CYBERSECURITY

New Scenario and Implementations

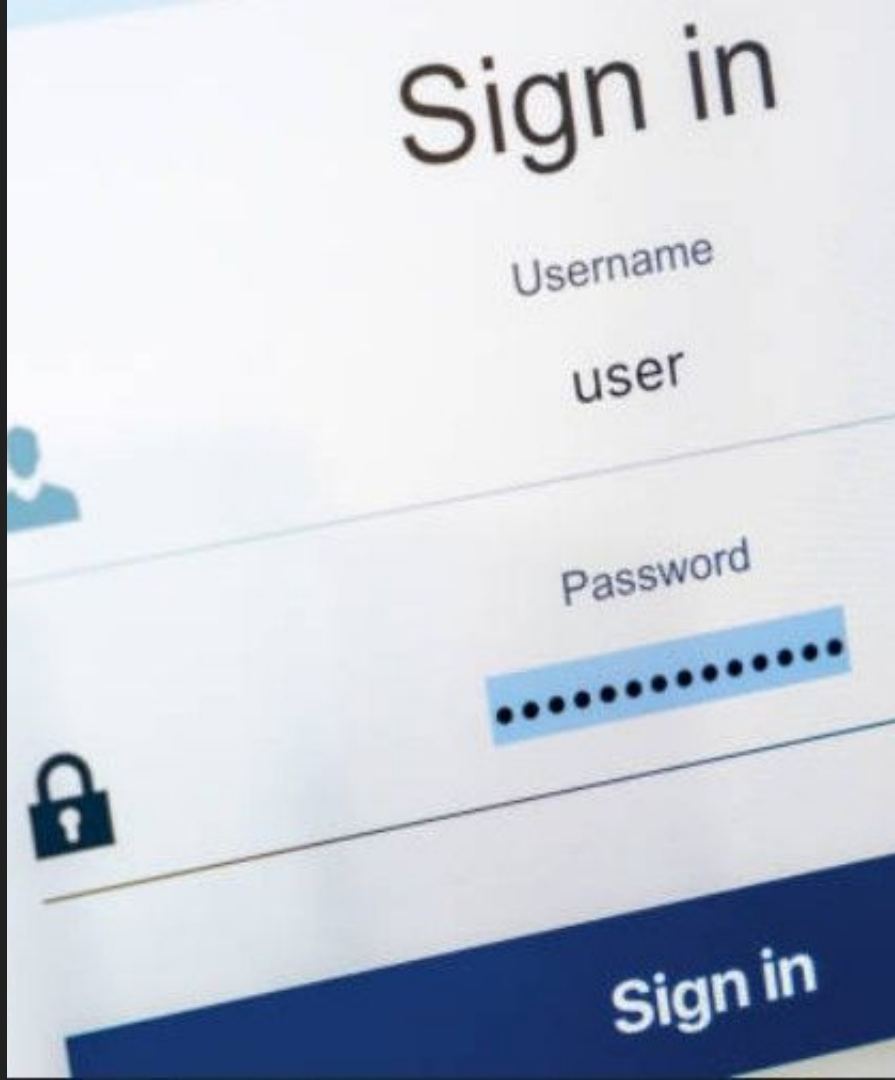
Mid November Report

Identified Issue:

Hackers are getting into our system via our employee accesses to steal data and implant virus into our system.

This is a Critical Severity Level since our customers information, company data and system are in hand of bad intentional people.

That case requires urgent action to solutionate.



