PROTECTING OUR BUSINESS: SECURITY ASSESSMENT FINDINGS AND RECOMMENDATIONS

Presented by Joshua Merren, Cybersecurity Analyst, Grey Matter LLC

Date: December 9th, 2024

This presentation summarizes the key security challenges we face and provides actionable steps to protect Grey Matter's operations, finances, and reputation in light of the BrainMeld acquisition.

• GREY MATTER

Introduction

The acquisition of BrainMeld brings opportunities but also risks.

Our cybersecurity assessment identified areas requiring immediate and long-term attention to protect our business.

Today's presentation will focus on:

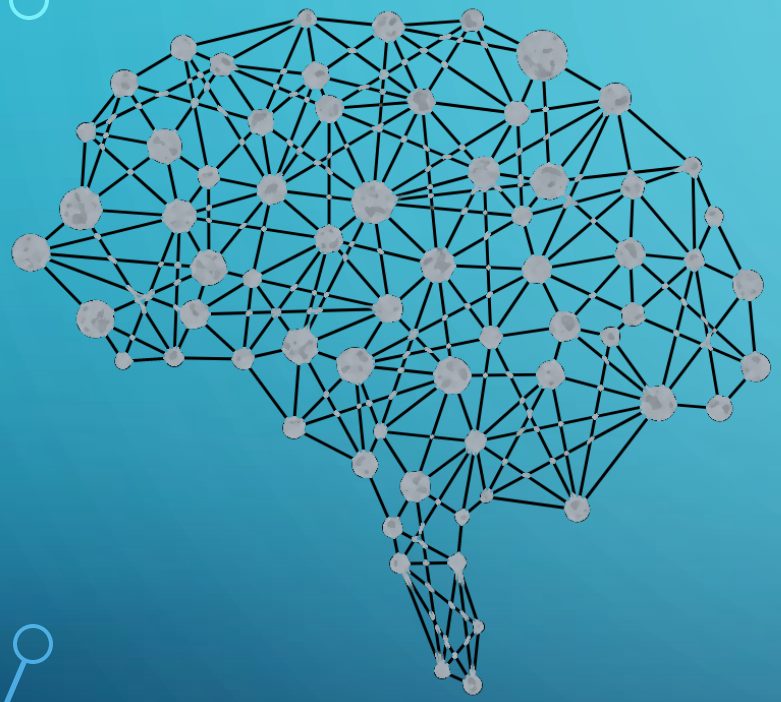
- Critical vulnerabilities identified.
- Recommended solutions and their importance.
- Steps to ensure future resilience.

Importance

- Cybersecurity is fundamental to successfully integrating BrainMeld's systems and protecting Grey Matter's growth. Without addressing these issues, we risk operational disruptions and financial loss.

Grey Matter

Key Findings



Grey Matter

Vulnerabilities discovered include:

- Unpatched systems (e.g., SMB server issues).
- Weak password practices.
- Outdated encryption protocols.

These weaknesses, if left unaddressed, create entry points for hackers.

- A single vulnerability can result in costly breaches, operational downtime, or loss of trust with customers. Strengthening these areas protects us from external threats.

Unpatched SMB Server Vulnerabilities

Unpatched Server

- SMB (Server Message Block) allows data sharing over networks but has known vulnerabilities.
- Example: The WannaCry ransomware attack exploited unpatched SMB servers, causing millions in damages globally.
- Recommendation:
  - Apply critical patches.
  - Disable outdated SMBv1 protocol.

Importance

- Unpatched systems are an open door for attackers, risking stolen data and ransomware incidents that could cripple operations.
- Protecting these systems ensures business continuity.

WEAK PASSWORD PRACTICES

Password-related risks identified:

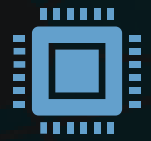
- Default credentials like "admin:guest."
  - Weak or reused passwords.
- Example: Cyberattacks often start by exploiting default passwords, leading to unauthorized access.
- Recommendations:
  - Enforce stronger password policies.
  - Implement account lockout for repeated failed attempts.

importance

- Weak passwords are like leaving the front door unlocked. Strengthening them ensures that only authorized individuals access our systems.

Grey Matter

OUTDATED ENCRYPTION METHODS



Issues:

Use of HTTP instead of HTTPS.

Weak SSL/TLS certificates vulnerable to interception.

Example:

Outdated encryption allows hackers to intercept sensitive information, like login credentials or customer data.

Recommendations:

Transition all systems to HTTPS.

Update encryption to meet modern standards (e.g., SHA-256).

Importance:

Encryption protects our communication and sensitive data. Modernizing encryption ensures customer trust and compliance with industry standards.

Grey Matter

POTENTIAL IMPACTS

Risks if vulnerabilities remain unresolved:

- Data breaches expose sensitive customer or employee information.
- Financial losses due to fraud, fines, or recovery costs.
- Loss of reputation, impacting customer trust and market position.
- "Without action, these vulnerabilities could disrupt business operations and undermine our credibility."

Importance

- Addressing vulnerabilities today prevents crises tomorrow, protecting our business and customers.

Grey Matters

RECOMMENDED IMMEDIATE ACTIONS

Quick steps to reduce risks:

- Apply software patches immediately.
- Disable outdated SMBv1.
- Strengthen password policies and encryption.
- "These actions provide an immediate shield against the most critical vulnerabilities."

Importance:

- These straightforward actions are cost-effective and reduce the risk of major breaches.

Grey Matter

LONG-TERM STRATEGIES

Strategies for ongoing security:

- Regular system audits.
- Employee cybersecurity training.
- Continuous policy updates to adapt to evolving threats.
- Example: Regular audits in similar companies reduced incidents by 50% (Business Tech Weekly, 2022).

Importance

- Security is not a one-time fix; it requires continuous effort to adapt to new threats.

Grey Matter

VISUAL AID

Vulnerability	Potential Impact	Recommended Action	Timeline
Unpatched SMB Server	Unauthorized access and ransomware attacks	Apply security patches, disable SMBv1	Immediate (1 week)
Weak Password Practices	Brute-force attacks and data breaches	Enforce strong passwords, set lockouts	Immediate (1 week)
Outdated Encryption (HTTP)	Data interception and loss of sensitive information	Transition to HTTPS, update SSL/TLS	Short-term (1 month)
Lack of Regular System Audits	Undetected vulnerabilities	Implement regular security audits	Ongoing

BENEFITS OF IMPLEMENTATION

Grey Matter

By taking these steps, Grey Matter will:

- Enhance system security.
- Protect customer trust.
- Avoid costly disruptions and fines.
- "Strong security is an investment in our company's future."

Importance:

- Proactive measures ensure Grey Matter remains competitive and trusted in the market.

CONCLUSION

Summary:

- Our findings highlight critical vulnerabilities.
- Immediate and long-term actions protect our business.
- Moving forward, ongoing efforts are essential.

Call to Action:

- "Together, we can secure Grey Matter's future by addressing these risks today."