**Getting Started Task 2 Template**

Use the template outline below to capture the rubric requirements and key points and to serve as your task report. After you have captured the appropriate data, massage each section into the required number of paragraphs and ensure you have captured all the required points highlighted.

**A. WLAN Vulnerabilities**

**First vulnerability for WLAN**

Evil Twin - "An evil twin attack is a spoofing cyberattack that tricks a user into connecting to a fake Wi-Fi access point that mimics a legitimate network". (Panda Security, Many Evil Twin attacks involve a captive portal, designed to mimic the captive portal login page of the original WLAN. This allows malicious attackers to harvest credentials. When an Evil Twin attack is used on a corporate WLAN the attacker is able to harvest domain credentials, they are also able to monitor traffic that is being passed through the Evil Twin.

**Second vulnerability for WLN**

Denial of Service (DoS) – “WLAN and mobile networks are vulnerable to both network-based DoS attacks and those created specifically to attack the inherent weaknesses of radio-based systems”. (Doherty, 2021) A denial of service can quickly bring an organization to a stop and prevent them from conducting business.

**B Mobile Vulnerabilities**

**First vulnerability for Mobile devices**

Wireless Phishing – “Phishing involves sending fame emails or SMS messages to a target in an attempt to get the victim to click a link that will take them to a fraudulent website”. (Doherty, 2021) Mobile phishing has been increasingly beneficial for attackers as URL obfuscation and shortening are increasingly difficult to detect. Due to the smaller screen size on phones users are less likely to scrutinize the full URL prior to clicking on links. This is quickly exacerbated by an organization with a B.Y.O.D cellular policy due to inconsistent mail application usage, spam filtering, and general lack of reliance on enterprise email security products generally used on an organizations network.

**Second vulnerability for Mobile devices**

Browser Exploits – “Specifically targeting mobile users, these exploits take advantage of vulnerabilities on mobile web browsers”. (Doherty, 2021) Increasingly difficult to protect against in an organization that follows a B.Y.O.D cellular policy. Less ability to manage updates or mandate an update schedule. This leaves mobile users vulnerable to exploitation by simply just visiting an unsafe site.

**C. Mitigation**

**First Mitigation for WLAN**

And steps, tools, and documentation (citation)

Evil Twin

To mitigate against an Evil Twin attack businesses that provide Wi-Fi to their employees and customer are advised to implement a “Wireless Intrusion Prevention System” (WIPS). This will assist in detecting the presence of an evil twin access point and significantly reduce any managed devices from connecting to one. (Orsi, 2018). An example of a WIPS is WatchGuard, which has a variety of methods for configuration, including acting as a hybrid access point and monitoring sensor at the same time. documentation and configuration can be found on the Guardsite website. (Watchguard, 2022)

**Second Mitigation WLAN**

And steps, tools, and documentation

Denial of Service

To mitigate the risk of a denial of service attack the SANS institute recommends that organizations deploy a WLAN Intrusion Detection System (WIDS). This intrusion detection system can be leveraged for logging and alerting however does not have the capability of stopping the attack. To further mitigate against denial-of-service attacks it is highly recommended that organizations use three or more sensors appropriately placed to assist with triangulation methods, this will assist in detecting the source of transmission. (“2108.pdf On”)

**First Mitigation for Mobile devices**

And steps, tools, and documentation

Wireless Phishing

To mitigate the risk against phishing on mobile devices, an email security software such as Proofpoint, Cisco’s Iron Ports, or Symantec’s Email Security.Cloud is recommended. Tools such as these are designed to perform advanced scanning of emails prior to delivery through the email systems. The further configuration of DKIM, SPF, and DMARC all play a vital role in reducing the number of malicious emails delivered to end users. In addition to reducing the over-all quantity of malicious emails, these services tend to offer a real-time scanner of links that are included in the in the emails. These tools can be configured to utilize a content engine, block/allow lists, and RBL checking. Proofpoint uses an advanced AI and Machine learning detection engine named “Advanced BEC Defense”, this detection engine analyzes multiple message attributes such as; message headers, sender IP addressing, and message body, applying logic to determine if the email is a threat. (“Email Protection - Email Security Solutions | Proofpoint US”)

**Second Mitigation for Mobile devices**

And steps, tools, and documentation

Browser Exploits

To mitigate the impact of browser exploits it is recommended that all servers have been supplied with a digital certificate for SSL/TLS and enforce HTTPS instead of allowing HTTP. This ensures the connection is encrypted prior to any critical data being provided. It is also recommended that any device that is being used for corporate function is configured to block “pop-ups” as this is the primary vector of attack for browser exploitation. (Doherty, 2021) It is also recommended to remove any unused/unwanted application, to check application permissions, and practice due diligence.

**D. Preventative Measures**

**In this section, you need to list preventive measures that will increase the security posture of the WLAN and mobile environment. You need to list a preventative measure for EACH**

**Preventative Measure for WLAN**

Description of measure and narrative (NIST 800-153 has good info for this)

CISA provides a list of recommendations and methods to further prevent WLAN attacks. CISA recommends the deployment of WIPS and WIDS on every network. This allows early detection and prevention. WIDS/WIPS should be configured to detect 802.11a/b/g/n/ac devices connected to the wired or wireless network and detect and block multiple WAPs from a single sensor device over multiple wireless channels. (*Securing Enterprise Wireless Networks | CISA*)

**Preventative Measure for Mobile environment**

Description of measure and narrative of preventative measure (NIST 1800-22 is a good source of information for this).

