DATEV

One Approach to a Cloud-Native Application Protection Platform from a Defender's Perspective

Pascal Güldiken
Security Operations Center

25.06.2025

Disclaimer

DATEV permits the use of these slides for internal purposes only. In particular, the user is prohibited from distributing, reproducing, otherwise exploiting, editing, making available, licensing or sublicensing to third parties in whole or in part.

About me

Cyberanalyst in the SOC @ DATEV

linkedin.com/in/pascal-g-8aabab170

Agenda

DATEV

- Introduction & Motivation
- Initial Situation & Problem Statement
- First Steps Toward Better Detection
- Implementing a CNAPP Solution: Improving Detection & Response
- Current Status & Implementation Challenges
- Lessons Learned & Next Steps
- Q&A

Goals of this talk

DATEV

- Share SOC-focused insights from a CNAPP implementation
- Improve detection & response in cloud and cloud-native environments
- Show what’s important for the SOC provided by CNAPP
- Highlight challenges & lessons from the PoC phase
- Provide actionable takeaways for SOC teams

Why is Cloud Runtime Security a Challenge for SOC teams?

- Dynamic environments
- Limited visibility
- High data volume & noise
- Lack of standardization
- Evolving threat landscape
- Separation of responsibilities

Leads to…

Difference between Traditional Security Monitoring and Cloud-Native Environments

- Static infrastructure (long-lived servers)
- Perimeter-based security (firewalls, VLANs)
- Centralized logging from fixed points
- Manual detection rules
- SOC is aware of the systems and logs

- Dynamic & ephemeral workloads (containers)
- Identity- and API-centric security
- Distributed telemetry from many services
- Scalable, automated detections (e.g., via CNAPP)
- Shared responsibility with DevOps & cloud teams

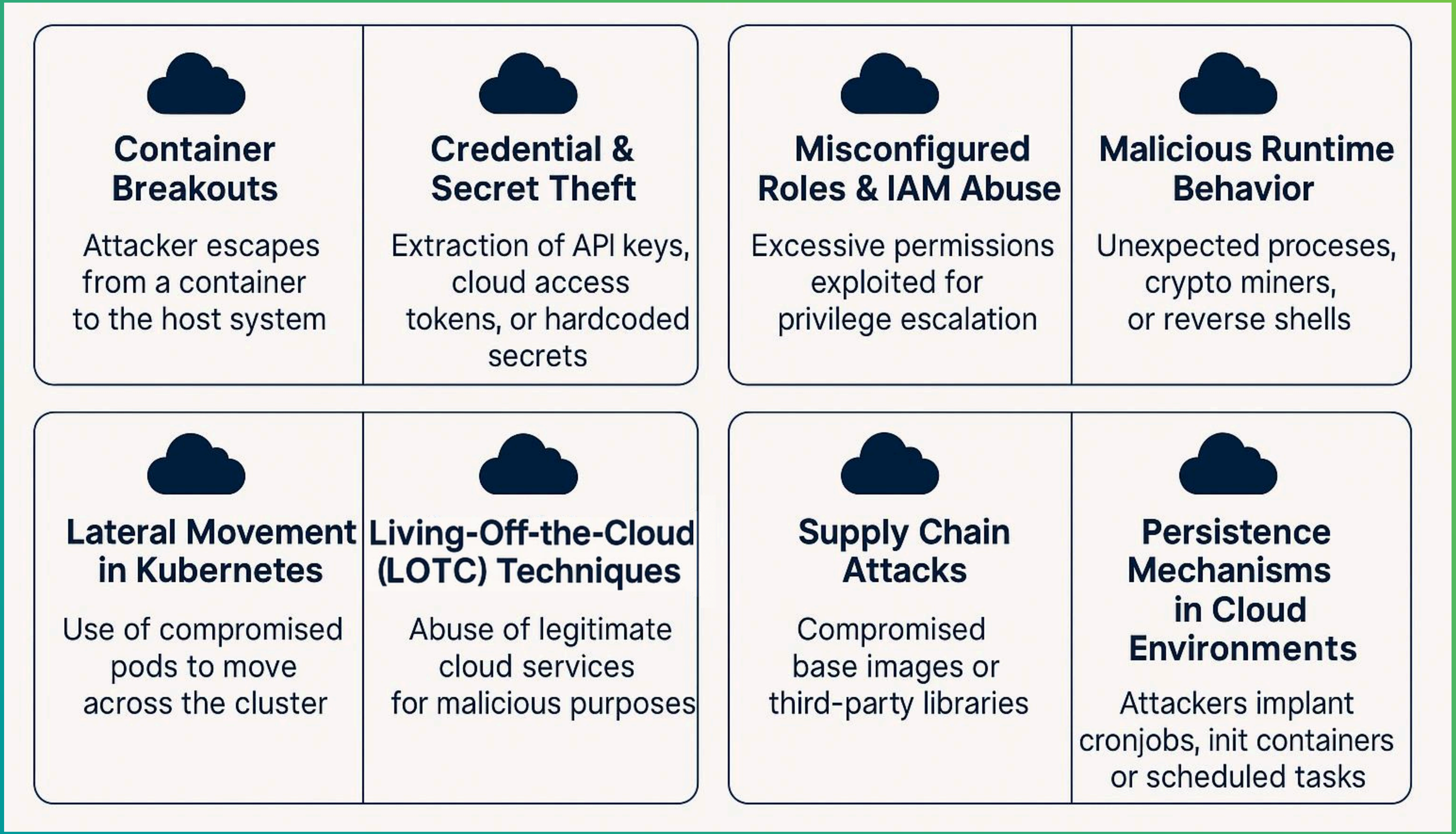
Our company‘s cloud transition: What changes are relevant for the SOC?

- Relocation of on-Premise resources to Cloud-Native & Public Cloud workloads
- Adoption of PaaS and CaaS (e.g. Kubernetes, Cloud Foundry)
- Existing SIEM didn‘t cover runtime behavior in cloud environments at all
- Need for collaboration with DevOps & Cloud teams
- SOC-Analysts faced skill gaps in cloud technologies

Why traditional SIEM-Monitoring is challenging nowadays

- **Cannot correlate identity, workload, and network behavior across dynamic environments**
- Struggles with the volume and velocity of cloud-generated telemetry
- Designed for static infrastructure (on-prem servers, fixed networks)
- **Manual rule creation isn't scalable for multi-cloud, fast-changing environments**
- Insufficient context from cloud provider APIs, metadata, and control planes
- **Often reactive, rather than proactive, in identifying modern cloud threats**
- Limited in detecting runtime threats within cloud workloads

