Document Reference:	UAIRP - 1	Effective Date:	26 April 2024
Document Name:	Unauthorised Access Playbook	Expiry Date:	26 April 2025

Unauthorised Access Incident Response Playbook

Redback Operations

Document Owner:	Pari	Last Modified By:	Pari
Next Review Date:	15 July 2024	Last Modified on:	26 April 2024

Version	Modified By	Approver	Date	Changes made
1.0	Pari			Initial Draft

Table of Contents

1 Introduction

1.1 Overview

A structured framework for handling incidents involving unauthorised access to our systems, networks, or data is provided by the Unauthorised Access Incident Response Playbook. It describes a methodical process for identifying, evaluating, containing, eliminating, and recovering from these kinds of circumstances. Our organisation intends to mitigate the impact of unauthorised access events, protect sensitive data, and preserve operational continuity by adhering to the measures described in this playbook.

1.2 Purpose

This playbook's purpose is to set clear detailed policies and processes for handling instances of unauthorised access. By following these procedures, we aim to reduce the possible harm that could be inflicted by unauthorised access, guarantee a coordinated reaction involving pertinent teams and stakeholders, pinpoint the underlying causes of occurrences, and put preventative measures in place to lessen risks in the future. This playbook also fulfils regulatory obligations and demonstrates our dedication to protecting the security and integrity of our systems and data.

1.3 Attack definition

Any attempt to access our systems, networks, or data without the necessary authorisation is considered unauthorised access. This covers a range of approaches, including social engineering assaults, insider threats, exploitation of software or configuration vulnerabilities, unauthorised login attempts using stolen credentials or brute-force methods, and compromised accounts or devices. It is essential to comprehend and recognise these attack vectors to respond to events of unauthorised access and put in place the necessary defences.

1.4 Scope

This playbook's scope includes any instances of unauthorised access that impact our company's end-user devices, data repositories, network infrastructure, and information systems. It is applicable to everyone who uses our networks, systems, or data in any way. This playbook ensures a uniform and well-coordinated approach to incident management across the organisation by offering guidelines for handling unauthorised access incidents across a variety of platforms and situations.

2 Attack Types

2.1 Unauthorized Login Attempts

Attackers that attempt unauthorised logins attempt to access accounts, systems, or applications by guessing passwords, utilising credentials that have been stolen, or using brute-force methods. To systematically attempt various login and password combinations until they find legitimate credentials, attackers may employ automated programmes. Such an assault could compromise user accounts, grant unauthorised access to confidential data, and cause data breaches. To reduce the possibility of unwanted login attempts, organisations must deploy robust authentication methods like multi-factor authentication (MFA).

2.2 Exploiting Vulnerabilities

Finding and exploiting flaws in hardware, software, or configurations allows attackers to obtain unauthorised access. This process is known as exploitation vulnerabilities. Operating systems, apps, web servers, and network devices can all have vulnerabilities that can be taken advantage of with the help of exploit kits or specially created exploits. Attackers may use zero-day vulnerabilities that have not yet been patched by vendors or known vulnerabilities with publicly available exploit code. To reduce the risk of exploitation, organisations should use security controls like firewalls and intrusion detection systems, perform vulnerability assessments and penetration tests, and patch and update software on a regular basis.

2.3 Social Engineering Attacks

Social engineering attacks use psychological tricks on people to compel them into disclosing private information, opening up systems, or taking other acts that put their security at risk. The danger of social engineering attacks can be reduced by imposing stringent access rules, putting email filtering and anti-phishing systems in place, and training staff to identify and report social engineering attempts. Social engineering techniques include phishing emails, pretexting, baiting, and tailgating, which are used to deceive individuals into divulging critical information or credentials.

2.3.1 Pretexting

Pretexting is the practice of fabricating a situation or pretext in order to force someone into divulging private information or allowing access to systems. Attackers may assume the identity of reputable people, such as IT support personnel, suppliers, or service providers, and create a convincing pretext, like a technical problem, account verification, or an urgent request, to deceive targets into disclosing private information or carrying out actions that

advance the attacker's interests. Pretexting attacks, which effectively deceive victims by establishing rapport and credibility, frequently take advantage of people's natural instincts to be helpful or cooperative.

