X-Force Red

IBM **Security**

X-Force Red Container Testing Services

Common Security Challenges

From configuration data and API keys to payment card information and social security numbers, containers can hold highly sensitive information, which can make them a top target for attackers. Many of the security problems surrounding containers are not inside the containers themselves, but rather within the systems, or context, used to run them at scale. Containers can run in different cloud environments, each of which has a different level of protection. In one instance, for example, permissions for an application inside a container may be incorrectly configured, or permissions to access an application may be too broad, enabling a person to access more resources than they need. Those types of flaws can enable attackers to use the container as a pivot point into other parts of the network.

The X-Force Red Container Testing Services can help you uncover and remediate flaws inside and around containers in the cloud. The testing covers the entire container attack surface, which includes container orchestrators (Kubernetes), applications and other parts of the supporting infrastructure. The X-Force Red Container Testing Services can be performed from an "assumed application compromise" or "admin access" standpoint (the latter is encouraged to best optimize results).

X-Force Red Container Testing Services

Discover and Access

- ✓ Details the components of your environment such as how containers are running, orchestrators they are using, and other technologies supporting the infrastructure.
- ✓ Maps potential attack access points into the containers themselves and surrounding environment.

Enumerate and Assess

- ✓ Identifies external paths of compromise against a cluster, including accessing applications and CI/CD pipelines.
- ✓ Determines the types of secrets, credentials, service account tokens, and other sensitive data an attacker could access.
- ✓ Enumerates which types of permissions are in the environment in combination with the accessible secrets, and types of applications, capabilities, and controls with which an attacker could interact.
- ✓ Identifies and analyzes secondary exploitation paths and how attackers can leverage them for lateral movement.

Exploitation

- ✓ Exploits findings to determine how attackers can leverage them, which assets they can access, and the impact of a compromise. Shows areas where sensitive data is exposed.

Reporting

- ✓ Delivers a report of findings, a narrative of explored attack paths and remediation recommendations.

Each test takes approximately 1-3 weeks to complete. For more information, visit https://www.ibm.com/security/services/cloud-testing