Common threats & attack scenarios in cloud runtime environments in general



Container Breakouts

Attacker escapes from a container to the host system

Credential & Secret Theft

Extraction of API keys, cloud access tokens, or hardcoded secrets

Misconfigured Roles & IAM Abuse

Excessive permissions exploited for privilege escalation

Malicious Runtime Behavior

Unexpected proceses, crypto miners, or reverse shells

Lateral Movement in Kubernetes

Use of compromised pods to move across the cluster

Living-Off-the-Cloud (LOTC) Techniques

Abuse of legitimate cloud services for malicious purposes

Supply Chain Attacks

Compromised base images or third-party libraries

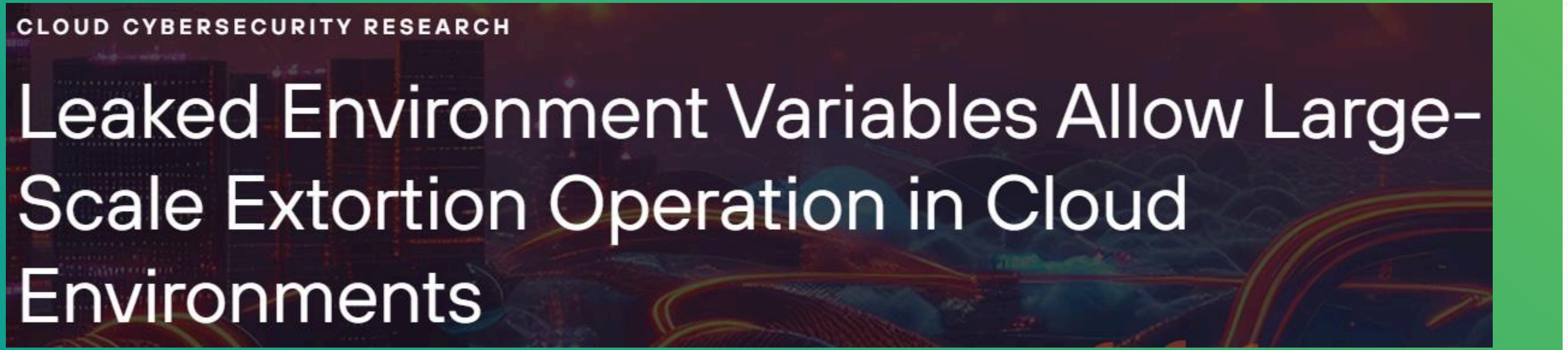
Persistence Mechanisms in Cloud Environments

Attackers implant cronjobs, init containers or scheduled tasks

Matrix - Enterprise - Cloud | MITRE ATT&CK®
Understanding CNAPP: Evolution, Components & Evaluation Criteria | Exabeam

Common threats & attack scenarios in cloud runtime environments – real world scenarios

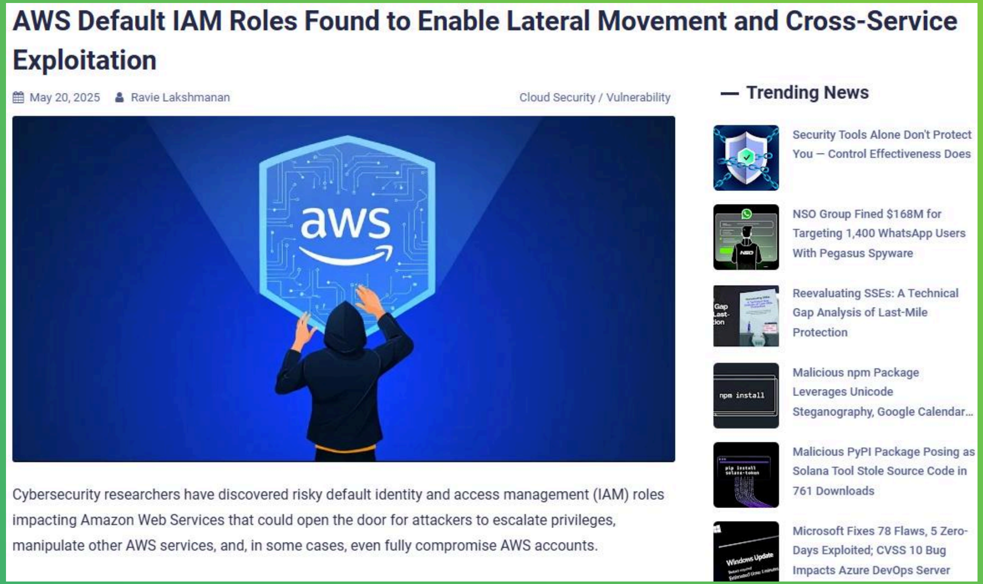
DATEV



CLOUD CYBERSECURITY RESEARCH

Leaked Environment Variables Allow Large-Scale Extortion Operation in Cloud Environments

Leaked Environment Variables Allow Large-Scale Extortion Operation in Cloud Environments



AWS Default IAM Roles Found to Enable Lateral Movement and Cross-Service Exploitation

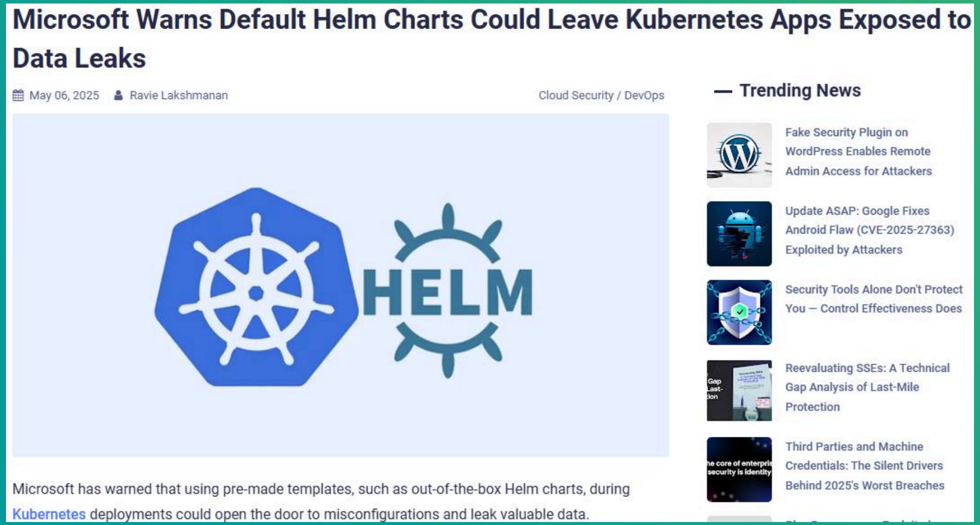
May 20, 2025 Ravie Lakshmanan Cloud Security / Vulnerability

Cybersecurity researchers have discovered risky default identity and access management (IAM) roles impacting Amazon Web Services that could open the door for attackers to escalate privileges, manipulate other AWS services, and, in some cases, even fully compromise AWS accounts.

— Trending News

- Security Tools Alone Don't Protect You — Control Effectiveness Does
- NSO Group Fined $168M for Targeting 1,400 WhatsApp Users With Pegasus Spyware
- Reevaluating SSEs: A Technical Gap Analysis of Last-Mile Protection
- Malicious npm Package Leverages Unicode Steganography, Google Calendar...
- Malicious PyPI Package Posing as Solana Tool Stole Source Code in 761 Downloads
- Microsoft Fixes 78 Flaws, 5 Zero-Days Exploited; CVSS 10 Bug Impacts Azure DevOps Server

AWS Default IAM Roles Found to Enable Lateral Movement and Cross-Service Exploitation



Microsoft Warns Default Helm Charts Could Leave Kubernetes Apps Exposed to Data Leaks

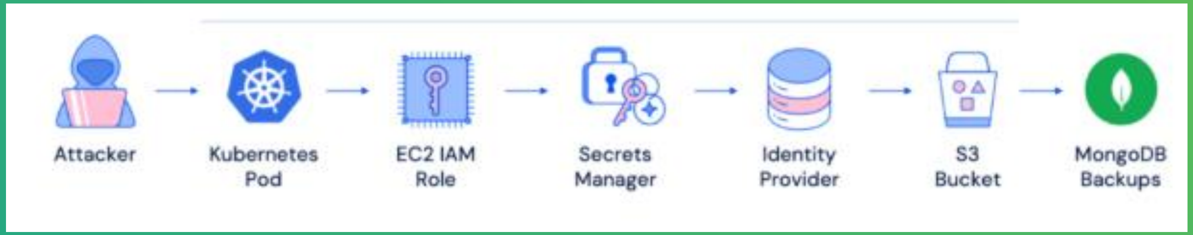
May 06, 2025 Ravie Lakshmanan Cloud Security / DevOps

Microsoft has warned that using pre-made templates, such as out-of-the-box Helm charts, during Kubernetes deployments could open the door to misconfigurations and leak valuable data.

