DevSecOps, SecDevOps, and Secure Cloud Transformation

Jay Thoden van Velzen, SAP

SAPinsider 2023

Produced by Wellesley Information Services, LLC, publisher of SAPinsider. © 2023 Wellesley Information Services. All rights reserved.

In This Session

A deep dive into how SAP manages security through the development and DevOps cycle

Computer systems are inherently sociotechnical

Lessons for post-deployment compliance and vulnerability scanning, data engineering, reporting and tracking

Building an organizational support culture and accountability structures that ensure findings are followed up, and managers know that security and accountability are part of their KPIs

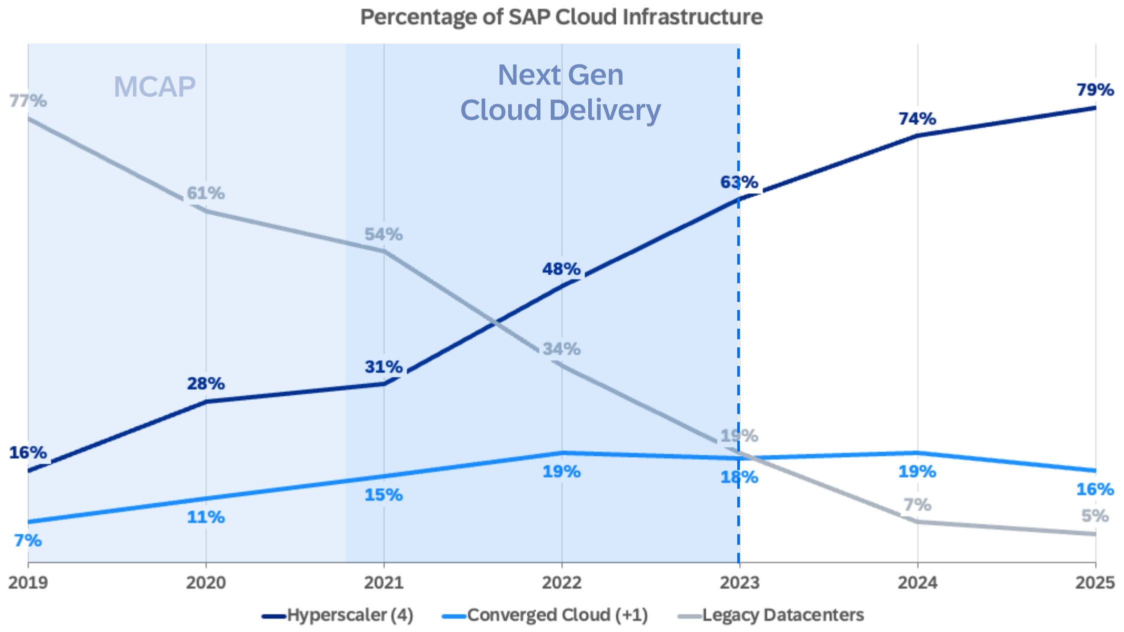
Introduction

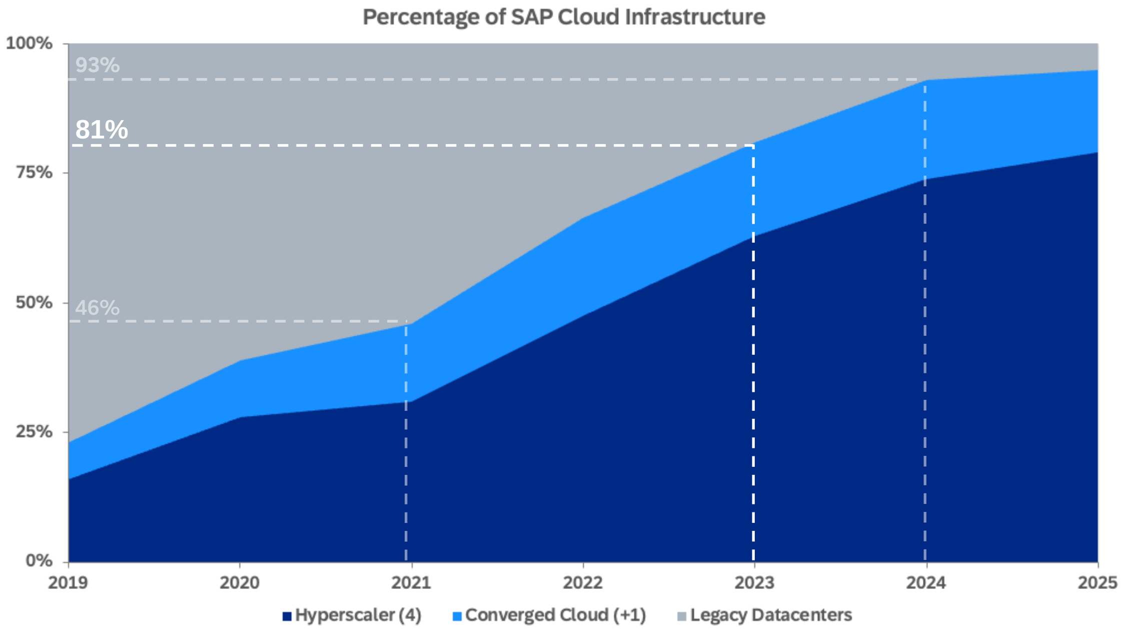
```
[root@localhost ~]# whoami
```

- Jay Thoden van Velzen
  - Strategic Advisor to the Chief Security Officer
  - SAP Global Security & Cloud Compliance Leadership Team
  - Initiative lead for several CSO and executive board sponsored cloud security transformation programs (2019 – 2022)
  - Former Head of Multicloud Security Operations
  - Business Objects veteran

Rapid Cloud Transformation

Next-Generation Cloud Delivery Changed the Landscape





Rapid Cloud Migration

- Traditional data center landscapes dropped from over half of the environment to just a 1/6th after NGCD, and projected to be just ~1/15th% by the end of 2023
- Public cloud grew to nearly two-thirds of the landscape through organic growth and cloud migrations

Accelerated Cloud Transformation

- Accelerated move into the 4+1 2001-2003
- RISE with SAP launched Jan 2021
- At 81% of the landscape start of 2023 and 95% by the end, the key security focus is to protect SAP’s cloud landscape

