QUANTUM EVOLVE

Phasers locked on: identify which third parties pose a security risk

Welcome, fellow space travelers, to a blog that delves into the technical controls of third-party vendors and assesses their security readiness in Star Trek terms!

As we explore the vastness of the galaxy, we encounter many alien races and cultures.

In the same way businesses rely on third-party vendors for various services, from software development to cloud hosting. However, relying on third-party vendors comes with the risk of exposing sensitive data and intellectual property.

Thus, it is essential to assess the security controls of these vendors to mitigate risks effectively.

Now, let's imagine we are on the USS Enterprise, and we have to validate the technical controls of a third-party vendor.

QUANTUM EVOLVE

Phasers Locked On: Identify All Third Parties

To begin our mission, we need to identify all the third-party vendors that have access to our systems and data. It's like scanning for cloaked Romulan ships in space. We need to identify them all to determine which ones pose a security risk. Once we have identified them, we will use our tricorders to scan their technical controls.

Tricorder Scan: Assess Third Party Security

We will use our tricorders to scan the technical controls of the third-party vendors. Our tricorders will analyse the vendor's security policies, procedures, and technology controls. We will look for evidence of the following:

Secure Authentication: Strong password policies, multifactor authentication, and encryption. It's like verifying the security codes on a Starfleet vessel before allowing them to dock.

Data Encryption: Data encryption at rest and in transit. It's like protecting sensitive data in a force field.

Vulnerability Management: Regular vulnerability assessments and patch management. It's like scanning for anomalies in subspace signals.

Incident Response: An incident response plan that includes backup and recovery procedures. It's like having a ready-to-go medical team in case of an emergency.

Compliance: Compliance with industry standards and regulations. It's like following the Prime Directive and abiding by Starfleet's code of ethics.

QUANTUM EVOLVE

Red Alert: Highlight Security Risks

After scanning the vendor's technical controls, we may identify some security risks. It's like detecting a Klingon ship on our sensors. We will raise a red alert and take action. We will notify the vendor of the security risks and require them to provide a plan of action to remediate the issues.

Warp Speed Ahead: Monitor Third Party Security

Once the vendor has remediated the security risks, we will monitor their security posture continuously. It's like maintaining a state of readiness while traveling at warp speed. We will use our tricorders to scan the vendor's technical controls periodically to ensure that they continue to meet our security standards.

In conclusion, assessing the technical controls of third-party vendors is essential to mitigate risks effectively.

Remember, always keep your phasers locked on, use your tricorders to scan, raise a red alert when necessary, and monitor their security posture continuously.

The Quantum Evolve Security Controls Assessment for Third Parties pinpoints those servers, desktops and other endpoints that are vulnerable and susceptible to hackers due to a lack of security controls.

Contact us to understand your business' Cyber Resilience against cybersecurity threats and response to Ransomware and other real-life cyber-attacks.

Live long and prosper!

www.quantum-evolve.com