5 TIPS for CONTAINER SECURITY

1 Shift left

Shift responsibility for security left into the hands of developers. Container security means making security an integral part of all release cycles, not a side concern to be picked up by operations down the pipeline.

2 Reduce attack surfaces

Build only what you need, so there are fewer vulnerabilities for hackers to exploit. Replace general-purpose OSes with container-specific equivalents that disable unnecessary services and functionalities.

3 Adopt container-specific tools

Container-specific tools, will be more able to understand the traffic in distributed networks and enforce security policies. Processes and tools must support the new ways of developing and running applications.

4 Group containers

Group containers by relative sensitivity and limit unbounded network access. Containers within unbounded networks can access each other and their hosts; once a container is exploited, all other containers within its kernel are also compromised.

5 Automate runtime configurations

Create standards for each type of container runtime and automate their configuration. Doing so will let you respond to vulnerabilities faster and with less operational burden.

cloudops.com/blog/a-brief-guide-to-securing-containers-at-scale/

CloudOps