SEC410 Web and Data Structured External Assignment (SEA) Project Paper

---

You have been hired as consultants to design and implement a security initiative for an expanding global eCommerce corporation with two websites and locations in New York and London. There are currently about 300 employees in the company.

In the next three months, the corporation will be acquiring another company in a different line of business with plans to offer products for sale online. This new company is in Paris and will have a Research and Development (R&D) and a Sale Dept., with 150 to 200 employees. They will create new products and sell them online.

Part of your role would be to recommend the best way to integrate both environments. However, not much information is available about the IT setup for the company being acquired. The other company might even have a mix of operating systems – it is unclear since the IT staff in that company is not very communicative.

Some critical staff members in the other company are not happy with the upcoming merger and have sworn to be as uncooperative as possible. The Network Manager for the other company has a complex personality. There are plans to fire him, but unfortunately, he is the only one who knows the network architecture entirely. Furthermore, he is unwilling to share. You must find out everything about the new environment and propose specifics on integrating both Enterprise Level environments seamlessly.

In the initial conversation with executives of the global company, you realize that the company does not have a security policy. After much discussion, they have agreed that you should develop a detailed security policy customized for the company.

In a follow-up meeting with the executives and IT staff of the global corporation, you are also assigned the task of identifying the following:

- Two (2) security audit tools (vulnerability/web scanners).
- Two (2) intrusion detection systems.
- Two (2) network firewall products that would be suitable for the global company.
- Two (2) automated network asset inventory tools to know what exists at the new location and determine what will be integrated into the merged company.
- You are to test and describe the features of selected security solutions.
- Indicating (a) which you prefer and (b) providing a convincing rationale for why you prefer a specific solution in each category. In other words, you

are to evaluate two products for each category and recommend one, giving the reasons for your choice.

Salient points: The new corporate acquisition will increase the total number of computers under your IT department's care to about 1,000 computers and network devices. The exact number is not precise: Even the management at the other company is not sure of the number of systems in that network because of the difficulty in finding the specifics about the company being acquired.

It appears the acquired company runs a mixture of a peer-to-peer network and the domain model. Part of the decision you would have to make would be how the integrated environments would be networked: You have the discretion to come up with the design and budget (subject to approval, of course) for the overall security initiative and covering:

- The security policy.
- Network audit to determine what devices and data.
- Seamless integration between the merging companies.
- Recommendation for IDS system(s).
- Recommendations for security audit tools (web/vulnerability scanners).
- Recommendations for network firewall device(s).

Deliverables for the Project:

1. The Security Policy Document (You can adapt an Acceptable Use Policy document from www.sans.org)
2. Plus, a minimum of eight-page (8) paper in APA format in Microsoft Word, double-spaced describing how you would go about implementing the overall security initiative for the company.
   - A 1-page summary of your overall strategy
   - A 1-page of network audit to determine what devices and data
   - A 1-page of information security-related recommendations for integrating both corporate enterprise environments
   - A 1-page for the Intrusion Detection System (evaluate two different products and recommend one, giving the reasons for your choice). Consider HIDS/NIDS & IDPS.
   - A 1-page for the web/vulnerability scanners (evaluate two different products and recommend one, giving the reasons for your choice
   - A 1-page for the network firewall devices (evaluate two different products and recommend one, giving the reasons for your choice)
   - A 1-page of your overall conclusions demonstrating your grasp of information security best practices and current trends
   - A Microsoft Visio or similar diagram network diagram of all components in a logical layout to show how the deliverables are related
   - A 1-page of Scholar/Product APA references
3. A 10-minute PowerPoints or similar audiovisual presentation of your project precise

Acceptable Use Policy of XXX Corp.

1. Overview: The publication of the Acceptable Use Policy (AUP) by XXX Corp. is not intended to impose restrictions that contradict the company's culture of openness, trust, and integrity. The AUP aims to protect employees, partners, and the organization from unlawful or detrimental actions, whether intentional or unintentional. This policy applies to various systems such as internet, intranet, extranet, computer equipment, software, operating systems, storage media, and network accounts. These systems are XXX Corp.'s property and must be used for legitimate business purposes during normal operations.

