**IS PROJECT**

**Members:**

**19K-0214 Ahmed Memon**

**20K-0297 Usaid Bin Rehan**

**20K-0409 Mukand Krishna**

**Handwritten Notes.**

**PROJECT BASED ON RISK ASSESSMENT AND THREAT MANAGEMENT**

**Company: Avanza Solutions**

**Sector: Digital Technology and Automation for Financial Services**

**Training**

**1. Do you conduct robust and frequent end-user cybersecurity awareness training?**

**Yes:** They conduct cybersecurity awareness training regularly, although resource limitations may impact the extent of training. Recognizing its importance, the organization invests in educating employees to maintain a strong security posture within budget constraints.

**2. Have you taught everyone how to securely store passwords or passphrases?**

**Yes:** They provide training on secure password storage practices, acknowledging the challenge of enforcing consistent application across diverse systems. Despite difficulties, the organization emphasizes security education to enhance overall awareness and practices.

**Access Control**

**6. Are only necessary services, protocols, daemons, and functions enabled?**

**Yes:** They maintain a policy of minimal exposure to reduce potential vulnerabilities. The organization enables only essential services, protocols, daemons, and functions, emphasizing continuous monitoring and updates.

**8. Are all accounts immediately disabled or deleted upon termination of employment?**

**Yes:** They take immediate action upon employee departure, ensuring account disablement or deletion to prevent unauthorized access. This proactive measure safeguards against potential security breaches.

**End User**

**11. Have you developed an administrator (admin) and user password or passphrase policy that eliminates the use of common or easy-to-guess passwords?**

**Yes:** They have implemented a password policy to enhance security. However, the enforcement of this policy might not be consistent across all users and systems. This inconsistency arises due to factors like user awareness, password change requirements and system limitations.

**End Points**

**12. Are all endpoint logs ingested by smart technology using threat intelligence and AI?**

**Yes:** They employ advanced technology to analyze endpoint logs, utilizing threat intelligence and AI. This enhances threat detection and response capabilities, fostering a proactive security approach.

**15. Do you prevent non-enterprise-controlled and secured devices from connecting to any portion of your network?**

**Yes:** They endeavor to control access to its network by preventing non-enterprise devices from connecting. However, the organization faces limitations in maintaining strict control over all external devices attempting to access the network. Like varied device types, evolving technologies, and the diverse locations from which devices connect.

**17. Do all endpoints have non-disabling antivirus with automatic updates?**

**Yes:** They ensure uniform antivirus deployment on all endpoints. The antivirus is designed to be non-disabling, and automatic updates are implemented, ensuring up-to-date threat protection.

**Event Management**

**22. Do you have a mature and well-organized cybersecurity incident response (in-house or in conjunction with third parties) that thoroughly investigates all incidents?**

**Yes:** They maintain a mature and well-organized cybersecurity incident response system, demonstrating a commitment to thorough investigations of all incidents. This preparedness is crucial for promptly addressing and mitigating potential cybersecurity threats, ensuring a resilient security posture.

**Security Architecture**

**23: Do you only give employees the tools and access needed to perform their job functions, and nothing else?**

**Yes:** They provide employees with access only to the tools and resources necessary for their specific job functions. They achieve this through a robust access control system that evaluates the job requirements and assigns access rights, accordingly, ensuring that each employee has just what they need to perform their duties effectively.

**24. Do you utilize the principle of least privilege?**

**Yes:** They practice the principle of least privilege across its network. This means that employees are granted only the minimum levels of access or permissions they need to carry out their job functions. The company manages this by regularly reviewing user roles and access rights, ensuring that privileges are aligned with job requirements and are not excessive.

**25. Do you deploy a zero-trust model?**

**Yes:** They have limited implementation of the zero-trust model. Implements some elements in place, the model is not fully integrated across the organization.

**27. Do you require MFA for internal authenticated network users to access key infrastructure and data inside the network (i.e., the crown jewels)?**

**Yes:** The enforcement of MFA for internal network users varies within They, especially when accessing critical infrastructure and data.

**28. Do you manage all credentials in an order that allows you to quickly conduct a password reset for every account on your network? (This includes service accounts.)**

**Yes:** They effectively manage all credentials on their network, including the ability to quickly conduct password resets for every account. Managed through a centralized credential management system that tracks and controls access credentials, ensures efficient and secure handling of password resets and account management, even for service accounts.

**29. Have you recently assessed your Active Directory to ensure that it is properly configured and secured?**

**Yes:** They regularly assess their Active Directory to ensure it is properly configured and secured. They conduct these assessments periodically to identify and rectify any security vulnerabilities, ensuring that the Active Directory remains robust and resistant to potential cyber threats.

**30. Are you actively monitoring the security of your Active Directory?**

**Yes:** They actively monitor the security of their Active Directory. This involves continuous oversight using specialized security tools and protocols to detect and respond to any irregularities or potential breaches, thereby maintaining the integrity and security of their directory services.

