



Virtualisierung zu Trainings- und Entwicklungszwecken

CODE Jahrestagung Workshop

DEFENCE AND SPACE

Dr Cora Perner, cora-lisa.perner@airbus.com

12 Juli 2023

AIRBUS

Was erwartet Sie bei diesem Vortrag?

- Welche Fragen stellen wir uns?
- Kurze Vorstellung der Implementierung
- Welche Bedeutung hat Virtualisierung im industriellen Kontext?

Was erwartet Sie bei diesem Vortrag?

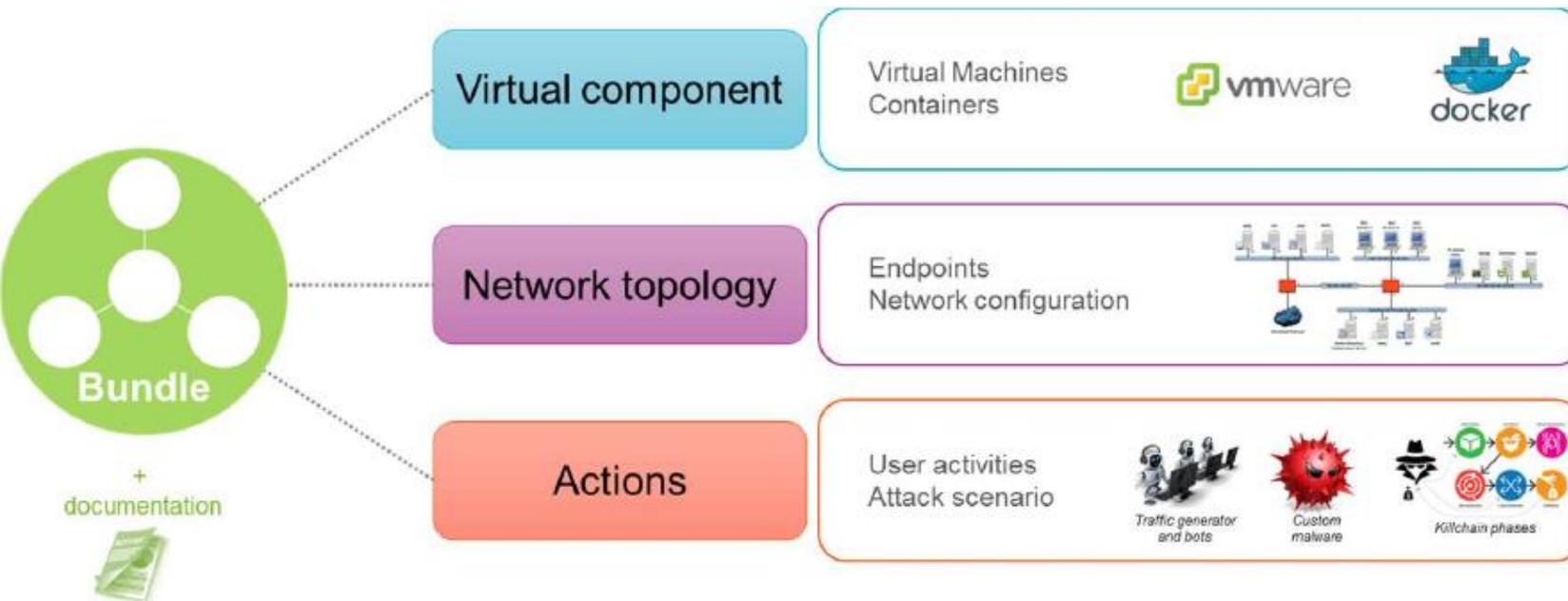
- Welche Fragen stellen wir uns?
- Kurze Vorstellung der Implementierung
- Welche Bedeutung hat Virtualisierung im industriellen Kontext?

