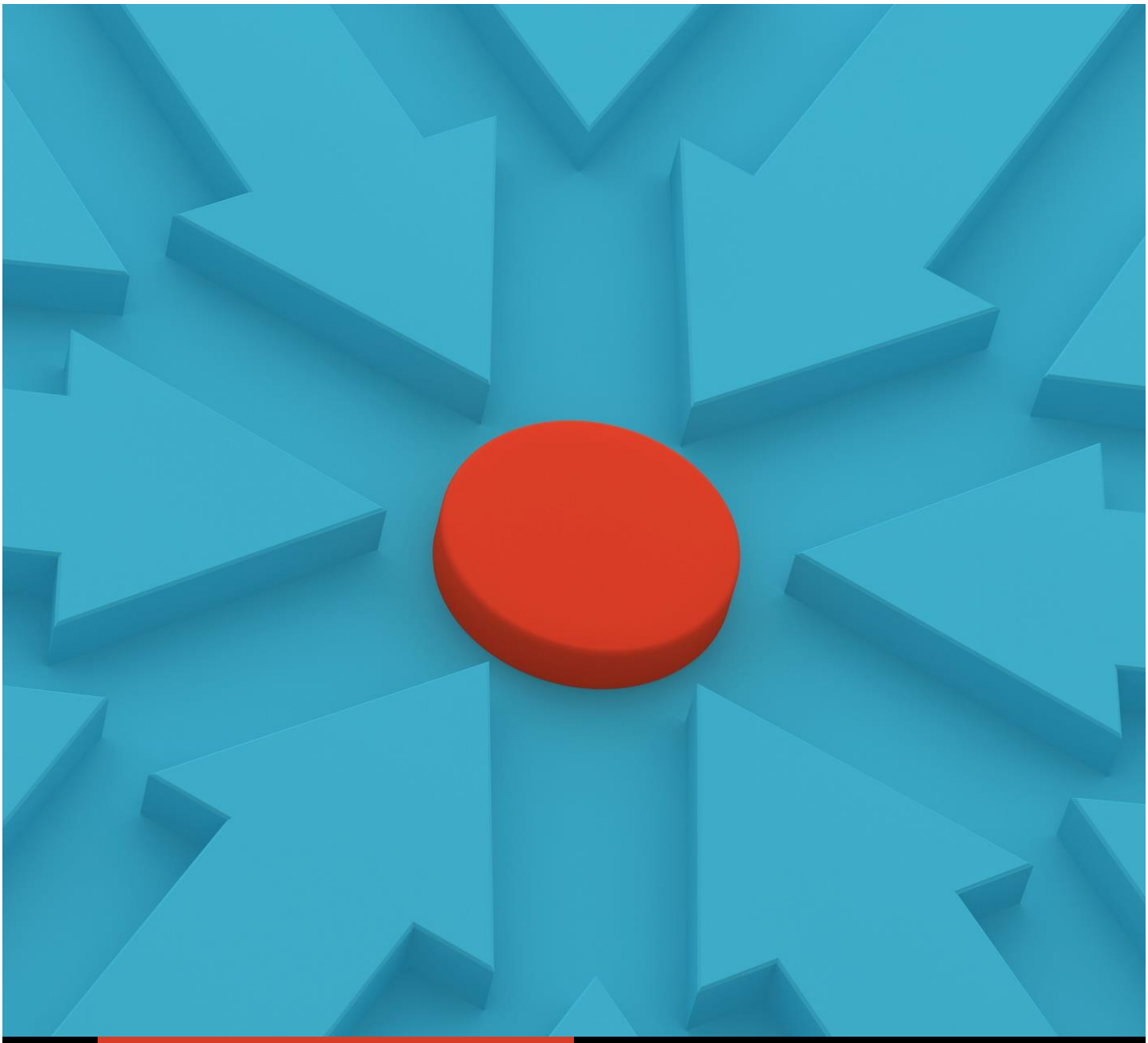

SECURITY ROADMAP

ACME COMPANY

ROAD RUNNER CORPERATION

soc@roadrunner.com

OVERVIEW

Executive Summary

This security roadmap outlines a structured approach for ACME Company to improve its cybersecurity posture over the next 12-18 months. The roadmap is divided into three key phases: 90 days, 6 months, and 12-18 months, each focusing on progressively more complex and resource-intensive tasks aimed at reducing vulnerabilities and minimizing risk.

The 90-day plan emphasizes quick wins that address critical issues such as patch management, vulnerability scanning, and firewall rule cleanup. The 6-month plan introduces essential, more complex initiatives like the roll out of two-factor authentication (2FA) and automating the patch management process. Finally, the 12-18 month plan covers advanced, resource-intensive measures such as the deployment of a SIEM system, integration with a Modern Honeypot Network, and comprehensive encryption upgrades.

This roadmap is designed to minimize risk across ACME's network, enhance security monitoring, and strengthen defenses against emerging threats, all while maintaining a balance between cost, complexity, and long-term security goals.

90 Day Plan:

- Ensure all hosts and applications are at the latest patch
- Start regularly scanning for vulnerabilities
    - Remediate high and critical vulnerabilities found
- Disable unnecessary services
- Cleanup firewall rules

6 Month Plan:

- Begin 2FA roll out
- Phishing training for all employees
- Automate the patch management process
- Continue remediating any vulnerabilities found

12 – 18 Month Plan:

- Begin SIEM implementation
- Configure SIEM for Active Threat Detection
- Integrate SIEM with Modern Honeypot Network
- Review and update encryption used throughout the organization

90 DAY PLAN

Quick Wins & Critical Issues

OS & Application Patch Management

- Establish a patch management process for all hosts on the network.
- Set up a patch management process for applications.

