Final Report

Information Security

Semester Project

Company: Cloudways

Submitted by:

Ayaz Hasan [20k-1044]
Ferdeen Bakht [20k-0219]
Syed Arsalan [20k-1718]

Submitted to:

Dr Abdul Aziz

Department of Computer Science BS(SE-7A)

FAST-NUCES Karachi

Questions and Answers

Training

Do you conduct robust and frequent end user cybersecurity awareness training?
Ans: Yes, however depending on the recruiting and the volume of projects, it may happen on a weekly or annual basis.

2. Have you taught everyone how to securely store passwords or passphrases?
Ans: Indeed, this is a required arrangement as they need to obtain encrypted passwords for whatever place we need them.

3. Do you conduct quarterly anti-phishing, smishing and vishing campaigns?? **Ans**: No because they don't do phishing.

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?
Ans: There is a clause in the contracts they sign with workers stating that they will be responsible for any security breaches. This paragraph states that you are in charge of your security and that you will participate in any inquiry.

Access Control

5. Are all vendor default accounts changed or disabled?
Ans: Yes, the default account needs to be changed, however occasionally, accounts are used for emergencies only they not change default changes. Accounts that are regularly used are updated based on requirements.

6. Are only necessary services, protocols, daemons and functions enabled?
Ans: Initially, they permit the necessary items; occasionally, you may need to provide them further access. Afterward, they use two methods: white testing and black testing. You offer everything you have at the beginning is black testing. White testing will first deactivate everything then you give permits.

7. Is all unnecessary functionality removed or disabled?
Ans: They disable unnecessary functionality from those systems where we have private and confidential data.

8. Are all accounts immediately disabled or deleted upon termination of employment?
Ans: Executive-level accounts are disabled right away, whereas ground level accounts are terminated gradually to give private data time to be retrieved.

9. Are all screen idle times set for 15 minutes, and do they require reauthentication to unlock?
Ans: Although it's not permanent, each person sets its prefer less than fifteen minutes. Reauthentication is necessary since anyone could act in your absence.

End User

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

Ans: Indeed, they use the Key Management System (KMS) programme, which has a master password. Whenever you use a password to get into any account. With the aid of the master password, the passwords are then activated. They use cloud-based for this.

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

Ans; yes, policy are as follow

- Length must be greater the 8
- Use Lowercase, uppercase, special character, and numbers
- No use common password
- If you don't want give your password you can generate random password

End Points

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

Ans: Yes, Cloudways employs smart technology that utilizes threat intelligence and AI for ingesting end point logs. This technology is designed to detect and respond to threats based on threat actor activities and heuristics, enhancing overall security.

13. Do you harden all endpoints and remove everything that is not needed for job functionality?
    Ans: Yes, Cloudways follows a policy of hardening all endpoints by removing unnecessary components that are not essential for job functionality. This helps to minimize potential attack surfaces and strengthens the overall security posture.

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])4 on all endpoints that utilizes a threat intelligence-based security analytics platform with built-in security context?

Ans: Yes, Cloudways has implemented next-generation anti-malware protection on all endpoints. The company utilizes a managed detection and response (MDR) solution with an integrated threat intelligence-based security analytics platform to provide enhanced endpoint detection and response (EDR) capabilities, ensuring a robust defense against evolving threats.

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

Ans: Yes, Cloudways strictly prevents non-enterprise-controlled and unsecured devices from connecting to any part of its network. This practice helps to maintain a secure and controlled environment, reducing the risk of unauthorized access and potential security breaches.

16. Do all end points have personal firewalls for accessing the Internet when not attached to the enterprise network?

Ans: Yes, all endpoints at Cloudways are equipped with personal firewalls for accessing the Internet when not connected to the enterprise network. This additional layer of security helps to protect endpoints from external threats and ensures secure Internet usage.

17. Do all end points have antivirus software installed that cannot be disabled and is automatically updated when new updates are available?

Ans: Yes, all endpoints at Cloudways have antivirus software installed, and it is designed to be nondisabling. The antivirus software is configured for automatic updates, ensuring that endpoint protection is up-to-date with the latest threat definitions for proactive defense.

18. Do all end points have a next generation anti-malware application installed?

Ans: Yes, Cloudways has implemented a next-generation anti-malware application on all endpoints. This additional layer of security complements the antivirus software, providing advanced capabilities to detect and respond to emerging malware threats effectively.

Event Management

19. Are all logs stored for at least 2 years?

Ans: Yes, all logs stored for at least 2 years also the government regulatory authority give you time this is mandatory. Minimum is 1 years.

