Phishing Incident Response Playbook

Redback Operations

Version	Modified By	Approver	Date	Changes made
1.0	Indiah Smith	Ben Stephens	17 December 2023	First draft
1.1	Pari	Joel Daniel	28 March 2024	Introduction, Attack types, Stakeholders
1.2	Devika Sivakumar	Joel Daniel	23 March 2024	Flow diagram
1.3	Priyanshu	Joel Daniel	28 March 2024	Incident Response Stages
1.4	Joel Daniel	Ben Stephens	2 April 2024	Removed DNS Spoofing and placed Terminology section last.
1.5	Joel Daniel	NA	5 April 2024	Grammatical modifications and update to vishing section
1.6	Devika Sivakumar		5 April 2024	Updated the flowchart with bolder letters and visible colours and given the usual starting symbol for the flowchart
2.0	Devika Sivakumar		02 August 2024	Comprehensive updates and refinements have been made to the attack definition and scope sections. Case studies have been added to the attack types, stakeholders have been updated, and changes have been made throughout. A RACI chart has been included, steps for monitoring threats have been added, and terminology has been updated

Contents

1. Introduction

1.1 Overview

One of the most common, simple yet dangerous security threats that all types of companies now must deal with are phishing emails. The confidentiality, integrity, and availability of vital assets and data are seriously jeopardised by these attacks. Organisations need to have a thorough and well-defined incident response policy in place to effectively counter this danger while adhering to the minimum actions and questions to be carried out as detailed in the Redback Operations Incident Response Policy.

1.2 Purpose

This playbook's main goal is to give organisation an organised, methodical strategy to identifying, stopping, and minimising the effects of phishing assaults. Its objectives are to help Computer Security Incident Response Team (CSIRT) teams avoid operational disruptions, secure sensitive data, respond quickly to phishing attacks, and preserve the organization's reputation. The playbook provides precise instructions and protocols for phishing attack preparation, detection, analysis, containment, eradication, discovery, and post-event actions. By adhering to the playbook's guidelines, an organisation can improve its incident response capabilities, quickly and effectively combat phishing threats, and solidify itself against changing cyberthreats in the modern digital landscape.

1.3 Attack Definition

Phishing is defined as the deceptive activity of someone pretending to be a reputable organization and sending emails, texts, or phone calls to trick people into disclosing sensitive information, including passwords, banking and credit card details, and personally identifiable information. These fraudulent communications often include links to fake websites or harmful attachments that aim to infect the recipient's device with malware or steal personal information. Phishing attacks pose a serious risk to cybersecurity and data privacy by utilizing social engineering tactics to trick individuals.

1.4 Scope

The scope of this playbook includes the handling of phishing attacks, covering post-event actions, coordination, communication, incident detection, response, and continuous improvement initiatives. The goal is to assist CSIRT teams in efficiently identifying, evaluating, and countering phishing attacks while minimizing damage to the company's assets and operations. The playbook also aims to enhance communication and collaboration among stakeholders during a phishing event and is intended for use by everyone involved in phishing incident management.

2. Attack Types

The different types of phishing attacks include:

2.1 Email Phishing

This is the most common type of phishing attack, in which hackers send fraudulent emails to people or businesses pretending to be trustworthy organisations like banks, governments, or well-known corporations. Usually, these emails have harmful attachments or links that are meant to fool recipients into downloading malware or disclosing private information.

Signs of Email Phishing:

1. Requests for personal information: Reputable businesses will never send you an email requesting personal information.
2. Urgent issue: Exercise caution when you receive urgent notifications, such as failed payments or account breaches. To verify, visit the website/ call bank directly rather than clicking any links.
3. Shortened links: Be wary of condensed or shortened links since they could be hiding harmful URLs.
4. Fourth-party email addresses: Verify the integrity of the sender email address; scammers frequently use aliases or other versions of reputable domains.
5. Spelling and grammar issues: Any email that has misspellings or grammar faults should be taken seriously as it may be a sign of phishing.
6. File attachments: Stay away from opening attachments unless they have been confirmed, especially if they have the.exe,.zip, or .scr extensions.
7. Sigle or blank image: Emails with just an image or one blank picture should be avoided since they can include malware that starts downloading automatically.