SAP’s Public Cloud Use: A Sense of Scale and Responsibility

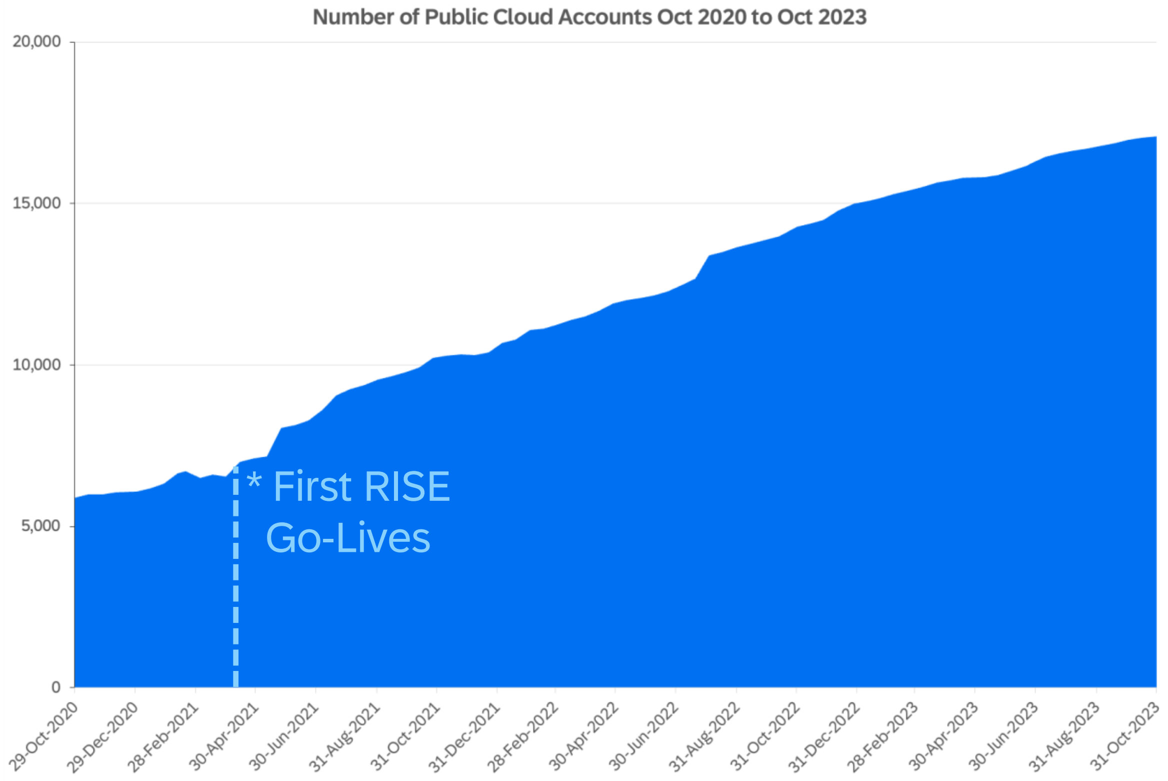
Unique Scale, Growth Rate and Multicloud

- Growth from 5,842 public cloud accounts at the start of Next Gen Cloud Delivery to 14,954 (+9,112) at the start of 2023 (+156%)
- ~17,000 today – 77.5% Production workloads
- SAP Top 5 fastest growing cloud providers while uniquely Multicloud in the Top 10

- Source: AccelerationEconomy.com Cloud Wars Top 10

With Growth Comes Increasing Responsibility

- This growth is set to continue for the foreseeable future
- Particularly sensitive and critical workloads


Number of Public Cloud Accounts Oct 2020 to Oct 2023

* First RISE Go-Lives

Large and Complex Organization

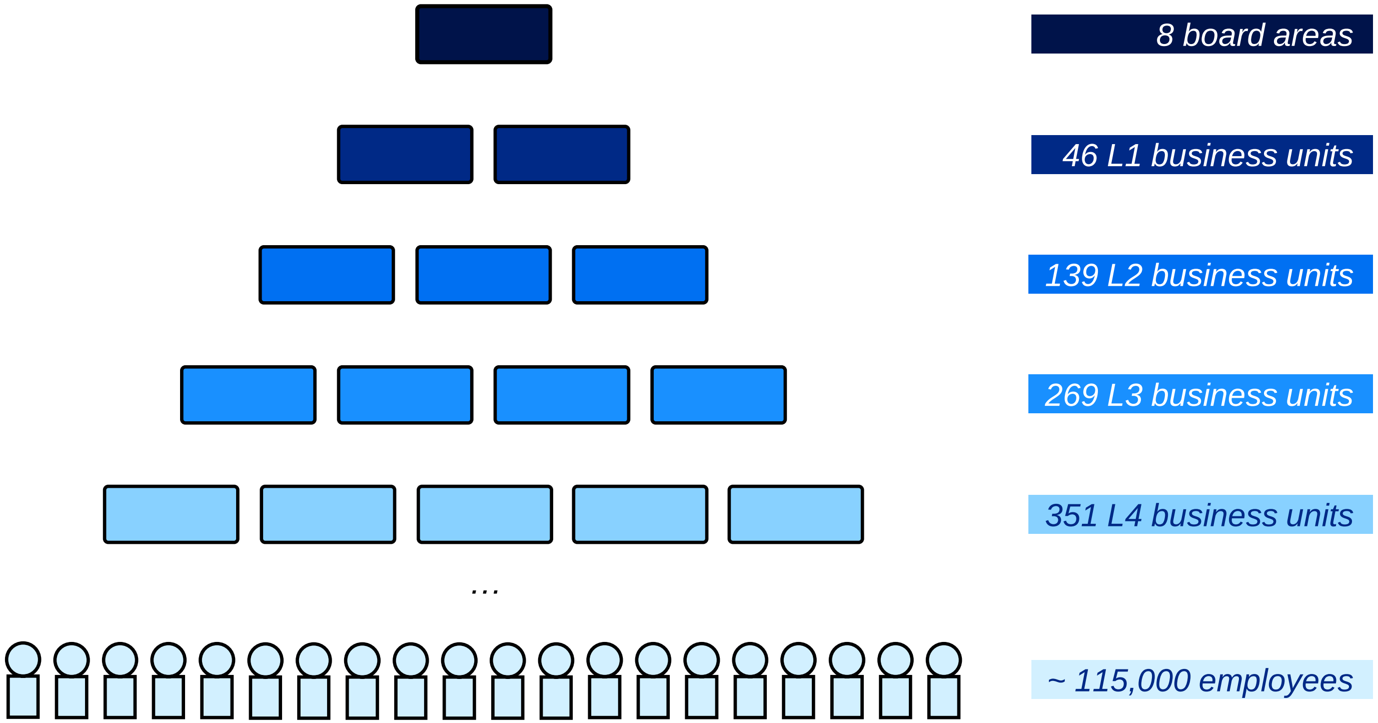
Multi-layered

- 6-8 levels of organizational hierarchy by cost center
- Organizational change happens regularly, as well as changes in the workforce