2.3.2 Baiting

Baiting attacks are designed to trick users into clicking on dangerous links or downloading files containing malware by offering them rewards, free software, or media downloads. Physical material, like USB drives, CDs, or DVDs, that are given out in public or addressed to targets, is frequently used in baiting assaults. After the victim engages with the bait, there's a chance that malware will infect their device, giving attackers access to their systems without authorisation or the ability to steal confidential data.

2.3.3 Tailgating (Piggybacking)

Tailgating is the act of physically trailing an authorised person into a secure facility or restricted area without the required authorisation or authentication. Attackers take advantage of people's innate inclination to open doors for others or to avoid conflict by letting unauthorised people enter restricted areas next to them. Once inside, attackers could be able to access facilities, equipment, or critical data, endangering an organization's physical security.

2.3.4 Phishing

One of the most common forms of social engineering attacks is phishing. It entails sending phoney emails that seem to be from reliable sources, such banks, social media sites, or reputable companies. Usually, these emails are full of misleading information and requests for the receiver to click on dangerous links, download infected attachments, or divulge private information like account numbers, login passwords, or personal information. Phishing attempts frequently work by instilling a sense of anxiety or urgency in users so they will act without verifying the legitimacy of the email.

2.4 Insider Threats

Insider threats are when members of an organization's authorised staff abuse their power to access resources, data, or systems without authorisation. Insider risks can be harmful, such when staff members unintentionally reveal confidential information or cause operations to be disrupted, or malevolent, like when staff members expose data by mistake because they were careless or ignorant. Since insiders may circumvent established security measures and already have authorised access to systems, insider threats can be difficult to identify and counter. Insider threat risk can be reduced by putting in place user activity monitoring, access limits, least privilege principles, and frequent security awareness training.

2.5 Backdoor Access

In order to retain ongoing unauthorised access, attackers establish backdoors or covert entry points within systems or networks. Backdoors can be installed using a variety of techniques, including employing secret communication channels, taking advantage of default credentials, and exploiting flaws. Backdoors, once installed, provide attackers the ability to go around security measures, avoid detection, and do destructive actions covertly. Comprehensive security assessments, such as network scans, code reviews, and endpoint monitoring, are necessary for identifying and eliminating backdoors. Backdoor access can also be avoided by putting in place network segmentation, enforcing stringent access rules, and routinely patching and updating systems.

2.6 Privilege Escalation

Attackers can increase their rights within a system or network by taking advantage of flaws or configuration errors. This is known as privilege escalation. Attackers can access confidential information, carry out unauthorised actions, or compromise more environment resources by elevating their privileges. Privilege escalation can happen in several ways, including via taking advantage of poor authentication procedures, misconfigured permissions, or software vulnerabilities. To reduce the risk of privilege escalation, organisations should apply the principle of least privilege, which allows users to have access only to the minimal amount necessary to carry out their responsibilities. Privilege escalation attacks can also be avoided by keeping an eye on user activity, verifying system configurations, and correcting known vulnerabilities.

2.7 Data Breaches

When unauthorised parties obtain sensitive information—like bank records, intellectual property, or personal information—data breaches happen. A variety of unauthorised access instances, including as social engineering attacks, account compromises, and vulnerability exploits, can lead to data breaches. Organisations that experience data breaches may face severe legal, financial, and reputational repercussions, such as regulatory fines, litigation, and harm to their brand's image. Organisations should have strong security measures in place, like encryption, access controls, data loss prevention (DLP) programmes, and frequent security audits and assessments, to avoid data breaches.

3 Stakeholders

Information Security Team/Incident Response Teams (IRT): This group oversees monitoring the security posture of the company and handling cases of unauthorised access. They are essential in identifying attempted illegal entry, limiting the situation, carrying out forensic investigation, and putting preventative measures in place. The group strives to maintain systems and networks safe, secure sensitive data, and guarantee adherence to security rules and guidelines.