Maintaining security is a collective effort involving everyone associated with XXX Corp. Each user must be familiar with the AUP's guidelines and ensure their actions align with them. By adhering to the AUP, XXX Corp. creates a secure and productive computing environment while upholding its core values.

2. Purpose: The purpose of the Acceptable Use Policy (AUP) is to define the appropriate use of computer equipment at XXX Corp. It safeguards both employees and the company from risks associated with inappropriate computer use, including virus attacks, network compromises, and legal consequences.

3. Policy:

3.1 General Use and Ownership

1. **Data Ownership and Confidentiality:**
    - All data created on XXX Corp.'s systems remains its property.

- While confidentiality is aimed to be maintained, users should understand that data stored on XXX Corp.'s network devices might not be entirely private.

2. **Personal Use of Internet/Intranet/Extranet Systems:**
    - Employees should use good judgment regarding personal use.
    - Individual departments can set guidelines for personal use.
    - If no specific policies exist, employees should consult their supervisor for guidance.
3. **Protection of Sensitive Information:**
    - Encryption of sensitive information is recommended.
    - Refer to XXX Corp.'s Information Classification Policy for guidance.
4. **Monitoring of Equipment and Network Traffic:**
    - Authorized personnel may monitor equipment, systems, and network traffic for security and maintenance purposes.
5. **Network and Systems Auditing:**
    - XXX Corp. may conduct periodic audits to ensure policy compliance.

3.2 Security and Proprietary Information

1. **Classification of Information:**
    - Information on Internet/Intranet/Extranet systems should be classified as confidential or non-confidential.
    - Employees must prevent unauthorized access to this information.
2. **Password Security:**

- Passwords must be kept secure and not shared.
- Review XXX Corp.'s Password Policy for guidance.

3. **Secure Workstations:**
    - Password-protected screen savers or logging off when unattended are required.
4. **Laptop Security:**
    - Portable computers must be protected according to the Laptop Security Policy.
5. **Virus Scanning:**
    - All devices connected to XXX Corp.'s networks need virus-scanning software with a current database.
6. **Caution with Email Attachments:**
    - Extreme caution must be exercised when opening attachments from unknown senders.

3.3 Unacceptable Use Engaging in illegal activities, unauthorized access, distribution of copyrighted materials, introducing malicious software, harassment, network intrusion, and activities compromising security are strictly prohibited. Violators will face disciplinary action.

3.4 System and Network Activities Several activities are prohibited:

1. Unauthorized access, copying, or dissemination of classified information.
2. Installing copyrighted software without an active license from XXX Corp. is prohibited.

3. Installing software without approval and virus scanning is not allowed.
4. Introducing malicious programs is strictly forbidden.
5. Sharing account passwords or allowing unauthorized access is prohibited.
6. Security breaches, network disruptions, and unauthorized access are not allowed.
7. Unauthorized port or security scanning is prohibited.
8. Unauthorized network monitoring is not allowed.
9. Bypassing security measures is strictly forbidden.
10. Denying service to users is not allowed.
11. Interfering with user terminal sessions is prohibited.

3.5 Email and Communication Activities

- Employees must represent XXX Corp. responsibly on the Internet.
- Unsolicited emails, harassment, unauthorized header information, chain letters, and unauthorized email use are prohibited.

3.6 Blogging and social media

- Blogging and social media usage must adhere to the policy.
- Confidential information, image, personal opinions, and intellectual property must be handled responsibly.

