TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

"T.I.S.P. Community Meeting 2021"

Berlin, 03.-04.11.2021

Managing IT Security in Cloud Infrastructures

Dominic Pfeil, DCSO GmbH

Security Technology

Provides an **overview of the IT security market**
Tests IT security products against customer use cases
Brings together **IT security experts** across borders

Dominic Pfeil

Senior Technology Analyst
with DCSO since 2017

The TEC Team

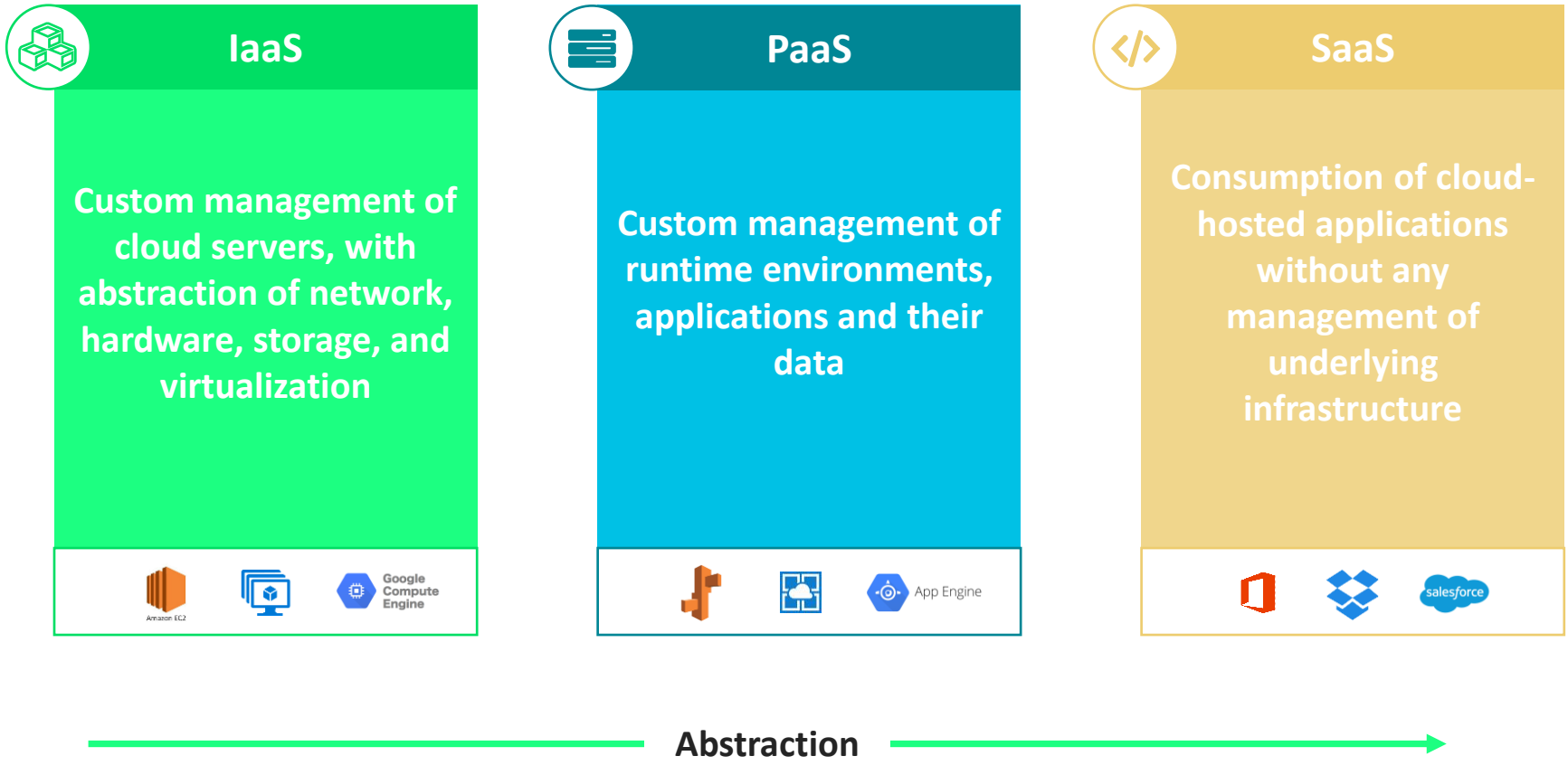
Tested over **80 products** from different domains
Participated in over **500 product demonstrations**
Active since 2017

DCSO
Engineering Security.
Together.