— Trending News

- Fake Security Plugin on WordPress Enables Remote Admin Access for Attackers
- Update ASAP: Google Fixes Android Flaw (CVE-2025-27363) Exploited by Attackers
- Security Tools Alone Don't Protect You — Control Effectiveness Does
- Reevaluating SSEs: A Technical Gap Analysis of Last-Mile Protection
- Third Parties and Machine Credentials: The Silent Drivers Behind 2025's Worst Breaches

Microsoft Warns Default Helm Charts Could Leave Kubernetes Apps Exposed to Data Leaks



Attacker → Kubernetes Pod → EC2 IAM Role → Secrets Manager → Identity Provider → S3 Bucket → MongoDB Backups

Wiz on Cloud Security in 2025: Navigating the Future of Cyber Threats and Defense | GuidePoint Security

Cloud Defense: Playing Catch-up?

	🔒	💀
Visibility	Limited and not centralized	Sees what's exposed, misconfigured, open
Time to act	Hours to days	Seconds to scan, minutes to exploit
Tooling	Fragmented: SIEM, CSPM, EDR, IAM	Unified: Automated tools, C2, Scripts
Focus	Rule-based, behavior and anomaly detection	Obfuscation, evasion, impersonation

Our first thoughts to get more visibility

DATEV

- Initial situation: Not that much visibility about Cloud-Native environments
- Goal: Implement different Use-Cases for the SIEM to increase detection
- Challenges:
  - Lack of knowledge about the generated logs
  - How does Kubernetes actually work?
  - How is PaaS and Caas implemented in our organization?
  - Which logs are important for the SOC?
  - What is critical for detection?
  - Who is responsible for which logs?
- Outcome: We need specialized expertise

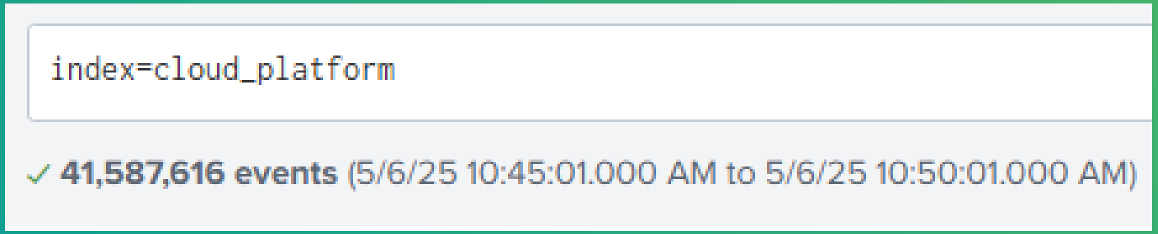
SwiftOnSecurity
@SwiftOnSecurity

One time I tried to explain Kubernetes to someone.
Then we both didn't understand it.

16:40 · 06/08/2019 · Twitter for iPhone

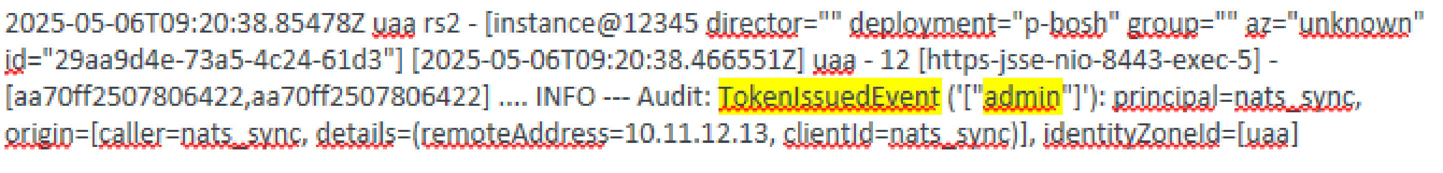
Analysis of existing log sources: What data was available, what was missing?

- Find the needle in the haystack! Get the relevant raw logs from several terabytes per day in our logging platform – What are the logging concepts?

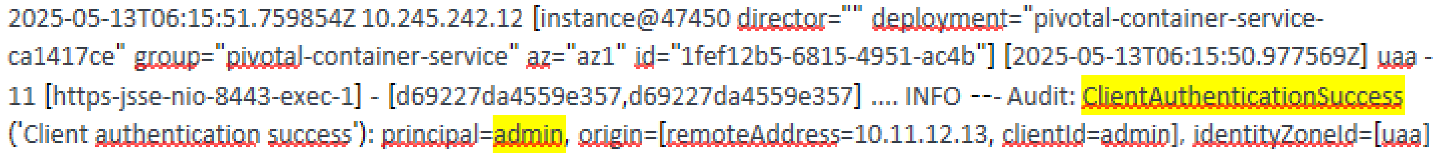


```
index=cloud_platform
```

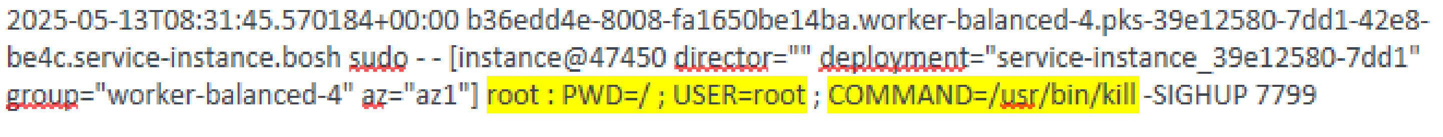
✓ **41,587,616 events** (5/6/25 10:45:01.000 AM to 5/6/25 10:50:01.000 AM)



```
2025-05-06T09:20:38.85478Z uaa rs2 - [instance@12345 director="" deployment="p-bosh" group="" az="unknown"
id="29aa9d4e-73a5-4c24-61d3"] [2025-05-06T09:20:38.466551Z] uaa - 12 [https-jsse-nio-8443-exec-5] -
[aa70ff2507806422,aa70ff2507806422] .... INFO --- Audit: TokenIssuedEvent ('["admin"]'): principal=nats_sync,
origin=[caller=nats_sync, details=(remoteAddress=10.11.12.13, clientId=nats_sync)], identityZoneId=[uaa]
```



```
2025-05-13T06:15:51.759854Z 10.245.242.12 [instance@47450 director="" deployment="pivotal-container-service-
ca1417ce" group="pivotal-container-service" az="az1" id="1fef12b5-6815-4951-ac4b"] [2025-05-13T06:15:50.977569Z] uaa -
11 [https-jsse-nio-8443-exec-1] - [d69227da4559e357,d69227da4559e357] .... INFO --- Audit: ClientAuthenticationSuccess
('Client authentication success'): principal=admin, origin=[remoteAddress=10.11.12.13, clientId=admin], identityZoneId=[uaa]
```



```
2025-05-13T08:31:45.570184+00:00 b36edd4e-8008-fa1650be14ba.worker-balanced-4.pks-39e12580-7dd1-42e8-
be4c.service-instance.bosh sudo - - [instance@47450 director="" deployment="service-instance_39e12580-7dd1"
group="worker-balanced-4" az="az1"] root : PWD=/ ; USER=root ; COMMAND=/usr/bin/kill -SIGHUP 7799
```