The configuration of a Mobile Device Management (MDM) suite such as offered by IBM in combination with a VPN such as offered by Palo Alto significantly reduces the threat landscape. The MDM provides a configuration platform to enforce security policies on mobile devices, and monitor compliance. The Palo Alto VPN would then further the security by providing a tool to control the network traffic and provide encrypted communication channels between mobile devices and network resources. (Boeckl et al.)

**Reference federal, state, or industry regulations that justify these measures.**

Here you must use a regulation to support your preventative measures. You can use any REGULATION from chapter 4 of the course material. **(NIST and ISOs are standards, not regulations, and will not suffice as such!!)**

The Payment Card Industry Data Security Standard provides 12 requirements, organized into six domains. Focusing on the build and maintain a secure network, maintaining a vulnerability management program, access control measures, continuous monitoring and testing of networks, and upkeep of governance such as information security policies. (Doherty,2021)

**E. Recommended BYOD Approach**

**First Recommendation**

The first recommendation for B.Y.O.D is to utilize a tool called Intune. Intune provides several different ways to deliver enterprise applications and information to users. Intune creates a “Personal-owned” work profile for every user. This work profile acts as a sandbox to keep personal applications and data separated from enterprise applications and data. (Lutgert, 2022) It even goes far enough to provide a secondary workspace on Android devices. Intune builds on existing infrastructure utilizing the network Active Directly and Domain Controllers, the configuration wizard walks through the setup process of enrolling devices and building policy and access controls. Intune allows for “user groups” to be built in order to manage what applications and data is needed and can be configured to follow department hierarchy. Through these user groups compliance policies can be configured, if a device no longer meets the compliance policies an alert will be triggered to the user to inform them of the steps required to meet the compliance standards of the Intune policy. Intune aids in completing regulatory steps needed to meet the Sarbanes-Oxley Act, which requires all publicly traded companies provide an annual report on internal controls. (Doherty, 2021)

**Second Recommendation**

Industry or academic research

NIST 1800-22 has some good guidance on the BYOD approach

The second recommendation for B.Y.O.D is to use IBM’s MaaS360. Similar to Intune, IBM’s MaaS360 provides the Watson AI to deliver contextually relevant security insights. Provides methods for threat management, containment, and endpoint convergence, including support for IoT. Where Alliah is preparing to go public and is quickly expanding the IBM platform does have some benefits with scalability while providing all the necessary components of MDM. (*IBM Security MaaS360® With WatsonTM - Overview*)

**References**

In-text, citations must be in an acceptable format. I recommend APA, but you can use MLA or Chicago style as well.

Doherty, Jim. *Wireless and Mobile Device Security*, Jones & Bartlett Learning, LLC, 2021.*ProQuest Ebook Central*, https://ebookcentral.proquest.com/lib/westerngovernors-ebooks/detail.action?docID=6461875.

Orsi, Ryan. “Understanding Evil Twin AP Attacks and How to Prevent Them.” *Dark Reading*, 14 Nov. 2018, [www.darkreading.com/attacks-breaches/understanding-evil-twin-ap-attacks-and-how-to-prevent-them](http://www.darkreading.com/attacks-breaches/understanding-evil-twin-ap-attacks-and-how-to-prevent-them).

*WatchGuard Wireless Intrusion Prevention System (WIPS)*. www.guardsite.com/WIPS.asp. Accessed 25 Sept. 2022.

“2108.pdf On.” *Egnyte*, sansorg.egnyte.com/dl/zdm4VXjMja. Accessed 25 Sept. 2022.

“Email Protection - Email Security Solutions | Proofpoint US.” *Proofpoint*, 9 Sept. 2022, [www.proofpoint.com/us/products/email-security-and-protection](http://www.proofpoint.com/us/products/email-security-and-protection).

Radack, S. (2012), Guidelines for Securing Wireless Local Area Networks (WLANs), ITL Bulletin, National Institute of Standards and Technology, Gaithersburg, MD, [online], <https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=910705>

*Securing Enterprise Wireless Networks | CISA*. [www.cisa.gov/tips/st18-003. Accessed 25 Sept. 2022](http://www.cisa.gov/tips/st18-003.%20Accessed%2025%20Sept.%202022).

Boeckl, Kaitlin, et al. “NIST SPECIAL PUBLICATION 1800-22A.” *NCCOE*, Mar. 2021, [www.nccoe.nist.gov/sites/default/files/legacy-files/mdse-nist-sp1800-22a-draft.pdf](http://www.nccoe.nist.gov/sites/default/files/legacy-files/mdse-nist-sp1800-22a-draft.pdf)

Lutgert, Aad. “Personal-owned Work Profile (BYOD) With Intune.” *VMLabBlog.com*, 2 Jan. 2022, vmlabblog.com/2021/04/personal-owned-work-profile-byod.

*IBM Security MaaS360® With WatsonTM - Overview*. www.ibm.com/products/maas360. Accessed 25 Sept. 2022.