4. Enforcement Violations may result in corrective action, termination, or legal consequences.

Implementing a Comprehensive Security Initiative for Integrated Enterprise Environments

Introduction

In the dynamic and interconnected digital landscape, the security of corporate enterprise environments has become an imperative concern. As organizations expand and integrate with new entities, the complexity of ensuring a seamless and secure environment magnifies. This article presents a comprehensive security initiative plan that addresses the unique challenges posed by an expanding global eCommerce corporation and its acquisition of a new entity. The plan encompasses strategic security policies, meticulous network audits, seamless integration strategies, evaluation and recommendations for intrusion detection systems (IDS), web/vulnerability scanners, and network firewall devices. Synthesizing insights from reputable sources in the field, this article aims to provide a coherent and robust security strategy that aligns with the organization's values and growth trajectory.

Summary of Overall Security Strategy

Creating a cohesive and effective security strategy requires a deep understanding of the organization's objectives and the ever-evolving threat landscape. It is imperative to craft a security policy that not only safeguards the organization's assets but also aligns with its broader business objectives. As highlighted by Musthaler (2010), security policies should be customized to resonate with the organization's mission and values. This approach not only ensures compliance but also establishes security as an enabler

rather than an impediment. Such alignment fosters a security-conscious culture that emphasizes the importance of every employee in maintaining the organization's security posture ("10 Strategic Security Initiatives for Every Organization," 2010).

Considering the dynamic nature of cyber threats, IANS Faculty (2021) emphasizes the significance of the human factor in security. Acknowledging that cybersecurity is a collective responsibility, organizations should prioritize user awareness and education. Employee understanding of security protocols and active participation can significantly enhance the organization's defense against cyber threats. Additionally, during integration processes, open communication plays a pivotal role in addressing potential resistance and fostering a collaborative environment ("Three Security Initiatives to Consider in 2022," 2021).

Data protection and network segmentation emerge as essential components of a comprehensive security strategy. In a world dominated by data breaches, safeguarding sensitive information is paramount. The insights from VAST (2023) underscore the organization's responsibility in this regard. Prioritizing encryption and implementing robust access controls not only secures data but also aligns with the principle of proactive data stewardship. By considering encryption practices, organizations demonstrate their commitment to securing their most asset ("Six Essential Cybersecurity Initiatives to Protect Your Business in 2023," 2023).

The integration of third-party vendors and partners cannot be overlooked in the pursuit of comprehensive security. As articulated by the Federal Communications Commission (FCC), vendor assessment and risk management should be integral to the

security strategy. A holistic risk management approach that extends beyond the organization's boundaries ensures that potential vulnerabilities are identified and addressed, thus enhancing overall security ("Cybersecurity for Small Businesses," n.d.).

Network Audit: Laying the Foundation

A network audit serves as the foundation of a seamless integration process. A meticulous examination of the network landscape helps organizations gain insights into devices, data flows, vulnerabilities, and security controls. This comprehensive audit involves several key components:

1. **Device Inventory and Configuration:** Thoroughly cataloging all devices in the network landscape, including servers, workstations, routers, switches, printers, and IoT devices. This inventory encompasses hardware specifications, operating systems, patch levels, and installed applications.
2. **Data Mapping and Flow Analysis:** Tracing the pathways of sensitive information within the network. Mapping data sources, destinations, storage locations, and interactions helps identify potential vulnerabilities and unauthorized access points.
3. **Access Controls and User Authentication:** Evaluating access controls and user authentication mechanisms. This step involves assessing user roles, permissions, and authentication methods across systems to ensure proper access rights and minimize the risk of unauthorized data exposure.
4. **Network Segmentation and Firewalls:** Analyzing network segmentation to isolate critical assets and prevent lateral movement during

security incidents. Additionally, examining firewall configurations verifies protection against external threats.

5. **Vulnerability Assessment:** Identifying security weaknesses, unpatched systems, and potential entry points for attackers through vulnerability scanning. This analysis guides patch management efforts and proactive risk mitigation.

6. **Logging and Monitoring:** Assessing the effectiveness of logging and monitoring mechanisms for network activities. This evaluation ensures real-time threat detection, incident response readiness, and the availability of actionable insights.

