1. **The Agenda**

* The revelations of the vulnerability scan
* Mercury USA business case
* License recommendation

This presentation focuses on the vulnerabilities identified in the Mercury USA system and how attackers might exploit the reported vulnerabilities. The presentation will also shed light on the business case at Mercury USA. This will entail information on the business areas that would likely fall prey to the attack if the vulnerabilities are not addressed quickly. There is also a recommendation to purchase licenses for Nessus to become part of the organization's cybersecurity tools.

1. **Our Business Case**

* The business stores confidential consumer data
* The CEO’s intent- protecting consumer data
* A cyber-attack would;
* Compromises consumer data
* Lead to a loss of consumer confidence

The CEO's main concern was the vulnerabilities that could be exploited to access consumer data leading to a loss in customer confidence. This is the same thing that had happened to their biggest competitors. The important data to the organization includes; order data, customer lists, sales leads, credit card information, among other pieces of pertinent information. The recommendations provided here-in will help the business in averting a potential crisis if a cyber-criminal decided to exploit the vulnerabilities identified.

1. **Our Security Posture**

* High threat levels
* Lack of a critical security update
* Operating system at the end of life
* Middle-level threat
* Running MSRPS services as a vulnerability

The first vulnerability identified as a threat to Mercury USA's operations is their host machine's lack of a critical security update. This is a security update published in Microsoft Bulletin MS17-010 (Fujimoto et al., 2019). Organizations should install security updates to ensure that they protect their systems from malicious attacks. They can also avoid vulnerabilities identified in outdated programs (Fleischmann et al., 2016). If Mercury USA does not handle this vulnerability, remote attackers can access the target machines in their organization. They will also execute code detrimental to the organization as the attackers can easily attack their entire system by elevating their privilege. The second vulnerability identified is that the host machine runs an operating system that has reached the end of life. Operating systems that have reached the end of life are not subject to any updates and are at a high risk of cyber-attacks because they do not receive any security updates. As such, Mercury U.S should ensure that it updates its operating system soon. The third vulnerability is a medium-level threat, although the organization should ensure it is taken earnestly and addressed as soon as possible. Running MSRPS services can be enumerated through connecting on port 135 and handling the relevant queries. This is an urgent matter because the first step that attackers engage in is the enumeration of the target system. Having such a vulnerability in the organization makes it easy for the attacker to create a successful attack strategy through information gathering. It is also important for all incoming traffic to this port to be filtered to protect the system.

1. **Our VM Process**

Our VM process took place in six steps. The first step was a discovery that involved taking an inventory of all organizational assets and identifying host details. This helped identify security vulnerabilities regularly through an automated schedule. The second step is categorizing assets into business units to determine the criticality of the units to the business operations. The assessment stage involves determining a baseline risk profile to eliminate risks based on the asset's criticality and classification and the threat. The report stage involves documenting a security plan, monitoring any suspicious activities, and a full description of the known vulnerabilities. Remediation is where the vulnerabilities are fixed according to the business risk they cause, leading to the verification stage where there is confirmation of the elimination of threats through follow-up audits.

1. **We Need a Good Scanner**

* Nessus tool and Open VAS
* Nessus tool is recommended due to;
* The custom audit files feature
* Affordability, quality, and efficiency

This tool will help Mercury USA with regulatory and standards compliance through its custom audit files provision. Nessus has a feature and a document syntax that helps technical professionals create custom audit files for any target system (Gula & Arboi, 2010). This reveals any compliance issues with the system at Mercury USA. The presentation has keen attention to detail and is well organized, immediately drawing the professional to critical vulnerabilities. Apart from affordability, this tool is quality and efficient and thus worth the cost. Mercury USA should purchase the tool to provide two benefits: vulnerability scanning alongside compliance checks.

1. **The Ask**

* The cost - $2960
* Manpower- Training the IT staff
* Success measures- analyzing scalability and reporting

The licensing of the Nessus tool is quite affordable since it stands at $2960 annually. On the manpower, the organization will need to fund a threat vulnerability analysis training where the IT staff members will learn how to use the Nessus tool. The management, however, may not be able to understand the report that the tool generates due to technical complexity. The IT staff will also receive training on how to interpret these results and make them easier for different stakeholders who are not technically versed with the tool. The measure of success will be by analyzing the tool's scalability and reporting before its installation and after that to determine whether there are any positive changes.

1. **Summary**

* Mercury USA should purchase the Nessus tool
* Automation of vulnerability scanning
* Assurance of competitive advantage and profitability
* All organizational stakeholders benefit from the purchase.

Mercury USA should purchase the Nessus tool because of the massive benefits that it holds for the organization. It will help in regulatory compliance while still identifying potential vulnerabilities for risk management in the organization. The management will reap benefits as they have an organization ready to address various risks with information security. The employees will get to understand various risks through the automation of vulnerability scanning. Wholesomely, the organization will ensure business continuity with minimal disruptions on the side of information security which is imperative for competitive advantage and profitability.

**References**

Fleischmann, M., Amirpur, M., Grupp, T., & Benlian, A., & Hess, Thomas. (2016). The role of software updates in information systems continuance - An experimental study from a user perspective. *Decision Support Systems*. 83. 83-96.

Fujimoto, Mariko., Matsuda, W., & Mitsunaga, Takuho. (2019). Detecting attacks leveraging vulnerabilities fixed in MS17-010 from Event Log. 2019 IEEE Conference on Application, Information and Network Security (AINS)

Gula, R., & Arboi, M. (2010). Demonstrating Compliance with Nessus Web Application Scans. *Tenable Work Security.* Retrieved from <https://www.tenable.com/sites/drupal.dmz.tenablesecurity.com/files/uploads/documents/whitepapers/Demonstrating%20Compliance%20with%20Nessus%20Web%20Application%20Scans.pdf>