Case Study: Google and Facebook (2013-2015)

- **Overview:** A Lithuanian man tricked Google and Facebook employees into wiring over $100 million by sending fake invoices and pretending to be a hardware vendor.
- **Signs of Activity:** The invoices appeared legitimate and were sent from fake email addresses that closely resembled the real vendor's address.
- **Impact:** Google and Facebook eventually recovered the funds, but the case highlighted the effectiveness of sophisticated email phishing.
- **Response:** Increased awareness training for employees and stricter verification processes for invoices and payment requests.

2.2 Spear Phishing

Spear phishing consists of extremely focused attacks directed at particular people or departments within a company. To create phishing emails that are more likely to be successful, attackers perform in-depth research to obtain personal information about their targets.

Signs of Spear Phishing:

1. Unusual requests: To prevent possible scams, confirm through a different channel if coworkers ask for credentials beyond the scope of their position.
2. Shared drive links: Stay away from accessing links that appear to be from internal sources since you probably already have access to shared drives.
3. Unsolicited emails: Be wary of emails offering unsolicited downloads; always verify the sender's authenticity.
4. Personal information: Email scammers may utilise needless personal information to win your trust, so be cautious when responding to such mail.

Case Study: U.S. Democratic National Committee (2016)

- **Overview:** Russian hackers used spear phishing emails to gain access to the DNC's computer network and steal sensitive information.
- **Signs of Activity:** Highly targeted emails that appeared to be from trusted sources, containing malicious links.
- **Impact:** Significant political fallout and disruption during the 2016 presidential election.
- **Response:** Improved email security measures, employee training, and enhanced monitoring for suspicious activities.

2.3 Whaling

Whaling attacks, sometimes referred to as CEO fraud, targets high-profile individuals in an organisation, such as CEOs or senior managers, with the intention of committing financial fraud or stealing confidential data. These attacks may spoof reliable connections or business partners and frequently entail advanced social engineering techniques.

Signs of Whaling:

1. Inaccurate domain address: To trick people, scammers frequently utilise identical but false domain domains. While checking email addresses, exercise caution.
2. Use of personal email: To reduce the danger of phishing, only use professional emails to communicate with executives or business partners. Verify the sender's identification over an offline channel if the request occurs from a personal email.
3. Requests for new contacts: Be wary of emails from vendors or partners you are not familiar with. Check these messages via proper channels or get in touch with the person in charge directly.

Case Study: Crelan Bank (2016)

- **Overview:** The Belgian bank lost over $75 million due to a whaling attack where attackers impersonated the CEO and requested a large wire transfer.
- **Signs of Activity:** Emails appearing to come from the CEO, urgent requests for wire transfers.

- **Impact:** Significant financial loss and reputational damage.
- **Response:** Stricter verification processes for high-value transactions and increased training for executives on identifying phishing attempts.

2.4 Vishing (Voice Phishing)

This utilises voicemails or phone calls to trick people into divulging private information or carrying out specific tasks, such sending money or exposing up vulnerable networks. Attackers may pretend to be legitimate by using methods like caller ID spoofing.

Signs of Vishing:

1. Blocked or unidentified numbers: Phishing calls often originate from blocked numbers. If a caller sounds suspicious, hang up immediately.
2. Requests for sensitive information or money: Various entities such as Government organizations, Medicare centres and financial institutions conduct business through official mail and never request personal information over phone calls.

Case Study: IRS Scams (Ongoing)

- **Overview:** Attackers impersonate IRS agents and call individuals, threatening them with arrest if they do not pay alleged back taxes.
- **Signs of Activity:** Threatening phone calls from individuals claiming to be IRS agents, requests for immediate payment via unconventional methods.
- **Impact:** Significant financial losses for victims and ongoing public awareness issues.
- **Response:** Public awareness campaigns by the IRS, encouraging individuals to verify the legitimacy of such calls and report suspicious activities.

2.5 Smishing (SMS Phishing)

Text messages, or SMS (Short Message Service), are used in smishing attacks to deceive targets into clicking on harmful links or compromising personal information. These messages, which frequently appear to be from reliable sources like banks or government organisations, may advise recipients to act immediately to prevent repercussions.

