Effective Container Security for Security and Compliance

Murray Goldschmidt[1]
[1]*Sense of Security*

Container-based virtualisation is an approach in which the hypervisor runs as an application within the operating system (OS). In this approach, the OS kernel runs with several isolated guest virtual machines (VMs) installed on top of it. The isolated guests are called containers and are highly flexible allowing apps or VMs to move from one hypervisor to another.

The rapid adoption of software containers presents a rare opportunity for security to become integrated early and maintained throughout the software delivery pipeline. It also provides the opportunity to share this knowledge across industry sectors so that all entities with DevOps environments can achieve “baked in” security with reduced effort tangible results.

While containers provide excellent opportunities, they also introduce unique new risks. But containers were not inherently architected with security in mind and are not always deployed securely.

Effective “securitisation of containerisation” will have wide scale positive impact for the future of online business.

This presentation will cover:

1. The difference between application virtualisation and virtual containers.
2. Managing vulnerabilities in container images
3. Attack surface reduction
4. Access control management
5. Configuration security and hardening
6. Automation for DevOps deployment processes
7. Implications for Compliance
8. Coverage for OS's, Apps