**Cyber Security Analyst Program**

**CYBERRANGE CAPSTONE PROJECT**

**A blue and black background with a letter

Description automatically generated**

**Cyber Security Network Risk Assessment Report**

**Tremaine Hinds**

**Due Date: August 23rd, 2024**

**Risk Assessment Template with Tables and Risk Matrix**

1. **Introduction**
   * **Overview**:
   * The Foundation for Atropistan K-series-Graphene from Exfoliation (FAKE) outsources IT protection duties to the Elite Eyes&Ears team (E3). FAKE provides in-house training specifically tailored for their needs. To collaborate with international experts, FAKE is trialing remote access, thereby increasing their threat surface. In preparation for a continuous development and integration pipeline, the web team is running beta testing with a mix of open-source code and their own in-house applications for more sensitive projects.
   * **Purpose and Scope**:

The purpose of this risk assessment is to identify, analyze, and evaluate the security risks present within the organization's network infrastructure and systems. By examining various indicators of compromise (IOCs) and previous malicious activities, this assessment aims to provide a comprehensive understanding of the potential threats that could impact the confidentiality, integrity, and availability of the organization's critical assets. The findings will serve as a foundation for developing effective remediation strategies, enhancing the organization's cybersecurity posture, and ensuring compliance with relevant regulations and best practices.

The scope of this risk assessment encompasses the organization's network infrastructure, including the evaluation of its architecture and connections to identify vulnerabilities that may be exploited by malicious actors. It also involves assessing critical systems, applications, and services, particularly those flagged for suspicious activity, such as MySQL servers and remote desktop services. Additionally, the assessment will review user access and privilege management practices to identify potential weaknesses that could lead to privilege escalation and unauthorized access.

Furthermore, the analysis will focus on detected malware activities, such as Cobalt Strike and TrickBot, to understand their impact and develop strategies for containment and eradication. The effectiveness of existing incident response protocols in addressing previous security incidents, including phishing attempts and unauthorized access, will also be evaluated. The assessment will examine the external threat landscape, including phishing, brute force attacks, and data exfiltration attempts, to assess the organization's exposure to these risks. Lastly, the assessment will identify relevant compliance requirements and industry standards to ensure that the organization's security practices align with legal and regulatory obligations.

The findings from this comprehensive assessment will be used to prioritize risks, recommend appropriate controls, and develop an actionable risk management plan to mitigate identified vulnerabilities and enhance the overall security of the organization.

1. **Risk Identification**
   * **List the Top Five Risks**:

Risk 1: Malware Infiltration

Risk 2: Privilege Escalation Vulnerabilities

Risk 3: Unsecured Remote Access

Risk 4: Phishing Attacks

Risk 5: Unusual Network Traffic

* + **In-Depth Description of the Top Three Risks**:

**Risk 1**:Malware Infiltration

* + - * **Description**: The detection of malware, including Cobalt Strike and TrickBot, indicates a significant risk of unauthorized access, data exfiltration, and potential compromise of sensitive systems. These malware strains are known for their ability to establish persistence and facilitate lateral movement within the network.

**Risk 2**: Privilege Escalation Vulnerabilities

* + - * **Description**: The presence of incidents involving privilege escalation suggests that attackers may gain elevated access rights, allowing them to manipulate critical systems and data. This can lead to unauthorized changes, data breaches, and increased attack vectors within the network.

**Risk 3**: Phishing Attacks

* + - * **Description**: The documented phishing incident highlights the risk of social engineering attacks that can compromise user credentials and lead to unauthorized access. Phishing remains a prevalent threat vector and requires ongoing user education and awareness training

1. **Risk Analysis**
   * **Likelihood and Impact**: Assess the likelihood and impact of each risk.

**Risk 1**: Malware Infiltration

* + - * **Likelihood**:8
      * **Impact**:9

**Risk 2**: Privilege Escalation Vulnerabilities

* + - * **Likelihood**:6
      * **Impact**:7

**Risk 3**: Unsecured Remote Access

* + - * **Likelihood**: 5
      * **Impact**:7

**Risk Matrix Calculations Table**:

| **Risk** | **Likelihood (1-9)** | **Impact (1-9)** | **Risk Score (Likelihood x Impact)** |
| --- | --- | --- | --- |
| Risk 1 | : Malware Infiltration | 9 | 72 |
| Risk 2 | Privilege Escalation Vulnerabilities | 6 | 42 |
| Risk 3 | Unsecured Remote Access | 5 | 35 |
| Risk 4 | Phishing Attacks | 8 | 56 |
| Risk 5 | Unusual Network Traffic | 6 | 36 |

* + **Categorize Risks Using the Risk Matrix**: Place each risk in the appropriate category on the risk matrix.

1. **Risk Evaluation**
   * **Prioritize Risks**: Based on the risk matrix, prioritize which risks need immediate attention.

**High Priority**: Malware Infiltration

**Medium Priority**: Phishing Attacks

**Low Priority**: Unusual Network Traffic

1. **Risk Treatment**
   * **Mitigation Strategies**: Propose and detail strategies for each risk.

**Risk 1**: Malware Infiltration

* + - * **Strategies**: **Intrusion Detection and Prevention Systems (IDPS)**:  
        Deploy IDPS to monitor network traffic for suspicious activity and take immediate action to block or contain potential threats
      * **Email Filtering**:  
        Implement advanced email filtering solutions to identify and block malicious attachments and links before they reach users’ inboxes.
      * **Endpoint Protection**:  
        Implement robust endpoint protection solutions that include antivirus, anti-malware, and behavior-based detection capabilities. Regularly update these tools to ensure they can detect the latest threats.