Signs of Smishing:

1. Unsolicited texts: Watch out for texts that provide you discounts or freebies on something you didn't sign up for. Phishing texts may also ask for personal information or account verification.
2. Unknown numbers: Exercise vigilance while sending information requests by text. For verification, use a free phone lookup service; stay away from links and other interactions.
3. Authentication requests: Requests for authentication that are not authorised can be signs of attempted account access. To protect your account, quickly change your password.

Case Study: Bank SMS Scam (2019)

- **Overview:** Attackers sent SMS messages pretending to be from a bank, asking recipients to click on a link to resolve a security issue with their account.
- **Signs of Activity:** Texts containing links to fake bank websites, urgent requests for account verification.
- **Impact:** Financial losses for victims who provided their banking information to the fake site.
- **Response:** Banks increased awareness campaigns and implemented better SMS filtering and detection technologies.

2.6 Clone Phishing

Clone phishing is the practice of copying and pasting authentic emails or messages, making little changes (like changing links or attachments), and then delivering them to targets pretending they were the original correspondence. This strategy tries to fool recipients into interacting with the malicious content by taking advantage of their familiarity with the original sender.

Signs of Clone Phishing:

1. Duplicate emails: Look for copies of emails and closely examine newly added links for any indications of phishing. Always cross-reference connections with earlier correspondence.
2. Misspelt email addresses: Small typos are a common feature of bogus emails, which are sometimes overlooked.
3. Text with hyperlinks: Hover your cursor over links to see the actual URL. Should it diverge from the text that is linked, it can be a sign of phishing.

Case Study: Dropbox (2014)

- **Overview:** Attackers cloned legitimate Dropbox emails, inserting malicious links to steal user credentials.
- **Signs of Activity:** Emails identical to official Dropbox communication but with malicious links.
- **Impact:** Compromised user accounts and data breaches.
- **Response:** Dropbox enhanced email security, user education, and implemented two-factor authentication.

2.7 Angler Phishing

Attackers that use social media to conduct angler phishing pose as customer service agents. They make up profiles and message unhappy persons they come across in posts or comments on social media. Once the fraudster has confirmed a few personal data, they offer help and a URL that claims to fix the problem. But the URL is infected with malware, which makes it possible to successfully exploit the victim.

Signs of Angler Phishing:

1. Unverified account: Official support pages are usually verified and linked directly to the main page. Check the company website for official support contacts.
2. Minimal profile history: Smaller businesses, though unverified, should have a history of customer interactions. New accounts with few followers and no posts are likely attempting to deceive unsuspecting users.

Case Study: British Airways (2018)

- **Overview:** Attackers posed as British Airways customer service on social media to steal personal information from customers.
- **Signs of Activity:** Fake customer service accounts, requests for personal information via direct messages.
- **Impact:** Compromised customer information and loss of trust.
- **Response:** British Airways improved social media monitoring and customer education on verifying legitimate accounts.

2.8 Evil twin phishing

Evil twin phishing involves creating a fraudulent Wi-Fi network that mimics a legitimate one, tricking users into connecting to it. Once connected, attackers can intercept sensitive information or deploy malware.

Signs of Evil twin phishing:

1. Duplicate Wi-Fi hotspots: If you see multiple Wi-Fi networks with the same name, connect only to the secured one requiring a password from the establishment. Connecting to unsecured networks is strongly discouraged for safety.
2. Unsecure warnings: If your device warns that a network is unsecured, consider connecting to a secure network or refrain from connecting altogether.

Case Study: Coffee Shop Incident (2019)

- **Overview:** Attackers set up an evil twin Wi-Fi network in a coffee shop, capturing data from users who connected to it.
- **Signs of Activity:** Multiple Wi-Fi networks with the same name, unsecure connection warnings.
- **Impact:** Stolen personal information and compromised accounts.
- **Response:** Increased public awareness about the dangers of connecting to unsecured Wi-Fi networks and encouraging the use of VPNs.

3. Stakeholders

To minimise the impact on the organisation and prevent further events, early and efficient reaction to a phishing attack depends on strong coordination and collaboration amongst key stakeholders. Responding to a phishing attack usually involves the following key stakeholders:

3.1 IT Security Team

Lead: Daniel McAulay (Senior Project Leader)

Responsibilities:

- Identifying, researching, and preventing phishing attacks.
- Leading technical response tasks such as phishing email analysis and malicious website blocking.

