Grey Matter

Cybersecurity report

Juliano Alves de Souza

Grey Matter

Project STATUS

Vulnerability Categorization:

- Schedule Maintenance
- Policy Update
- Other Security Issues

Grey Matter

PROGRESS Recomendations

WEEK 1

→Focus on high-severity vulnerabilities

- Applying patches

MONTH 1

→medium-severity vulnerabilities

- Upgrades

- MONTH 2

→High-severity vulnerabilities

- Major Upgrades

Grey Matter

ATTENTION AREAS

Values

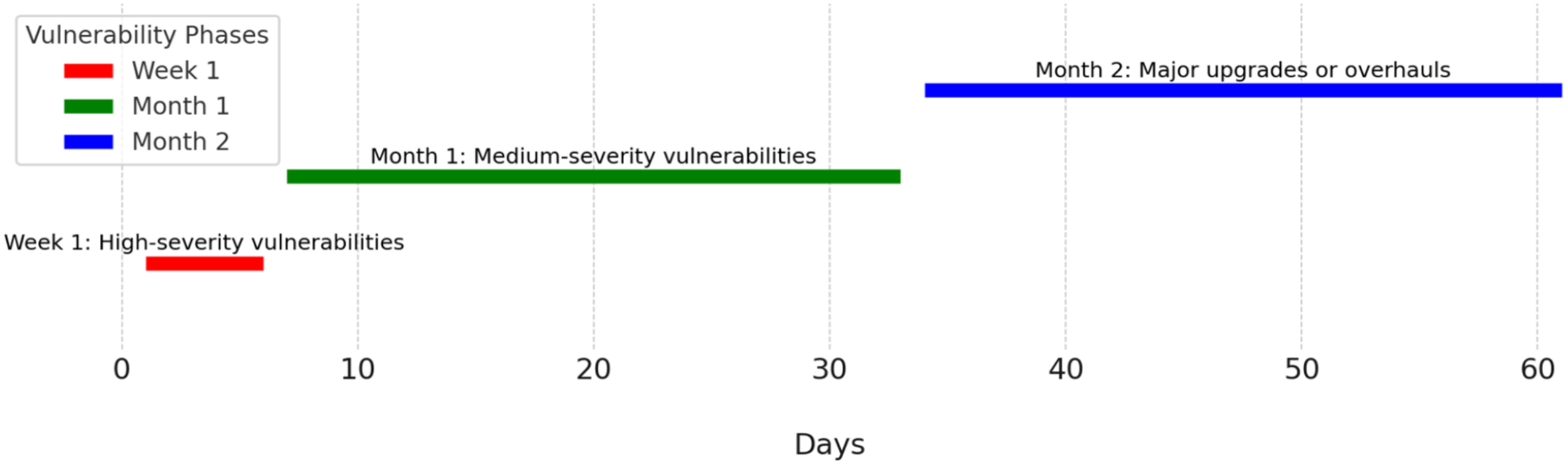
- immediate threats to network security are addressed promptly while allowing adequate time for the careful planning and implementation of more complex solutions.

Strategy

- This phased approach to vulnerability management demonstrates a proactive and strategic posture towards cybersecurity, essential for maintaining trust and safeguarding critical assets in the merger process.

Grey Matter

SCHEDULE



Grey Matter

Policy UPDATE

Password complexity, such as minimum length, inclusion of special characters, uppercase and lowercase letters, and numbers.
Auditing user accounts to ensure compliance with the password policy.

Maintaining overall network security

Utilize automated tools to enforce the password policy

Grey Matter

Protocols vulnerability

DATA SQL

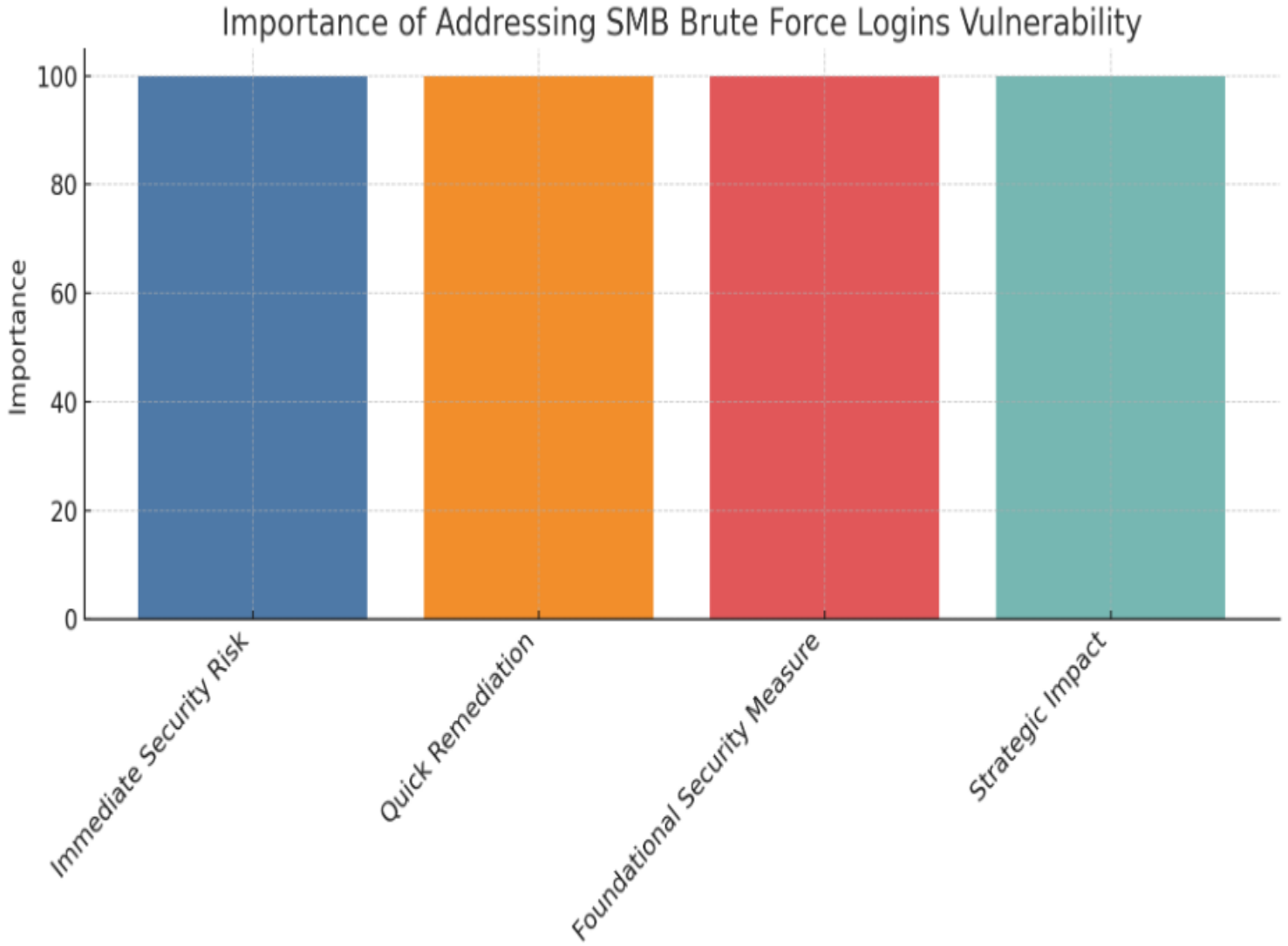
- Upgrade protocols
- Generate or Renew New Certificates
- Monitoring
- Security Best Practices