Pervasive Cloud Use

- Product (59%) and Platform (37%) board areas dominate cloud account use, but still leaves 4% (~700) for internal IT, and other board areas
- Variety of resources, cloud maturity, and skill level

Teams operating active cloud accounts



Cloud Challenges

Scale

- This size becomes very abstract
  - You can’t walk through a data center to get a sense
- Even small mistakes get amplified quickly
- Every manual process breaks

Growth During Transformation

- There is no time – growth drives its own momentum
  - Delay makes any problem bigger
- Organizational change is hard
  - Even more for non-tech teams!

Level of Complexity

- Multicloud by strategy
- Large portfolio of products, often deployed in regulated industries
- Transitioning to cloud-native and micro-service architectures
- Large organization with high autonomy within business units and developer teams

Cloud Security Challenges

Scale

- Large scale means many findings (good or bad) – everything is an engineering job
- Everything can break at any time, no “test” environment

Growth During Transformation

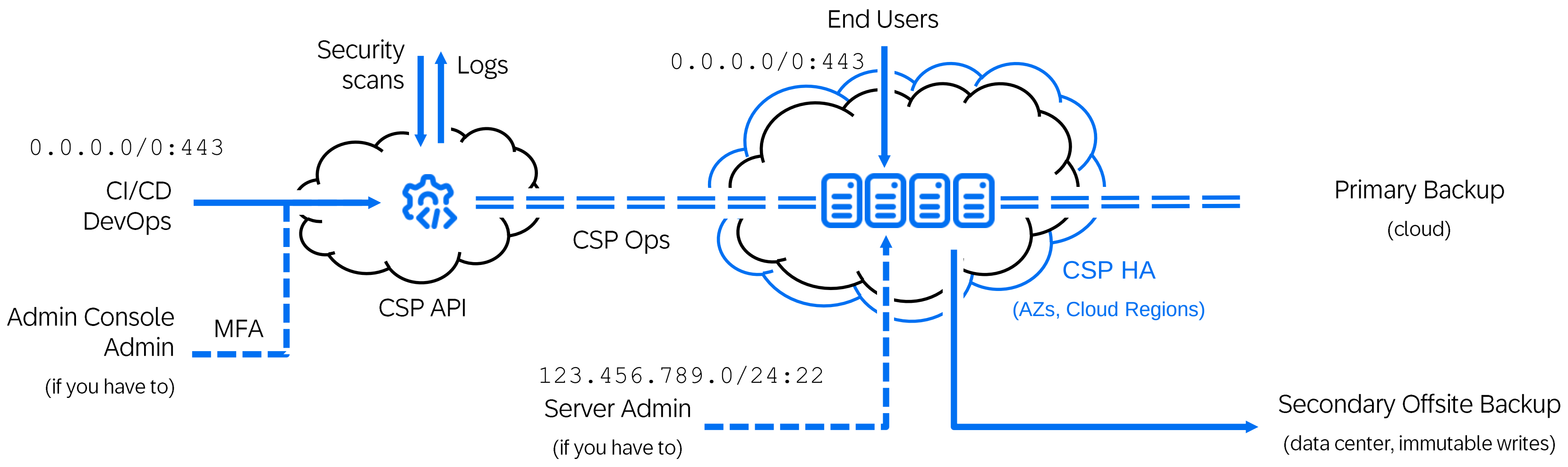
- Our security budget doesn’t grow linearly with growth in the landscape – does yours?
- Security organizations often don’t run or adapt to change as fast as DevOps teams

Level of Complexity

- How do you centralize security functions when developer teams have even more autonomy?
- How do you make them not hate you, for making them do work to get more work?
- How do you get access to systems or get tooling deployed?

Security and Administration – Cloud Focus

Infrastructure-as-Code, Out-of-Band Administration, High Availability, Secure Backups



API-based Administration and Monitoring

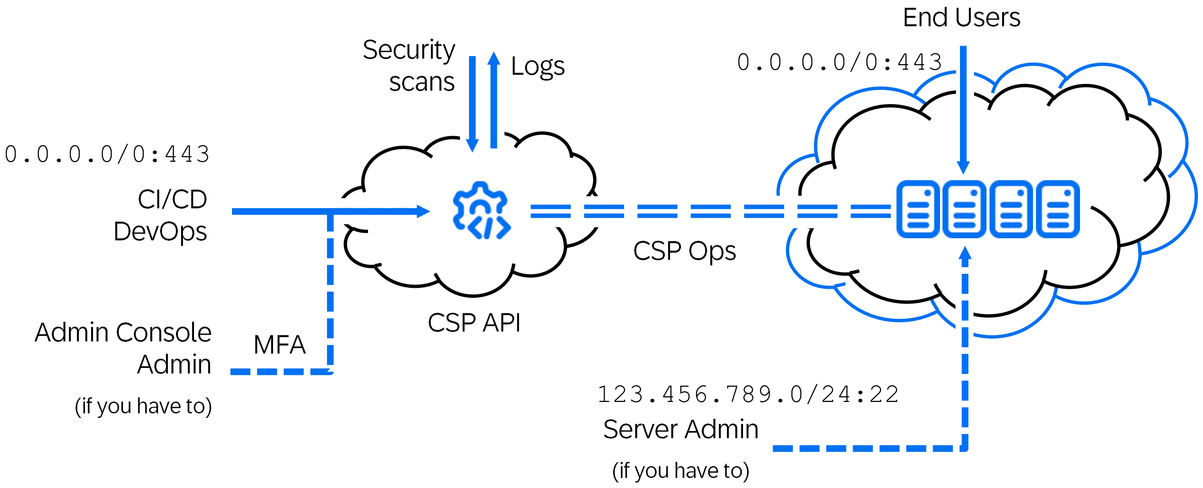
- Deployments typically through CI/CD pipelines and DevOps – we discourage the use of web admin console
- Direct SSH server administration discouraged – if inevitable must be via approved CIDR ranges
- (Most) security scans and log collection via cloud API and cloud organizational policy controls

