Robert Jacoby

Vulnerability management is an important part of a wholistic security plan. Most threat actors use existing vulnerabilities when attacking systems, this makes scanning and mitigating known vulnerabilities a very important part of your plan. To be successful, your strategy should include automating approved security patches. Your plan should include immediate updates for 0 day vulnerabilities, include applications and OS patches, and test environments to ensure that your patches do not cause widespread outages. This will ensure successful rollouts of your patches and decrease your time to mitigate these vulnerabilities. After your successful plan to mitigate and patch systems is complete, scanning your systems to ensure that the patches have been installed and no new vulnerabilities are found. Vulnerability scanning will also notify you of misconfigured applications that may have undesirable authentication or additional unnecessary services and ports open and running. These types of vulnerabilities will require you to work closely with the application teams to ensure they can test and deploy required application changes. Having only of these mitigation types in place will still leave you vulnerable to attack, so ensure that your strategy looks at patching and monitoring to protect your data and systems.

Johnny santos

Vulnerability management plays a key role in an information security plan because without the proper channels to identify vulnerabilities in your organization's network, you would surely leave opportunities for threat actors. It is extremely important to reduce the window of opportunity for threat actors. If there are many windows of opportunity for attackers, they will take it and cause many issues for your organization in the process. That is why it is important to reduce the window of opportunity as much as possible and ensure all employees are familiar with the processes and procedures in the event of an attack. Vulnerability scanners are useful because after analyzing the data from the scanner, the organization can identify opportunities for increased security posture. Patch management is just as important because all of the software used by your organization needs to be kept up to date to decrease the window of opportunity for attackers. All of the topics covered are crucial in order to keep an organization's security posture well rounded.