

Intern Reflection: Identifying and Understanding Basic Security Controls

Author: Julian Samonte

Role / Program: Cybersecurity Intern

Objective: To independently identify, observe, and document basic security controls used within the organization, and reflect on their purpose and importance.

Purpose of This Exercise

The goal of this document is not to list security controls from a textbook, but to **actively discover and understand them in a real operational environment**. By observing systems, asking questions, and reviewing configurations, I am developing practical insight into how security controls are implemented and why they matter. The goal is to be able to transform this into a knowledge-based document for all employees to see if they want a better understanding of the basic security controls of the building.

This reflection helps connect theoretical cybersecurity concepts to real world IT operations.

Learning Objectives

By completing this exercise, I aim to:

- Identify common security controls used in a production environment
 - Understand **why** each control exists and **what risk it mitigates**
 - Recognize how multiple controls work together rather than in isolation
 - Reflect on gaps, limitations, or opportunities for improvement
-

How I Identified Security Controls

I discovered these controls by observing Microsoft Defender, Microsoft Intune, Atera, and other software that are used for their unique purposes. I was able to review some policies in Intune and that helped me to understand some baseline policies that a organization should have when it comes to security. Shadowing IT staff as well as asking them questions has also helped me to gain a better understanding of these security controls. They were

able to show me applications and software that they use in order to regulate everything technology related.

Observed Security Controls

1. Access Control

What I observed:

Access is controlled in the Windows file server. This access control makes it so where only certain groups or users can access certain files in the file server. For example, everyone is able to access the JCC files in comparison to only 4 groups/users being able to access the HR files. Another example of access control in this environment is that if users are traveling for whatever reason they need to request that HR let them access local network resources from wherever they are traveling. One more example is that if an employee leaves, their manager must request from HR and IT to gain access to that employee's email login.

What this control does:

Access control limits who can access systems, applications, and data.

Why this control is important:

It reduces the risk of unauthorized access and ensures users only have access needed for their role.

Reflection:

This is enforced well in the file server as I can clearly see who has permission to access each file and who doesn't. It is also good security that it's made so that employees that are traveling need to request access rather than just letting them log in wherever they please. An improvement that is going to be made is that role-based access is going to be fine in the environment. For example, a manager will have more access to things than somebody working under them would.

2. Multi-Factor Authentication (MFA)

What I observed:

MFA is a feature that adds another layer of security when signing into an account. MFA should be enforced for people logging into administrative roles to prevent any unauthorized logins or tampering with the sensitive information that they have access to. It is also

important for employees that aren't in administrative roles to have MFA in order to protect their devices and any sensitive information that they have access to.

What this control does:

MFA adds an additional verification step beyond a password.

Why this control is important:

It protects accounts even if credentials are compromised.

Reflection:

Looking at Microsoft Defender secure score, under recommended actions, I can see that 373 out of 391 users aren't registered with MFA. I can also see that 5 out of 10 users with administrative roles aren't registered with MFA. This can increase risk because if an attacker were to figure out an employee password, they would easily be able to get in without that extra layer of security. If the users register with MFA, then their accounts will be more protected against those attackers and lower the risk of unauthorized access.

3. Endpoint Protection (Antivirus / EDR)

What I observed:

According to Microsoft Intune, the default policy is to use Microsoft Defender for Endpoint Protection. This software program has a ton of capabilities that will help in defending against threats and potential attackers. This software includes Microsoft Defender Antivirus which offers real time protection and behavior monitoring. It also offers Endpoint Detection and Response (EDR) that provides another layer of continuous monitoring and threat detection. It offers exposure and vulnerability management as well as a ton of other features that will make devices in the environment more secure. This environment also uses BitLocker encryption which is a feature that does full-disk encryption and encrypts entire drives. This feature makes unauthorized access almost impossible without the correct key. MacOS Filevault is also mentioned in Intune. This is another encryption feature that encrypts the entire startup disk and prevents unauthorized access.

What this control does:

Endpoint protection monitors devices for malicious activity.

Why this control is important:

It helps detect and stop malware, ransomware, and suspicious behavior.

Reflection:

This is not visible to users and is already a feature that is included on their workstations. It is already set up to where if a person is doing something suspicious then it will be blocked and an email will be sent to IT about it. IT is then able to look at what a person is doing and decide if what they're doing is harmful to the environment or not. If BitLocker was misconfigured that would make it much easier for an attacker to get into and steal people's data because it wouldn't encrypt the data before it hits the network. Making it extremely easy for attackers to see and analyze any traffic that employees would be a part of.