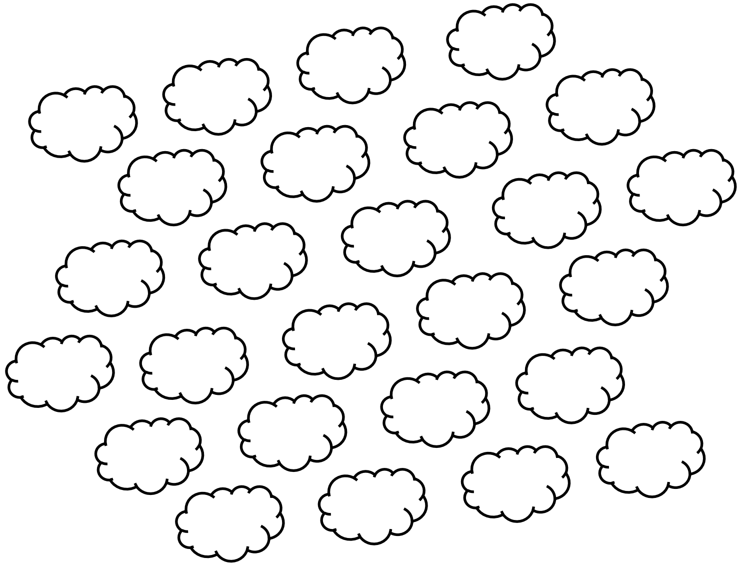
Resiliency

- Built-in cloud resiliency capabilities (AZs, Multi-Region)
- Primary and secondary (offline immutable) backup
- Enforced encryption standards
- Restoration of landscapes by restoring backups and redeploying landscape – if needed

Security and Administration – Cloud Focus

Out-of-Band Administration at Mass Scale and Tenant Isolation





API-based Administration and Monitoring

- Deployments typically through CI/CD pipelines and DevOps – we discourage the use of web admin console
- Direct SSH server administration discouraged – if inevitable must be via approved CIDR ranges
- (Most) security scans and log collection via cloud API and cloud organizational policy controls

Separate Isolated Islands

- Different cloud accounts for different purposes are not connected unless explicitly required, reducing blast radius dramatically
- Utilizes cloud providers' built-in tenant isolation
- Many SAP solutions single-tenant deployed
  - A bit more complicated for multi-tenant solutions but general principle holds

Cloud Security Posture Management

- Started with CSPM in 2018
- Tracking and enforcement since 2019
- 95% reduction of high severity misconfigurations in 2020
- Home-grown solution deployed 2022
- ~99% compliance rate

		inside the VM	inside the container	own-run Kubernetes	own-run serverless
	CIEM	attack paths	on disk	PII/DSPM	own-run databases
cloud API	IAM	public/private	encryption, secrets, keys	managed Kubernetes (EKS)	managed databases
		network configuration	compute (EC2)	block storage (EBS)	object storage (S3)

Cloud Service Configuration

Leverage the IaaS Providers’ Organizational Policy Engines

Cloud Defender Techniques via Cloud API and Organizational Roles

General Administration

- Forcing all cloud accounts into organizations enables powerful defensive capabilities and controls to make them behave more secure-by-default

Logging

- Centrally enforced logging that cannot be removed ensures a direct event ingestion into SIEM that attackers can neither see nor manipulate

Internet-Facing/Publicly Accessible

- Protects against common cloud network misconfigurations of unintentionally publicly accessible resources

Encryption

- Enforcing encryption-at-rest and in-transit standards, and secure key and secrets management

- All accounts in SAP cloud provider organization
- Enforce password policy
- Enforce MFA for cloud admins

- API/Audit and storage access logging applied and cannot be de-activated
- Logs centrally collected and ingested into SIEM

- Enforce block-listed ports not exposed to internet
- No block storage, storage buckets or snapshots public

- Enforce TLS 1.2+
- Encryption enforced on block storage and storage buckets
- Enforce secure KMS/Key Vault config

Version 1 – 4 of Cloud Asset Management Attribution

Who Owns What So We Can Direct Alerts to the Appropriate Team

	Improvement	Reason
Version 1 2017	• Account owner, Cost Center Owner and Cost Object on account creation • Allows assignment to org hierarchy	• Assigns who pays and who is responsible for administration • Forced all accounts into SAP orgs
Version 2 Sep 2020	• Established mandatory periodic updates of metadata and new tags • Non-compliance can lead to account locking, and even deletion	• Version 1 was optimized for growth, not full lifecycle management • Out-of-date metadata complicated assignment and tracking
Version 3 Oct 2022	• Resource asset management (rather than cloud account) for more fine-grained alert and incident assignment	• Multiple resources deployed by different teams in the same cloud account; redistribution of findings • Delays in remediation, added admin
Version 4 TBD	• Refocusing towards a release-based rather than asset-based approach to ensure shortest path to those who can remediate any finding	• Who owns the release and last touched a configuration matters more than who owns the asset

Visibility Higher Up the Stack

How visibility higher up?

