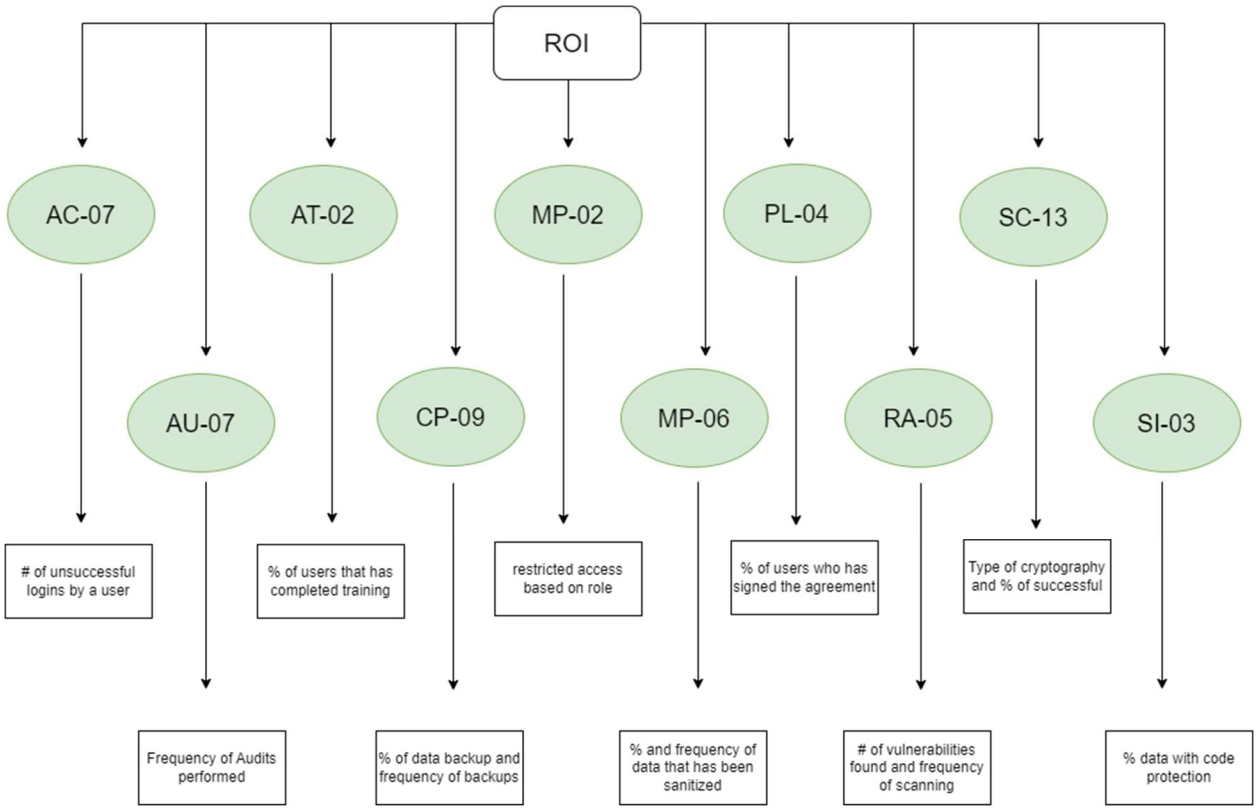
Alex Smetana

CIS 360 – Lab 04

05/13/2023



AC-07 – Unsuccessful Login Attempts

– Enforces a limit of consecutive invalid access attempts by a user. The number of unsuccessful logins will allow for better protection of a user's account by preventing the use of brute force attacks. The number of unsuccessful login attempts will better detail any outliers into suspicious login activity. When an outlier of login attempts occurs to an individual, the account be temporarily blocked.

AU-07 – Audit Reduction and Report Generation

– The information system provides an audit reduction and report generation capability. It is important to do regular audits on a company's security. Auditing a company will allow for better security overall and allow a company to improve its security. This metric can be measured by the frequency of audits and scores generated by each audit.

AT-02 Security Awareness – Provides basic security training to all users. Providing security awareness training to users is crucial in protecting businesses. Better security awareness will result in better security. AVs are not full proof, so it is important to train individuals. This metric can be measured by the frequency and number of users who have completed training.

CP-09 Information System Backup – Organization conducts backups of both user-level and system level information. Backing up data is very important and must occur regularly. In the event of a data breach, it is important to have backups in case of a loss of data. This metric can be measured by the frequency of data backup.

MP-02 Media Access – Restricts access to information system media to authorized individuals. Restricting the access of information to authorized individuals is important in protecting information. It is important that only authorized individuals can read or write the data. This metric can be measured by assigning individuals roles and applying restrictions.

MP-06 Media Sanitization – Organization sanitizing both physical and nonphysical media. Sanitizing data is very important in the security lifecycle. If data is not needed, then it needs to be sanitized due because it can pose a threat. This metric can be measured by the percent and frequency of the data sanitized.

PL-04 – Rules of Behavior – Agreement to the individual acknowledging that they agree to the behavior. Having individuals sign an agreement to a policy helps with recognition of training. The agreement may vary but acknowledges agreement to security rules. This can be measured by the % of individuals that has signed the agreement.

RA-05 – Vulnerability Scanning – Organizations scans for vulnerabilities and reports them when found. Scanning for vulnerabilities is important to prevent attacks from happening. This allows for these vulnerabilities to be patched before they can be exploited. This metric can be measured by the number of vulnerabilities found and patched.

SC-13 – Use Of Cryptography – Uses cryptography during the transfer of data. The use of cryptography is important in the transfer of data. Encrypting data is important in ensuring the integrity of data. This metric can be measured by the type of cryptography and the percentage of data encrypted.

SI-03-Malicious Code Protection – The information system implements malicious code protection. Malicious code protection, as it implies helps protect from malicious code. This metric can be measured by the percentage of data using malicious code protection.