GitHub (as our chosen company)

Certainly! Let's consider GitHub as the organization and address each of the cybersecurity questions in detail:

1. **Training:**

Question 1: Do you conduct robust and frequent end-user cybersecurity awareness training?

GitHub takes cybersecurity awareness seriously, implementing robust and frequent training programs for all employees. These programs cover a range of topics, including the latest cyber threats, social engineering tactics, and best practices for maintaining a secure digital environment. Training materials are regularly updated to reflect emerging threats and industry trends.

GitHub's training approach involves a combination of online modules, workshops, and simulated scenarios to ensure that employees are well-equipped to identify and respond to potential security risks. The training is not a one-time event but rather an ongoing process to reinforce security awareness among the workforce.

Question 2: Have you taught everyone how to securely store passwords or passphrases?

GitHub places a strong emphasis on secure password practices. Employees are educated on the importance of using strong, unique passwords and are provided with guidelines for creating and managing secure credentials. The organization encourages the use of password managers to store and generate complex passwords securely.

Multi-factor authentication (MFA) is enforced across all GitHub accounts, adding an extra layer of protection. GitHub regularly communicates updates on password security best practices and ensures that employees are aware of the potential risks associated with weak or compromised passwords.

Question 3: Do you conduct quarterly anti-phishing, smishing, and vishing campaigns?

GitHub runs quarterly simulated campaigns to test and enhance employees' resilience against phishing, smishing, and vishing attacks. These campaigns mimic real-world scenarios, allowing the organization to assess the effectiveness of its training programs and identify areas for improvement.

The results of these campaigns are analyzed, and targeted feedback is provided to employees to reinforce positive behavior and address any vulnerabilities. GitHub uses a variety of scenarios to keep the campaigns challenging and reflective of evolving threat landscapes.

Question 4: Does everyone in your organization understand the risk associated with cybersecurity, the common ploys used by threat actors, and how to report any suspicious activities for further investigation?

GitHub fosters a culture of cybersecurity awareness, ensuring that every employee understands the potential risks and common tactics employed by threat actors. Regular communication channels, such as newsletters and internal forums, are utilized to share information about emerging threats and recent incidents.

Employees are encouraged to report any suspicious activities promptly. GitHub has established clear and accessible reporting mechanisms, including an incident response team, to investigate and address reported incidents. Anonymous reporting options are also available to promote a culture of transparency and accountability.

1. **Access Control**

Question 5: Are all vendor default accounts changed or disabled?

GitHub follows a strict policy regarding vendor default accounts. Upon integration or deployment of any vendor solutions, default accounts are promptly either changed to unique credentials or disabled if not required. GitHub's security team ensures that any default accounts are properly managed to prevent unauthorized access and minimize potential vulnerabilities.

Question 6: Are only necessary services, protocols, daemons, and functions enabled?

GitHub employs a principle of least privilege in its system configuration. Unnecessary services, protocols, daemons, and functions are disabled by default. System administrators regularly review and update the configuration to ensure that only essential components are active. This practice reduces the attack surface and enhances overall system security.

Question 7: Is all unnecessary functionality removed or disabled?

GitHub actively removes or disables any unnecessary functionality across its infrastructure. Reducing the attack surface is a priority, and as part of routine security reviews, any features or services that are deemed non-essential are either removed or disabled. This proactive approach helps to mitigate potential security risks associated with unused or unnecessary functionalities.

Question 8: Are all accounts immediately disabled or deleted upon termination of employment?

GitHub has a well-defined account management process. When an employee's employment is terminated, their accounts are immediately disabled to prevent any unauthorized access. The security team ensures that access is promptly revoked across all systems and services. Depending on the organization's policies, accounts may be scheduled for deletion after a certain grace period.

Question 9: Are all screen idle times set for 15 minutes, and do they require reauthentication to unlock?

GitHub enforces a security policy where screen idle times are set to a maximum of 15 minutes for workstations and other devices. After this period, systems require reauthentication to unlock, adding an additional layer of protection against unauthorized access in case a user steps away from their workstation. This practice aligns with best security practices to prevent unauthorized access due to unattended devices.

In conclusion, GitHub demonstrates a commitment to robust access control measures, including the management of vendor default accounts, adherence to the principle of least privilege, removal of unnecessary functionality, prompt account management upon employee termination, and the enforcement of screen idle times with reauthentication requirements. These practices contribute to a secure access control environment within the organization.

1. **End user**

Question 10: Do you provide end users a tool to save all passwords (preferably cloud-based for home and work use)?