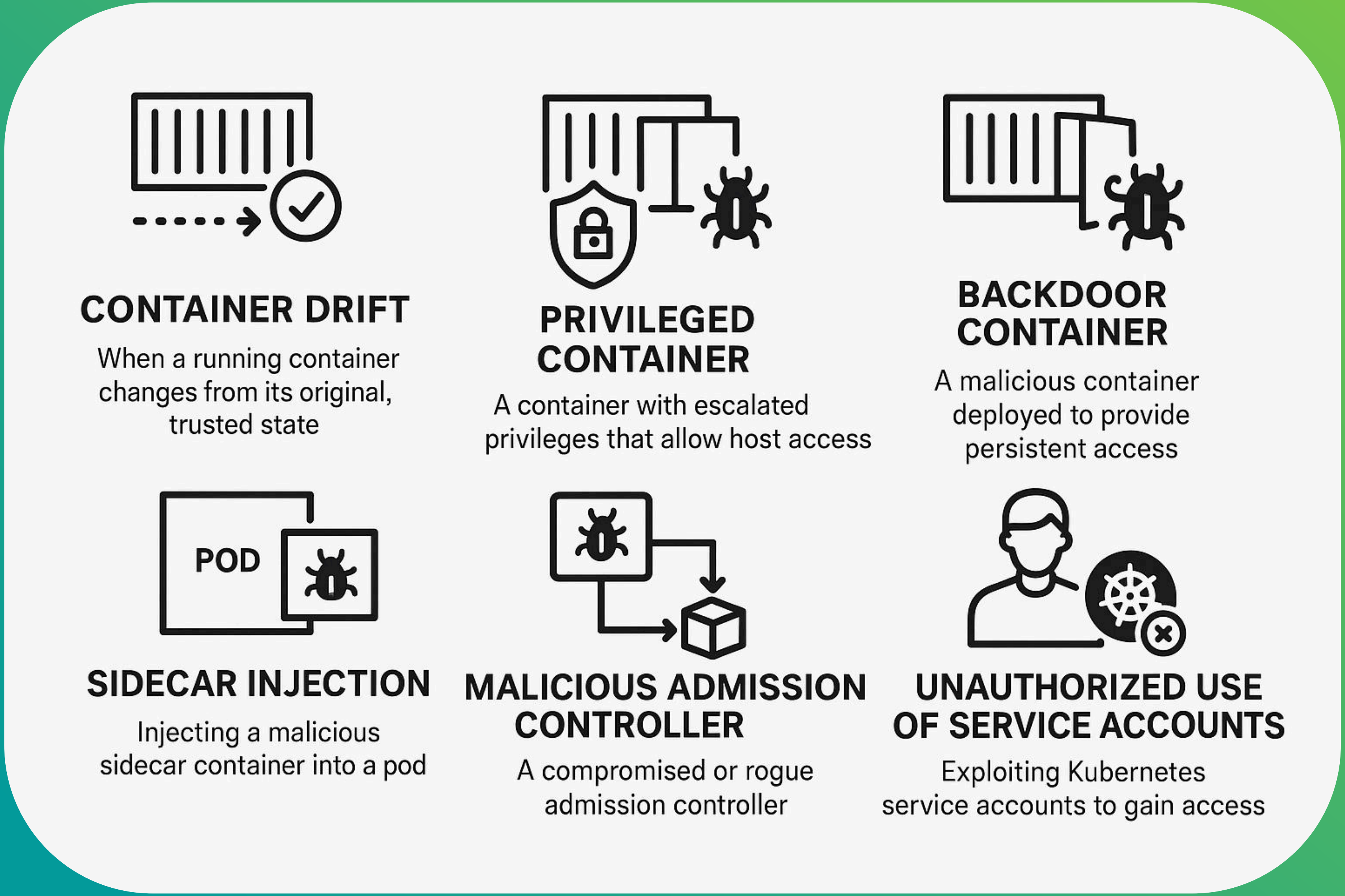
Analysis of existing log sources: What data was available, what was missing?

- Platform: Logs from the K8s-Platform itself
  - Audit
  - Kubelet
  - Kube-Proxy
  - Admission Configuration
- Application: Logs from the Applications which are running in K8s
- Runtime: Logs from behavior of the Pods and Clusters

→ Platform & Application Logs are good information for enrichment and correlation

Runtime Logs are essential for detection Use-Cases!

First theoretical detection Use-Cases for the SIEM



CONTAINER DRIFT

When a running container changes from its original, trusted state

PRIVILEGED CONTAINER

A container with escalated privileges that allow host access

BACKDOOR CONTAINER

A malicious container deployed to provide persistent access

SIDECAR INJECTION

Injecting a malicious sidecar container into a pod

MALICIOUS ADMISSION CONTROLLER

A compromised or rogue admission controller

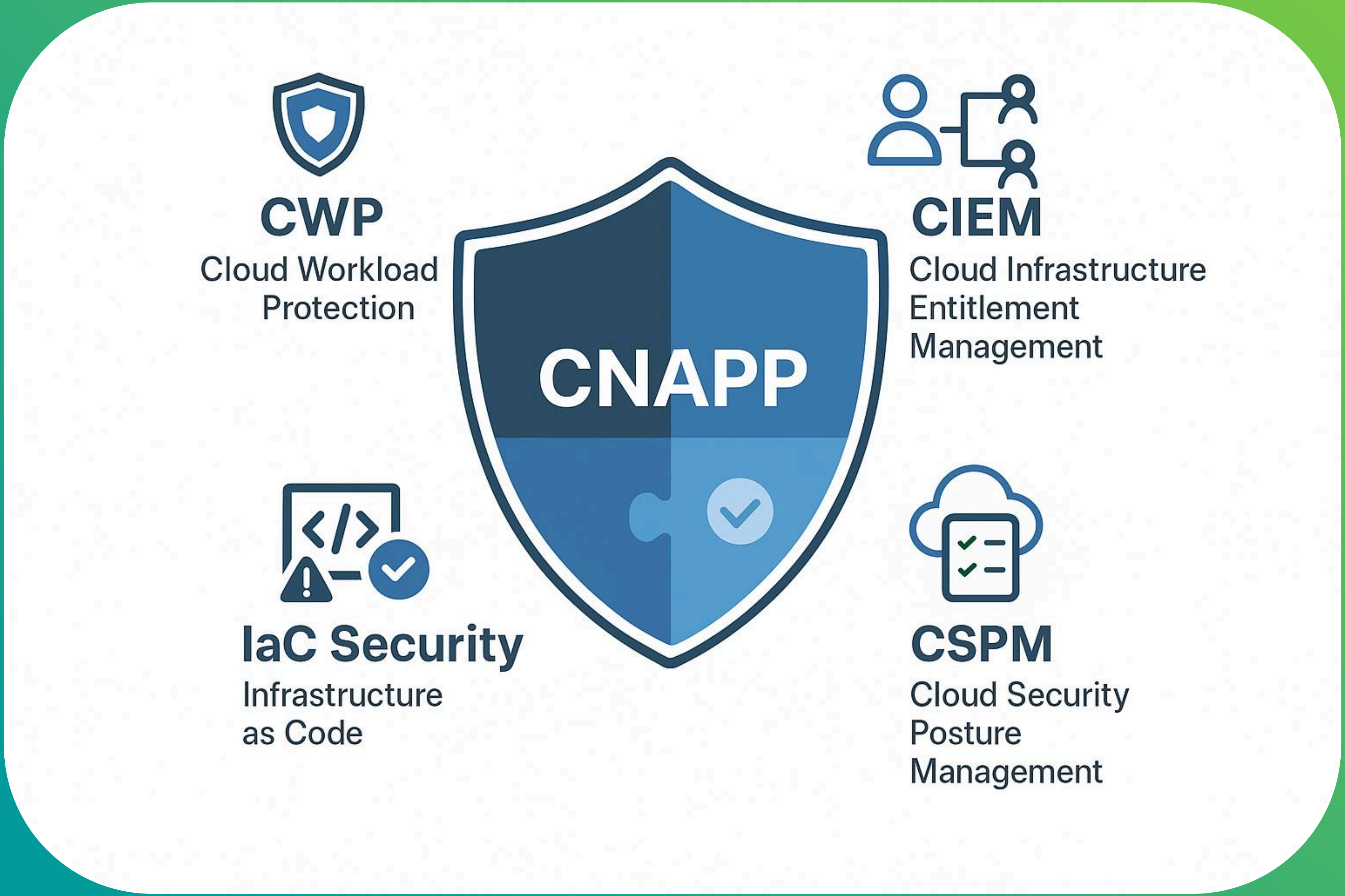
UNAUTHORIZED USE OF SERVICE ACCOUNTS

Exploiting Kubernetes service accounts to gain access

Challenges & limitations of manual detection mechanisms

- **Network, storage, and indexing costs can skyrocket without filtering**
- **Time-consuming implementation and maintenance of Use-Cases**
- High maintenance overhead to reflect changes in cloud services & rule tuning
- Limited scalability – Handcrafted rules don’t scale across dynamic environments
- **Lack of detecting Advanced Threats like behavioral anomalies & Zero-Days**
- Environments are too dynamic – Challenging for Asset Inventory

Here comes…



CNAPP

CWP
Cloud Workload Protection

CIEM
Cloud Infrastructure Entitlement Management

IaC Security
Infrastructure as Code

CSPM
Cloud Security Posture Management

CNAPP – what?