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 phishing 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

Responsibilities:

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

Phishing Incident Response RACI Chart

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

Monitor system logs and traffic	A, R	R	I	I	I	I	I
Use IDS and SIEM tools	A, R	R	I	I	I	I	I
Analyse alerts	A, R	R	I	I	I	I	I
Analysis							
Collect forensic data	A, R	R	I	I	I	I	I
Identify attack methods	A, R	R	I	I	I	I	I
Determine impact	A, R	R	I	I	I	I	I
Containment							
Isolate compromised systems	A, R	R	I	I	I	I	I
Implement access restrictions	A, R	R	I	I	I	I	I
Block malicious traffic	A, R	R	I	I	I	I	I
Eradication							

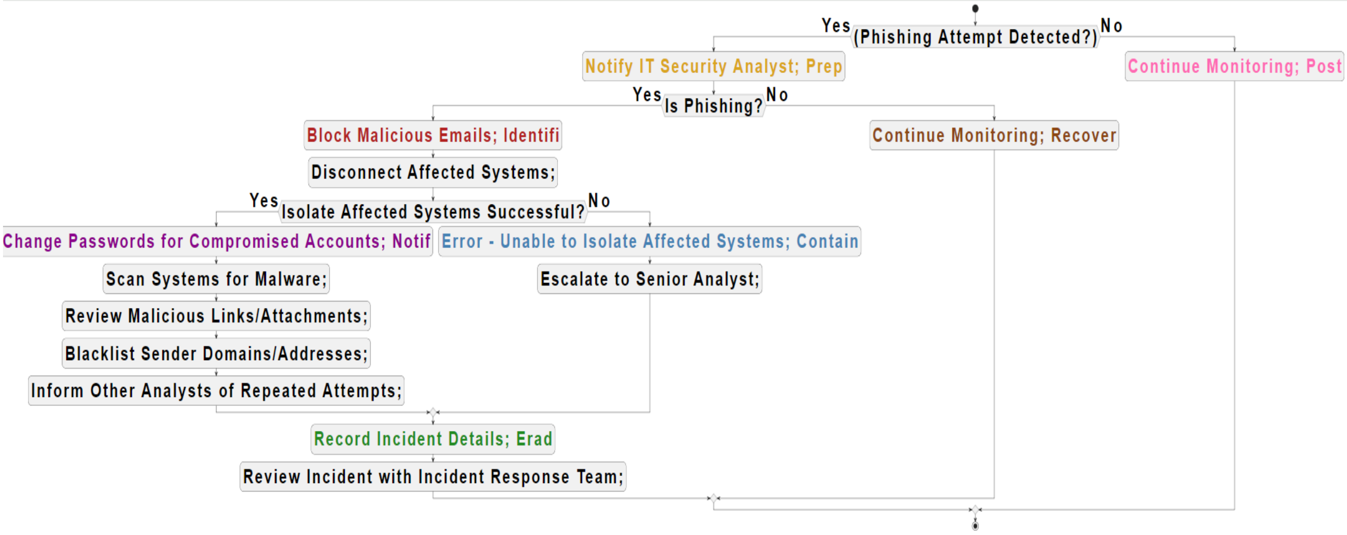
Remove malicious software	A, R	R	I	I	I	I	I
Patch vulnerabilities	A, R	R	I	I	I	I	I
Update security policies	A, R	R	I	I	I	I	I
Recovery							
Restore backups	A, R	R	I	I	I	I	I
Rebuild systems	A, R	R	I	I	I	I	I
Conduct user training	A, R	R	I	I	I	I	I
Post-Incident Review							
Review incident response	A, R	R	I	I	I	I	I
Document lessons learned	A, R	R	I	I	I	I	I
Update response procedures	A, R	R	I	I	I	I	I
Communication							

Create communication plans	C	C	A, R	I	C	I	I
Draft communication materials	C	C	A, R	I	C	I	I
Manage media relations	C	C	A, R	I	C	I	I
Provide updates	C	C	A, R	I	C	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 Diagram


(Phishing Attempt Detected?)
Yes
No
Notify IT Security Analyst; Prep
Continue Monitoring; Post
Is Phishing?
Yes
No
Block Malicious Emails; Identifi
Continue Monitoring; Recover
Disconnect Affected Systems;
Isolate Affected Systems Successful?
Yes
No
Change Passwords for Compromised Accounts; Notif
Error - Unable to Isolate Affected Systems; Contain
Scan Systems for Malware;
Escalate to Senior Analyst;
Review Malicious Links/Attachments;
Blacklist Sender Domains/Addresses;
Inform Other Analysts of Repeated Attempts;
Record Incident Details; Erad
Review Incident with Incident Response Team;

