Practical Course
Container Security

Patrick Stöckle

Benedikt Hofmann

Organization

Lecturers

- Patrick Stöckle patrick.stoeckle@siemens.com
- Benedikt Hofmann hofmann.benedikt@siemens.com

Company/Department

Siemens AG
Technology
Cybersecurity & Trust
Security Architecture

SIEMENS

Products & Services Industries Company

Company > Innovation > Siemens Company Core Technologies > Cybersecurity & Trust

Cybersecurity & Trust

Organization

Biweekly, on-site theory sessions. 3h hours slots (no worries, we will have 5min after ~55min)

There will be graded exercises via Artemis. You can hand in your solutions for the exercises on Artemis until Wednesday, 23:59. You can get X points in the graded exercises.

If you have questions regarding the exercises, you can post them in the Artemis question section.

Furthermore, there will be a team project. In the team project, you must apply the learned concepts to real-world scenarios. In the end, each team will present their projects results. We will grade the presentation and your code, and you can get again X points.

Thus, the final grade will be determined by your performance in the exercises and the projects.

Previous Knowledge Expected

- IN0006: Introduction to Software Engineering
  - Programming skills
  - Version control with git
- IN0009: Basic Principles: Operating Systems and System Software
  - General knowledge about the Linux OS
- IN0010: Grundlagen Rechnernetze und Verteilte Systeme
  - General knowledge about networking and firewalls
- IN0042: IT Sicherheit
  - General knowledge about security concepts like hash functions, encryption schemas, signatures

We do **NOT** assume that you are a Docker/container expert, but that you **SHOULD** have built/run your own containers already

Topics

Container Fundamentals

Attack surface reduction via multistage builds and minimized base images, e.g., Google distroless

Runtime restrictions, e.g., via seccomp profiles and Linux capabilities

Rootless container runtimes, e.g., podman

Anomaly detection for containers, e.g., via falco

Container image signing and secure container registries

Topics

K8s native network restrictions

Policy enforcement with Open Policy Agent

Role-based access control on orchestrated container runtimes

Secret and certificate management, e.g., Vault and cert-manager

Secure logging

Service meshes, e.g., Istio and Cilium

Vulnerability scanning, e.g., trivy

Questions?