DAST
CI/CD
CIEM
IAM
CWP
CSPM
CDR
SAST
KSPM
IAC
DSPM

Why CNAPP?

- **CNAPP combines different security features into a single platform**
- Proactive breach prevention
- **Provides full-stack visibility – Containers, Serverless, IAM policies, API-Security**
- Continuous monitoring in fast changing environments
- **Direct integration of Alerts and Incidents in the SIEM**
- Good starting point with „out of the box" detection Use-Cases

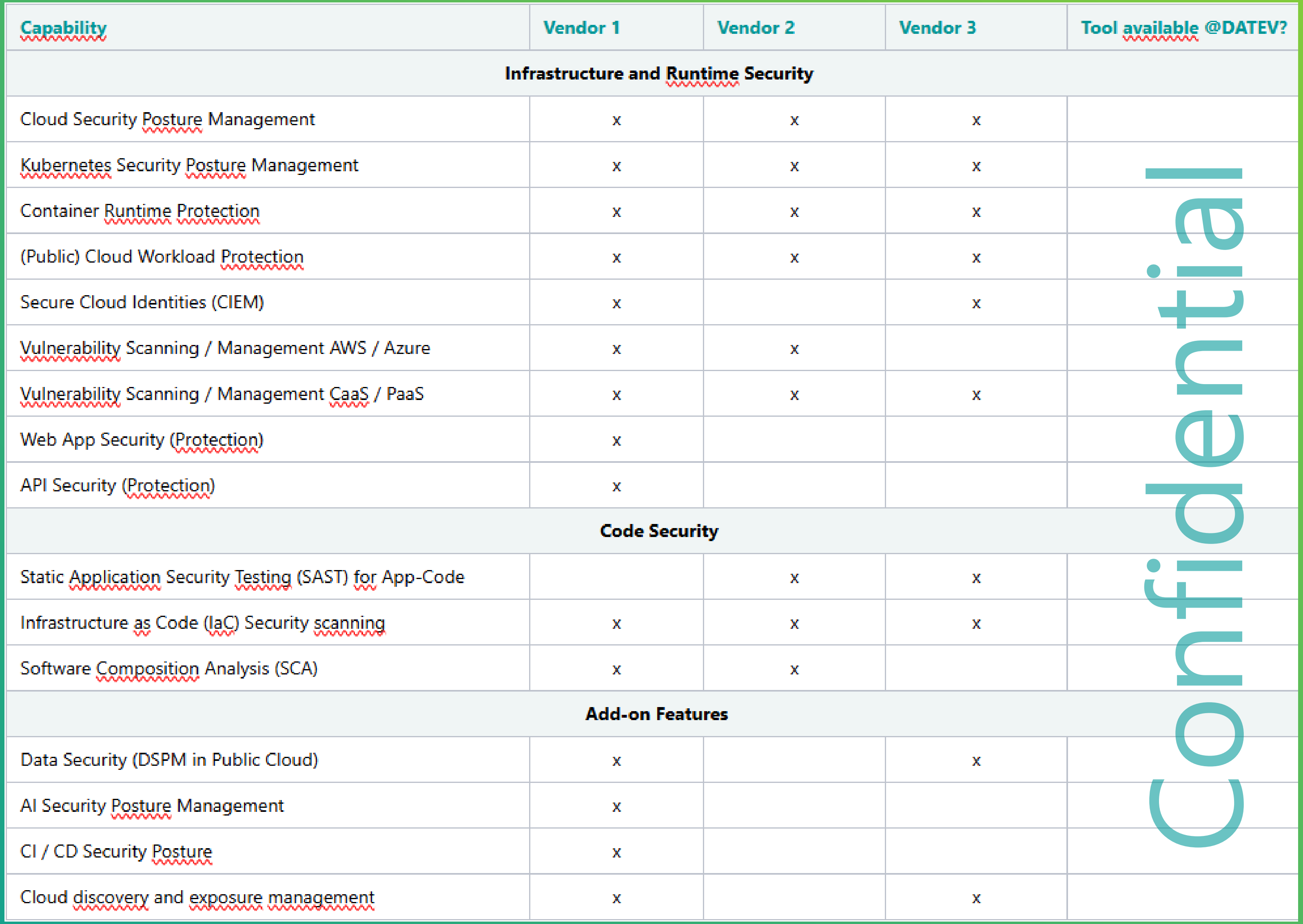
Who can benefit from CNAPP

- 🔒 SOC-Team: Improved detection & runtime visibility
- 🧑‍💻 DevOps & Platform Engineers: Insights into build & deployment risks
- 🧑‍💼 Cloud Security Architects: Centralized posture management
- 📦 Application Developers: Early vulnerability feedback (Shift-Left)
- 🕵️ Compliance & Risk Team: Continuous compliance & auditability
- 🏢 IT-Leadership / CISO: Enhanced security posture & simplified tooling