1. Preparation (Prep): Yellow

- Notify IT Security Analyst- The first thing to do is to alert the assigned IT security analyst as soon as you suspect a phishing attempt. To start the incident response procedure as soon as possible, the analyst must be notified. Important information including the threat's nature, the systems that are impacted, and any preliminary findings or proof are all included in this warning.

2. Identification (Identify): Red

- Block Malicious Emails: As soon as the phishing attempt is verified, all incoming emails that are suspected of being fraudulent should be blocked. By taking this preventive step, users are protected from possible danger and more intrusion into the company's systems are prevented.

- Disconnect Affected Systems: Meanwhile, all suspected or verified hacked systems are unplugged from the network. The goal of this isolation phase is to reduce possible harm to other systems or data while containing the danger and preventing its spread.

3. Notification (Notif): Violet

- Change Passwords for Compromised Accounts: Passwords for hacked user accounts are quickly changed as part of incident response to stop unwanted access. This preventive action reduces the possibility that malicious individuals will continue to abuse the situation.

- Scan Systems for Malware: The impacted computers are thoroughly scanned to find and eliminate any malware or harmful files. Through this scanning procedure, the systems' integrity is guaranteed, and any potential threats are stopped in their tracks.

- Review Malicious Links/Attachments: All attachments and URLs that might be connected to the phishing effort are carefully examined. This research provides light on the attackers' methodology and motivations in addition to helping to identify the strategies they employ.

- Blacklist Sender Domains/Addresses: Email addresses and sender domains connected to the phishing effort are blocked. Companies can actively fight against future attacks and protect customers from similar hazards by limiting communication from these sources.

- Inform Other Analysts of Repeated Attempts: Other security analysts are informed about the phishing effort, including attack tactics and indications of compromise (IOCs). This cooperative strategy strengthens protections against recurring threats and improves situational awareness.

4. Containment (Contain): Sky Blue

- Error - Unable to Isolate Affected Systems: If isolating the compromised systems doesn't resolve the issue, a senior analyst is notified so they may investigate it more and take appropriate action. By taking this action, you may be confident that the right steps are done to limit the problem and stop it from getting worse.

- Escalate to Senior Analyst: To help in reaching a well-informed decision, the senior analyst is briefed on the circumstances and given relevant details. By elevating the issue, you can make sure that it gets the focus and resources it needs to be handled successfully.

5. Eradication (Erad): Light Green

- Record Incident Details: Carefully documented are all the specifics of the happening, such as the timing, effects, and reaction activities. For post-event analysis, legal compliance, and future incident response planning, this material is an invaluable resource.

- Review Incident with Incident Response Team: Together with the incident response team, a thorough analysis of the occurrence is carried out. The objectives of this post-event study are to identify areas for incident response method improvement, security control gaps, and lessons learned.

6. Recovery (Recover): Brown

- Continue Monitoring: Ongoing monitoring operations are restarted following the mitigation of the immediate threat and the incident. This entails keeping an eye on user activities, system records, and network traffic to spot any remaining dangers or illegal access.

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

- Continue Monitoring: Even after the issue has been resolved, ongoing surveillance is still necessary to identify any reappearance of the danger or any fresh security flaws. To improve future issue handling skills, post-event steps should also involve a complete examination of incident response protocols and the implementation of any necessary enhancements.

5. Incident Response Stages

5.1 Preparation

Objective: Establish the foundation for an effective phishing incident response.

Activities:

- Develop and document an incident response plan.
- Form an incident response team with defined roles and responsibilities.
- Conduct regular risk assessments.
- Implement security measures like antivirus programs, firewalls, and intrusion detection systems.
- Create and maintain backups of critical data.
- Conduct employee training and awareness campaigns.
- Establish communication channels for reporting and coordinating incidents.

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

5.2 Detection

Objective: Identify indications of phishing attacks or unauthorized access.