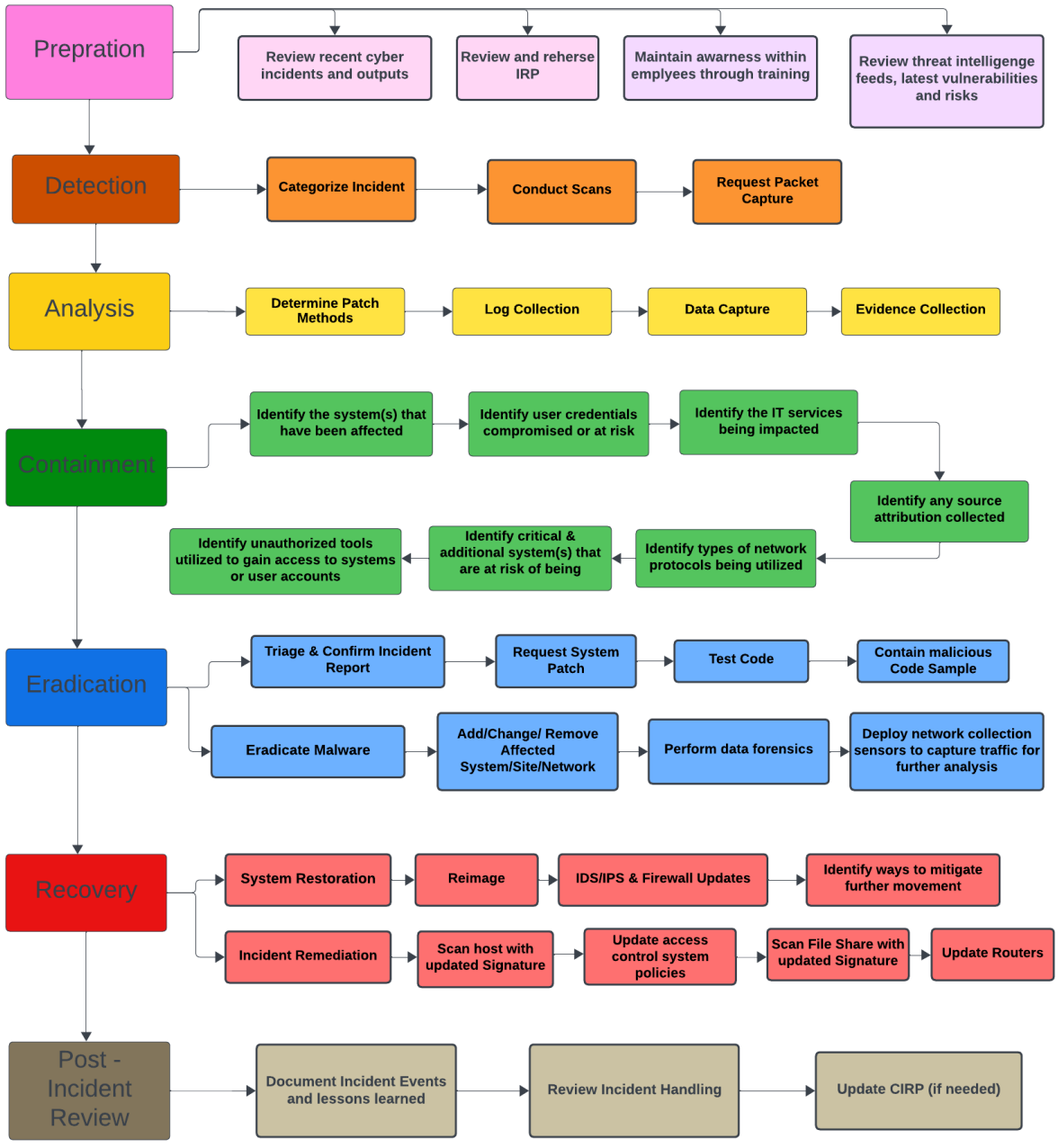
IT Operations Team: This group responsible for overseeing and maintaining the company's servers, networks, and endpoints. They work together with the information security team to detect and handle incidents of unauthorised access, repair impacted systems and services, and put security measures in place to stop future exploitation. The IT Operations Team also supports the investigation of incident causes and the application of corrective actions.