4. Patch Management**What I observed:**

In this environment, patches are scheduled to be completed on a certain date and time. As of right now I know that they are automated for the security workstations and the SIA workstations in Atera. In Intune there are update rings that control when updates take place and can be paused if updates are causing any unwanted errors.

What this control does:

Patch management keeps systems up to date with security fixes.

Why this control is important:

Unpatched systems are a common attack vector.

Reflection:

A challenge that exists is that patch management and updates are under different services. Like some are under Atera and some are under Intune, so it will be more challenging to keep track of all the patch and update schedules.

5. Backup and Recovery

What I observed:

Data from very important VMs is backed up things like the hvac systems, school systems, and other systems. Backups in this environment are stored locally and with a variety of apps that use the cloud. This variety includes applications such as Microsoft Azure, UrBackup, FOG Project, ThinStation, and Veeam. These apps can store the backups virtually, physically, and in the cloud. UrBackup is a client/server backup system that is meant for image and file backups. It is an open-source solution meaning it is flexible and is free to use, making it great for this environment. It is also multi-platform and can do backups via internet with servers around the world making it a convenient and effective service for any device. FOG project is a service that allows backups to be directed to a network NAS or a local USB hard drive. This allows for the option of both virtual and physical backups. It is recommended to install FOG project inside a virtual machine to be able to have easier access to backups and upgrades. ThinStation is also an open-source thin client operating system. Backups and recovery in ThinStation involve synchronization of backups from primary drives or network locations while making sure the previous backups are overwritten after synchronization. Veeam is a proprietary software, which is different from all of the other software listed before. This means that it was created and is maintained by a specific company. It allows IT administrators to be able to create reliable backups, perform fast restorations, replicate workloads, and integrate with cloud storage for offsite protection.

What this control does:

Backups allow data to be restored after loss or compromise.

Why this control is important:

They reduce the impact of ransomware, hardware failure, or human error. This control is very important just in case the security systems are unable to prevent an attacker from getting in. If the attacker causes some kind of outage or deletes everything for some reason, these backups come in handy and will help to hopefully make a full recovery.

Reflection:

I am confident that data could be restored if needed. With all these techniques and applications there should be images of all the important systems that are essential to this environment.

6. Network Security Controls

What I observed:

This environment uses a Firewall for Windows in order to allow traffic from certain port ranges as well as blocking traffic from certain port ranges. Microsoft Intune is also able to detect what devices have the firewall enabled. There is also blackholing in port security which is if an unknown device tried to connect to a secure port then it would not be able to access the network. The port would recognize that this device has an unauthorized MAC address and the unauthorized traffic would be quietly discarded. VLANs are also used to control who can reach what inside of a network. This works by preventing a device from one VLAN from directly communicating with devices from another VLAN unless it is explicitly allowed. It also prevents lateral movement meaning if an attacker got into one part of the network they still wouldn't have control over every other part of the network.

What this control does:

Network controls restrict and monitor traffic between systems.

Why this control is important:

They limit lateral movement and unauthorized access.

Reflection:

If the Firewalls were misconfigured, then that would mean all sorts of traffic would be able to come through. If port security was misconfigured, then anybody would have access just by simply plugging into the network which makes the network insecure. If the VLANs were misconfigured then there would be no depth or layers in the network security. Making it so that an attacker would have access to the whole network if they got into one part of it. This would lower the security of the devices in the environment and expose the organization overall.

7. Logging and Monitoring**What I observed:**

There are active logging and monitoring occurring in this environment. There are multiple layers to logging here. Endpoints create logs through Microsoft Defender, and Microsoft Defender sends emails to the IT group if a person were to visit or download something suspicious. The switches and firewalls also log traffic and connection activity. The computers onsite are unable to download anything due to the regulations that are set in place here, but if a person were to sign in at home and download something suspicious then the Defender would let the IT group know. Authentication is logged by domain

controllers and cloud identity services. Microsoft 365 generates audit and activity logs. There is also the app called SPLUNK that basically ingests everything and assists the IT group giving them analytics, datasets, reports, and alerts on the activity that is happening in the environment. Defender and SPLUNK are detective controls that are more monitoring than logging. They collect data from log sources and investigate any suspicious behavior even if it is not actively watched in real time. This is useful in post event detection and alerting, being able to find out the source of an incident that may have occurred. We are also working on a platform called Zabbix that is used to monitor servers, networks, applications, cloud resources, virtual machines, and services. It provides real time performance monitoring, alerting, data visualization, and analytics. Some features Zabbix offers related to monitoring are real-time monitoring, alerting & incident response, visualization & dashboards, and distributed monitoring. Features including logging include operating system logs, application logs, and windows event logs. Zabbix can also detect errors/warnings inside logs, track patterns via regular expressions, count occurrences of events over time, extract timestamps from log lines, and support log rotation without losing monitoring state.