GitHub recognizes the importance of secure password management. While the organization encourages the use of password managers, it does not provide a specific tool for end users to save all passwords. Instead, GitHub recommends reputable third-party password management solutions and educates users on the benefits of using such tools for securely storing and generating complex passwords. GitHub ensures compatibility and integration with various password management applications to facilitate user adoption and enhance overall security.

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

GitHub has implemented a comprehensive password and passphrase policy for both administrators and users. The policy includes guidelines that prohibit the use of common or easily guessable passwords. GitHub encourages the use of strong, complex passwords or passphrases that meet specific criteria for length, complexity, and uniqueness.

Regular communication and training programs reinforce the importance of adhering to the password policy. GitHub employs mechanisms, such as password complexity requirements and regular password expiration, to ensure that user accounts maintain a high level of security. The organization also encourages the use of multi-factor authentication (MFA) to enhance overall account protection.

Question 12: Are all endpoint logs being ingested by a smart technology that uses threat intelligence and artificial intelligence (AI) based on threat actor activities and heuristics?

GitHub employs an advanced endpoint security solution that includes a smart technology capable of ingesting endpoint logs. This technology leverages threat intelligence and AI-driven algorithms to analyze and detect potential security threats. The system continuously evolves based on threat actor activities and heuristics, enhancing GitHub's ability to identify and respond to emerging security risks in real-time.

Question 13: Do you harden all endpoints and remove everything that is not needed for job functionality?

GitHub follows a rigorous endpoint hardening process. Endpoints are configured to adhere to the principle of least privilege, removing unnecessary components and functionalities that are not essential for job functionality. Regular security audits and reviews ensure that endpoints are hardened to minimize attack surfaces and enhance overall endpoint security.

Question 14: Do you have next-generation anti-malware protection (e.g., managed detection and response [MDR], extended detection and response [XDR], endpoint detection and response [EDR]) on all endpoints that utilize a threat intelligence-based security analytics platform with built-in security context?

GitHub has implemented next-generation anti-malware protection on all endpoints. This includes features such as managed detection and response (MDR), extended detection and response (XDR), and endpoint detection and response (EDR). These solutions leverage a threat intelligence-based security analytics platform with built-in security context, enhancing the organization's ability to detect, respond to, and mitigate advanced threats.

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

GitHub enforces strict access controls to prevent non-enterprise-controlled and unsecured devices from connecting to any part of the network. This is achieved through network segmentation, strong authentication mechanisms, and regular monitoring of connected devices. Unauthorized or non-compliant devices are promptly identified and prevented from accessing GitHub's network.

Question 16: Do all endpoints have personal firewalls for accessing the Internet when not attached to the enterprise network?

All endpoints at GitHub are equipped with personal firewalls, especially when accessing the Internet outside the enterprise network. These firewalls provide an additional layer of protection, helping to secure endpoints against potential threats and unauthorized access, particularly in external or untrusted network environments.

Question 17: Do all endpoints have antivirus software installed that cannot be disabled and is automatically updated when new updates are available?

GitHub ensures that all endpoints have antivirus software installed, and the security settings are configured to prevent users from disabling the protection. Automatic updates are enabled to ensure that the antivirus software stays current with the latest threat definitions and security patches.

Question 18: Do all endpoints have a next-generation anti-malware application installed?

GitHub has deployed next-generation anti-malware applications on all endpoints. These applications use advanced techniques and threat intelligence to proactively identify and mitigate malware threats. Regular updates and continuous monitoring contribute to the effectiveness of the anti-malware solution.

Question 19: Are all logs stored for at least 2 years?

GitHub adheres to a log retention policy that ensures all logs are stored for a minimum of 2 years. This practice aligns with industry best practices and compliance requirements, allowing for historical analysis, forensic investigations, and regulatory compliance.

Question 20: Are all devices generating logs?

GitHub has implemented a comprehensive logging strategy where logs are generated on all devices across its infrastructure. This includes servers, workstations, network devices, and other relevant endpoints. Centralized logging mechanisms are employed to aggregate and manage logs efficiently.

Question 21: Are all logs being reviewed daily by inside and/or outside sources?

GitHub conducts daily log reviews, leveraging both internal resources and, when applicable, external sources. This proactive approach ensures prompt detection of any anomalous activities or security incidents. The review process involves analyzing logs for signs of potential threats, unauthorized access, or other security-related events.

Question 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?

GitHub has established a mature and well-organized cybersecurity incident response framework. The incident response team, whether in-house or in collaboration with third parties, is trained and equipped to thoroughly investigate all incidents. The process includes identification, containment, eradication, recovery, and lessons learned phases.

GitHub's incident response plan is regularly tested through simulations and drills to ensure effectiveness and readiness. Post-incident reviews contribute to continuous improvement, refining response procedures based on lessons learned from each incident.