- Agent-based solutions, requiring developer effort
- Not very cloud-native, data center tooling
- Run and operating costs
- Slow onboarding process
- Tool sprawl

agent	→	inside the VM	inside the container	own-run Kubernetes	own-run serverless
	CIEM	attack paths	on disk	PII/DSPM	own-run databases
cloud API	IAM	public/private	encryption, secrets, keys	managed Kubernetes (EKS)	managed databases
		network configuration	compute (EC2)	block storage (EBS)	object storage (S3)

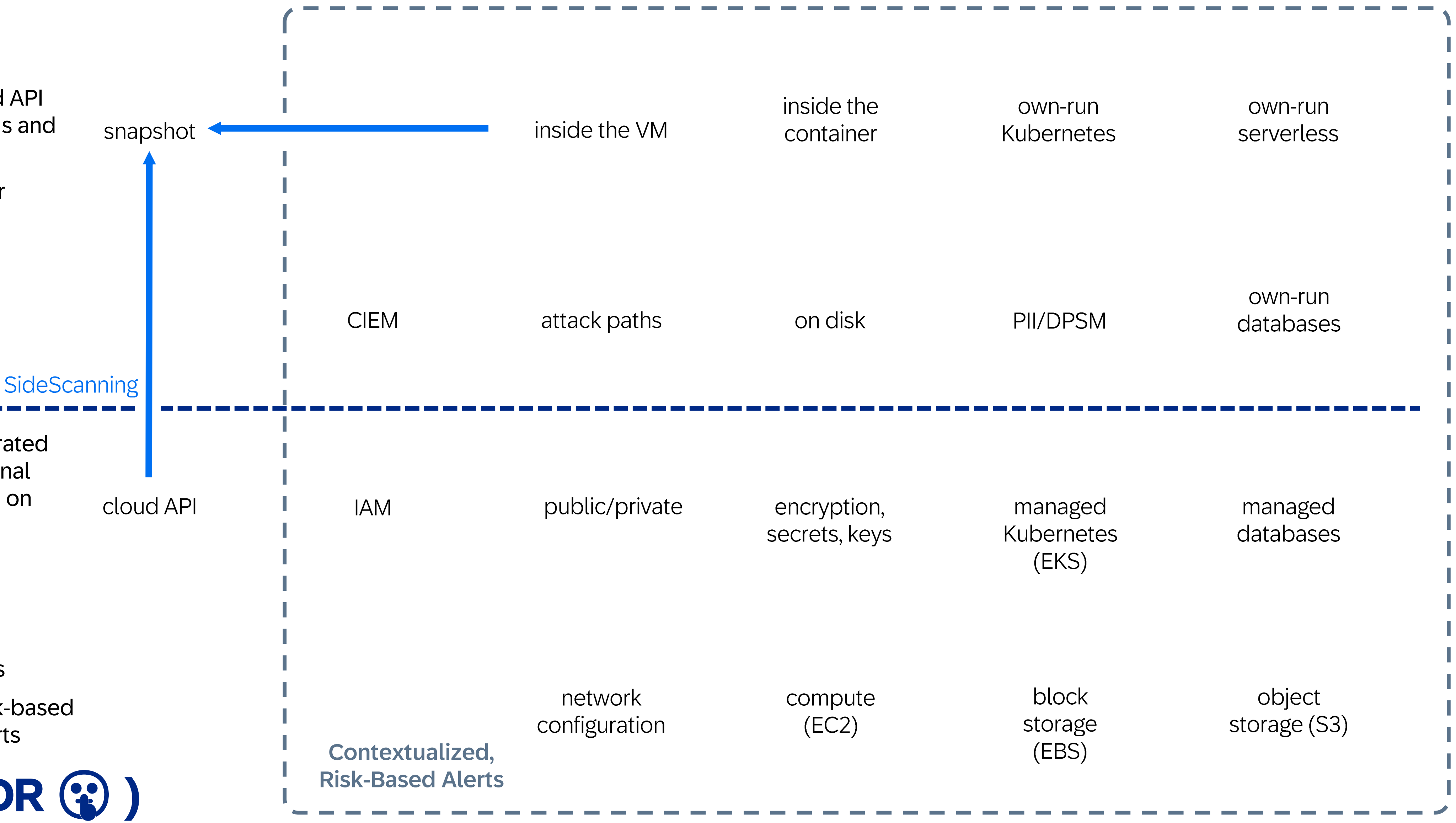
- Started with CSPM in 2018
- Tracking and enforcement since 2019
- 95% reduction of high severity misconfigurations in 2020
- Home-grown solution deployed 2022
- ~99% compliance rate

Cloud Service Configuration

Visibility Higher Up the Stack

Visibility higher up

- Sidescans via cloud API for visibility into VMs and containers
- AV/EDR solution for runtime



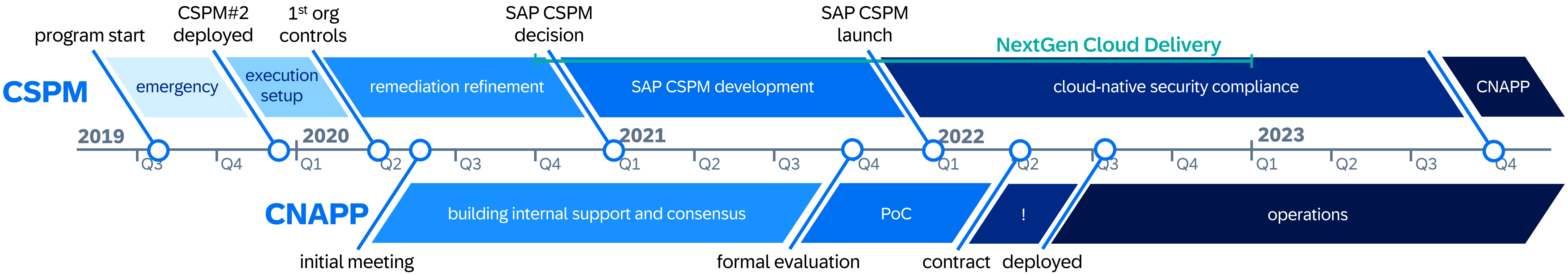
	inside the VM	inside the container	own-run Kubernetes	own-run serverless
CIEM	attack paths	on disk	PII/DPSM	own-run databases
IAM	public/private	encryption, secrets, keys	managed Kubernetes (EKS)	managed databases
	network configuration	compute (EC2)	block storage (EBS)	object storage (S3)

Contextualized, Risk-Based Alerts

- Deployed and operated through organizational roles, without effort on developer teams
- Can’t be turned off
- Not visible to any attackers
- Variety of use cases
- Contextualized, risk-based prioritization of alerts

CNAPP (CDR 🤫)