Spezifische Fragestellungen:

- Wie kann anwendungsspezifisches Wissen in komplexen, sicherheitskritischen Systemen erzeugt werden?
- Wie können Effekte von Cyberangriffen auf reale Systeme veranschaulicht werden?
- Wie können reale/realistische Szenarien erzeugt werden, um sie für Entwicklung, Wartung und Betrieb zu nutzen?

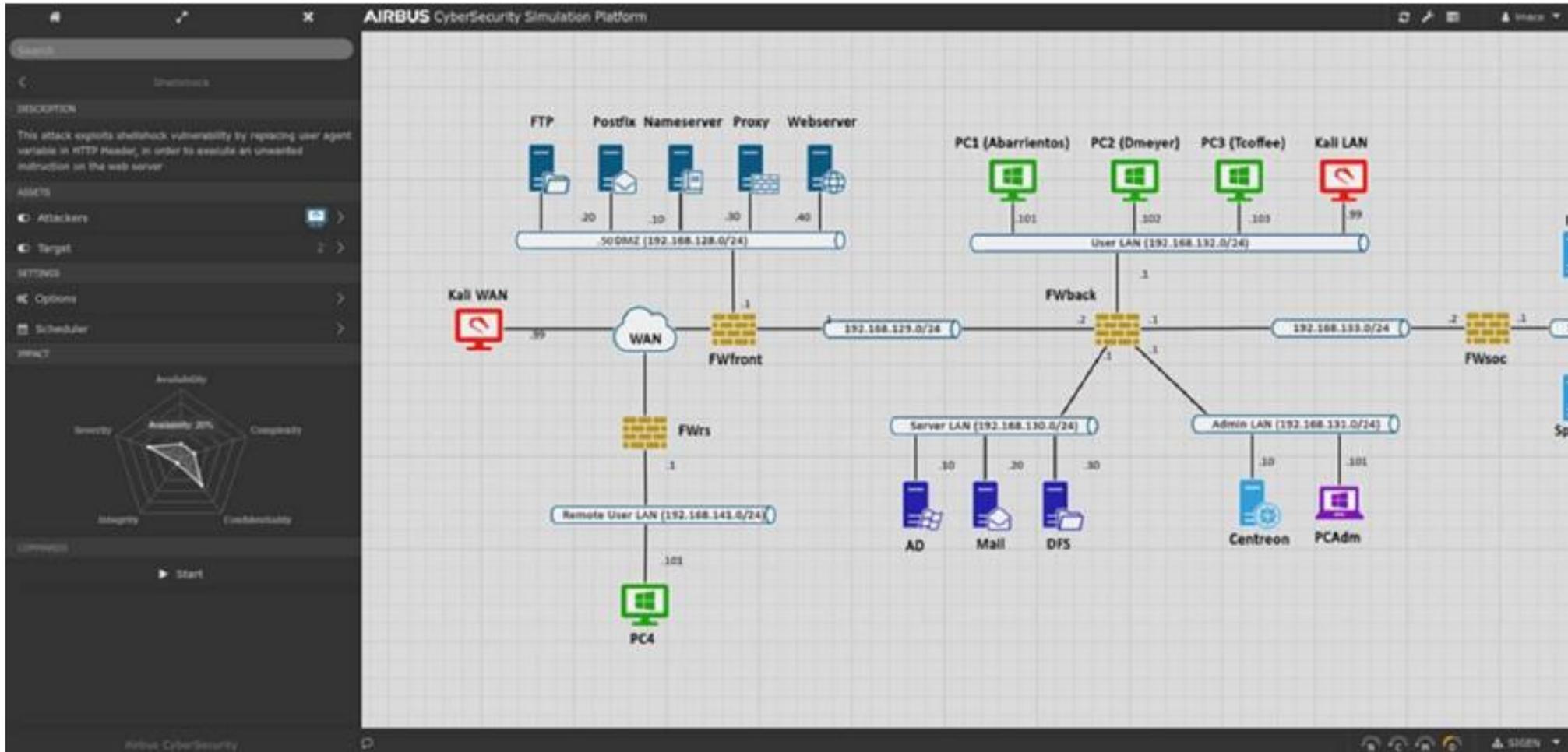
Technische Implementierung

- Eigenes Softwarepaket integriert mit den Virtualisierungsmechanismen (Docker & VMWare)
- Benutzer interagieren über einen Webbrowser
- Verschiedene Varianten: Stand-alone, im Rechenzentrum integriert oder virtuell
- Einbindung von physikalischen Systemen möglich

