Proactive Ethical Hacking Strategy

Defending ACME Technology's Digital Assets

EXECUTIVE SUMMARY

Executive Summary

- Goal: Protect ACME's digital assets through proactive ethical hacking.
- Scenarios: High-Budget vs Medium-Budget defense plans.
- Outcome: Full threat mitigation roadmap + custom security product.

UNDERSTANDING THE ASSET

ACME Digital Asset Overview

- Internal applications & customer databases.
- R&D and cloud infrastructure.
- Value: High-risk if compromised (reputation, IP, compliance).
- Threats: APTs, insiders, ransomware, misconfigurations.

PENTESTING METHODOLOGY

Penetration Testing Phases

- 1. Pre-engagement Interactions
- 2. Information Gathering
- 3. Threat Modeling
- 4. Vulnerability Analysis
- 5. Exploitation
- 6. Post-Exploitation
- 7. Reporting

TOOLS & TECHNIQUES

High vs Medium Budget Tools

- High: Maltego, Burp Suite Pro, Cobalt Strike, Nessus, Rapid7
- Medium: OSINT Framework, OpenVAS, Metasploit, Nikto, SQLmap
- Aligns with OWASP, PTES, and MITRE ATT&CK.

STRATEGIC APPROACHES

High vs Medium Budget

- High Budget: Full Red Team, Zero Trust, Enterprise SOC, AI monitoring.
- Medium Budget: Periodic pentesting, open-source tools, outsourced SOC.
- Focus: Realistic coverage with resource alignment.

CASE STUDIES

Real-World Examples

- High: AFA Tech stopped $3M breach with Cobalt Strike.
- Medium: E-commerce firm used OpenVAS + freelancer, saved 60% budget.

CUSTOM SECURITY PRODUCT

ACME SecurePulse Dashboard

- Vulnerability scanning, risk scoring, and compliance modules.
- Tech: React, Node.js, PostgreSQL, Docker/Kubernetes or Render.
- Tiers: High-end with AI, mid-tier with essential tools.

FINAL SUMMARY

Takeaways

- Security is continuous, not a one-time audit.
- Proactive defense works under any budget.
- ACME SecurePulse provides long-term scalable protection.