Name: Ray Montes Jr.

Date: 4 Apr 25

Diving into SCADA Systems

BLUF

Simply put, this write-up will cover the vulnerabilities and the roles on mitigating risks that pertain to SCADA Systems and the infrastructure and applications.

Vulnerabilities

When we think of vulnerabilities, we can think of prioritizing functionality over security. The last thing we need for SCADA Systems is some type of malware infection or unauthorized access cyberattack. This can lead to possible insider threats, or even some type of third-party vendor risks. Additionally, in today's time, we seek to continuously update and utilize new hardware and software since outdated ones can become issues with the continuous updates and patches that companies spend millions/billions on. If vulnerabilities aren't identified within businesses, corporates or even government industries, this can cause an issue and allow them to become a target for cyberattacks.

Roles on Mitigating Risks

While SCADA continuously monitors for unusual activity, this can allow for productivity on how to better systems or issues that might be ongoing. Seen quite often, access control to authorized personnel is always being updated which can be incorporated with two step or multi factor authentication to continue to mitigate risks. Patch and system updates are vital to this system as it mitigates vulnerabilities that can be linked to old software that is being phased out. Lastly, having secure protocols can prevent leaks of

information, but it is best to believe that they are not always safe since someone out could be trying to hack the system.

Conclusion

SCADA Systems are vital in managing and keeping a secure critical infrastructure. While vulnerabilities exist due to malware infections, unauthorized access, insider threat, outdated hardware and software, etc., we can also keep an eye out and update systems and include an enhanced method of authentication. This would allow for strengthening security measures and to allow better safeguarding of material.