Moderne Cloud Native Security

Andreas Schneider
Field CISO EMEA

https://www.linkedin.com/in/ciso-andreas-schneider/

The clash of “Beliefs”

On-prem Era

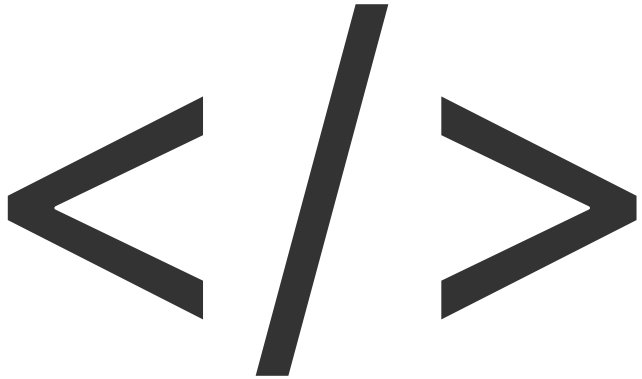
Cloud Era

The “Cloud”

is not

just someone else’s computer!

LACEWORK



CI/CD


Continuous
CI/CD

Automation

Scale

Security?

Modern security is

less network

more data
more identity

Resilience based Security Architecture

CONTINUOUS RESILIENCE METERING

Modern Cyber Security Building Blocks

Zero Trust Architecture

IDP Security
Device, Compromise and Identity Context
EDR and Workplace Security
Mobile Device Mgmt

Product & Cloud Security

DevSecOps
DDOS, WAF
AppSec, Bug Bounty
Cloud Security

Decentralized Security Operations

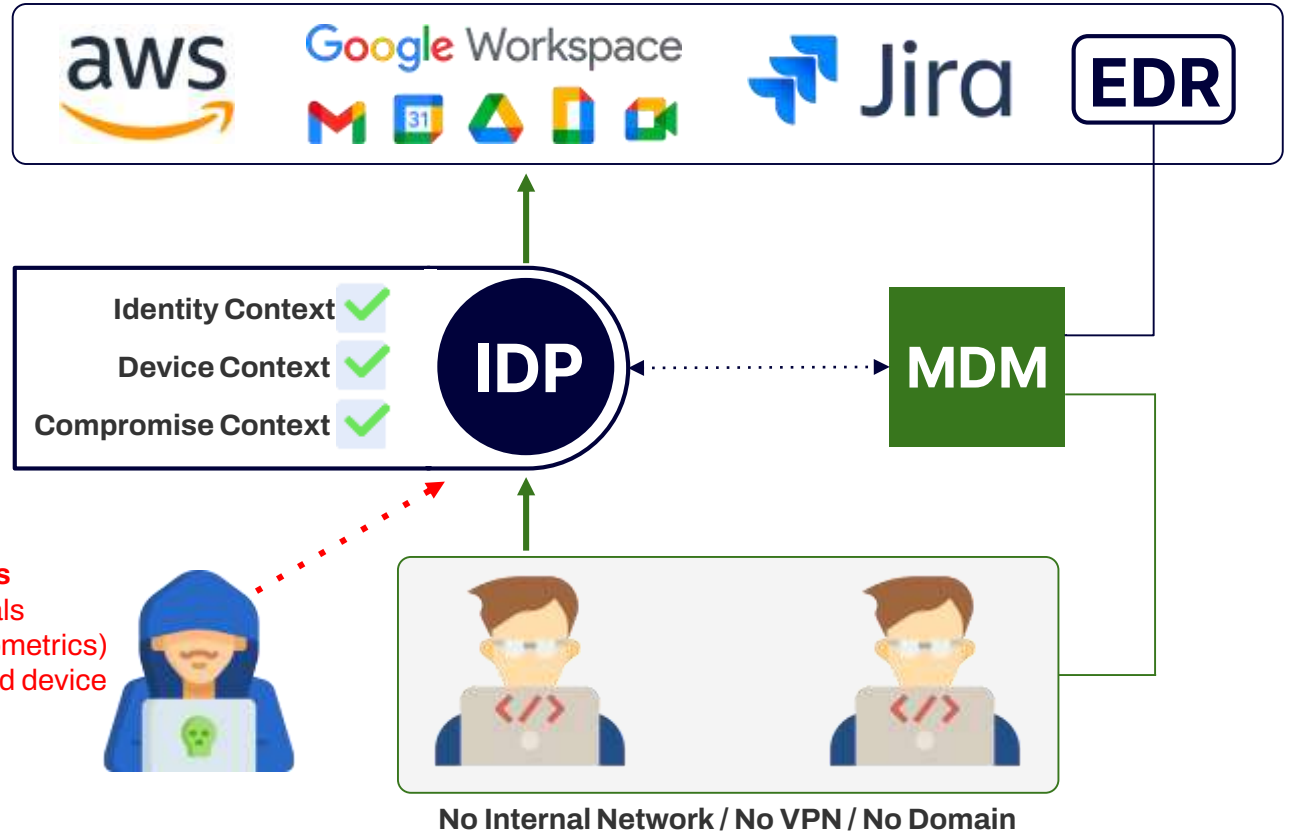
DevSecOps
Security Champions
Security Success Mgmt
Security Leadership
User Focus