**31. Do your perimeter firewalls have a deny-all rule unless otherwise authorized?**

**Yes:** Perimeter firewalls are configured with this rule unless specific authorization is provided. This strict approach ensures that only verified and necessary traffic is allowed through the network, significantly enhancing the company’s network security.

**34. Do you deploy anti-spoofing technology to prevent forged IP addresses from entering the network?**

**Yes:** They deploy anti-spoofing technology to protect their network. Which helps prevent forged IP addresses from entering the system, which protects against certain types of cyber-attacks based on IP spoofing.

**35. Do you prevent the disclosure of internal IP addresses and routing information on the Internet?**

**Yes:** They take measures to prevent the disclosure of internal IP addresses and routing information on the Internet. They employ various security protocols and configurations to ensure that sensitive internal network details are not exposed to external parties.

**Threats**

**42. Do you perform periodic targeted threat hunts?**

**Yes:** They conduct targeted threat hunts periodically. These hunts are designed to proactively identify and mitigate potential cyber threats but are not frequent. They use a combination of manual expertise and automated tools to execute these hunts effectively.

**43. Do you ingest current threat intelligence (preferably from more than one source) and have a procedure to implement rapid countermeasures based on good threat intelligence?**

**Yes:** They actively use threat intelligence from various sources to stay ahead of potential cyber threats. They utilize specialized tools for analyzing this intelligence, helping them quickly identify and respond to emerging security risks.

**45. Do you closely monitor all vendor and third-party supply-chain connections for compliance and untoward issues?**

**Yes:** They maintain a robust monitoring system for their vendor and third-party connections. This includes regular audits and automated systems to ensure compliance and detect any security issues, safeguarding their supply chain.

**Testing**

**46. Do you conduct at least 1 penetration test annually, performed by a third party?**

**Yes:** They conduct at least one penetration test annually with the help of a third-party service. This approach ensures an objective evaluation of their network and systems' security. The third-party experts bring a fresh perspective and specialized skills to identify vulnerabilities that internal teams might overlook.

**47. Do you conduct routine vulnerability scans and remediate all vulnerabilities with a Common Vulnerability Scoring System (CVSS) score of 4 or more within 30 days, and all other vulnerabilities within 90 days?**

**Yes:** They routinely perform vulnerability scans and stick to a strict protocol to remediate identified issues. They prioritize fixing vulnerabilities with a CVSS score of 4 or more within 60 days and address all other vulnerabilities within 120 days. This systematic approach helps in maintaining a strong defense against potential cyber threats.

**48. Do you routinely scan your Internet-facing infrastructure for penetration and vulnerabilities?**

**Yes:** They conduct scans of their Internet-facing infrastructure, but these scans may not be as frequent or comprehensive as required. Regular and thorough scanning is crucial for detecting potential vulnerabilities and penetration risks, and there might be a need for more frequent or detailed assessments.

**49. Do you perform an annual business impact analysis/risk analysis report with insider and outside auditors?**

**Yes:** They attempt to perform annual business impact analyses and risk analysis reports with the help of internal and external auditors. However, they encounter challenges in conducting these analyses annually, due to the complexity of the process and sometimes the need for more in-depth collaboration with auditing experts.

**Data Management**

**60. Is storage of confidential data kept to a minimum and securely deleted after it's no longer needed?**

**Yes:** They maintain strict practices for storing confidential data. They keep such data storage to a minimum and ensure it is securely deleted once it's no longer needed. This approach is part of their broader data management and security strategy, aiming to reduce the risk of data breaches and comply with data protection regulations.

**62. Do you deploy a network and cloud-based data loss prevention (DLP) program anywhere confidential data reside?**

**Yes:** They have deployed data loss prevention programs in some areas where confidential data resides, but the coverage may be inconsistent. This variation in deployment could be due to differing levels of risk assessment, resource allocation, or the complexity of integrating DLP solutions across various network and cloud environments.

**63. Do you prevent confidential data from being copied to external devices and external devices from being attached to endpoints?**

**Yes:** They have implemented robust measures to prevent the copying of confidential data to external devices and restrict external devices from being connected to endpoints. This is achieved through a combination of technical controls, such as device management software, and policy enforcement, ensuring that sensitive data remains secure and is not exposed to risks associated with external device usage.

**Software Development**

**64. Are processes and mechanisms for developing and maintaining secure systems and software defined and understood?**

**Yes:** Processes and mechanisms for secure software development are defined at Avanza, but their universal understanding and adoption may be limited. The organization emphasizes secure development practices, although challenges in ensuring widespread implementation exist.

**67. Are these applications protected against attacks?**

**Yes:** They have implemented measures to protect public-facing web applications against attacks. The organization is proactive in addressing security concerns, employing various strategies to enhance the resilience of these applications against potential threats.

**68**. **Are preproduction environments separated from production environments, and is separation enforced with access controls?**

**Yes:** They maintain separation between preproduction and production environments, although enforcement with access controls may face challenges. The organization recognizes the importance of environment separation but acknowledges ongoing efforts to strengthen and ensure consistent enforcement.