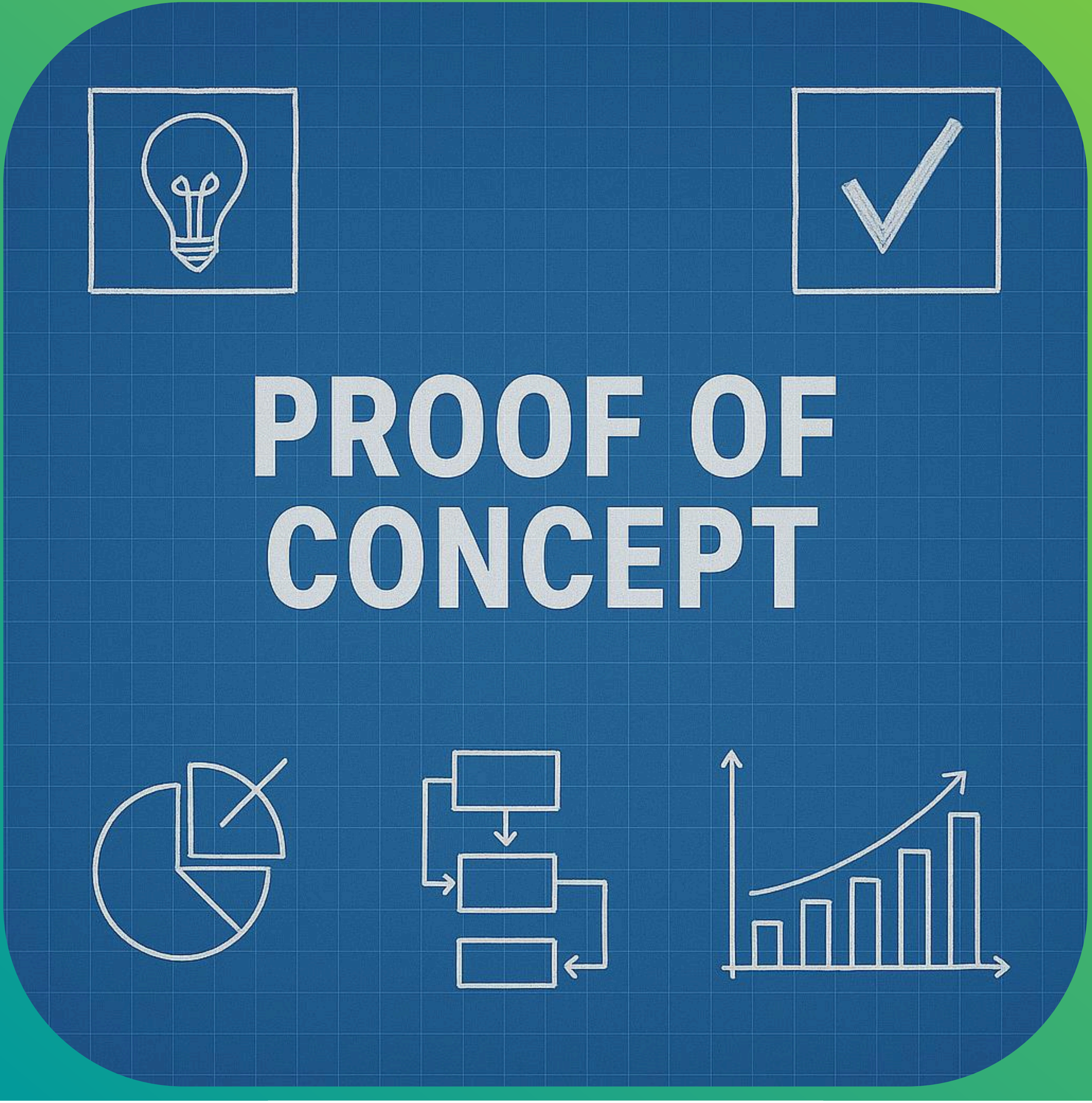
Security capability map

DATEV

- Goal: Identify blindspots in all of our security tools
- What do we have? What's missing? What is ongoing? Who is responsible?
- What's important for us?
- Best of Suite vs. Best of Breed
- Matching of capabilities to CNAPP



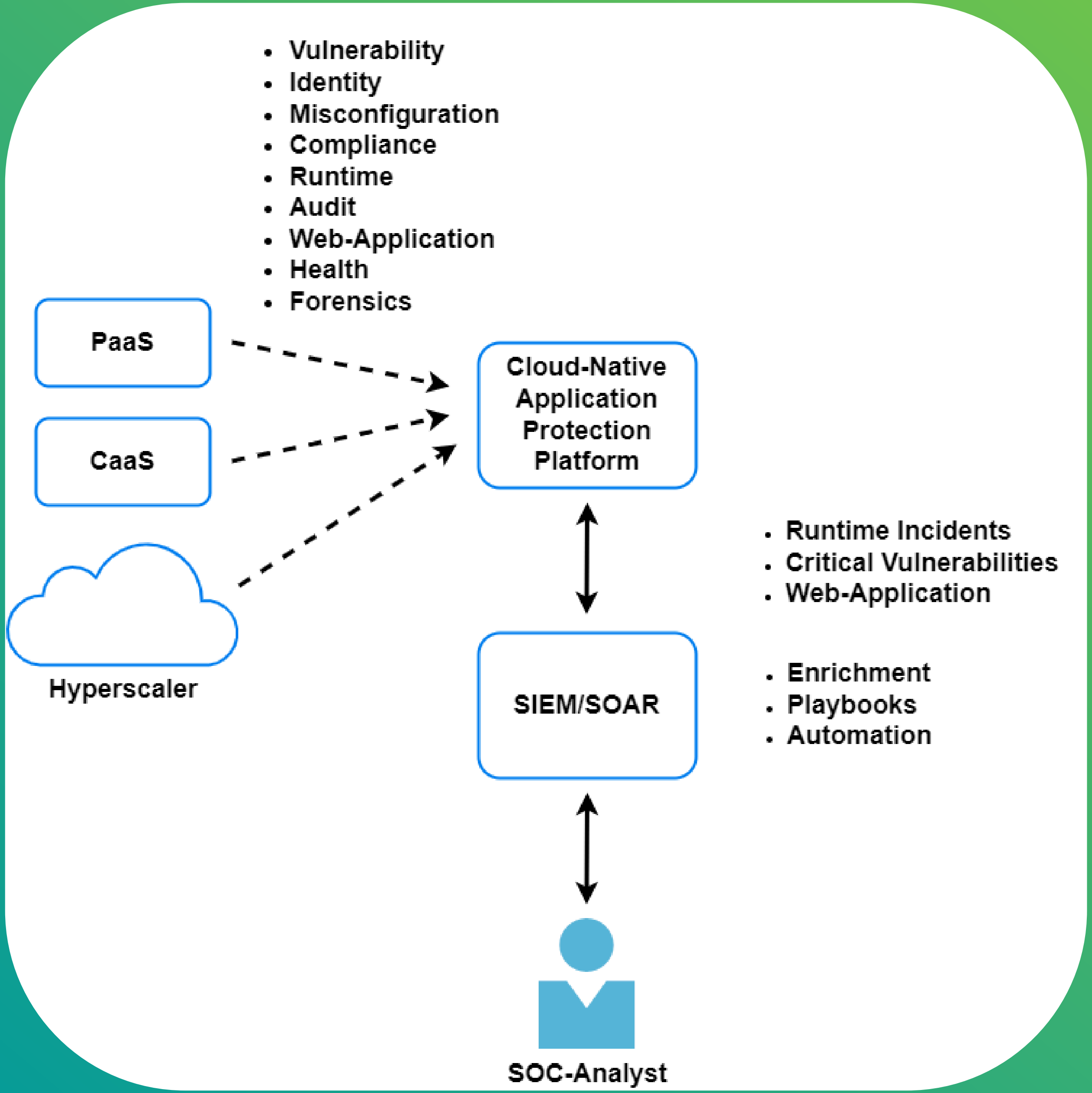
Capability	Vendor 1	Vendor 2	Vendor 3	Tool available @DATEV?
Infrastructure and Runtime Security				
Cloud Security Posture Management	x	x	x	
Kubernetes Security Posture Management	x	x	x	
Container Runtime Protection	x	x	x	
(Public) Cloud Workload Protection	x	x	x	
Secure Cloud Identities (CIEM)	x		x	
Vulnerability Scanning / Management AWS / Azure	x	x		
Vulnerability Scanning / Management CaaS / PaaS	x	x	x	
Web App Security (Protection)	x			
API Security (Protection)	x			
Code Security				
Static Application Security Testing (SAST) for App-Code		x	x	
Infrastructure as Code (IaC) Security scanning	x	x	x	
Software Composition Analysis (SCA)	x	x		
Add-on Features				
Data Security (DSPM in Public Cloud)	x		x	
AI Security Posture Management	x			
CI / CD Security Posture	x			
Cloud discovery and exposure management	x		x	


PROOF OF
CONCEPT

How CNAPP enhances SOC threat detection capabilities

- Runtime behavior visibility – On Prem & Hyperscaler
- **Incident / Alert integration into SIEM**
- **(Auto)-containment**
- Attack paths
- MITRE ATT&CK mapping
- Agent-based -> Vulnerability exploitable?
- **Aggregated data for analysis**
  - Network activity
  - Process activity
  - Timeline mapping

Integration of CNAPP data into the SIEM



- Vulnerability
- Identity
- Misconfiguration
- Compliance
- Runtime
- Audit
- Web-Application
- Health
- Forensics

