Vulnerability Management Process

This playbook outlines the steps for identifying, classifying, remedying, and mitigating vulnerabilities in an organization's IT ecosystem. The process is crucial for maintaining IT security and reducing the risk of exploitation.

Step 1: **Identification**

Scan the IT infrastructure using automated tools to identify potential security vulnerabilities. This should include all systems such as servers, endpoints, and network devices.

Step 2: **Classification**

Categorize the identified vulnerabilities based on their severity, potential impact, and exploitability. Common classifications include critical, high, medium, and low severity.

Step 3: **Analysis**

Analyze the classified vulnerabilities to understand the root cause, affected systems, and potential impact on the organization's infrastructure and data.

Step 4: **Prioritization**

Prioritize the remediation of vulnerabilities based on the classification, the value of the affected assets, and the organization’s risk tolerance.

Step 5: **Remediation**

Develop and implement a plan to address the vulnerabilities. This could include applying patches, changing configurations, or employing compensating controls.

Step 6: **Verification**

Following remediation, verify that the vulnerabilities have been fixed. Re-scan the systems to ensure that no new vulnerabilities have been introduced during the remediation process.

Step 7: **Documentation**

Record the vulnerability management process details, including identification data, remediation actions, and verification results, for future reference and compliance requirements.

Step 8: **Continuous Monitoring**

Implement ongoing surveillance of the IT environment to detect new vulnerabilities. Keep the vulnerability management process iterative and responsive to new threats.

General Notes

Tool Selection

Choose appropriate vulnerability scanning tools that align with your organization's systems and infrastructure for effective identification.

Stakeholder Engagement

Involve relevant stakeholders in the process, including IT staff, security teams, and executive management, to ensure comprehensive risk management.

Regulatory Compliance

Be aware of compliance requirements with industry standards and regulations which may dictate specific vulnerability management practices.