Congratulations! You passed!

Grade received 100% | Latest Submission Grade 100% | To pass 80% or higher

Go to next item

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

- Single Sign-On using AD for authentication on Intranet, Productivity Apps (Teams, Office 365, OneDrive), Email, User Account, etc - Sync with RADIUS/OpenLDAP
- Use Firewall from Big 5 brands.
- Allow commonly used ports such as SSH, HTTP/S, etc. block access to unwanted IP address (autom. from Firewall config), disable Torrent access.
- To have a secure network there should be several VLAN implemented : for server, for printer & workstation, iot, experiments, for public access (smartphone, tablet, etc)
- Provide VPN access with SSO.
- Set Wireless VLAN as well for Office Laptop (same VLAN with printer & workstation) & Personal Smartphone/Tablet. Auth using WPA Enterprise combine with SSO/Radius
- Implement MS Endpoint to control all workstations/laptops/smartphone/tablet with all of its apps policy
- Implement also MS SCCM/WSUS
- Laptop & Workstation all have same config by using same OS image with necessary drivers and applications. this will significantly reduce installation time. Both have Bitlocker activated. Join into domain as well on MDM on Microsoft Endpoints. VPN Client installed into laptop
- Define GPO for different type of users.
- Implement IPS&IDS on network.
- Disable user access immediately after the leave organization.

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.