Risk in the Workplace

Users

Incident Handling

Graded Assessments

Video: Final Assessment
22 sec

Quiz: Creating a Company Culture for Security
10 questions

Quiz: Creating a Company Culture for Security - Design Document
1 question

Reading: Final Project - Sample Submission
10 min

Discussion Prompt: Connect with Google IT Support Certificate graduates
10 min

Course Wrap Up

Congratulations! You passed!

Grade received 100%

Latest Submission Grade 100%

To pass 80% or higher

Go to next item

Creating a Company Culture for Security - Design Document

Quiz • 30 min

Submit your assignment

Due Jul 2, 11:59 PM +08 Attempts 3 every 24 hours

Try again

Receive grade

To Pass 80% or higher

Your grade
100%

View Feedback

We keep your highest score

Like Dislike Report an issue

1. **Overview**: Now that you're super knowledgeable about security, let's put your newfound know-how to the test. You may find yourself in a tech role someday, where you need to design and influence a culture of security within an organization. This project is your opportunity to practice these important skillsets.

1 / 1 point

Assignment: In this project, you'll create a security infrastructure design document for a fictional organization. The security services and tools you describe in the document must be able to meet the needs of the organization. Your work will be evaluated according to how well you met the organization's requirements.

About the organization: This fictional organization has a small, but growing, employee base, with 50 employees in one small office. The company is an online retailer of the world's finest artisanal, hand-crafted widgets. They've hired you on as a security consultant to help bring their operations into better shape.

Organization requirements: As the security consultant, the company needs you to add security measures to the following systems:

- An external website permitting users to browse and purchase widgets
- An internal intranet website for employees to use
- Secure remote access for engineering employees
- Reasonable, basic firewall rules
- Wireless coverage in the office
- Reasonably secure configurations for laptops

Since this is a retail company that will be handling customer payment data, the organization would like to be extra cautious about privacy. They don't want customer information falling into the hands of an attacker due to malware infections or lost devices.

Engineers will require access to internal websites, along with remote, command line access to their workstations.

Grading: This is a required assignment for the module.

What you'll do: You'll create a security infrastructure design document for a fictional organization. Your plan needs to meet the organization's requirements and the following elements should be incorporated into your plan:

- Authentication system
- External website security
- Internal website security
- Remote access solution
- Firewall and basic rules recommendations
- Wireless security
- VLAN configuration recommendations
- Laptop security configuration
- Application policy recommendations
- Security and privacy policy recommendations
- Intrusion detection or prevention for systems containing customer data

Organization: Fictional Online Widget Retailer

1. Authentication System:
- Implement a robust authentication system to ensure secure access to all systems.
- Utilize strong password policies, enforcing complex passwords and regular password changes.
- Enable two-factor authentication for all user accounts.
- Implement account lockout policies to prevent brute-force attacks.
- Consider implementing a single sign-on (SSO) solution for ease of use and enhanced security.
2. External Website Security:
- Implement Secure Sockets Layer/Transport Layer Security (SSL/TLS) encryption for the external website.
- Utilize a web application firewall (WAF) to protect against common web-based attacks such as SQL injection and cross-site scripting (XSS).
- Regularly scan the website for vulnerabilities using automated web vulnerability scanners.
- Implement a robust intrusion detection and prevention system (IDPS) to monitor and block malicious traffic.
3. Internal Website Security:
- Implement access controls and role-based permissions for the internal intranet website.
- Utilize SSL/TLS encryption for secure communication between employees and the internal website.
- Regularly patch and update the internal website's underlying software to address any security vulnerabilities.
- Conduct regular security audits and penetration testing to identify and address any potential weaknesses.
4. Remote Access Solution:
- Implement a Virtual Private Network (VPN) solution for secure remote access for engineering employees.
- Utilize strong encryption protocols (e.g., IPSec, SSL/TLS) to protect data transmitted over the VPN.
- Implement multi-factor authentication for remote access, combining something the user knows (password) with something the user has (token or app-based authentication).
5. Firewall and Basic Rules Recommendations:
- Deploy a next-generation firewall (NGFW) to provide advanced threat protection and granular control over network traffic.
- Configure the firewall to block all incoming connections by default and only allow necessary services.
- Implement strict egress filtering to prevent data exfiltration attempts.
- Regularly update and patch the firewall to ensure it is protected against the latest threats.
6. Wireless Security:
- Implement strong encryption (WPA2/WPA3) and secure authentication (WPA2-Enterprise) for the wireless network.
- Enable network segmentation by implementing separate VLANs for guest access and internal network access.
- Regularly monitor wireless network traffic for any signs of unauthorized access or suspicious activity.
7. VLAN Configuration Recommendations:
- Implement VLANs to segregate network traffic and enhance security.
- Create separate VLANs for different departments, such as Engineering, Sales, and Finance, to restrict access to sensitive resources.
- Implement access control lists (ACLs) to control traffic flow between VLANs and enforce security policies.
8. Laptop Security Configuration:
- Implement full disk encryption (FDE) to protect data in case of theft or loss.
- Enforce strong password policies and screen lock timeouts on laptops.
- Install and regularly update anti-malware and endpoint protection software on all laptops.
- Implement remote wipe capabilities to ensure data can be securely erased from lost or stolen laptops.
9. Application Policy Recommendations:
- Implement a strict application whitelisting policy to prevent unauthorized software installations.
- Regularly update and patch all applications and operating systems to address known vulnerabilities.
- Conduct regular security assessments and vulnerability scanning of all applications to identify and mitigate any potential risks.
10. Security and Privacy Policy Recommendations:
- Develop comprehensive security and privacy policies that outline acceptable use, data protection, incident response, and compliance requirements.
- Educate employees about security best practices and provide regular training on cybersecurity awareness.
- Implement a robust incident response plan to address and mitigate security incidents

✓ **Correct**

Thank you for your submission!

A great submission should include:

- Two authentication system requirements, like Security Key-based multifactor or OTP-based multifactor, and some kind of centralized authentication system (e.g., LDAP or Active Directory).
- A description of HTTPS.
- Recommendation for both a VPN service and a reverse proxy solution.
- A description of two or more types of firewall services (e.g., implicit deny rule, remote access, websites).
- Requirement for 802.1X.
- A description of four VLAN requirements, including Engineering VLAN, Sales VLAN, Infrastructure VLAN, and Guest VLAN.
- Three laptop security requirements, including FDE recommendations, antivirus recommendation, and a binary whitelisting recommendation.
- Requirement for a software update requirement policy and a requirement for restrictions on the types of applications permitted.
- Recommendations for rules protecting access to user data and for rules protecting the storage of user data.
- A description of four of the following security policy recommendations: passwords requiring a minimum of 8 characters; passwords requiring special characters; requiring periodic password changes > 6 months; and some form of mandatory security training for users.
- A requirement for a NIPS/NIDS on the network for customer data and a requirement for HIPS/HIDS on systems containing customer data.