**Risk 2**: Phishing Attacks

* + - * **Strategies**: **Multi-Factor Authentication (MFA)**:  
        Require multi-factor authentication for accessing sensitive systems and data. This adds an extra layer of security, making it more difficult for attackers to gain unauthorized access even if credentials are compromised.
      * **Domain Protection**:  
        Implement domain protection measures, such as Domain-Based Message Authentication, Reporting & Conformance (DMARC), to prevent domain spoofing and ensure that only authorized parties can send emails on behalf of the organization.
      * **User Training and Awareness**:  
        Conduct regular training sessions to educate employees about phishing tactics, including how to recognize suspicious emails, links, and attachments. Use simulated phishing campaigns to test and reinforce this knowledge.

**Risk 3**: Unusual Network Traffic

* + - * **Strategies**: **Establish Baselines for Network Traffic**:  
        Create baseline traffic patterns for normal network behavior. By understanding what constitutes typical activity, security teams can more easily identify deviations that may indicate malicious activity.
      * **Traffic Analysis and Filtering**:  
        Utilize traffic analysis tools to filter out known malicious IP addresses, protocols, and services. This helps reduce the likelihood of unusual traffic entering the network.
      * **Regular Security Audits**:  
        Conduct regular security audits and vulnerability assessments to identify potential weaknesses in the network. Address any findings to strengthen overall network security.
      * 

1. **Monitoring and Review**
   * **Ongoing Monitoring**: Outline a plan for continuous monitoring of identified risks.

**Plan**: The continuous monitoring plan for identified risks aims to enhance the organization's cybersecurity posture by establishing clear monitoring objectives aligned with overall security and compliance goals. It begins with the identification of Key Risk Indicators (KRIs) for each of the top risks, including malware infiltration, phishing attacks, and unusual network traffic. For example, KRIs for malware infiltration may include the number of malware detections and the frequency of endpoint alerts, while phishing attack KRIs could involve the number of reported phishing attempts and click-through rates on suspicious emails. Unusual network traffic may be monitored through anomalies in traffic patterns and alerts from intrusion detection systems.

To support this monitoring, appropriate security tools and technologies will be deployed, such as Security Information and Event Management (SIEM) systems for centralized log management, Intrusion Detection Systems (IDS) to monitor network traffic, Endpoint Detection and Response (EDR) solutions for threat monitoring on endpoints, and email filtering solutions to detect and block phishing attempts. Regular data collection and analysis will be scheduled at intervals such as daily or weekly, with automated processes in place to identify trends and anomalies.

In conjunction with monitoring, incident response protocols will be established for each identified risk, ensuring that monitoring results are integrated with the organization's incident response plan to enable rapid action when risk thresholds are exceeded. Periodic risk assessments will be conducted to review and update the risk landscape, ensuring new threats are identified and monitored effectively. Ongoing training and awareness programs will be implemented for security personnel and all employees to recognize phishing attempts and report unusual activity.

Documentation of monitoring processes, findings, and incidents will be maintained, with regular reports generated to summarize KRI trends and responses for stakeholders. A feedback loop will be established to evaluate the effectiveness of monitoring efforts, allowing for adjustments based on feedback and the evolving threat landscape. Lastly, engaging key stakeholders in monitoring efforts will foster a culture of security awareness and vigilance across the organization, ultimately leading to a proactive approach in managing identified risks.

1. **Conclusion**
   * **Summarize Key Findings**: In conclusion, the continuous monitoring plan for identified risks is a vital component of the organization's overall cybersecurity strategy. By establishing clear Key Risk Indicators, deploying appropriate security tools, and implementing structured incident response protocols, the organization can effectively track and respond to potential threats such as malware infiltration, phishing attacks, and unusual network traffic. Regular data collection, analysis, and periodic risk assessments will ensure that the organization remains vigilant and adaptable in the face of evolving threats. Furthermore, fostering a culture of security awareness among employees will enhance the organization’s resilience against cyberattacks. Through these proactive measures, the organization can significantly reduce the likelihood and impact of cybersecurity risks, safeguarding its critical assets and maintaining the trust of stakeholders.
   * **Importance of Risk Management**: Risk management is crucial for organizations as it provides a systematic approach to identifying, assessing, and mitigating potential threats to operations and assets. It helps organizations proactively address risks before they escalate, ensuring continuity and stability. By enabling informed decision-making and efficient resource allocation, effective risk management maximizes returns while safeguarding compliance and protecting against legal issues. It enhances an organization’s resilience, allowing for quicker recovery from unexpected events, and fosters trust among stakeholders, contributing to a positive reputation. Ultimately, a robust risk management framework supports continuous improvement and positions organizations for sustainable success in an ever-changing environment.

**Risk Matrix**

| **Impact** | **Low (1-3)** | **Moderate (4-6)** | **High (7-9)** |
| --- | --- | --- | --- |
| High (7-9) |  |  |  |
| Moderate (4-6) |  |  |  |
| Low (1-3) |  |  |  |
| Likelihood | High (7-9) | Moderate (4-6) | Low (1-3) |

**Legend for Risk Matrix**

* **High Priority**: Indicates risks with a high impact and/or high likelihood. These risks require immediate attention and mitigation. (Color optional)
* **Medium Priority**: Indicates risks with a moderate impact and/or likelihood. These risks should be addressed in a timely manner. (Color optional)
* **Low Priority**: Indicates risks with a low impact and/or low likelihood. These risks can be monitored and addressed as needed. (Color optional)