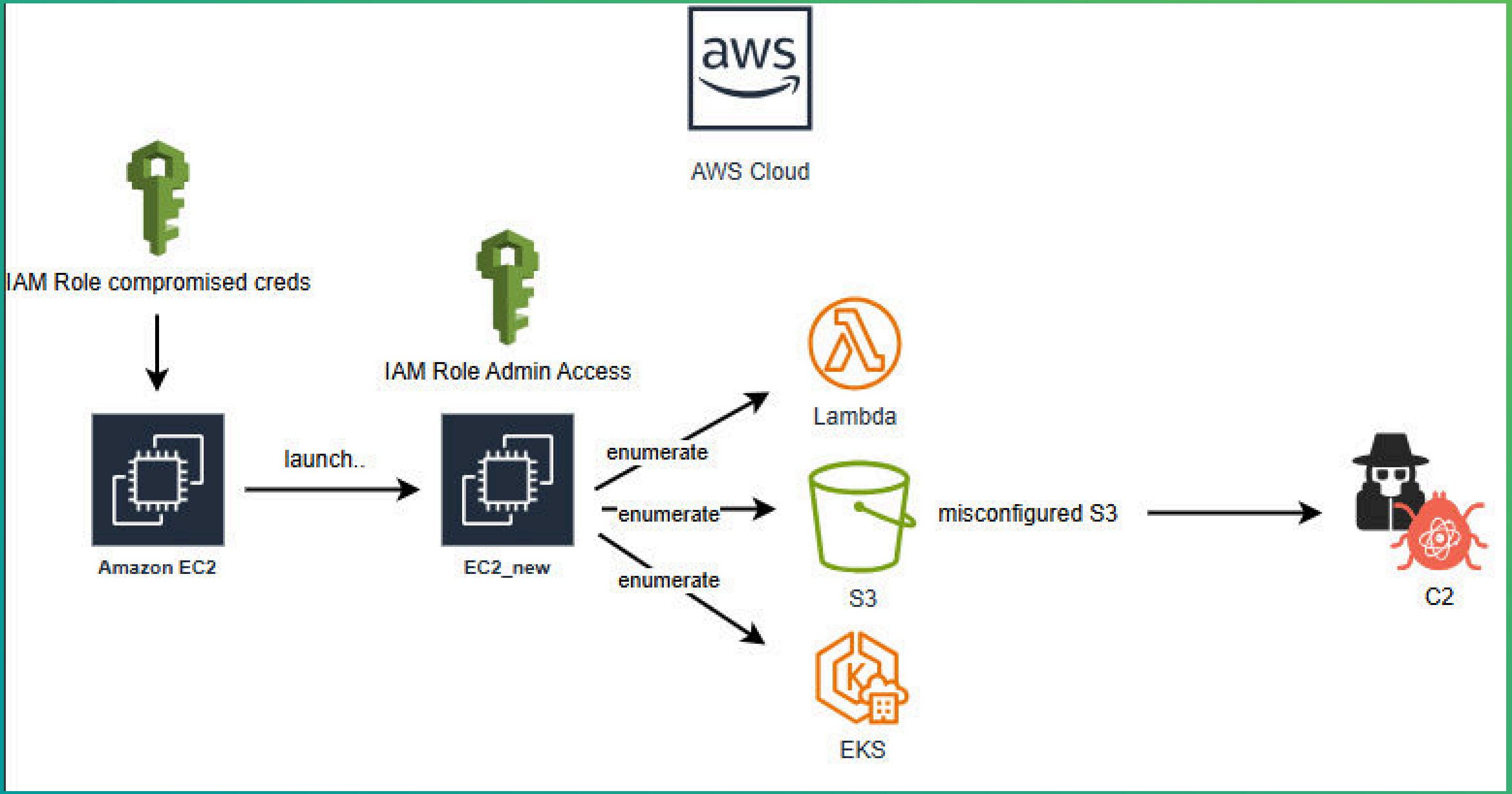
- Runtime Incidents
- Critical Vulnerabilities
- Web-Application

- Enrichment
- Playbooks
- Automation

Some detection Use-Cases

- **AWS IAM effective permissions are over-privileged**
- Azure Virtual Machine does not authenticate using SSH keys
- Suspicious process „/usr/bin/nmap“ launched possible portscan
- **Possible RCE due to vulnerable OpenSSH AWS EC2 instance -> CVE-2023-38408**
- Private keys stored in deployed image
- Network activity: Suspicious DNS-Query to crypto-mining associated domain
- **Possible Cross-Site Scripting attempt from suspicious IP address**
- **TOR related network activity detected**

Example 1: Misconfiguration to Data Exfiltration in AWS



Options which should be enabled in AWS to detect attacks like this:

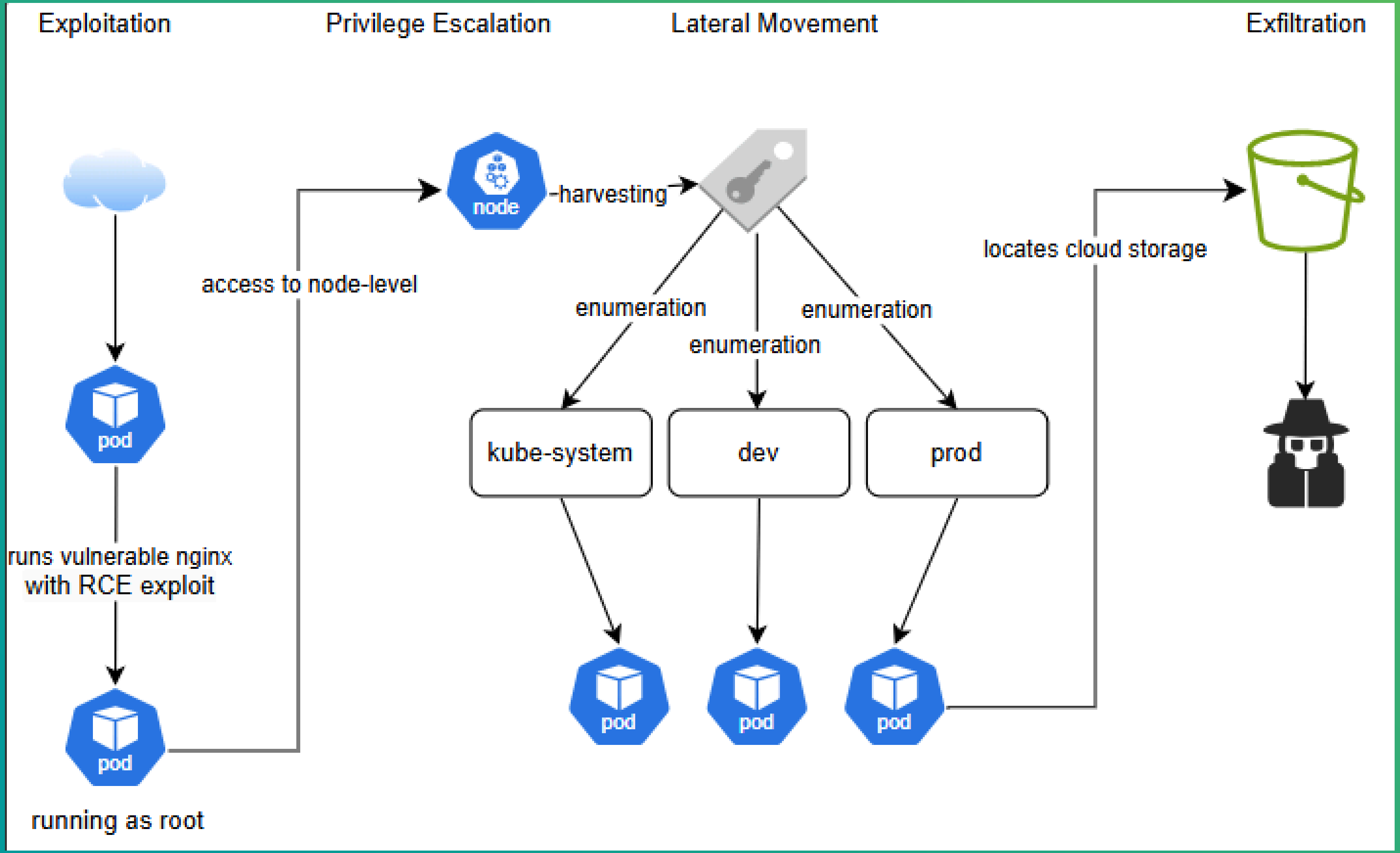
- GuardDuty
- CloudTrail
- IAM logs
- S3 logs
- VPC Flow logs

→ CNAPP combines the different AWS logs and merge it to alerts

Example 1: How does CNAPP help?