Teams for Communication: During incidents, effective communication is essential. These groups oversee communications both inside and outside the company, guaranteeing transparency and preventing harm to the company. They create communication plans and communicates with partners, consumers, and regulatory bodies to reassure stakeholders of the company's dedication to security.

Affected Users or Customers: Stakeholders include those whose accounts or data were compromised. They might have to keep an eye on accounts, change passwords, or take other precautions.

Management and Executives: Senior leadership and executive management offer supervision and guidance throughout an incident. They are responsible for determining the risk tolerance of the company, assigning funds to incident response initiatives, and making choices about communication, escalation, and containment of incidents. Executive Management makes sure that stakeholder expectations and corporate objectives are met via incident response activities.

4 Flow Diagram



Preparation (Pink)

- Develop and maintain Cyber Incident Response Plan (CIRP) for incidents.
- Identify critical assets and prioritize them.
- Train incident response teams and employees.

Detection (Orange)

- Continuously monitor network traffic.
- Set up alerts for suspicious patterns.
- Validate incidents.

Analysis (Yellow)

- Determine patch methods.
- Perform log collection, data capture and evidence collection.

Containment (Green)

- Identify affected system, credentials compromised services impacted.
- Identify services at risk (servers, laptop, desktop, mobile or VM).

Eradication (Blue)

- Identify vulnerabilities.
- Patch and remediate.
- Verify closure of attack vector.

Recovery (Red)

- Gradually restore services.
- Validate restoration.
- Monitor for recurrence.

Post-Incident Review (Brown)

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

5 Incident Response Stages

5.1 Preparation

An effective unauthorised access event response strategy starts with preparation. In this phase, the company sets up the rules, practices, and tools required to find, address, and lessen instances of unauthorised access.

Key Actions:

- Creating an Incident Response Plan: Draft a thorough incident response plan those details roles and responsibilities, communication protocols, escalation procedures, and techniques for mitigating occurrences involving unauthorised access.
- Training and Awareness: Educate staff members on incident response protocols, threat detection strategies, and security best practices through frequent training and awareness initiatives.
- Applying Security Controls: To stop unwanted access and lessen the effect of incidents, use security controls including firewalls, intrusion detection systems, access controls, and encryption.
- Creating an Incident Response Team: To coordinate response activities, form a cross-functional incident response team with members from executive management, IT and security.

5.2 Detection

In order to launch a reaction, detection entails promptly recognising signs of situations involving unauthorised access.

Key Actions:

- Monitoring Systems: Put technologies and methods to use to keep an eye out for unusual activity, illegal access attempts, and irregularities in system logs, network traffic, and user behaviour.
- Alerting Mechanisms: Set up automated notifications and alerts to quickly inform the incident response team about possible security breaches or occurrences involving unauthorised access.
- User Reporting: Using established channels, like a dedicated hotline or email address, users are encouraged to report any suspicious activity, unauthorised access attempts, or security issues to the incident response team.
- Threat information: Keep an eye on external threat information sources, like vendor advisories, security bulletins, and threat feeds, to spot new threats and weaknesses that could result in incidents involving unauthorised access.

5.3 Analysis

Analysing entails determining the extent, significance, and gravity of the incident involving unauthorised access.

Key Actions:

- Incident Triage: Assign a priority to and classify incidents according to their level of severity, possible consequences, and importance to the organization's resources and activities.
- Forensic analysis: Examine impacted systems, logs, and network traffic to find the source of the issue, gauge the degree of unauthorised access, and collect data for further enquiry and repair.
- Attribution: Ascertain the origin and reasons for the instance of unauthorised access, including if it was caused by automated malware, insiders, or external attackers.
- Impact Assessment: Evaluate the incident's effects on the organization's operations, data, systems, reputation, and legal compliance responsibilities.

5.4 Containment

Containment entails acting quickly to stop more illegal access, lessen the incident's impact, and safeguard important assets.