7. **Encryption and Data Protection:** Identifying encryption practices for data security in transit and at rest. This evaluation ensures compliance with encryption standards and best practices for protecting sensitive information.

8. **Third-Party Integrations:** Assessing the security posture of third-party vendors and partners. This analysis is aligned with the organization's commitment to transparency and holistic risk management.

By conducting a comprehensive network audit, organizations lay the groundwork for a successful integration process. This audit provides valuable insights for informed decision-making, risk mitigation, and a robust security posture. As highlighted by resources such as N-able's guide on network audits ("How to Perform a Network Audit: A Step-By-Step Guide," 2020) and Enterprise Networking Planet's insights on the subject

("What is a Network Audit?" 2022), a thorough network audit is integral to effective cybersecurity strategies.

Intrusion Detection Systems: Navigating Threat Landscapes

Intrusion Detection Systems (IDS) play a pivotal role in identifying and mitigating cyber threats within network environments. The evaluation and selection of the appropriate IDS solution can significantly impact an organization's security posture.

Two prominent IDS solutions, Suricata and Snort, warrant examination to determine the optimal choice for the organization's integrated environments.

Suricata: Suricata stands out for its high-performance capabilities, offering multi-threading support, protocol analysis, and signature matching. With the ability to function as both an IDS and an Intrusion Prevention System (IDPS), Suricata provides a dynamic approach to threat detection.

Snort: Snort, an open-source IDS solution, boasts versatility through customizable rules for signature-based and anomaly-based detection. Its active community support ensures regular rule set updates and adaptability to emerging threats.

Recommendation: Suricata is recommended due to its high-performance detection, dynamic capabilities, advanced signature matching, and ability to transition from detection to prevention. These features align well with the organization's need for proactive threat response.

Web/Vulnerability Scanners: Unveiling Security Weaknesses

Web and vulnerability scanners are indispensable for identifying security weaknesses within applications and systems. Evaluating two prominent solutions, Acunetix and OWASP ZAP, is essential for informed decision-making.

Acunetix: A commercial solution with comprehensive scanning capabilities, Acunetix excels in identifying a wide range of vulnerabilities. Its vulnerability knowledge base, automated scanning, and integration with development tools enhance its utility.

OWASP ZAP: An open-source solution known for its versatility and active community support. ZAP offers automated and manual testing options, making it a flexible choice for identifying security issues.

Recommendation: Acunetix is recommended due to its comprehensive scanning capabilities, extensive vulnerability knowledge base, and integration with development tools. Its commercial offering ensures accurate vulnerability detection and efficient remediation.

Network Firewall Devices: Safeguarding Network Traffic

Network firewall devices are pivotal for maintaining the security and integrity of network traffic. Evaluating Cisco ASA and Palo Alto Networks Firewall helps determine the optimal choice for the organization's integrated environments.

Cisco ASA: A robust and scalable solution, Cisco ASA encompasses firewall, VPN, and advanced threat protection. Its established reputation and comprehensive security services make it a preferred choice.

Palo Alto Networks Firewall: A next-generation firewall offering advanced threat prevention and application visibility. Its emphasis on user-based policies, integration with threat intelligence, and sandboxing capabilities positions it as a contender.

Recommendation: Palo Alto Networks Firewall is recommended due to its advanced threat prevention, application visibility, user-based policies, integration with threat intelligence, and proactive security approach.