20. Are all devices generating logs?

Ans: Yes, all devices are producing logs. This is because, in the event of a breach, all events are recorded in the log and will be useful to organization later. However, some devices are unable to create logs, therefore in order to improve speed and avoid storage issues, they destroy them.

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

Ans: all logs being reviewed daily, because some time thieir are attack under the radar. This is inhouse security they the security team for their reviewed logs daily

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?

Ans: Yes, their cybersecurity staff is experienced and professionally run. They have established the hierarchy for that procedure, and the chief operating officer is in charge of establishing the hierarchy and determining how to handle any incidents.

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

Ans: It is mandatory to give employees the tools necessary for their job role only and with limited access to avoid breach of privileges and which can also lead to “privilege escalation attack”.

24. Do you utilize the principle of least privilege?

Ans: Yes, the principle of least privilege is utilized by our organization to prevent employees from gaining access to any sensitive data.

25. Do you deploy a zero-trust model?

Ans: In our critical systems we deploy the zero-trust model but the endpoints like workstation then there we may have, or haven't this model implemented as like your workstation so when it is connected to the VPN it becomes trusted.

26. Do you require multifactor authentication (MFA) for all connections outside of the network?

Ans: Yes, as password cracking is easy nowadays using brute force attack so Multifactor authentication is required for the connections outside the network.

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

Ans: Yes, we use MFA for internal authenticated network users. This is required to ensure that the employees get to know the password of each other they can't access it by using MFA.

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.)

Ans: Yes, it is managed by the authentication server to the database, and it generates a password reset token to quickly conduct a password reset for every account.

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

Ans: Active Directory is properly configured to check for any folders or important documents that they are not comprised it's Secured by applying authentication to allow only the users with the privileged access rights.

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

Ans: For critical systems, the security is monitored actively while for the endpoint systems like websites it is not monitored actively due to the workload the performance can be decreased.

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

Ans: Yes, we have applied deny all rules on our perimeter firewall which uses the concept of white listing to refrain from unlawful events.

32. Is your demilitarized zone (DMZ) secured?

Ans: Yes, we do penetration testing on monthly basis to ensure that DMZ is secured.

33. Has it been ensured that there are no data, databases or stored accounts on the DMZ?
Ans: Checklist is made to ensure which data is accessible using DMZ.

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

Ans: No, Anti- spoofing technology is not implemented because it is the very expensive technology.

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

Ans: IP addresses are blocked by using the firewall to not allow the certain IP addresses to be disclose.

36. Do you segment key infrastructure from other parts of the network with restrictive firewalls (e.g., segmenting WiFi, confidential data, virtual machines and printers away from crown jewels)?
Ans: Yes, Segment key infrastructure is protected using restricted firewalls so that Confidential data and database access is controlled and accessing to the infrastructure is secured by segmenting WiFi.

Cryptography

37. Are procedures defined and implemented to protect cryptographic keys used to protect stored data against disclosure and misuse?

Ans: Yes, procedures are defined and implemented at Cloudways to protect cryptographic keys used for storing data. This includes robust measures to prevent disclosure and misuse, ensuring the security of sensitive information.

38. Are cryptographic keys stored in the fewest possible locations with at least dual custodians?
Ans: Yes, cryptographic keys at Cloudways are stored in the fewest possible locations, and access is controlled by dual custodians. This dual custodian approach adds an extra layer of security and accountability in key management.

39. Do you utilize full disk encryption on all appropriate drives?

Ans: Yes, Cloudways employs full disk encryption on all appropriate drives. This helps safeguard data at rest, enhancing overall data security and mitigating the risk of unauthorized access to stored information.

40. Do you use secure encryption in motion-at least Transport Layer Security (TLS) 1.1 or higher?

Ans: Yes, Cloudways uses secure encryption in motion, with at least Transport Layer Security (TLS) 1.1 or higher. This ensures that data transmitted over the network is encrypted, protecting it from interception and unauthorized access.

41. Is all nonconsole administrative access encrypted using strong cryptography?

Ans: Yes, all non-console administrative access at Cloudways is encrypted using strong cryptography. This practice enhances the security of administrative interactions, preventing unauthorized parties from gaining access to sensitive systems and information.

Threats

42. Do you perform periodic targeted threat hunts?

Ans: No, Cloudways does not perform periodic targeted threat hunts. The company relies on other security measures to safeguard its systems.

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?

Ans: Yes, Cloudways does ingest current threat intelligence from multiple sources and has procedures in place to implement rapid countermeasures based on the received threat intelligence. This helps enhance overall cybersecurity.

44. Does it include performing routine dark web reconnaissance to learn what exists on the dark web about your brand and enterprise structures?

