INFO 6027 -W2023 Assignment 1

Gihan Shamike Liyanage

1142109

Information Security Management

20/01/2023

Cybereason is a cybersecurity software that provides Fileless attack prevention, Automated ransomware hunting, Automated prevent malicious encryption, Pre and post execution malware inspection, In-memory application-layer protection and rapid remediation capabilities with incident response. Therefore, it can certainly be a valuable tool in a company's cybersecurity program, but it is not enough to address all of a company's cybersecurity needs.

A comprehensive cybersecurity program should include multiple layers of protection, including network security, endpoint security, incident response capabilities, firewalls, anti-virus software, intrusion detection and prevention systems, but also organizational and management elements such as risk assessment, Documented incident response plan, employee education and training, regular security audits, consistent security assessments and regular penetration testing compliance with relevant regulations and industry standards. Additionally, regular employee training and security awareness programs are critical to detect and respond to social engineering attacks and other types of threats that can't be addressed by technology alone. In on the other hand insider attacks can’t be identified by a tool or a software. There are 3 attack surfaces as Network, Software and Human. Vulnerabilities created by personnel or outsiders, such as social engineering, human error, and trusted insiders are very difficult to identify by an automated tool such as Cybereason. Some of the attacks can be on the outside of the boundary of software like blackmailing a system user to do certain things or purposely leaking data by insider which is similar to what happened with Wikileaks. Hence strong organizational information security policies must be implemented to prevent such incidents.

Additionally, depending on the organizational complexity and the nature of the company's operations, it may need to comply with various regulations, standards and best practices such as ISO 27001, NIST, SOC 2, FedRAMP and HIPAA. Even from the system design and development stage these best practices should be implemented because prevention is better than cure. It is important to have disaster recovery plans in place because cybersecurity is a complex and ever-evolving field, no system is ever perfectly secure.

Criminal attackers are super motivated and continuously researching new techniques. There is a famous quote from hackers saying “There is no security on earth. There is only opportunity.” This attack techniques and defense techniques are like a cycle and that cycle does not stop like evolution. The one who gets the lead wins. The only thing we can do is evolve faster than our adversary. Therefor the best thing we can do is take advantage of any technique rather than depending on one tool.

As a summery Cybereason can play an important role as a part of a comprehensive cybersecurity program, providing advanced threat detection and response capabilities. But it is not enough and should be accompanied with other tools, compliances, industry standards and best practices to protect a company from cyber threats in the real world.