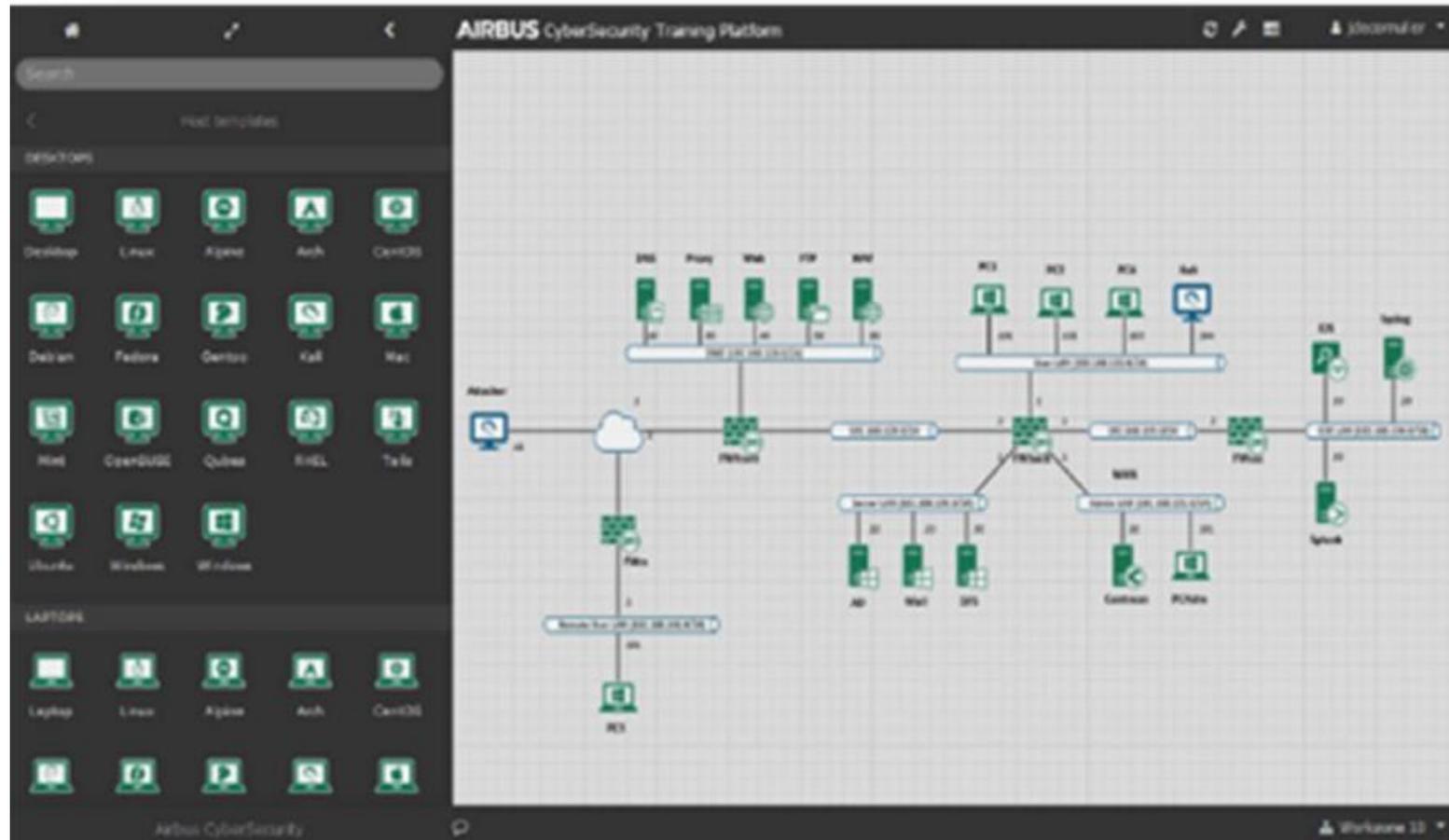


Airbus CyberRange

Integrierte Vorlagen und Szenarien



Airbus Cyber range Baukastensystem



Kollaboration

- Fertige Topologien können exportiert werden und geteilt werden

AIRBUS CyberRange Hub Explore Administration

Explore Bundles

Search bundle ... 1 - 15 on 17 Most Popular

Filters:

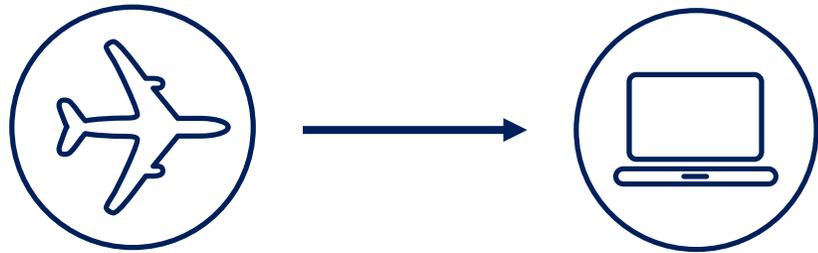
- Favorites

Labels:

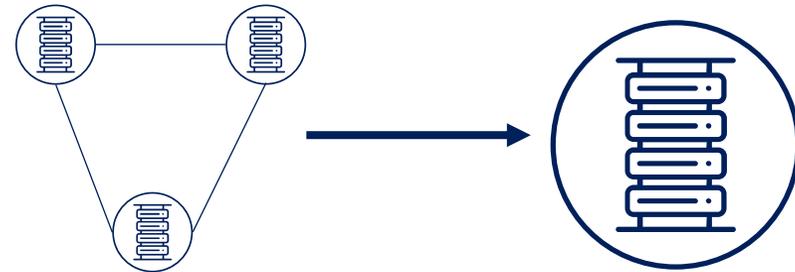
- Redteam
- C2
- Attack
- Linux
- SOC
- IDS
- Incident
- Realist
- Response
- Software
- Custom label ...

Bundle Name	Version	Download Count	Labels
SIGEN	1.0.3	14	Realist
Starter-Pack-IT-Linux	21.5	17	Linux
Velociraptor	0.6.3	-	FORENSIC, DFIR
C2	1.0.0	-	C2, Attack, Redteam
Starter Pack IT Linux	22.01.1	1	Linux, starter-pack
PoshC2 - Command and Control	7.0.0	-	C2, Attack, Redteam
Caldera - Command and Control	4.0.0	-	C2, Attack, Redteam
Empire - Command and Control	4.3.3	-	C2, Attack, Redteam
Starter-Pack-IT-Scenarios	21.5	11	Linux
Aurora Incident Response	0.8.6	-	CSIRT, Response, Incident

Abtrennung digitaler Zwilling vs. Cyber range vs. cyber-physikalische Systeme?



Digitaler Zwilling
(physikalisches System)



Cyber Range
(IT System)



Cyber-physikalisches System?

Cyber ranges im industriellen Kontext

- Training
Anschaulichkeit, insbesondere für nicht-technische Teams (Illustration von Konsequenz von Cyberangriffen)
- Als Integrationsplattform
Sichere Testumgebung für neue Entwicklungen
- Zur Entwicklung?
Generierung von realistischen Datensätzen vor Einsatz von Überwachungssystemen