SAP Public Cloud Security Timeline



program start

CSPM#2 deployed

1st org controls

SAP CSPM decision

SAP CSPM launch

NextGen Cloud Delivery

CSPM

emergency

execution setup

remediation refinement

SAP CSPM development

cloud-native security compliance

CNAPP

2019 Q3 Q4 2020 Q1 Q2 Q3 Q4 2021 Q1 Q2 Q3 Q4 2022 Q1 Q2 Q3 Q4 2023 Q1 Q2 Q3 Q4

CNAPP

building internal support and consensus

PoC

!

operations

initial meeting

formal evaluation

contract

deployed

Cloud Security Posture Management

- Remediation of cloud security misconfigurations for those already in public cloud
- 96% reduction in 2020, despite doubling cloud resources
- Commercial solutions faltering

NextGen Cloud Delivery

- Oct 1, 2020 announcement SAP accelerates cloud migration for remaining teams by end of 2022
- Continued quadratic growth
- Development and launch of SAP's own CSPM solution

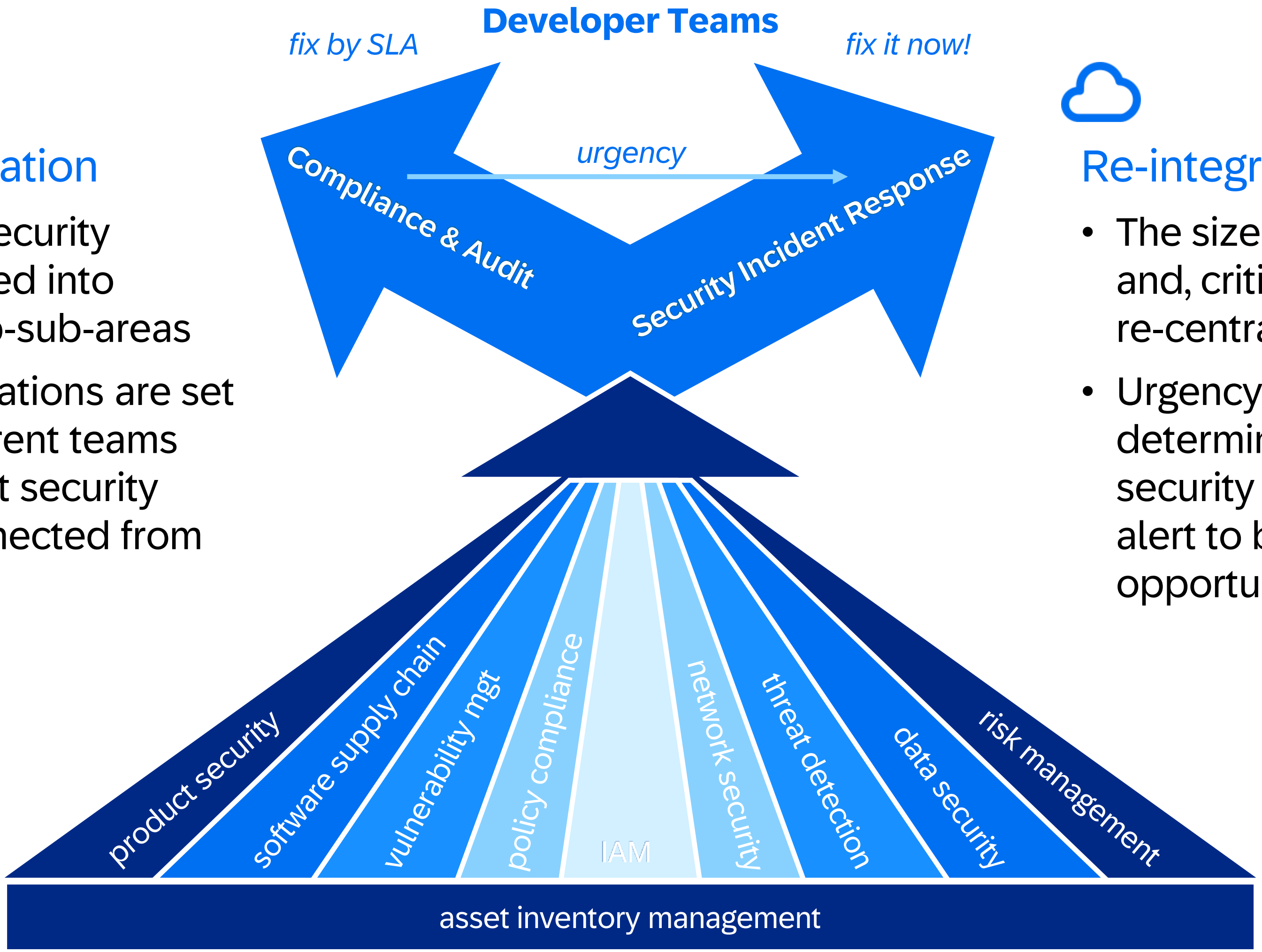
Cloud-native Application Protection Platform

- Selection of CNAPP provider and deployment into landscape
- Operationalization of findings into central services for asset mgt., compliance, vulnerability mgt. and attack surface reduction, threat and malware detection

Rethinking Cybersecurity's Fragmentation

20 Years of Fragmentation

- As Infosec matured, security increasingly fragmented into different sub- and sub-sub-areas
- Many security organizations are set up this way, with different teams taking care of different security topics – often disconnected from each other

