**Security Vulnerability Assessment of Arctic Wolf Networks**

Sweta Kharel

Central Washington University

Cyber Security Fundamentals IT 647

March 8, 2024

**Arctic Wolf**

Arctic Wolf Networks is a cybersecurity company that offers services focused on security monitoring to identify and address cyber threats. The company surveys on-site computers, networks, and cloud-based assets, safeguarding against malicious activities such as cybercrime, ransomware, and malicious software attacks. Utilizing an open XDR architecture, the Arctic Wolf Platform integrates seamlessly with our Concierge Delivery Model to function as an extension of the team, actively safeguarding your environment and enhancing your security stance.

The services provided include:

* Managed Detection and Response: Identifying, responding, and recovering from sophisticated threats.
* Cloud Detection and Response: Identifying and responding to advanced threats directed at cloud infrastructure and applications.
* Managed Risk: Identifying, evaluating, and fortifying the environment against digital risks.
* Cloud Security Posture Management (CSPM): Assessing, fortifying, and simplifying cloud environments to mitigate misconfiguration vulnerabilities.
* Managed Security Awareness: Engaging and preparing employees to detect and neutralize social engineering attacks.
* Incident Response: Ensuring swift recovery from cyberattacks and breaches, covering threat containment to business restoration.

**Assessment of Potential Vulnerabilities**

A vulnerability assessment involves testing procedures aimed at identifying and categorizing security flaws within a specific time frame of an organization. By conducting such assessments, Arctic Wolf can mitigate the risk of data breaches by detecting vulnerabilities and safeguarding sensitive data.

Arctic Wolf is built in an open, Extended Detection and Response (XDR) which is a cybersecurity system that brings together various security tools to protect all parts of a company's technology, including users, computers, emails, applications, networks, cloud services, and data. The security model in Arctic Wolf works with the preexisting IT and security solutions of their client, which means that it does not require the client to change or replace vendors. It collects information from computers, network devices, infrastructure, and cloud services to make sure it can detect threats from every direction. This suggests potential vulnerability could include the service from the client’s third-party technology vendors, supply chain management, XSS injections, phishing emails, insider threats, misconfigured system security, outdated firewalls and system patches, and weak networking protocol implementation.

A scenario of supply chain management vulnerability for arctic wolf: for instances company ABC is using Microsoft cloud services for data storage and Arctic Wolf Cloud Detection and Response that identifies and stops threats across IaaS and SaaS resources. Reports suggest that a recent Microsoft attack by Midnight Blizzard was able to inject and leave hidden malicious code in Microsoft cloud services products. Chances are high that it can cause lateral damage in ABC company which can infect Arctic Wolf in case of weak system configurations and access management in the company's security system.

Similarly, XDR architecture is combined with the concierge delivery model that gathers and enhances endpoint, network, and cloud data, which is subsequently analyzed using various detection engines. The platform also uses threat intelligence and machine learning to automatically find sophisticated threats and offers additional community protection leading to vulnerabilities such as data poisoning and training data interface. Machine learning works by taking huge amounts of data and learning its patterns to filter reliable sources of data. Attackers use fake machine codes to trick machines into thinking malware as a reliable source. Also, data inference attacks exploit the information revealed by machine learning systems and using it to jeopardize the confidentiality of training data and endangering the privacy of individuals or organizations whose data was utilized in training dataset.

**Identification of Priority Risk Areas**

Security vulnerabilities are present in every digital environment. Identifying and prioritizing risk areas in vulnerability assessment is important for risk minimization, incident response, resource allocation, and efficiency of business. Identification of priority risk areas in security vulnerability assessment enables organizations to make informed decisions to reduce their overall risk exposure and strengthen their cybersecurity defenses effectively.

In the case of the Arctic Wolf network, major priority risk areas include third-party software vendors, supply chain management, networking systems, insider account security, and misconfigured network and software firewalls. As discussed, the Arctic Wolf network uses XDR architecture, machine learning, and threat intelligence that involves interacting with a number of end users and machine learning to gather information that can be tricked into bypassing malicious emails and accessing the company’s system and security. Insiders, third-party vendors, and supply chain management are major risk areas in this case. Similarly, misconfigured firewalls, open permissions, and weak network security enable open doors for malicious traffic and unauthorized access to the company’s system leaving the system vulnerable.

**Review of Potential Remediation Tactics**

Cybersecurity vulnerabilities, whether in software, systems, or networks, present opportunities for malicious exploitation by exploiters, leading to unauthorized access, data theft, or service disruptions. Vulnerability remediation entails identifying and mitigating these security weaknesses proactively to minimize the risk of cyber-attacks and reduce potential security breaches.

The process of vulnerability remediation involves several key steps:

* Detection of vulnerabilities: The initial phase involves assessing potential weaknesses through vulnerability scans, penetration testing, and risk assessments.
* Prioritization of vulnerabilities: Identified vulnerabilities are then assessed and ranked based on severity, likelihood of exploitation, and potential impact. This prioritization helps the organizations in addressing the most critical vulnerabilities first.
* Development of a remediation plan: A complete plan is formed containing detailed actions to address each prioritized vulnerability. This includes utilization of patch management tools, adjusting security configurations and implementing additional layers of protective measures.
* Execution of the remediation plan: The remediation plan is implemented, which involves deployment of security patches, configuring system settings, or updating security protocols.
* Validation of effectiveness: After the implementation of the remediation plan, it is essential to verify its efficiency of the plan by retesting systems and confirming that vulnerabilities have been adequately resolved.
* Ongoing monitoring and maintenance: Continuous surveillance and upkeep of systems are required to identify and address emerging vulnerabilities.

Organizations can effectively manage and mitigate security vulnerabilities by following these steps along with enhancing their overall cybersecurity position and reducing the possibility of potential cyber-attacks.

**Recommendation**

Arctic Wolf security system involves frequent engagement with end users and third-party vendors, frequent assessment of software configuration, system patches, and open permissions of codes is required to ensure strong security protection of the company's system. Similarly, Attribute-based access control is essential which helps the company to limit the access of materials and sources to authorized individuals to remediate risks of vulnerability with supply chain management and insider’s threat.

Arctic Wolf uses machine learning and threat intelligence to strengthen its security system by keeping up with the updated threats and vulnerabilities in the industry. Constant configuration checks and updates help ensure machine learning is free from data poisoning and works at its best efficiency. Network and system firewalls need to be constantly updated and configured. Network monitoring, and the use of secured network protocols, encryption systems, and IDS are important to keep the company and its data in the most secure system. Applying these procedures helps the company reduce risks of security vulnerability and strengthen its security infrastructure.

# **References**

*The leader in security operations*. Arctic Wolf. (2024, February 28). <https://arcticwolf.com/>

ManageEngine, communications@manageengine. com. (n.d.-a). *Experience perfect harmony between vulnerability management and Patch Management.* Experience perfect harmony between vulnerability management and patch management. - ManageEngine Vulnerability Manager Plus. <https://www.manageengine.com/vulnerability-management/integrated-vulnerability-and-patch-management.html?network=g&device=c&keyword=vulnerability+management&campaignid=9145452449&creative=463439600553&matchtype=p&adposition=&placement=&adgroup=94262446004&targetid=kwd-110482344&location=9033668&target=&gad_source=1&gclid=CjwKCAiA0bWvBhBjEiwAtEsoWyPZnXpJaWb3UJFRirbtHD558WRCezgUC4gWWGYM4rMzl3TdLf_nxhoCiPgQAvD_BwE>