Deutsche Cyber-Sicherheitsorganisation GmbH

Founded 2015
Joint Venture of Allianz SE, BASF SE, Bayer AG, and Volkswagen AG
Offers shared cyber-security services and coordinates collaboration efforts

Cloud Computing: Technical Implementation
Abstraction Levels in Cloud Environments



Cloud Computing
Cloud Workloads

1. **Virtual Server**
   Access to virtualized server systems with complete management of resources, operating system, network, and application stack

2. **Cloud Application**
   Deployment of (web) applications in a runtime provided by the cloud provider — abstraction of underlying server, with management options for scalability

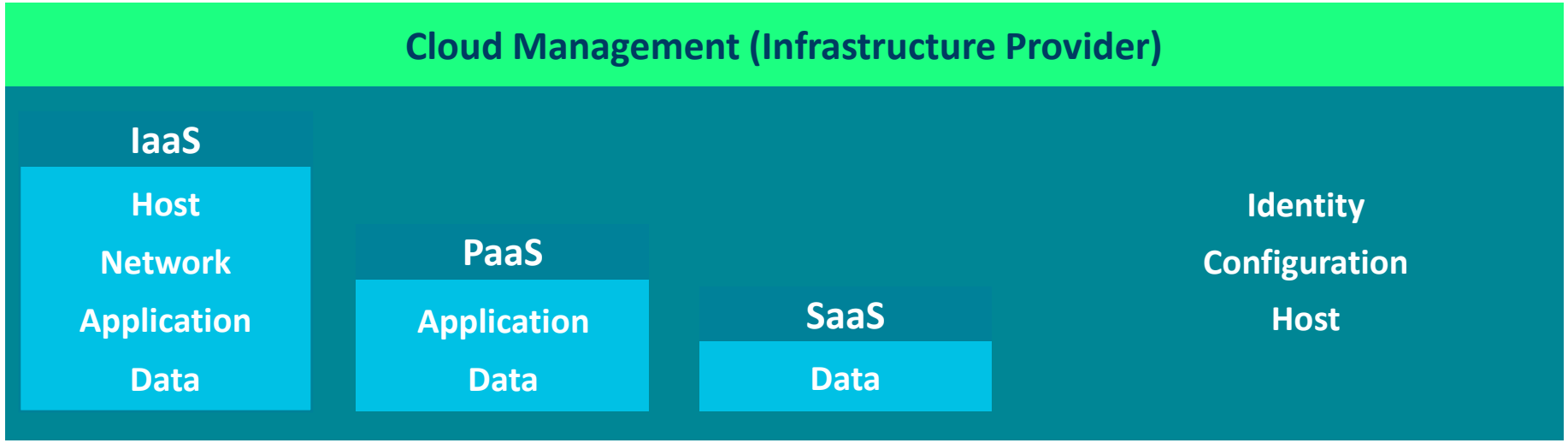
3. **Container**
   Deployment and management of containers in cloud environments by utilizing either provider-specific or standardized orchestration solutions

4. **Database**
   Managed SQL/NoSQL database services without access to underlying server infrastructure

5. **Object Storages**
   Unstructured object storage accessible through API, without management of storage resources, their capacity, or scalability for users

6. **Cloud Functions**
   Execution of stateless functions that suppose the availability of all necessary components to execute the business logic — easy horizontal scaling available due to missing state

Cloud Computing
Protected Assets per Security Measure



Host – Platform to consume or provide services
Network – Components that enable enterprise communication
Application – Service provided on top of a host

Data – Information at rest or in motion
Identity – Context, aspects and rights related to human and machine identities
Configuration – Management of cloud environments

Securing Cloud Computing
Challenges of Diverse Infrastructures

- **Multi-cloud, multi-account environments**
- **Diverse target assets**
- **Large number of assets, accounts and applications leading to huge amounts of events**
- **Policy enforcement within dynamic & individual environments**

Missing visibility of IT Security Operators in Cloud Environments

Inapplicability of “Traditional” IT Security Solutions

Securing Cloud Computing
Comparison to know IT Security Capabilities

“Traditional” IT Security Products may work in cloud environments but lack capabilities to

- Cover and handle **security events in an abstracted way** (e.g., cloud infrastructure, host system)
- Scale across **large numbers of assets and networks**
- Target **volatile applications** and **storage systems**
- Engage a **broad attack profile**