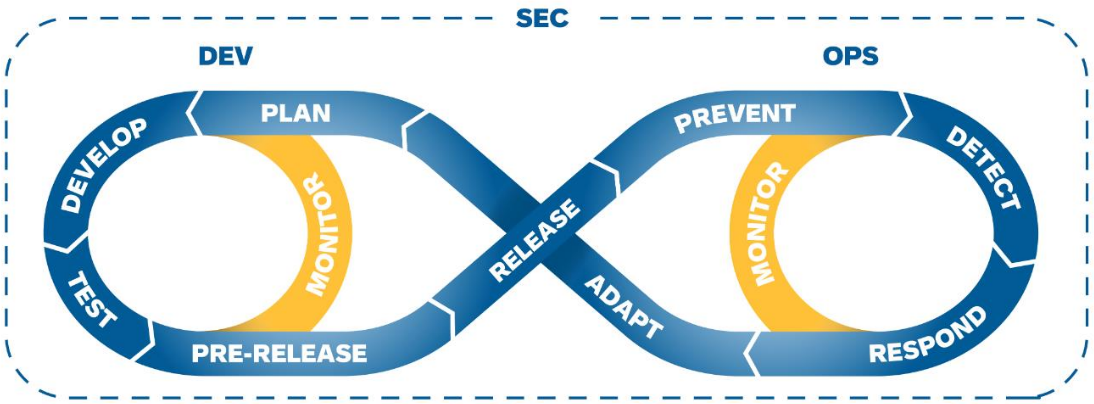


Re-integration for Cloud

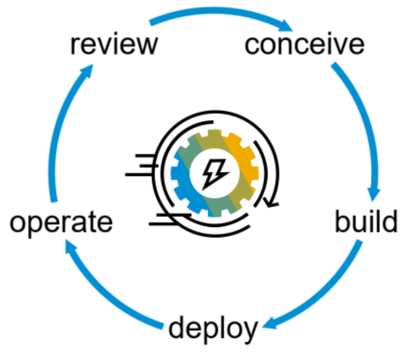
- The size of the landscape, context and, critically, **alert recipients** are re-centralizing these functions
- Urgency and severity of alerts determine whether treated as a security incident, or a compliance alert to be cycled out at next opportunity
  - New CNAPP solutions specifically useful in this contextualized re-integration

Cloud-native DevSecOps and SecDevOps

Secure DevOps Practices Paired with DevOps Security Operations for Aligned Agility



DevSecOps



Review *new or updated controls, etc. with stakeholders and wider community, leading to…*

Operate *and monitor the solution*

Conceive *of new or updates to existing controls, pipelining, etc.*

Develop and ***Build*** *new or update existing controls, pipelining, etc.*

Deploy *the new or updated controls, pipelining, etc. and test across the dev, pre-prod and prod landscapes*

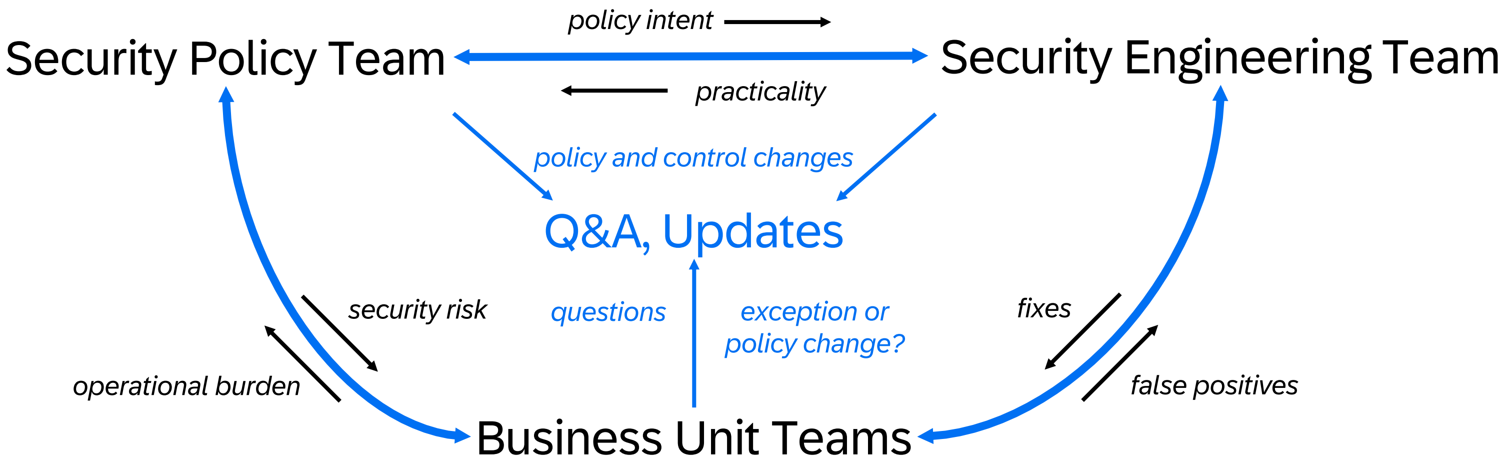
SecDevOps

Recommended Reading

Security Chaos Engineering: Sustaining Resilience in Software and Systems,
Kelly Shortridge with Aaron Rinehart, 2023

Security Chaos Engineering and Security Engineering Amid Chaos: Cloud-native Cyber Resilience,
SAP Community

Continuous community engagement



Ex.: Cloud Security Office Hours

- Weekly meeting open to all interested
- Voluntary, but regularly drawing 50+ attendees, 100+ on occasion
- Running since August 2019
- Tuesdays 4:05PM CET, 3:05PM UK, 10:05AM US East, 7:05AM US West, 7:35PM India, 10:05PM China

Community trust

- Close to the LoB security teams and security champions
- Fast response
- Potentially avoiding unnecessary and burdensome exception processes
- Impactful changes debated early and adjusted if needed

Driving effective security outcomes

- Ensure policies are practical and achievable, even under stress
- Balance security risks with operational burden
- Identify potential central services and controls for automation
- Demonstrate the effectiveness of security and compliance controls and central services

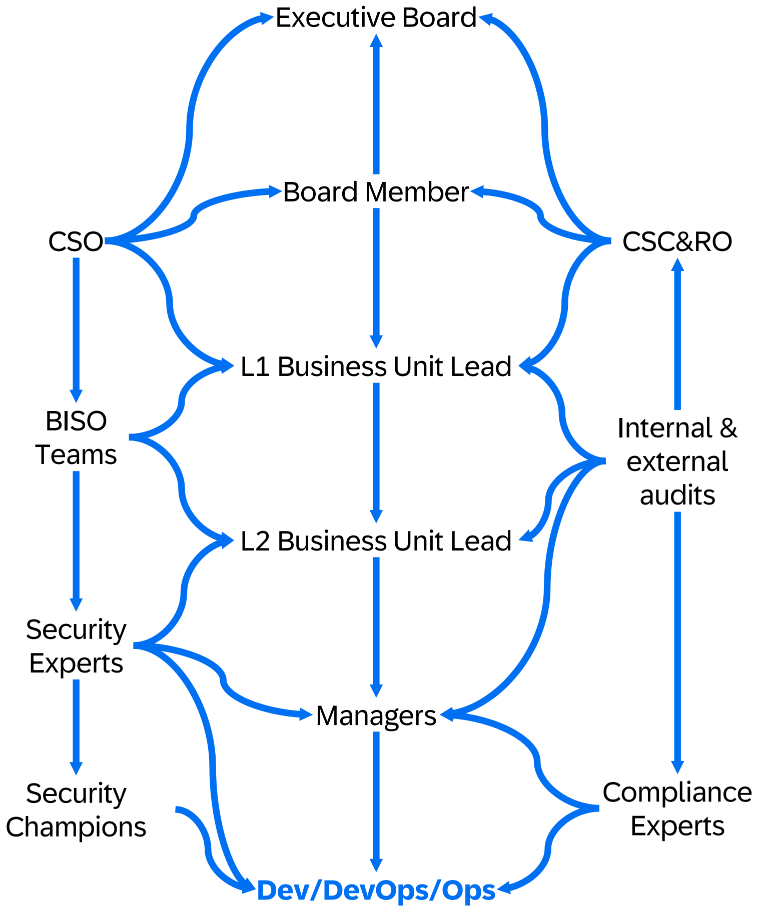
Accountability throughout the organizational hierarchy