Conclusion: A Unified and Secure Environment

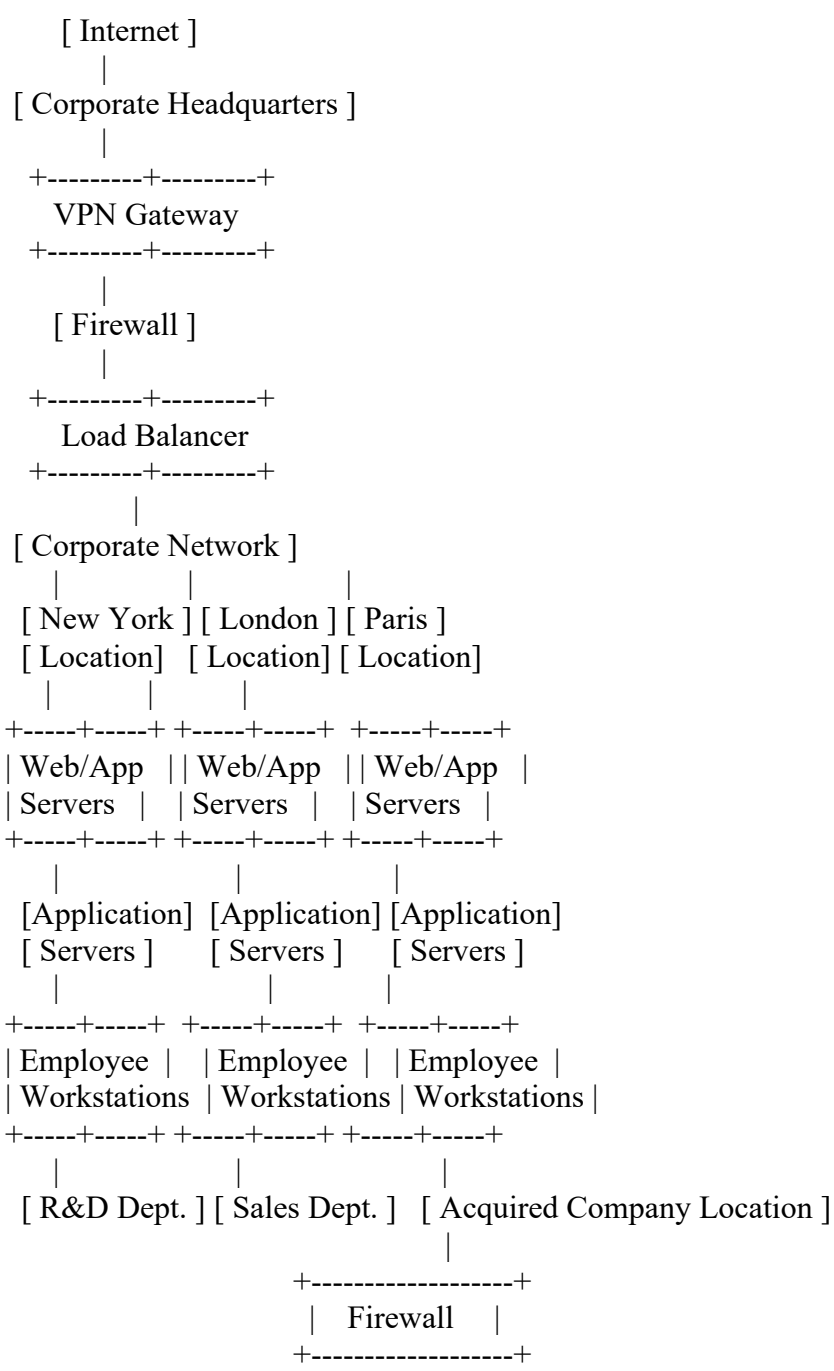
In conclusion, crafting a comprehensive security initiative plan for integrated enterprise environments requires a balanced approach. By aligning security policies with business objectives, fostering cross-functional collaboration, safeguarding data, and integrating robust security tools, organizations create a resilient and secure environment. Drawing insights from industry thought leaders, this plan encapsulates the essence of proactive and holistic cybersecurity.

