X-Force Red

IBM **Security**

X-Force Red Cloud Testing for AWS

Common Security Challenges

Whether it's Elastic Compute Cloud (EC2), Elastic Container Service (ECS) or serverless applications, many companies are implementing AWS platforms. If not implemented and managed securely, these platforms may expose sensitive data to an attacker, which is why security should go hand-in-hand with all cloud migrations.

Unintentional developer mistakes can be the most prevalent flaws in an AWS environment. Containers are spun up quickly, without proper security vetting. Misconfigurations, a lack of hardening, application logic flaws, exposed credentials, default passwords, and other security weaknesses can provide potential attackers too much visibility into sensitive AWS applications. Serverless applications can contain authorization flaws, which enable users to obtain too much access. Just one authorization token that's not configured correctly can allow a user to see other users' data. Some containers are also designed without security in mind, creating opportunities for abuse.

X-Force Red Cloud Testing

X-Force Red's team of veteran hackers has extensive expertise helping secure cloud environments, which includes AWS environments. The team's services include:

Testing AWS deployment

– X-Force Red's penetration testing identifies flaws such as S3 and Lambda misconfigurations, and excessive key rights, and helps fix vulnerabilities prior to deployment.

Vulnerability management for Elastic Compute Cloud environments

– X-Force Red Vulnerability Management Services (VMS) tracks new containers, assesses software versions in use, checks for secure provisioning, scans for known vulnerabilities, automatically ranks findings, and facilitates remediation.

Reporting and recommendations

– X-Force Red presents a detailed report, which includes findings, methodology, an attack narrative and recommendations for remediation.

Testing serverless applications

– X-Force Red pulls apart applications, reviews source code, assesses security controls on browsers and mobile applications, assesses authorization token configurations, looks for AWS access keys and unauthorized method calls, and abuses functionality to test security controls' response.

– Tests are performed before and after applications are released.

Testing Elastic Container Service

– X-Force Red tests sample containers and images before they are released.

– Tests identify logic flaws, open ports, insecure application deployment and more.

– X-Force Red VMS scans for known vulnerabilities in the ECS framework.

X-Force Red offers flat rate project-based work or subscriptions and provides on demand access to all X-Force Red security testing services. Learn more at **https://www.ibm.com/security/services/cloud-testing**