Ans: No, Cloudways does not routinely perform dark web reconnaissance to monitor information about its brand and enterprise structures on the dark web. The focus is on other security measures.

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

Ans: Yes, Cloudways closely monitors all vendor and third-party supply-chain connections to ensure compliance and address any untoward issues promptly. This proactive approach helps mitigate potential security risks.

Testing

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

Ans: No, Cloudways does not conduct at least one penetration test annually performed by a third party. The company relies on other security measures to maintain the integrity of its systems.

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?

Ans: Yes, Cloudways routinely conducts vulnerability scans and strives to 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. This ensures a timely response to potential security risks.

48. Do you routinely scan your Internet-facing infrastructure for penetration and vulnerabilities?
    Ans: Yes, Cloudways routinely scans its Internet-facing infrastructure for penetration and vulnerabilities, maintaining a proactive stance towards identifying and addressing potential security issues.

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

Ans: No, Cloudways does not perform an annual business impact analysis/risk analysis report with insider and outside auditors. The company may focus on other risk management practices to ensure overall security and compliance.

Physical

52. Are processes and mechanisms for restricting physical access to servers, consoles, backup and network equipment in place and properly safeguarded?

Ans: All of the network equipment is protected, and RFID is utilised for maintenance to determine which items are in operation and which are in storage. They are physically isolated.

53. Are physical and/or logical controls implemented to restrict the use of publicly accessible network jacks within the facilities?

Ans: Yes there are physical and/or logical controls. Since police are defined thing are authorise and are properly approved. Untested things are not allowed.

Plans

54. Do you have a good cyberincident response plan (CIRP) that is reviewed and practiced yearly?
Ans: Cloudways has a well-established Cyber Incident Response Plan (CIRP) that undergoes regular reviews and is practiced annually through tabletop exercises, ensuring preparedness for potential cyber incidents.

55. Do you have playbooks with technical instructions for handling common cybersecurity incidents?
Ans: No, Playbooks for incidents may face challenges.

Inventory

56. Do you have thorough diagrams of the entire network, including WiFi?
Ans: Yes, cloudways possesses comprehensive network diagrams, including WiFi infrastructure, providing a clear overview of the entire network architecture.

57. Do you have a complete inventory of all assets that includes business criticality levels, owners, co-owners and restoration? Does this inventory include instructions with time periods to recover?
Ans: Cloudways maintains a complete inventory of all assets with business criticality levels, owners, co-owners, and restoration instructions. This ensures a structured approach to asset management and recovery.

58. Do you have a full set of data flow diagrams?
Ans: Cloudways has a full set of data flow diagrams, facilitating a thorough understanding of how data moves within the organization's systems.

Data Management

59. Do you utilize file integrity monitoring (FIM) of the crown jewels of the organization? Ans: FIM of critical data may vary.

60. Is storage of confidential data kept to a minimum and securely deleted after it's no longer needed?
Ans: Cloudways follows a policy of minimizing and securely deleting confidential data once it's no longer needed, adhering to best practices for data protection and privacy.
61. Do you require data classification throughout the network?
Ans: Yes, Cloudways implements data classification throughout the network to ensure proper handling and protection of sensitive information.

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

Ans: Yes, Cloudways deploys both network and cloud-based Data Loss Prevention (DLP) programs to safeguard confidential data across various environments.

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

Ans: Yes, Cloudways implements measures to prevent confidential data from being copied to external devices and restricts the attachment of external devices to endpoints to enhance security.

Software Development

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

Ans: Yes, Cloudways has well-defined processes and mechanisms for developing and maintaining secure systems and software, ensuring that security standards are understood and followed.

65. Are software engineering techniques or other methods defined and in use by software development personnel to prevent or mitigate common software attacks and related vulnerabilities in all software?

Ans: Yes, Cloudways employs software engineering techniques and methods to prevent and mitigate common software attacks, enhancing the overall security of its software applications.

66. With regard to public-facing web applications, are new threats and vulnerabilities addressed on an ongoing basis?

Ans: Yes, Cloudways addresses new threats and vulnerabilities in public-facing web applications on an ongoing basis, ensuring a proactive approach to security.

67. Are these applications protected against attacks?

Ans: Yes, Cloudways protects its public-facing web applications against various attacks, implementing security measures to safeguard user data and system integrity.

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

Ans: Yes, Cloudways separates preproduction environments from production environments and enforces this separation with access controls to minimize the risk of unauthorized access or changes to critical systems.

Mobile Devices

69. Are all mobile devices governed by effective mobile device management (MDM) policies?
Ans: Mobile device governance may vary.

70. Do you disallow any connectivity of mobile devices not controlled by enterprise security mechanisms?
Ans: Disallowing connectivity may be challenging.