Central reporting and SLA Tracking

- Experience shows policies are not followed unless centrally tracked and verified
- Scans, alerts and findings along do not make an organization move
- Multi level reporting and tracking to establish visibility and accountability throughout the organizational hierarchy
- Regular meetings across organizational levels

Secure-by-Default Platforms and Svcs

- Embed security into engineering and operations
- Reduce duplication of effort and security compliance toil through the adoption of central security infrastructure, platform and pipeline services



Cut through competing priorities

- Security and compliance competes with many different priorities, both within technical teams as well as higher up the organizational hierarchy
- Developers and DevOps engineers don't set priorities, managers do, VPs do
- Security and compliance support required to ensure priorities are understood

Automated Control Testing

- To reduce manual burden, solutions and services must be self-describing, self-auditing
- Include compliance checks in development, build and deployment processes to prevent them as much as possible in production landscapes

From “Shared Fate” to “Shared Faith”

“Fate implies we share the same destiny. Whatever happens, we are in the same boat together, condemned to each other. It also implies events beyond our control. It sounds inherently ominous, and for a partnership involving those in the public sector or under regulatory requirements in a critical industry, this may not meet the desired comfort level.”

“Faith, on the other hand, connotes complete trust or confidence in something or someone. Such trust and confidence can only be fostered by greater transparency. Such a trust relationship goes beyond secure defaults and security services that allow customers to run more securely. This is about proving to customers *we as cloud provider* run securely.”

Customer responsibility and control

Shared Responsibility	Shared Fate	Shared Faith
Clear definition of responsibilities between cloud provider and customer	Clear definition of responsibilities between cloud provider and customer	Clear definition of responsibilities between cloud provider and customer
	Making it easier for customers to operate securely in the cloud	Making it easier for customers to operate securely in the cloud
		Greater transparency in the secure operations of the cloud provider

Depth of impact on critical business operations

Customer demand for greater transparency and trust

[Shared Responsibility, Shared Fate, and Shared Faith: An Evolution in Trust in Cloud Services]

NIST CSF structures SAP’s risk management, security programs and capabilities

** Current version 1.1 - NIST CSF 2.0 adoption planned for 2024*

Govern	Identify	Protect	Detect	Respond	Recover
• Organizational Context • RM Strategy and Supply Chain Risk Management • Roles, Responsibilities and Authorities • Policies, Processes & Procedures • Oversight	• Asset Management • Risk Assessment • Improvement	• Identity Management and Access Control • Awareness and Training • Data Security • Platform Security • Technology Infrastructure Resilience	• Continuous Monitoring • Adverse Event Analysis	• Incident Management • Incident Analysis • Incident Response Reporting and Communication • Incident Mitigation	• Incident Recovery Plan Execution • Incident Recovery Communication
Risk, Policy and Oversight	Asset Management	Preventive Measures	Scans and Analysis	Response and Remediation	Resiliency and Recovery
• Cloud accounts by policy in SAP cloud organizations • Risk management strategy • TPRM and Office of OSS Mgt • Roles, responsibilities and mandates • Security policies, processes and validation (DevSecOps) • Internal and 3rd party audits	• CCIR/SISM, MCDB and metadata tagging • Central scans and asset discovery • Vulnerability Management • Threat intelligence • Risk assessment and FAIR quantitative risk management • Gap analysis and prioritization	• IAM, MFA and Cloud Infrastructure Entitlement Mgt (CIEM) • Mandatory Security Fundamentals, DevLearning, 3rd party training, events • Data Privacy and Protection • Cloud guardrails and secure resource orchestration, incl. Golden Images, CI/CD build checks	• Continuous CSPM and CNAPP scans, cloud audit logs • Host and container runtime detection • Network security, incl. IDS/IPS, WAF, DNS • SIEM ingestion, data enrichment, automation, distribution and reporting • Threat detection and hunt	• Cyber Fusion Center, incl. SIEM, SOAR, DFIR and SOC, LoB security response teams • Incident communication processes • Security and compliance reporting, dashboarding, SLA tracking, audit findings mgt. • BISO Council, Security Execution, Office Hours • Continuous improvement	• Cyber resiliency processes, incl. primary and secondary back-ups, CI/CD, anti-ransomware • Product security response and patch management • Post-incident RCA and continuous improvement • Trust Office, Cyber Legal and MCC

Key Points to Take Home

Make it easier on yourself – cloud-native in cloud is easier than copying data center approaches

Utilize the power of cloud provider organizational policies and controls

The network may no longer be the key battleground – but instead a carrier of encrypted traffic

Carefully select tooling, and consider onboarding and operationalization

Community engagement and accountability

Shift-left, Cloud First, Customer-centric, Data-centric, Automation

Jay Thoden van Velzen

jay.thoden.van.velzen@sap.com

Please remember to complete your session evaluation.

SAPinsider

SAPinsider.org

PO Box 982Hampstead, NH 03841

Copyright © 2023 Wellesley Information Services.
All rights reserved.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies. Wellesley Information Services is neither owned nor controlled by SAP SE.

SAPinsider comprises the largest and fastest growing SAP membership group worldwide, with more than 750,000 global members.