Key Actions:

- Isolating Systems: To stop illegal access from spreading and reduce the chance of data exfiltration or additional compromise, confine impacted systems, networks, or applications.
- Blocking Access: To stop illegal access attempts and stop attackers from taking advantage of other vulnerabilities, use firewalls, access controls, or network segmentation.
- Disabling Accounts: To stop attackers from exploiting compromised user accounts, passwords, or privileged access permissions to obtain more access to systems or private data, temporarily disable them.
- Interim Control Implementation: To address immediate threats and vulnerabilities discovered during the incident response process, implement interim security controls or procedures.

5.5 Eradication

Eradication includes eliminating vulnerabilities, addressing the underlying cause of the unauthorised access incident, and bringing the impacted systems back to a secure condition.

Key Actions:

- Patching and Remediation: To address the underlying cause of the incident and stop similar assaults in the future, apply security patches, updates, or fixes to susceptible systems, applications, or configurations.
- Removing Malware: To find and eliminate harmful software, backdoors, or unapproved access methods from compromised systems, use antivirus software, malware detection tools, or manual analysis procedures.
- Resetting Passwords: To stop unwanted access and stop attackers from exploiting the compromised account or system further, change the passwords, access keys, or cryptographic keys linked to it.
- Putting Security Enhancements into Practice: To improve incident response capabilities and fortify the organization's defences against unauthorised access, implement security controls, configurations, or policies based on lessons gained from the incident.

5.6 Recovery

Following an event of unauthorised access, recovery entails returning impacted systems, data, and operations to normal functioning.

Key Actions:

- Data Restoration: To replace any lost or corrupted information as a result of the incident, recover and restore data from backups, archives, or redundant systems.
- System Rebuild: To make sure compromised systems or infrastructure components are clear of malware, illegal alterations, and lingering vulnerabilities, rebuild or reimage them.
- Service Restoration: After the impacted systems have been successfully eliminated and recovered, restore normal operations and services to ensure minimal disruption to business processes and uninterrupted company operations.
- Communication and Notification: As needed, notify all relevant parties about the incident, its effects, and the organization's response actions, such as partners, employees, and regulatory authorities.

5.7 Post Incident Review

Evaluation of the organization's response to the incident of unauthorised access, identification of lessons learned, and implementation of enhancements to improve future incident response capabilities are all part of the Post-Incident Review process.

Key Actions:

- Incident Debriefing: Conduct a thorough debriefing session with the incident response team to go over the procedure, evaluate the success of the response measures, and pinpoint areas that need improvement.
- Root Cause Analysis: To determine the underlying causes of the unauthorised access occurrence, like as vulnerabilities, control deficiencies, or human mistake, conduct a root cause analysis.
- Learnings: To build organisational resilience and guide future incident response activities, keep a record of the incident's lessons learned, including its successes, failures, and opportunities for development.
- Modifying Protocols and Guidelines: In order to close any gaps, enhance coordination, and expedite response activities in the event of future crises, update incident response policies, procedures, and playbooks in light of the lessons learned from the incident.

6 Terminology

- **Multi-Factor Authentication (MFA):** With multi-factor authentication (MFA), a user's identity is verified by requiring them to provide at least two pieces of proof, like their password and a temporary passcode. It offers an extra degree of security beyond just using a password, making it more difficult for unauthorized users to get access to crucial accounts or information.

- **Data Loss Prevention (DLP):** It is a security tactic which aims to stop private or sensitive information from being misplaced, stolen, or accessed by unauthorised parties. It includes both policy-based controls, such personnel training and data classification, and technical controls, including encryption and access restrictions.

- **CIRP (Cyber Incident Response Plan):** It is a documented set of procedures and guidelines for organization to follow when responding to and managing security incidents. It outlines roles, responsibilities, communication channels, and technical steps necessary to detect, analyse, contain, eradicate, and recover from incidents. It

is essential to have a well-prepared CIRP for effective incident response and minimizing the impact of security threats.

- **Intrusion Detection System (IDS):** It is a network security technology which keeps an eye on devices and network traffic for known hostile activities, questionable activity, or infractions of security policies. Its major function is to detect and inform security managers to potential dangers within the network.