Securing Cloud Computing
Product Capabilities

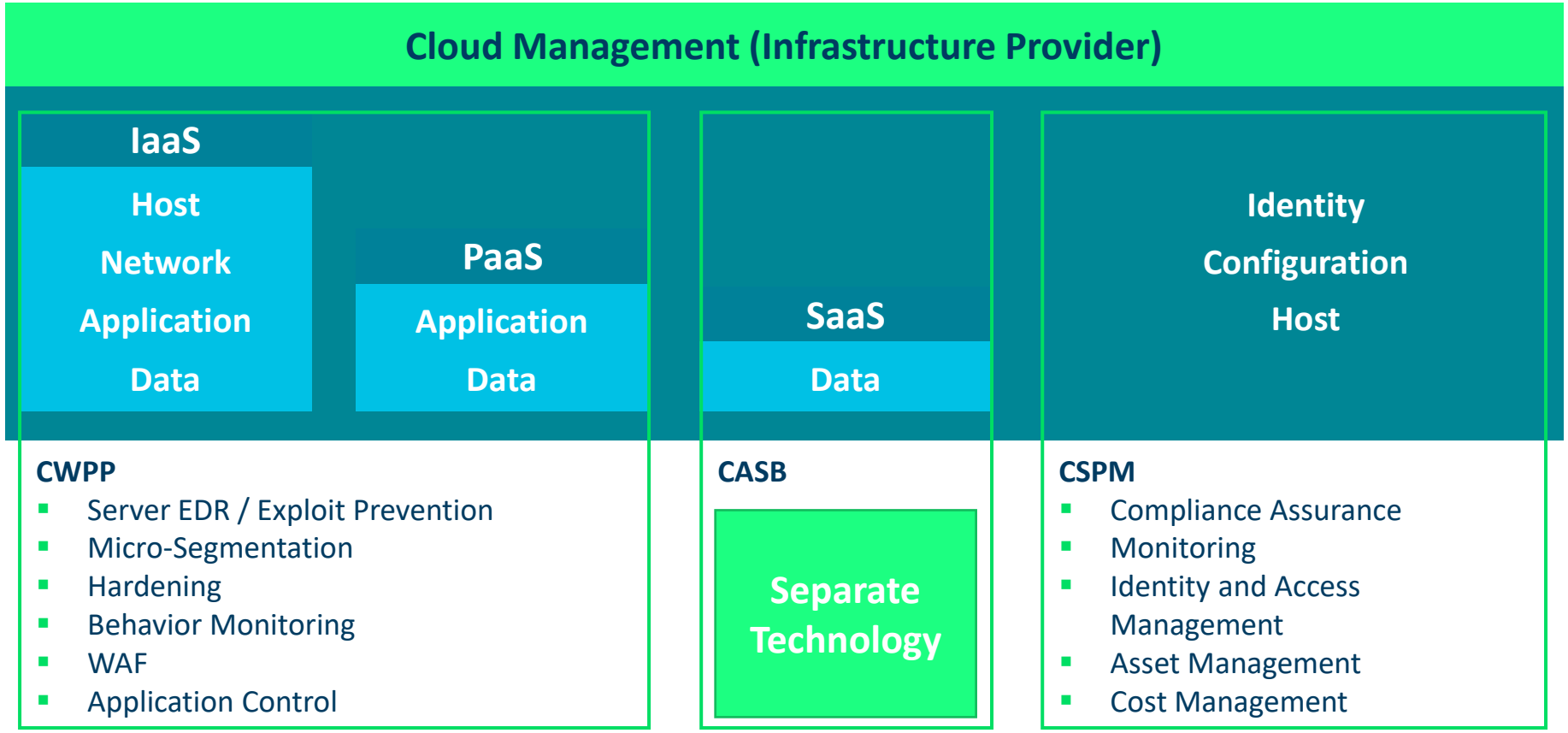
Cloud Security Posture Management (CSPM)

- Monitoring of cloud hyperscalers (e.g., AWS, MS Azure, GCP) and their configuration
- Comparison and attestation of compliance against industry frameworks
- Remediation of insecure configuration
- Detection of identities and their access rights
- Cost management

