Container and Orchestration Review

Container Engine Review

Systems running software like Docker or Podman generally run standalone and provide the ability to run multiple instances of containerised software on a single host. A container engine review will help you to understand the risks and vulnerabilities introduced to your environment and provide guidance in improving security in these areas.

Containerisation reviews are typically performed white-box, and cover areas such as host service and network hardening, authorization and authentication, and a review of running container configuration.

Findings typically range from low-level container primitives (e.g. Linux namespacing and resource isolation) to high-level perspectives such as overall organisational use of containers.

These reviews typically include container breakout attempts, both from a container to the running host and from a container to any accessible network services such as the node's local network or any cloud infrastructure services.

Orchestration Configuration Review

Orchestration technologies such as Docker Swarm or Kubernetes bring many benefits but also bring a significant increase in complexity, and the associated attack surface. An orchestration review addresses these complexities and identifies your platform's adherence to best practices.

This includes working with development teams to understand your deployment workflows and ensure that developers are given the freedom to deploy workloads while maintaining security throughout your environment.

Our recommendations will consider the threat model of your environment, including considerations such as multi-tenancy and the use of any cloud resources, and provide actionable recommendations. Like a container engine review, these assessments are typically performed from a white-box perspective.

As part of the assessment, we will consider scenario-based positions tailored to your environment, such as authenticating as a developer with a "standard" set of permissions.

Container Image Review

Applications packaged as container images are a core part of a containerised environment, and the security of individual images can have as much of an impact on the security of the container runtimes and orchestration platforms.

A container image review is a deep dive into individual images and provides insights and recommendations around image patching and distribution, secrets management, and overall adherence to best practices.

Compromised Container Assessment

If an attacker can compromise a containerised service, it is key that you understand the potential blast radius of this compromise. During a compromised container assessment, we perform breakout testing from a crafted container in your environment, and attempt to gain access to other services or to move laterally to other systems. These activities are typically performed as part of a wider assessment but can be performed stand-alone as required.

For more information from NCC Group on our G-Cloud 15 service, please contact:

+44 (0)161 209 5200

bidteam@nccgroup.com