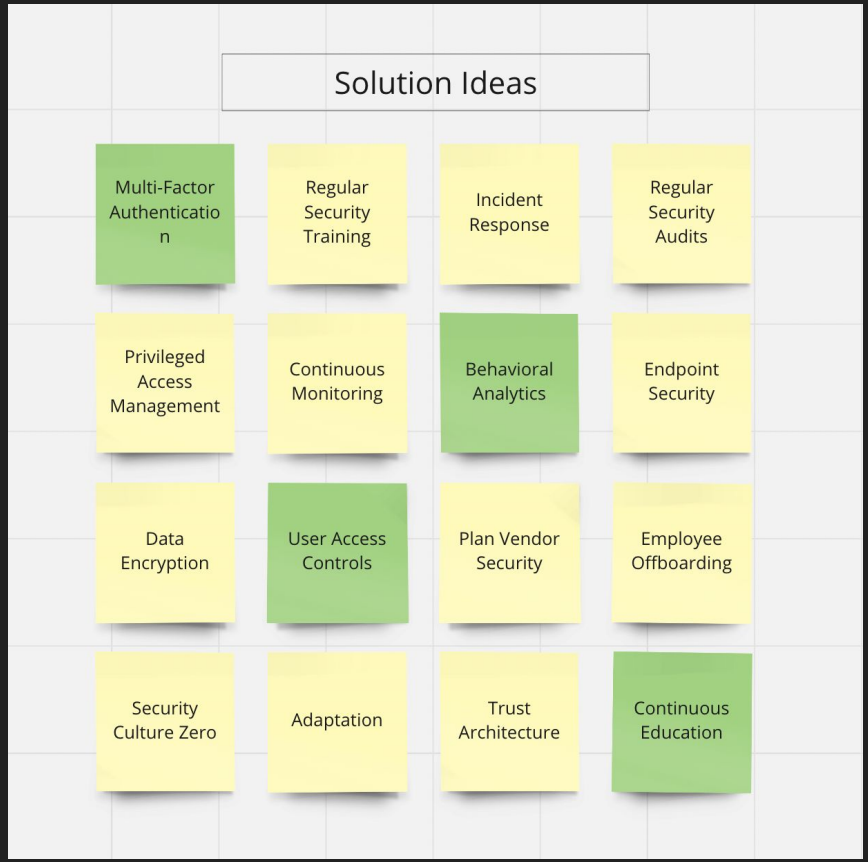
Brainstorm

Since the problem was identified, the team was brought together for a meeting to exchange ideas.

A brainstorm was made and the ideas which came up in the Brainstorm were:

Best Options

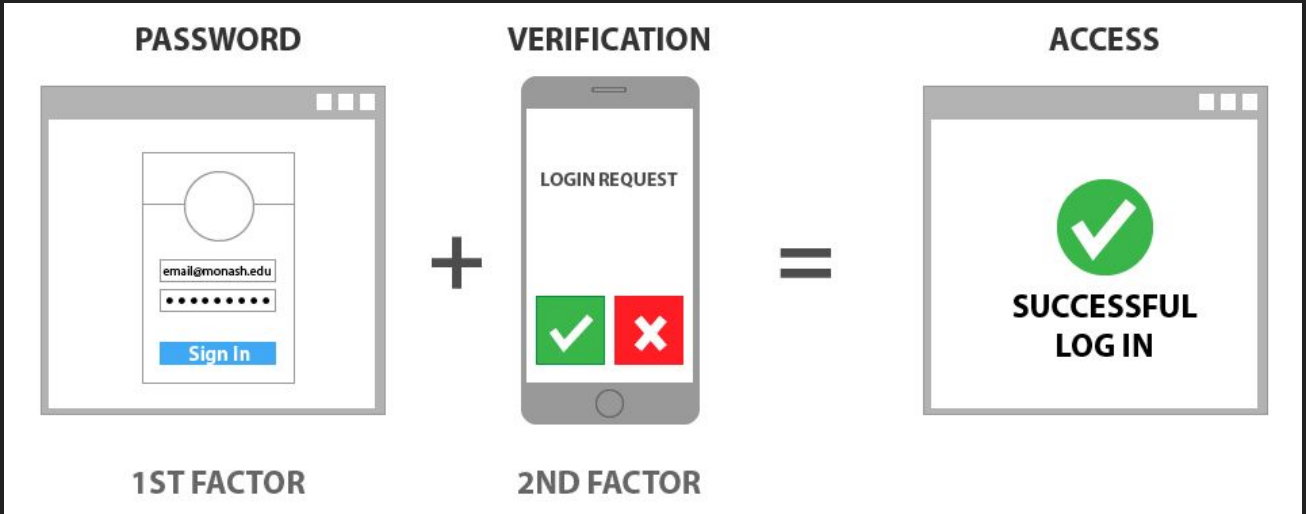
The fastest and most efficient ideas were selected (highlighted in green) for immediate implementation.



Multi-Factor Authentication

How it Works

When Implemented, MFA will add an extra layer of security. Even if a hacker obtains login credentials, they would still need additional verification.



Multi-Factor Authentication

Implementation

We have integrated Google Authenticator as the chosen option for enhancing the security of our software. With Google Authenticator, we aim to provide an additional layer of protection to your accounts and ensure a more secure authentication process.

Here's how we will implement Google Authenticator in our system:

1. User Setup: Users will have the option to enable Google Authenticator for their accounts within our software.
2. QR Code or Secret Key: During the setup process, users will be provided with a QR code or a secret key that they can scan or manually enter into the Google Authenticator app on their mobile device.
3. Time-Based One-Time Passwords (TOTPs): Google Authenticator will generate time-based one-time passwords (TOTPs) that will serve as the second factor for authentication.
4. Authentication Process: When users log in to our software, they will enter their username and password as usual. Afterward, they will be prompted to enter a verification code generated by Google Authenticator.
5. Enhanced Security: By implementing Google Authenticator, we are adding an extra layer of security to prevent unauthorized access to user accounts. This helps safeguard sensitive information and ensures a more secure user experience.

Behavioral Analytics

How it Works

In the realm of cybersecurity, behavioral analysis involves observing activity within a system to discern between normal behavior and atypical or anomalous activity and identify potential threats. Traditional cybersecurity methods have relied on predefined, rules-based systems or signature-based detection.

Behavioral Analytics

Implementation

We will implement software that identifies the interaction patterns on our platform made by our employees. From this, when finding any anomaly or suspicious activity, such as interactions outside working hours, identifying that a login was made from different computers in a short period of time or any other type of unusual interaction. When this suspicion is identified, our cybersecurity team will be notified so that a manual review can be carried out of what may be happening.

User Access Controls

How it Works

In its simplest form, access control involves identifying a user based on their credentials and then authorizing the appropriate level of access once they are authenticated. Passwords, pins, security tokens—and even biometric scans—are all credentials commonly used to identify and authenticate a user.