Prevention	Detection
Identifies over-permissive roles and privilege escalation paths	Alerts when a AWS service is accessed from EC2 unexpectedly
Detects policy drifts from baselining, e.g. unauthorized IAM policy updates	**Detects anomalies in data access, e.g. sudden S3 synchonization from new instance**
Flags misconfigurations in Terraform before deployment	Flags and correlates mass downloads

Example 2: Kubernetes – From Exploitation to Lateral Movement



Tools which can detect attacks like this:

- AWS GuardDuty
- Kubernetes Audit Logs
- Falco open source
- EDR for containers

CNAPP detects the different phases in the attacker kill chain and combines different capabilities

Example 2: How does CNAPP help?

Prevention	Detection
Scans K8s policy which detects containers running as root	Detects shell activity in containers and container breakout attempts
Prevents insecure configurations before deployment via Infrastructure-as-Code scanning	**Alerts on lateral movement, e.g. unexpected API calls**
Identifies overly permissive Service Accounts and dangerous Role Bindings	Correlates suspicious cluster behavior with cloud resource access

Initial things we saw

DATEV

- Which clusters and containers are present in our environment
- Which hyperscaler environments are running
- Asset information – Cluster name, namespace, OS, image information
- Vulnerability information
- Compliance information
- Runtime events and incidents
- Webapplication events and information
- Forensics data for analysis – running processes, network information

→ All this in one centralized GUI

Incident Response capabilities

Full-Stack visibility from one place

- Correlates runtime, identity, infrastructure, misconfiguration
- From API misuse to source code or misconfiguration

Enriched, actionable alerts

- Contextual alerts
- Which workload was involved and what triggered the alert
- Reduced alert fatigue

Real-Time runtime detection

- Alerts suspicious network connections and processes
- Lateral movement across services
- Abnormal use of cloud APIs and roles

Workflow integration

- SIEM for alert correlation
- SOAR for auto-response
- Ticketing tool for incident assignment and tracking

Where we currently stand

- 🔄 Finalize RBAC model
- 🔄 Documentation
- 🔄 Onboarding of SOC-Team members
- 🔄 Onboarding of Azure and AWS environments
- 🔄 Policy definition for runtime
- 🔄 SIEM/SOAR integration + Playbooks
- 🔄 Onboarding of key stakeholders

Organizational & technical challenges

Organizational	Technical
Siloed Teams	Complex Environments
Skill Gaps	Integrating with existing tools
Resistance to change	Noise & False positives
Undefinded Responsibilities	Limited runtime coverage

Collaboration between SOC, cloud teams and DevOps

DATEV

Cloud teams

Understanding of infrastructure

SOC

Threat detection & response expertise

DevOps

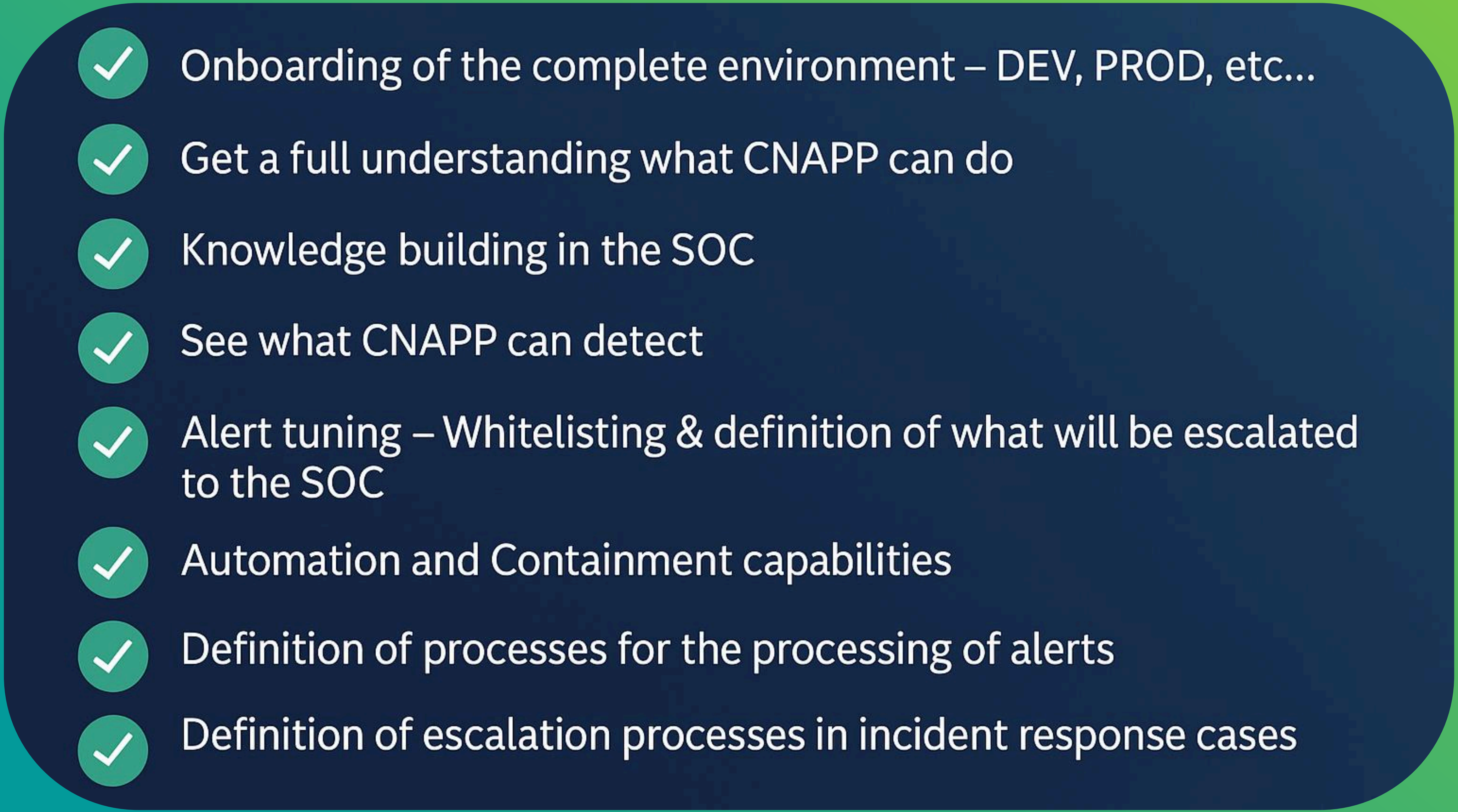
How code is built, deployed and run

Best practices for SOC teams to improve cloud runtime security

DATEV

- **Gain runtime visibility across workloads – centralized or decentralized solutions**
- **Build detections with context through correlation and enrichment**
- Implement baseline behavior monitoring
- Tighten IAM and service permissions
- **Test detection rules in real environments**
- Collaboration with cloud teams & DevOps
- Centralize telemetry and alerting

What‘s next?



- ✓ Onboarding of the complete environment – DEV, PROD, etc…
- ✓ Get a full understanding what CNAPP can do
- ✓ Knowledge building in the SOC
- ✓ See what CNAPP can detect
- ✓ Alert tuning – Whitelisting & definition of what will be escalated to the SOC
- ✓ Automation and Containment capabilities
- ✓ Definition of processes for the processing of alerts
- ✓ Definition of escalation processes in incident response cases

Key takeaways

DATEV

- 🔒 Getting a Cloud environment is done in 5 minutes – securing it is not
- 🧠 Visibility is good, but not everything -> Context is!
- 🤝 Cloud security is a team sport
- ⚙ CNAPP doesn‘t work out-of-the-box
- 🔄 Big changes also in the SOC to deal with cloud environments
- 🕒 Don‘t try to reach 100% in the first months – trust the process

Q&A & Thank you!