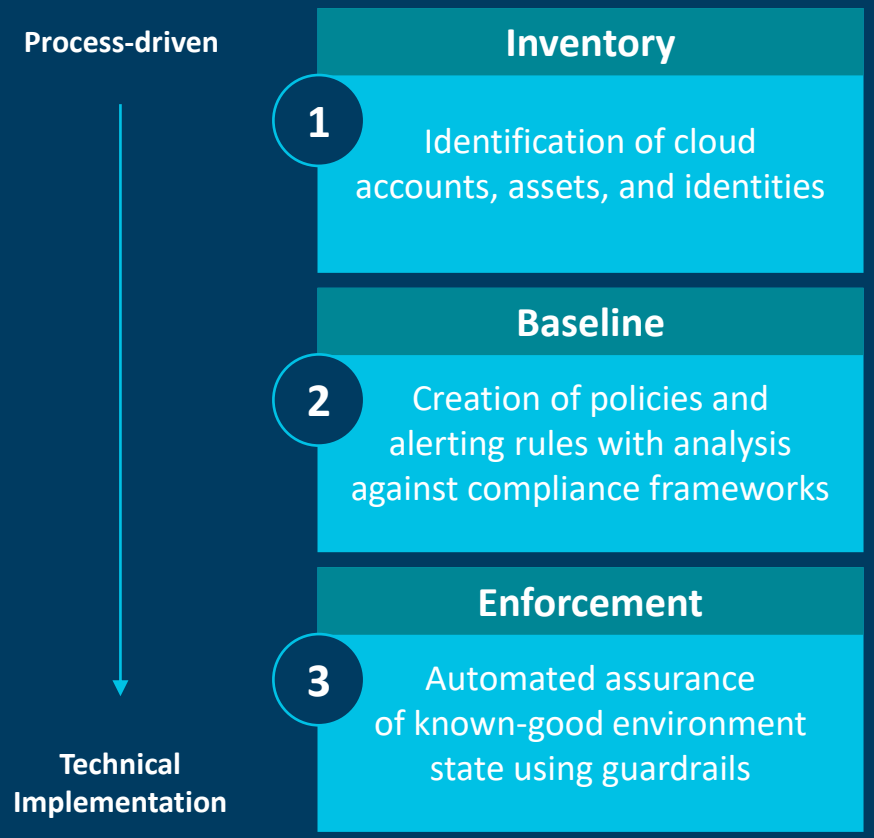
Cloud Workload Protection Platform (CWPP)

- Diverse functionality per asset type located in hyperscaler (differences in abstraction)
- Segmentation of networks and hosts
- Threat protection (Antivirus, Exploit Prevention, IDS/IPS)
- Application control, Web application firewall
- Container (Kubernetes) security

Cloud Computing
Protected Assets per Security Measure



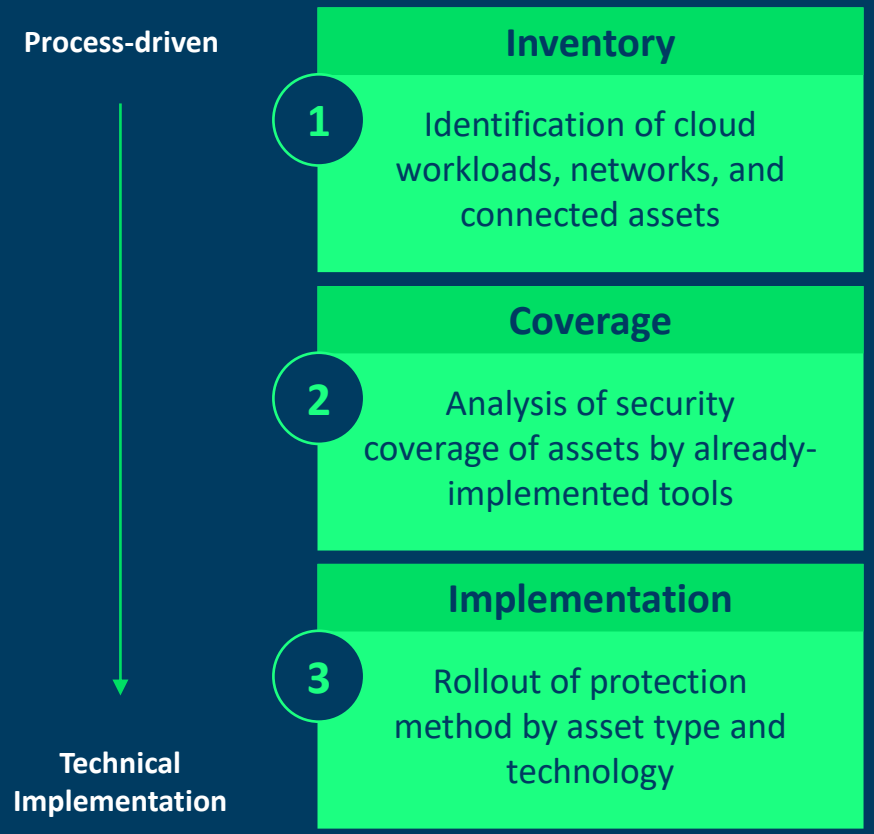
Securing Cloud Computing
CSPM: Designing a Setup Process



- Exchange of ideas and approaches with DevOps teams
- Definition and restriction of providers and technologies

- Backed by continuous refinement process
- Gradual extension of automated enforcements
- Audit-safe, continuous assurance of compliant infrastructure state

Securing Cloud Computing
CWPP: Designing a Setup Process



- Exchange of ideas and approaches with DevOps teams
- Alignment of protection methods with “traditional” asset types

- Extension of in-place technologies to cloud environments
- Gradual extension of covered asset types and technologies

DCSO
Engineering Security.
Together.

DCSO Deutsche Cyber-Sicherheitsorganisation GmbH
EUREF-Campus 22
10829 Berlin

dominic.pfeil@dcso.de

+49 151 43157947