User Access Controls

Implementation

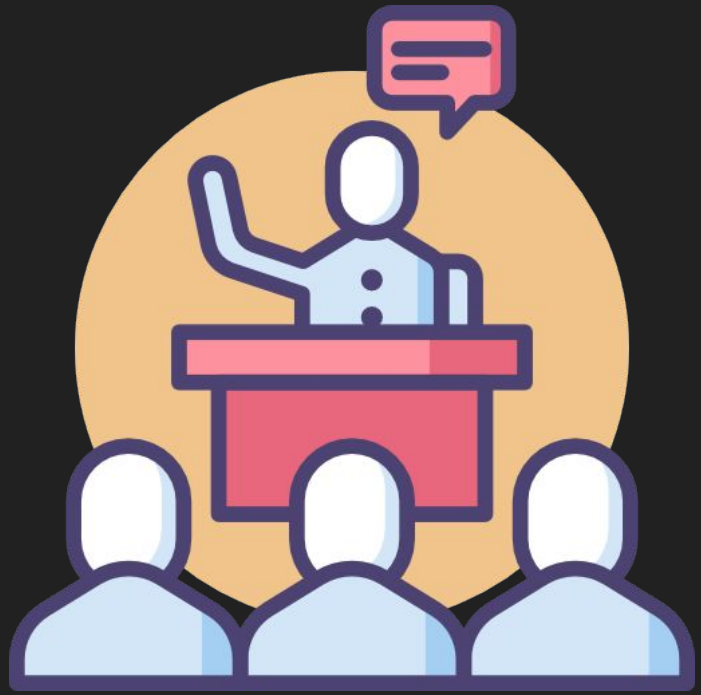
User Access Controls allow us to carefully manage and restrict the level of access granted to employees based on their roles and responsibilities within the organization. This means that employees will only have access to the information and functionalities necessary for their job duties, reducing the risk of accidental or intentional exposure of sensitive data.

By implementing User Access Controls, we can effectively limit access to certain information contained within our software, ensuring that only authorized personnel can view or interact with sensitive data. This proactive approach enhances our overall cybersecurity posture and minimizes the potential impact of security breaches or insider threats.

Continuous Education

Seminars, meetings, activities, collaborative work, dynamic interactions and other modes of interaction will be used in order to educate our employees with new security methodologies, in addition to being aligned with new trends used by criminals in invading systems.

These interactions will be done once a month making it information frequently remembered by our employees, making them more familiar with the topics and reducing the likelihood of error.



Stronger Password

A strong password is a combination of characters, symbols, and numbers that is difficult for others to guess or crack through brute-force attacks. It typically includes a mix of uppercase and lowercase letters, numbers, and special characters, and is at least 12-16 characters long.

All user access to our system will get their password reset and will require all the specification in a Strong Password.

Next Steps

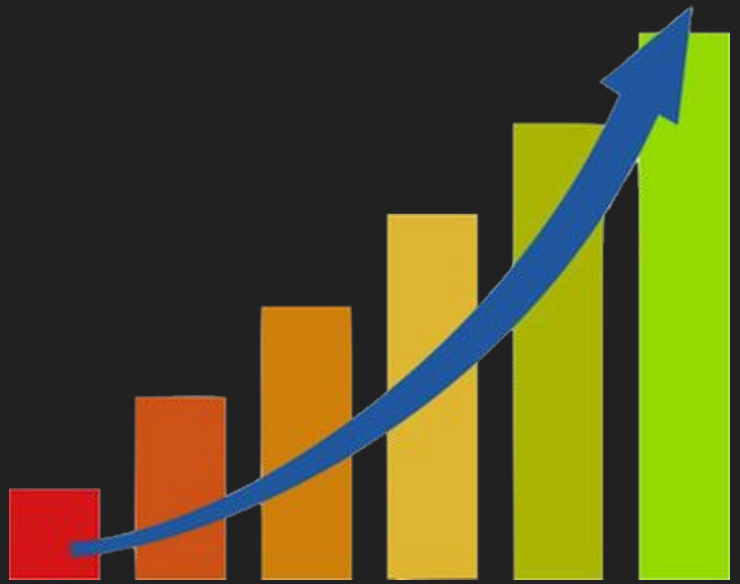
1. Implementation of all the new cybersecurity systems in our software;
2. Reset in all employee password access;
3. Implementation of new password requirements;
4. Provide training to employee;
5. Testing and monitoring of the new implementations;
6. Analyze results of security with expectation of improvement.

Expectations

By implementing the new methods, we anticipate significant improvements in the following areas:

- Enhanced Authentication Security
- Improved Threat Detection and Response
- Granular Access Control
- Increased Security Awareness
- Strengthened Password Security

Overall, we anticipate that these proactive security measures will collectively strengthen our cybersecurity posture, reduce the likelihood of successful cyber attacks, and better protect our organization's sensitive information and assets. By prioritizing security and investing in these initiatives, we aim to safeguard our systems, mitigate risks, and uphold the trust and confidence of our stakeholders.



Thank You