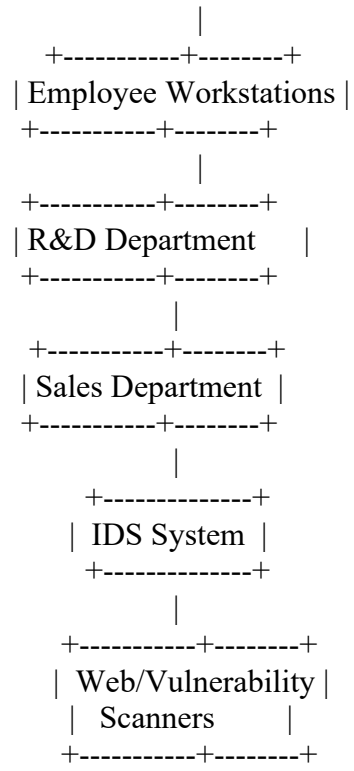
Through meticulous network audits, strategic security policies, and the implementation of advanced tools, organizations ensure seamless integration, bolster defense mechanisms, and create a collaborative and secure culture. This approach aligns with the values of the organization, embraces emerging trends, and safeguards against the ever-evolving threat landscape.

Ultimately, the success of a security initiative plan hinges on its adaptability, alignment with organizational goals, and proactive response to emerging threats. By

embracing this comprehensive plan, organizations can navigate the intricate realm of integrated enterprise environments with confidence, ensuring a secure, collaborative, and resilient future.

The Network Diagram:





Explanation:

- VPN Gateway connects Corporate HQ to the Acquired Company.

- Firewall protects Corporate HQ and Acquired Company networks.

- Load Balancer distributes traffic across New York, London, and Paris locations.

- Corporate Network is the internal network of Corporate HQ.

- Web/App Servers host online platforms and applications.

- Application Servers support specific business applications.

- Employee Workstations are individual computers.

- R&D and Sales Departments are part of the Acquired Company.

- IDS System monitors network traffic for intrusion detection.

- Web/Vulnerability Scanners identify potential vulnerabilities in systems.

References

Alireza Shojaifar, Samuel A. Fricker. (2023) Design and evaluation of a self-paced cybersecurity tool. Information & Computer Security 41.

Alex Moriarty (Dec 31, 2022). Suricata vs. Snort: Similarities and Differences. Retrieved from https://www.netgate.com/blog/suricata-vs-snort.

Federal Communications Commission, Cybersecurity for Small Businesses. Retrieved from https://www.fcc.gov/communications-business-opportunities/cybersecurity-small-businesses.

IANS Faculty (Dec 2, 2021). Three Security Initiatives to Consider in 2022. Retrieved from https://www.iansresearch.com/resources/all-blogs/post/security-blog/2021/12/02/three-security-initiatives-to-consider-in-2022.

Linda Musthaler (Feb 19, 2010). 10 strategic security initiatives for every organization. Retrieved from https://www.networkworld.com/article/2244946/10-strategic-security-initiatives-for-every-organization.html.

N-able (Oct 01, 2020). How to Perform a Network Audit: A Step-By-Step Guide. Retrieved from https://www.n-able.com/blog/how-to-perform-network-audit.

PeerSpot (2023), Acunetix vs OWASP Zap comparison. Retrieved from https://www.peerspot.com/products/comparisons/acunetix_vs_owasp-zap.

pp_pankaj, Intrusion Detection System (IDS), retrieve from https://www.geeksforgeeks.org/intrusion-detection-system-ids/.

Susnigdha Tripathy (Dec 01, 2022) What is a Network Audit? Retrieved from https://www.enterprisenetworkingplanet.com/data-center/network-audit/.

VAST (Jan 4, 2023). Six Essential Cybersecurity Initiatives to Protect Your Business in 2023. Retrieved from https://vastitservices.com/blog/six-essential-cybersecurity-initiatives-to-protect-your-business-in-2023/.

Xuping Huang, Shunsuke Mochizuki, Akira Fujita, Katsunari Yoshioka. (2023) Simulating and Estimating the Effectiveness of Security Notification by ISP to Malware-Infected Users. Journal of Information Processing 31:0, pages 165-173. https://www.geeksforgeeks.org/intrusion-detection-system-ids/