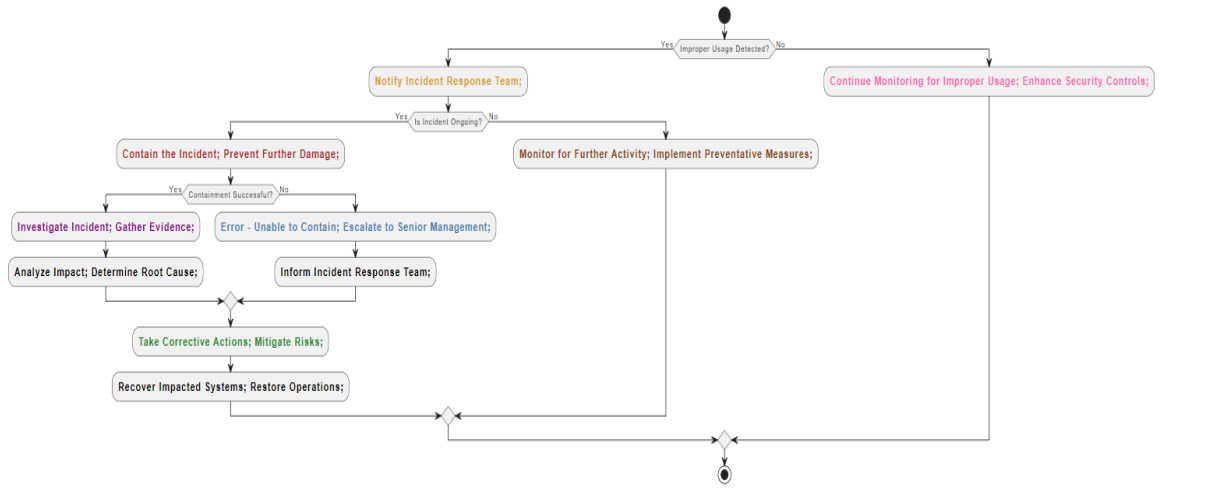
3. **Legal and Compliance Department:** Regarding regulatory compliance and the legal ramifications of occurrences involving inappropriate usage, the Legal and Compliance Department offers supervision and counsel. They minimise legal liabilities and reputational risks for Redback Operations by making sure incident response actions comply with relevant laws, regulations, and contractual commitments. Furthermore, they work in conjunction with outside legal counsel and law enforcement organisations as required to handle the legal ramifications of instances of inappropriate usage and assist Redback in reducing risks and safeguarding its interests.

4. **System Administrators**: Using their technical know-how and domain experience to restore system integrity and functionality, system administrators, as stewards of organisational systems and networks, have a significant impact on the identification, investigation, and resolution of root access issues.

5. **Management**: Setting organisational priorities, allocating resources, and spearheading strategic efforts aimed at bolstering the organization's resilience against root access threats are all crucial tasks performed by executive leadership, which includes C-suite executives and senior management.

6. **External Consultants**: Organisations may hire outside consultants or third-party vendors to supplement their incident response capabilities in situations requiring specific knowledge or resources. These vendors can help with forensic analysis, threat intelligence, and remediation efforts.

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. Terminology

Terminology in incident response encompasses a range of concepts and terms essential for effective communication and understanding within the cybersecurity domain. It provides a common language for incident responders, enabling precise and unambiguous communication during incident response activities.

- An essential part of Redback Operations' cybersecurity setup is an intrusion detection system (IDS). IDS keeps an eye on network traffic to look for indications of malicious activity, unauthorised access, or security lapses. Network packets and system logs are analysed by IDS to find anomalies or patterns that point to possible security risks. When an improper usage occurrence occurs, Redback's occurrence Response Team can investigate and take appropriate action based on the alarms generated by IDS.
- SIEM, or Security Information and Event Management, is essential to Redback's incident response operations. SIEM provides real-time visibility into security incidents by gathering, correlating, and analysing security event data from several sources throughout the IT architecture of the company. SIEM improves Redback's overall security posture and resilience against improper usage incidents by aggregating and correlating security data, making it easier to identify and respond to security threats.
- Redback uses vulnerability assessment as a preventative strategy to find and fix security flaws in its networks and systems. Redback performs vulnerability assessments to find known vulnerabilities, misconfigurations, or weaknesses that threat actors could exploit through routine scanning and analysis. Redback improves its security defences and lowers the possibility of improper usage situations by prioritising remediation activities according to the severity and impact of vulnerabilities.
- Redback's cybersecurity defences face a substantial challenge from zero-day vulnerabilities. These vulnerabilities are security holes in software or systems that were previously undiscovered or revealed, making organisations open to abuse by hostile parties. Redback keeps a quick response capability to handle new threats and continually searches for zero-day vulnerabilities. Redback increases its resilience against sophisticated cyber threats and reduces the danger caused by zero-day vulnerabilities by putting proactive measures like threat intelligence sharing and patch management into place.