Detect and Respond

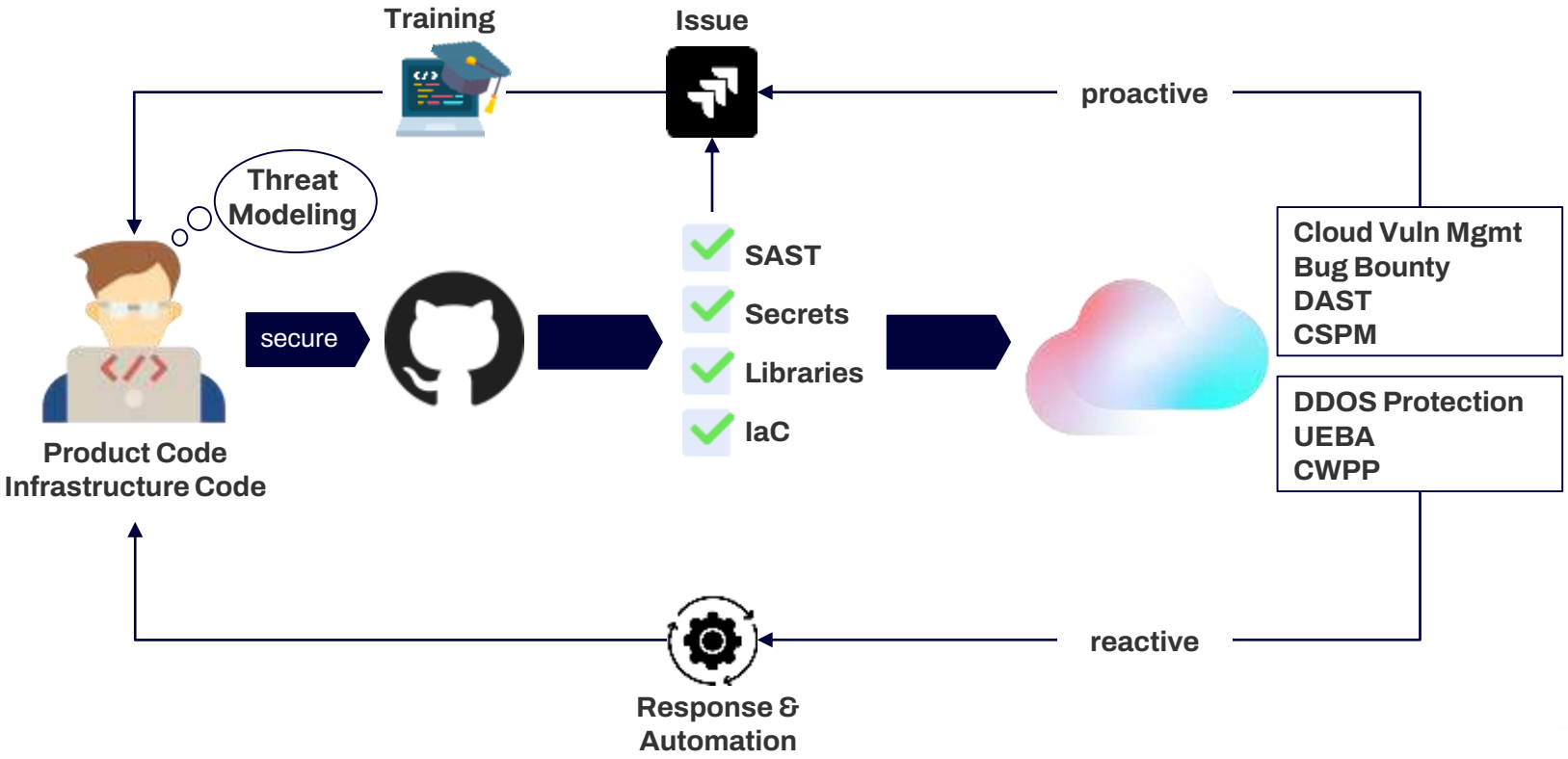
CNAPP (CSPM, CWPP, Vulnerability Mgmt, UEBA)
Response & Automation
XDR / SIEM

