Memorandum

To: CEO David Murray
From: Jardel Thomas Security Engineer
Date: May 2, 2024

Subject: Proposal for Cybersecurity Enhancements

Dear CEO Murray,

Hopefully, you are doing well as I write this memo. My goal as a Security Engineer at UBNetDef is to make sure that the network infrastructure of our company is constantly shielded from cyberattacks. With this objective in mind, I'm happy to share the report that follows, which outlines cybersecurity enhancement recommendations that should be considered.

Thank you for your attention to this matter.

Sincerely,

Jardel Thomas
Security Engineer
UBNetDef

Jardel Thomas
Security Engineer
Cse 427
May 4th, 2024

Table of Contents

1.0 Executive Summary

Proposal 1: Deployment of Intrusion Detection and Prevention Systems (IDPS)

UBNetDef finds that the deployment of Intrusion Detection and Prevention Systems (IDPS) To quickly identify and respond to potential threats, IDPS solutions are designed to monitor network traffic for malicious activity or security policy violations. By implementing an IDPS, UBNetDef can improve incident response capabilities, reduce the risk of cyber attacks and increase threat visibility. IDPS implementation will cost approximately $30,000, including the purchase of hardware and software licenses. Additional requirements may include network configurations and assessments, which our security engineer can complete in approximately 60 hours.

Proposal 2: Implementation of Endpoint Detection and Response (EDR) Solution

UBNetDef finds that the implementation of an Endpoint Detection and Response (EDR) solution is critical to strengthening our organization's endpoint security. EDR solutions provide advanced threat detection and response capabilities at the endpoint level, enabling detection and remediation of malicious activity and unauthorized access attempts. By implementing an EDR solution, UBNetDef can better protect endpoints against advanced cyber threats, improve incident response capabilities, and improve overall security resilience. The estimated cost of implementing an EDR solution, including endpoint agents and management console access, is approximately $20,000. Additional requirements may include endpoint assessment and implementation, which our security engineering team can complete in approximately 70 hours.

2.0 Technical Findings

2.1 **Endpoint Detection and Response**

UBNetDef suggests enhancing cyber security by putting in place an Endpoint Detection and Response (EDR) system. EDR enhances our capacity to identify and neutralize advanced threats by offering endpoint-level real-time threat monitoring and response capabilities. In the absence of EDR, UBNetDef becomes more susceptible to malware and ransomware, lengthens the time it takes to respond to incidents, and raises the possibility of data breaches and compliance infractions. The estimated cost of implementing EDR, which accounts for hardware requirements, software licensing, implementation, and ongoing support, is ±20,000.

2.2 Intrusion Detection and Prevention Systems

UBNetDef advises putting in place an Intrusion Detection and Prevention System (IDPS) to enhance cyber security. IDPS offers continuous network traffic monitoring, which makes it easy to swiftly identify and halt suspicious behavior as well as potential security concerns including malware invasions, denial-of-service attacks, and unauthorized access. Without IDPS, UBNetDef is vulnerable to network-based attacks that compromise the integrity and confidentiality of our data assets. The anticipated cost of deploying IDPS is $30,000. This includes the price of software license, hardware requirements, implementation, and ongoing maintenance.

3.0 Cited page

Network Security best practices. (n.d.). Netwrix. https://www.netwrix.com/network_security_best_practices.html

Liquid Web. (2024, April 1). *Dedicated Server hosting | Best Custom Servers | Liquid Web*. https://www.liquidweb.com/products/dedicated/?cq_src=google_ads&cq_cmp=12291257432&cq_con=141499399597&cq_term=virtual%20server%20cost&cq_med=&cq_plac=&cq_net=g&cq_pos=&cq_plt=gp&gad_source=1&gclid=CjwKCAjw88yxBhBWEiwA7cm6pRcQEPCLCwRgt_T9RHjRtdTNz2N_JNz5Mrsfh4Eob61dyB_EexTphhoC5AgQAvD_BwE&gclsrc=aw.ds#hosting-plans-pricing

Security QRADAR EDR - Pricing | IBM. (n.d.). https://www.ibm.com/products/qradar-edr/pricing