Activities:

- Monitor system logs and network traffic for unusual activity.
- Use IDS and SIEM tools to detect phishing attacks.
- Analyse alerts to differentiate between legitimate and malicious activity.
- Conduct regular security audits and scans to find vulnerabilities.

Outcome: Early identification of phishing threats enables rapid response.

5.3 Analysis

Objective: Determine the nature and scope of the phishing incident.

Activities:

- Examine security events to assess the impact.
- Gather and analyse supporting documentation.
- Identify TTPs and IOCs of threat actors.
- Collaborate with IT departments, legal advisors, and law enforcement if needed.
- Document findings and maintain a chain of custody for evidence.

Outcome: Comprehensive understanding of the phishing incident, including causes and effects.

5.4 Containment

Objective: Stop further unauthorized access or data leakage.

Activities:

- Isolate compromised systems from the network.
- Disable compromised user accounts or services.
- Implement interim solutions to mitigate the impact.
- Communicate containment efforts and expected downtime to relevant parties.

Outcome: Effective handling of the phishing incident, minimizing damage.

5.5 Eradication

Objective: Remove malicious elements and restore system integrity.

Activities:

- Identify and remove malware from impacted systems.
- Fix security vulnerabilities.
- Perform thorough audits to ensure all compromises are eliminated.

- Restore systems from clean backups.
- Update security measures to prevent recurrence.

Outcome: Complete removal of phishing threats and reduction of vulnerabilities.

5.6 Recovery

Objective: Restore normal operations while maintaining security.

Activities:

- Test restored systems and applications.
- Communicate progress to all relevant parties.
- Conduct post-event evaluations to identify opportunities for improvement.
- Update incident response plans, policies, and training materials based on lessons learned.

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:

- Document the incident response process, including timelines, actions taken, and outcomes.
- Review the effectiveness of response activities and identify gaps or deficiencies in protocols.
- Conduct a lesson learned meeting with the incident response team and relevant parties.
- Update incident response documentation based on post-event evaluation findings.
- Share insights and recommendations with upper management to strengthen overall security posture.

Outcome: Enhanced incident response capabilities and preparedness for future phishing incidents.

6. Steps for Monitoring Threats

6.1 Establish a Monitoring Strategy

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

Activities:

- **Objectives:** Clearly define the objectives for threat monitoring, such as detecting phishing emails, identifying unauthorized access, and monitoring unusual network traffic indicative of phishing activities.
- **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 email filtering software.
- **Baselines:** Establish baselines for normal user activity, system Behavior, and network traffic patterns to identify deviations that may indicate phishing presence.

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

6.2 Deploy Monitoring Solutions

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

Activities:

- **Install and Configure Tools:** Deploy the selected monitoring tools across networks, systems, and endpoints. Ensure they are configured to detect phishing-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 phishing 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 phishing threats.

6.3 Continuous Monitoring and Analysis

Objective: Maintain continuous monitoring and analysis to promptly detect and respond to phishing threats.

Activities:

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

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

6.5 Investigate and Respond

Objective: Conduct thorough investigations and implement appropriate actions to mitigate identified phishing 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 phishing 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 phishing threat from the environment.

Outcome: Effective investigation and mitigation of phishing 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 phishing 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): An intrusion detection system (IDS) is a security instrument that keeps an eye on system or network activity for any illegal activity or policy infractions.

- Phishing: The deceptive practice of sending emails, texts, or phone calls to trick individuals into disclosing sensitive information.

- Security Information and Event Management (SIEM): A solution called Security Information and Event Management (SIEM) offers in-the-moment security alarm analysis from network hardware and application sources.

- Vulnerability assessment: Vulnerability assessment is the procedure for locating, measuring, and ranking security holes in a system.

- Threat Intelligence: Information concerning possible or existing dangers to the security infrastructure of an organisation is known as threat intelligence.

- Zero-day vulnerabilities: Zero-day vulnerabilities are security holes in hardware or software that are not known to the developer or vendor, leaving attackers free to take advantage of them before a patch or remedy is made available.

- Social Engineering: Manipulative techniques used by attackers to trick individuals into divulging confidential information or performing certain actions.

- Spam Filter: A tool that identifies and filters out unsolicited and potentially harmful emails.

- Two-Factor Authentication (2FA): An additional security layer requiring not only a password and username but also something that only the user has on them, such as a piece of information only they should know or have immediately to hand, such as a physical token.