LACEWORK

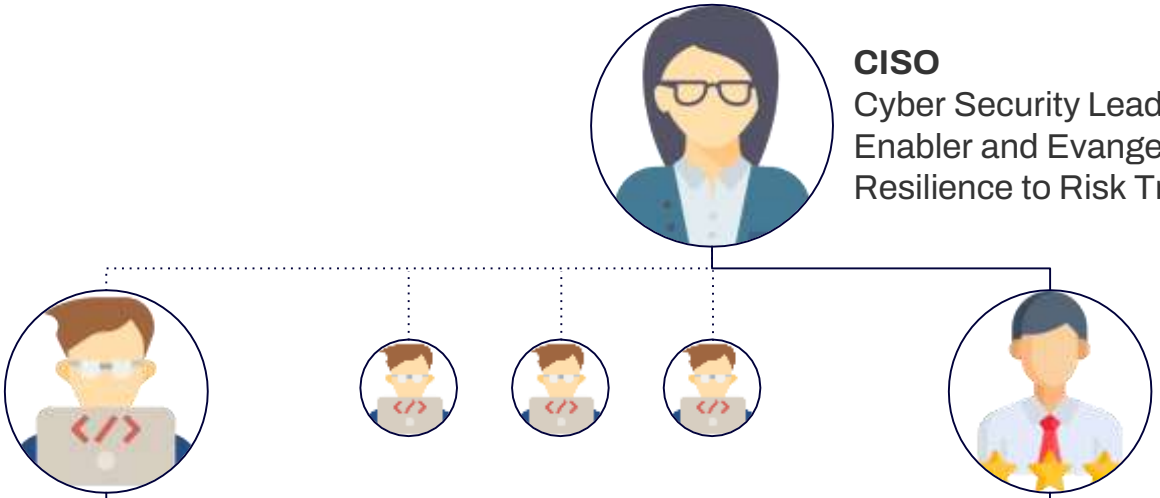
Zero Trust


aws
Google Workspace
Jira
EDR
Identity Context
Device Context
Compromise Context
IDP
MDM
Attacker needs
- valid credentials
- valid MFA (biometrics)
- MDM managed device
- EDR bypass
No Internal Network / No VPN / No Domain

