Security Roadmap Report: Strengthening ACME Anvils' Security Posture

Executive Summary:

This security plan with timelines outlines the security posture of ACME Anvils and the roadmap to improve it. The plan aims to reduce risk across the organization, plan the budget appropriately, and keep the cyber insurance premiums lower.

Current Security Posture:

Currently, ACME Anvils' security posture is a concern. The organization has been buying random widgets to stop-gap security issues, which is not a sustainable strategy. To address this issue, we need to identify the current security posture, including exploitable vulnerabilities.

The Risk Assessment Process:

To identify the current security posture, we performed a risk assessment process. We used a risk matrix to evaluate the likelihood and impact of potential threats. The threats were categorized based on their severity, and the results showed that ACME Anvils is vulnerable to several threats.

Security Roadmap:

Based on the results of the risk assessment, we created a security roadmap to improve the security posture of ACME Anvils. The roadmap includes what we can fix or mitigate in the next 90 days, 6 months, and 12-18 months.

90 Days:

In the next 90 days, we recommend implementing the following security controls:

* **Active Phishing Training:** This control is a quick win for the organization, and the cost is low. It will help employees identify and avoid phishing attacks.
* **OS Patch Management:** Implementing OS patch management will reduce the risk of exploitation due to unpatched vulnerabilities. It requires medium resources, but the initial cost is low, and the impact on employees is medium.

6 Months:

In the next 6 months, we recommend implementing the following security controls:

* **Application Patch Management:** Implementing application patch management will reduce the risk of exploitation due to unpatched vulnerabilities in the software applications. It requires medium resources, and the initial cost is medium.
* **Forensics Contract:** This control is a quick win for the organization, and the cost is low. It will help the organization respond to security incidents effectively.

12-18 Months:

In the next 12-18 months, we recommend implementing the following security controls:

* **2-Factor Authentication:** Implementing 2-factor authentication will provide an extra layer of security for user authentication, reducing the risk of compromised credentials. It requires medium resources, and the initial cost is medium.
* **Threat Detection via IOCs:** Implementing threat detection via IOCs will help the organization identify potential security incidents proactively. It requires high resources, and the initial cost is high.

In conclusion, the security plan with timelines outlines the current security posture of ACME Anvils and the roadmap to improve it. The security roadmap includes what we can fix or mitigate in the next 90 days, 6 months, and 12-18 months. Implementing the recommended security controls will reduce the risk across the organization, plan the budget appropriately, and keep the cyber insurance premiums lower.