What this control does:

Logs record activity and monitoring detects anomalies.

Why this control is important:

They enable detection, investigation, and accountability.

Reflection:

Logs are actively used as activity is being monitored by Splunk and Microsoft Defender. As the logs are being monitored by these apps, they are continuously looking for any suspicious activity to report to the IT team.

8. Security Awareness and Training

What I observed:

One training program that is used in this environment is wizer training which is a security awareness training program that will help the employees here to better understand what could be seen as a phishing attempt or an attempt at an attack on the organization. There were also 2 articles that have been created by the IT team in this environment that teach employees what a fake email or spoofing could look like. The system automatically will

highlight the email if it comes from an external email not from within the organization. In the case that an email is pretending to come from an someone it's not then there will be a notification "[POSSIBLE SPOOFING]" and the email will be quarantined. Microsoft 365 also offers email focused security awareness training designed to help employees with the skills and knowledge to defend against cyber threats. It gets employees familiarized with Microsoft tools, helps them to recognize what a phishing attempt may look like, and show them how to report it.

What this control does:

It educates users on safe security practices.

Why this control is important:

Human error is a major source of security incidents. It is almost impossible for rules, policies, and security systems to do their job against threats if the users are just welcoming them in.

Reflection:

The training is not completely set up so I wouldn't think it would be very effective as of right now. However, there doesn't seem to be any large scale cyberattacks in the history of this environment that I know of. If all the employees complete the training and read up on what the IT team has written up, then the human firewall should be basically impenetrable.

9. Physical Security Controls

What I observed:

As I stated earlier, only authorized people with a badge can enter the building. On top of that, there is a security guard at both entrances that can monitor who is coming into the building as well as cameras that watch the campus. There are also rooms and doors that are locked behind the badges as well. Another physical security control is the background checks that employees must get before working in the building. If somebody's background is suspicious then they will be turned away from employment and won't be able to work at or enter the building.

What this control does:

Physical controls protect facilities and equipment.

Why this control is important:

Physical access can bypass many technical controls.

Reflection:

The area that is most critical to protect physically is probably the front entrance and the background check. If the security at the front desk works perfectly then there will be no suspicious people in the building and that seems very safe. Also, without background checks potentially suspicious people could have access to the building and at that point the security would also be letting them enter.

Overall Reflection

- **Which security controls seemed most critical to daily operations?**
 - To me it seems like the security controls most critical to daily operations are access controls, physical security, and security awareness and training.
 - These three make the environment safer daily, and one slip up from either one of these could put the organization in danger.
- **Which controls depend heavily on user behavior?**
 - Multi-factor authentication depends heavily on user behavior because users must enable it which they all should.
 - Security awareness and training also depend heavily on user behavior. They have to take the time to be aware of what a threat may look like to protect themselves and not put any other people at risk.
- **Where do multiple controls work together to reduce risk?**
 - Access control and physical security must work together to know who to let in the building. One or the other is not safe enough, they need both the badge and a security officer to let them in.
 - Logging and monitoring and endpoint protection must work together to monitor what a user is doing and make sure that they don't put themselves at risk.
 - Patch management and network security controls work together in assessing what and who it could be risky to communicate with and then creating a patch to protect users from that risk.

- **What gaps or improvement opportunities did I notice?**

- An improvement opportunity that I noticed was that some of the ideas are not finished completely, but once they're finished, they should have a secure environment.
- One gap that I saw is that not a lot of people have MFA and that is a tiny fix that could improve security by a lot.

Key Takeaways

I learned that there are a ton of controls that go into making sure a network and organization is stable and stay that way. It's way more complicated than I would have realized. A real cybersecurity environment is surprisingly very dependent on its users and their behavior on their devices. If a user is unable to identify what a threat may look like or their account is easily hackable, that could put the whole environment at risk even with the best policies put in place. I have also learned that there is no set application or software set that a company needs to use to improve their security. If there is an IT company that puts in the research, then they are able to use whatever they can get their hands on.

Next Steps / Follow-Up Questions

I am very interested in network controls, logging and monitoring, and patch management. I think that these three are very useful in this field of study. I also really liked learning about them during this exercise and will investigate them more in my career. I also would like to look deeper into the physical networking aspect of cyber I was very interested when I went into the server rooms the other day. A question I have is have we ever experienced a cyberattack that hit us hard and if not do we have an incident response plan that would get us back up as fast as possible?

Reviewer / Mentor Notes: