X-Force Red

IBM **Security**

X-Force Red Cloud Testing Services

With more companies moving to public, hybrid or multi-cloud environments, misconfigured cloud services and assets become more commonplace. Developers who focus on delivering a production application under strict deadlines, may use suboptimal coding practices (such as poor secrets management) or fail to enforce the principle of least privileges. Many companies also incorrectly assume their Cloud Service Providers (CSPs) are responsible for building security into their products.

While CSPs offer security tools for their customers, those controls are not one-size-fits-all and are not tailored “out-of-the-box” to protect each company’s unique requirements around data protection. This is true even in cases where cloud services are provided as a fully managed offering (PaaS) by a CSP, where security controls may be included as part of the service, however, companies may not be configuring them properly. X-Force Red Cloud Testing Services can uncover and help fix cloud vulnerabilities and misconfigurations that may expose your most valuable data to attackers.

Cloud Configuration Review

–X-Force Red assesses public cloud instances to validate secure configurations, protocols and best practices are being followed.

–X-Force Red uses CSPs’ native tools, as well as open-source and in-house developed tools to find known vulnerabilities and misconfigurations, ranks the flaws "critical" “high” “medium” or “low” and provides a report of findings and remediation recommendations.

–Configuration reviews can help you understand which problems you should fix immediately.

Cloud Penetration Testing

– X-Force Red hackers determine how attackers may exploit misconfigurations and other flaws in the cloud infrastructure. The team looks for over-privileged users and roles, bad development practices, poor access controls, etc. and shows how attackers can use them to escalate privileges and access sensitive data.

– X-Force Red provides a customized narrative of what they found, how they leveraged the flaws to gain deeper access, and what attackers could potentially do with your data. Reports include a risk ranking and remediation recommendations so that you know which actions to take to reduce your risk of an attack.

To learn more visit **https://www.ibm.com/security/services/cloud-testing**