Product & Cloud Security



Decentralized Security Operations

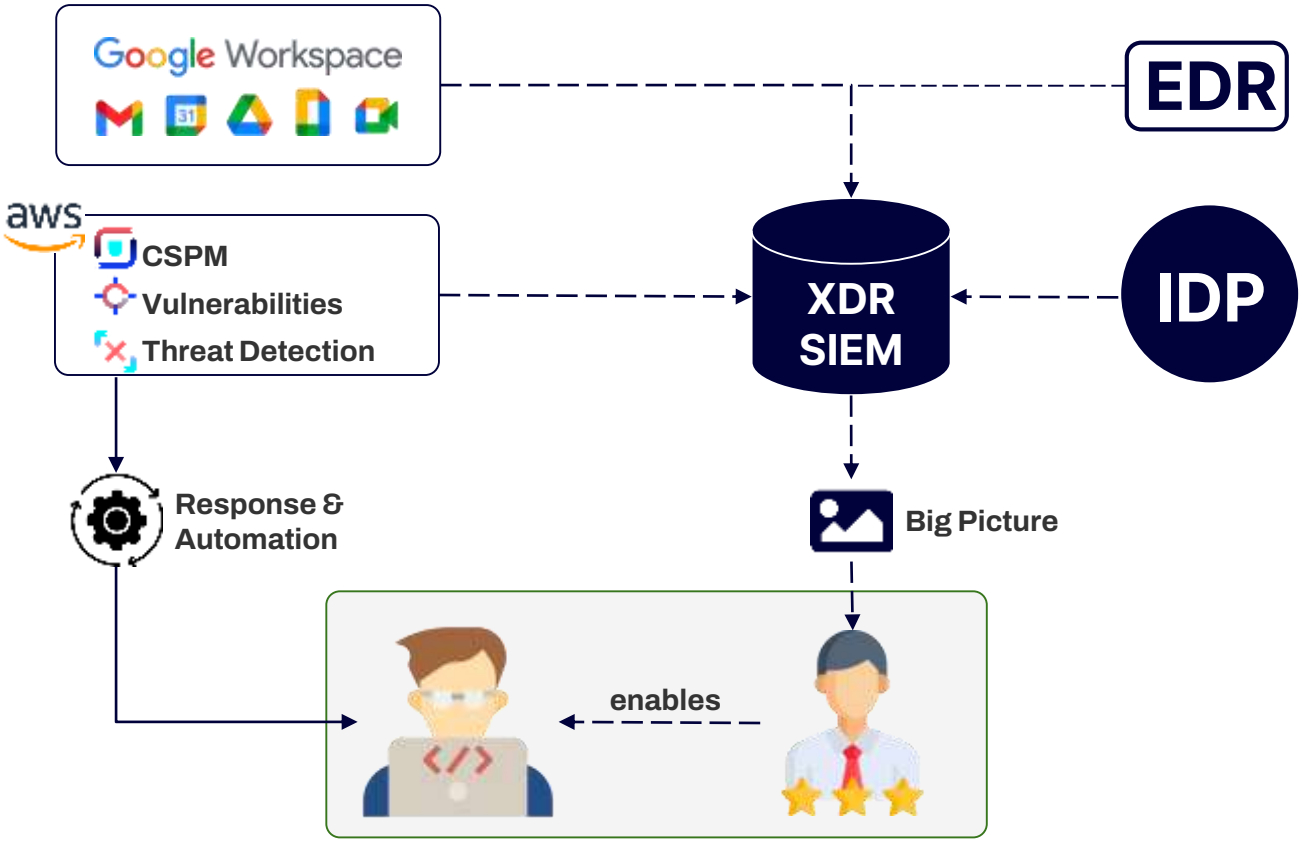


CISO
Cyber Security Leader
Enabler and Evangelist
Resilience to Risk Translator

Security Champion
Operate decentral security stack
Embed Security into Pipeline
Remediate vulnerabilities
Respond to Threats
Threat Modelling

Security Expert
Tool & Trend Scout
Enabler for Security Champions
Security Success Manager
Awareness and Trainings

Detect and Respond



Continuous Resilience Metering

Maturity Levels with Security Stories

Maturity/Resilience Level per Building Block

Zero Trust Architecture

Product & Cloud Security

Decentralized Security Operations

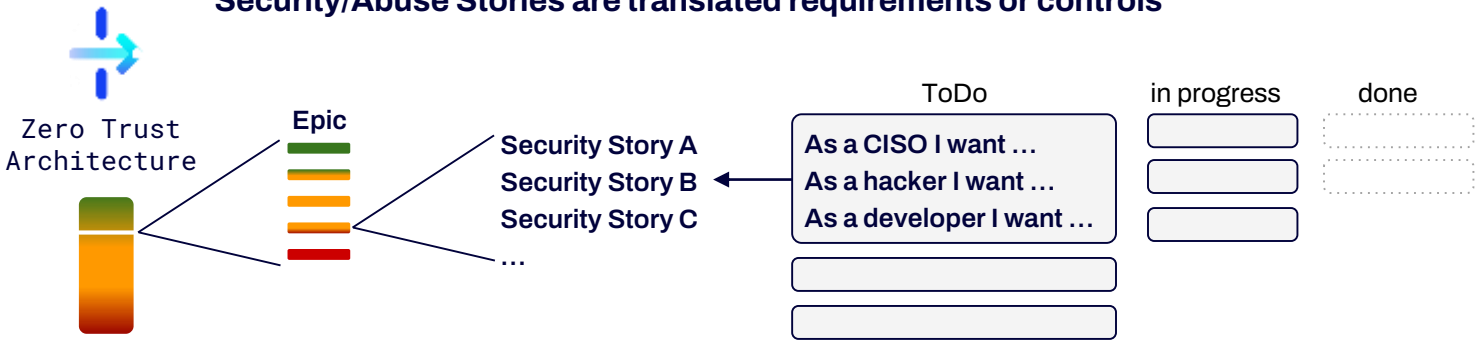
Detect and Respond

LACEWORK

Continuous Resilience Metering

Maturity Levels with Security Stories

A Building Block Level consists of Security Epics
A Security Epic consists of Security Stories / Abuse Stories
Security/Abuse Stories are translated requirements or controls



LACEWORK

- Do not lift and shift your security, rebuild it “cloud-native”
- Focus on data and identities
- Move away from rule-based approaches and make use of data at scale and M/L
- Do more with less

Thank you.

Andreas Schneider
Field CISO EMEA

https://www.linkedin.com/in/ciso-andreas-schneider/