Implementing regular patch management for operating systems and applications reduces the risk of exploitation of outdated software. By addressing patching early, ACME can greatly reduce risks at a relatively low cost and complexity. This process can be automated later down the road to have less user impact.

Vulnerability Scanning

- Implement regular vulnerability scanning across all three subnets.
- Focus on patching critical and high-severity vulnerabilities identified in the vulnerability scan and previously provided vulnerability assessment.

Vulnerability scanning is a low-cost, high-impact measure. Continuous scanning identifies and prioritizes vulnerabilities for remediation, focusing on critical issues. This process can be automated to allow for minimal disruption to the business, making it an ideal step toward improving the security posture.

Disable Unnecessary Services

- Conduct an audit of all services running on network hosts and identify those not essential for business operations.
- Disable or remove unnecessary services on all systems. (e.g., VNC, rsh)

Disabling unnecessary services reduces the attack surface of ACME's network by limiting potential entry points for attackers. Many default services are not required for normal business operations and can introduce vulnerabilities. By conducting a thorough audit and removing or disabling these services, ACME can significantly reduce risk with relatively low effort and cost.

Basic Firewall Rule Review and Cleanup

- Review and remove outdated or overly permissive firewall rules.
- Tighten rules to allow only necessary traffic.

Regular firewall rule cleanup helps eliminate unnecessary access points and reduces the risk of unauthorized network traffic. This is a straightforward process with high impact on reducing exposure, ensuring that only legitimate traffic flows through the network

6 MONTH PLAN

2FA Implementation

- Implement two-factor authentication (2FA) across all critical systems, particularly those accessing sensitive or proprietary information.
- Educate and train employees on the use of 2FA to ensure smooth adoption.

Implementing 2FA adds a strong layer of security against unauthorized access, especially for sensitive systems. While it requires moderate setup and user adjustment, it significantly reduces the risk of account compromise and phishing attacks. Once in place, it requires minimal ongoing maintenance, making it a high-impact security measure.

Active Phishing Training

- Implement ongoing phishing awareness training for all employees.
- Conduct regular phishing simulations to test employee readiness.

Phishing training raises awareness and reduces the risk of human error leading to breaches. This is a low-cost, high-impact solution that requires minimal resources but significantly strengthens the company's defense against phishing attacks. Regular simulations keep employees alert and improve their response to real-world threats.

Patch Management Automation

- Automate patching for all applications as well as all the hosts across all three subnets.

By automating patch management, ACME can ensure that vulnerabilities are consistently addressed in a timely manner, reducing exposure without requiring manual intervention. This ensures ongoing compliance with patching processes, lowering the risk of exploitation.

Continued Vulnerability Mitigation

- Continue remediating vulnerabilities identified in the vulnerability scans, now focusing on medium and low-risk items.
- Incorporate these mitigations into an ongoing vulnerability management program.

Based on the scan results, remediating medium and low-risk vulnerabilities over the six-month period reduces ACME's overall risk exposure. While these vulnerabilities are not immediately critical, addressing them as part of an ongoing process helps maintain a secure environment and prevents potential exploitation over time. This gradual approach aligns with resource management while ensuring consistent improvement of the security posture.

12 – 18 MONTH PLAN

Implement a Security Information and Event Management (SIEM) System

- Deploy a SIEM solution for centralized log collection and analysis. (i.e., Splunk, ArcSight)
- Set up basic alerting for critical security events.

A SIEM system provides real-time visibility into security events across the network, enabling ACME to detect, analyze, and respond to potential threats faster. Although it involves medium to high costs and complexity, a SIEM is crucial for ongoing security monitoring, compliance, and incident response. It consolidates logs from multiple sources, making it easier to identify patterns and potential breaches.

SIEM Integration with Modern Honeypot Network

- Connect the SIEM system to the Modern Honeypot Network, which includes Cowrie, Dionaea, and Glastopf honeypot instances.
- Configure the SIEM to collect and analyze logs and alerts from the honeypots.

Integrating the Modern Honeypot Network with the SIEM allows ACME to gain deep insights into potential attack patterns and malicious activities targeting the network. These honeypots provide valuable data on real-world attacks. By feeding this information into the SIEM, ACME can track threat behaviors, enhance detection accuracy, and improve incident response. This integration is relatively complex but highly valuable for proactive threat intelligence and early warning of emerging threats.

Advanced Threat Detection

- Implement advanced threat detection capabilities across the network.
- Integrate threat intelligence feeds and continuous IOC (Indicators of Compromise) monitoring into the SIEM.

Advanced threat detection via IOC monitoring enhances ACME’s ability to identify sophisticated attacks early. By integrating external threat intelligence feeds, the system stays up-to-date with the latest indicators, such as malicious IPs, domains, and file hashes. While it has moderate complexity and cost, this proactive approach allows for real-time detection of emerging threats, improving the organization's ability to respond to incidents before they escalate.

Comprehensive Encryption Upgrade

- Upgrade all systems to support only strong encryption protocols and ciphers
- Disable weak SSL/TLS versions and insecure cipher suites
- Implement proper certificate management

Upgrading encryption across all systems ensures that data in transit and at rest is protected with strong, modern encryption standards. This is a high-complexity task, particularly if legacy systems are in use, but it is critical for preventing data breaches and protecting sensitive information. Proper encryption strengthens ACME’s defenses against attacks targeting cryptographic weaknesses.