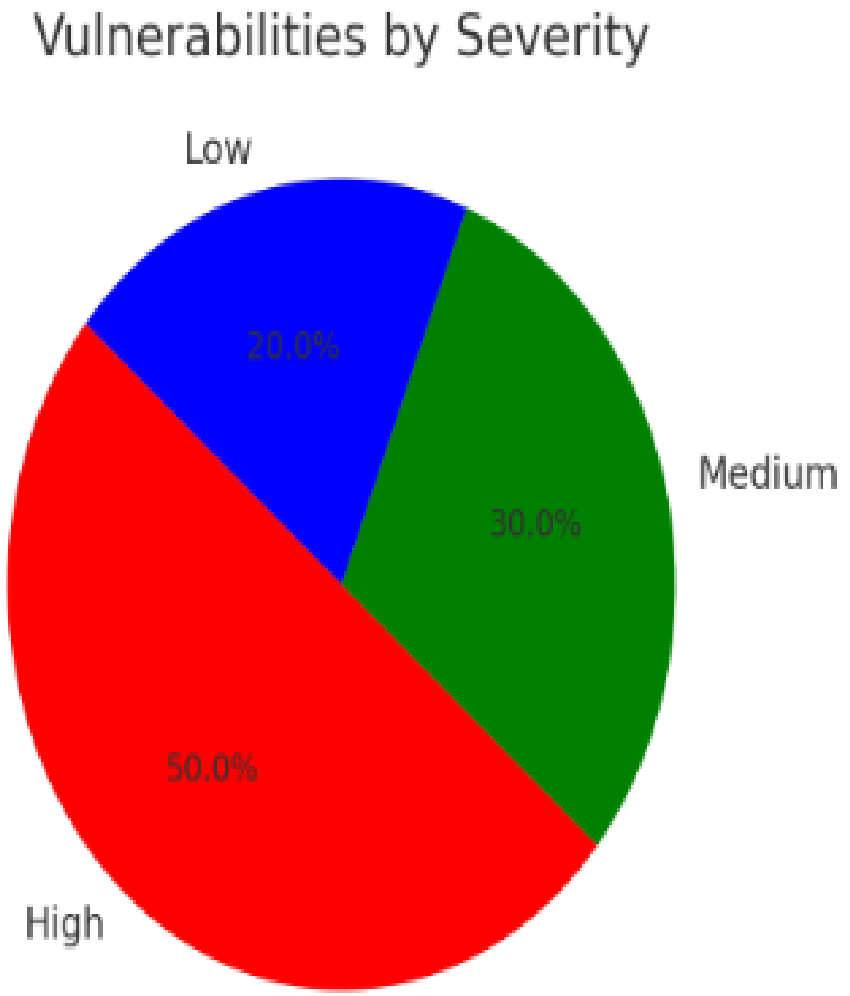
SERVERS

- Path Management
- Version Upgrade
- Firewalls
- Audits

Grey Matter

BRUTE FORCE LOGINS





FINAL RECOMENDATIONS

→Our security findings reveal critical risks that could lead to unauthorized access and data breaches. By addressing these vulnerabilities promptly, we protect the network from attacks and ensure the safety of sensitive information.

→This underscores the importance of timely action to maintain network security and protect sensitive information, demonstrating the significance of the security findings for safeguarding digital assets.

Grey Matter

- Strategic Importance: Emphasize the foundational nature of these steps in enhancing overall cybersecurity posture.
- Remediation Plan: Outline a phased approach: address high-severity vulnerabilities in Week 1, medium-severity in Month 1, and system overhauls in Month 2.
- Immediate Action: Prioritize changing default credentials to mitigate SMB Brute Force Logins, a critical and easily exploitable risk.