



Stabilba' vagy bástya? (avagy tudjuk-e, miről is beszélünk cloud sec témában)

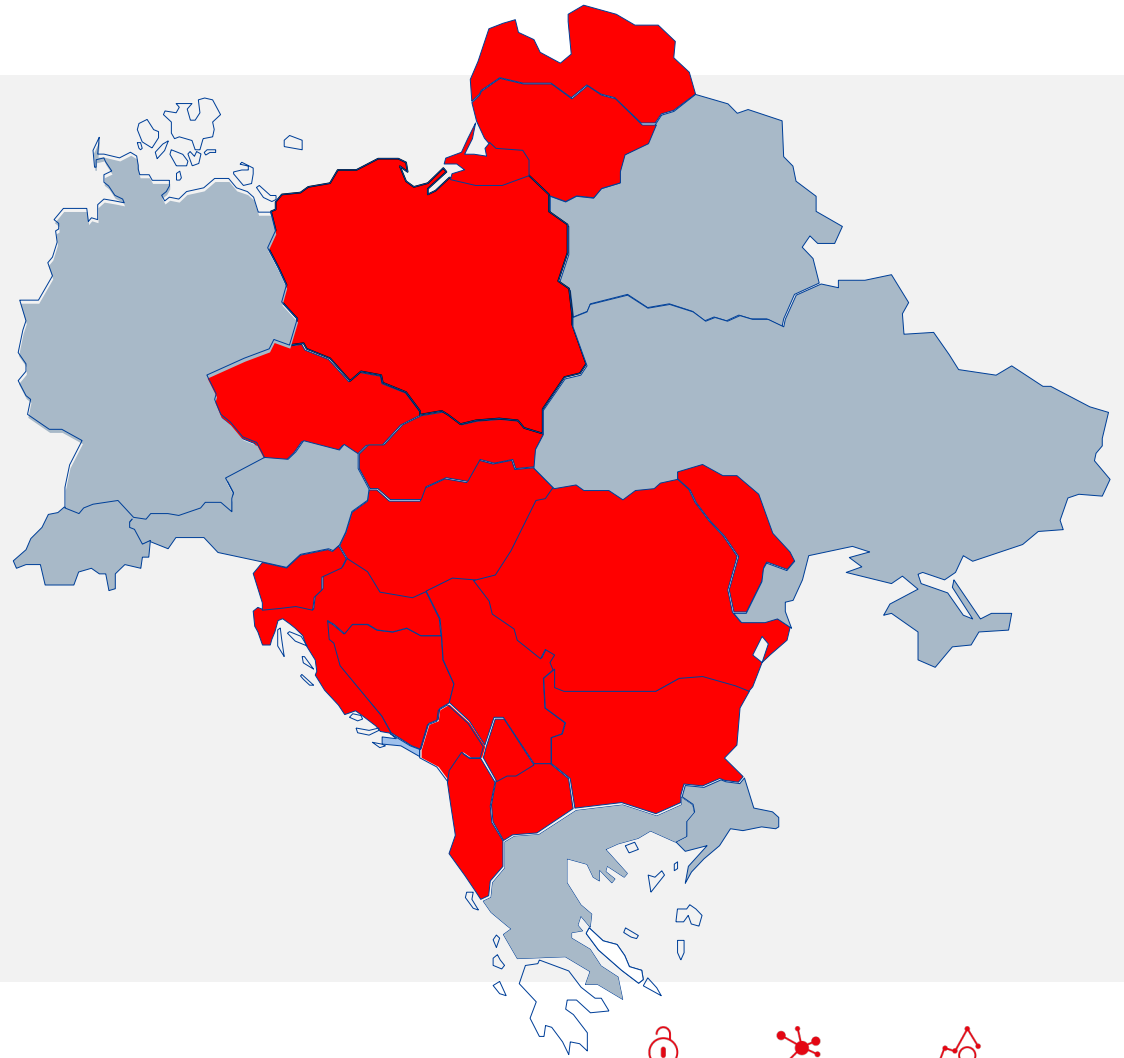
Csinos Tamás
country manager

Budapest, 2023.09.05



A CLICO Európában

- Lengyelország: Központ Krakkóban, irodák Varsó, Katowice és Rzesow
- Csehország és Szlovákia: Prága
- Magyarország: Budapest
- Románia: Bukarest
- Bulgária: Szófia
- Horvátország: Zágráb
- Szlovénia: Ljubljana
- Szerbia: Belgrád
- Erős jelenlét a Baltikumban



Cloud Workload Protection Platform (CWPP)

Folyamatos monitorozás és észlelés a fenyegetések és sérülékenységek esetén

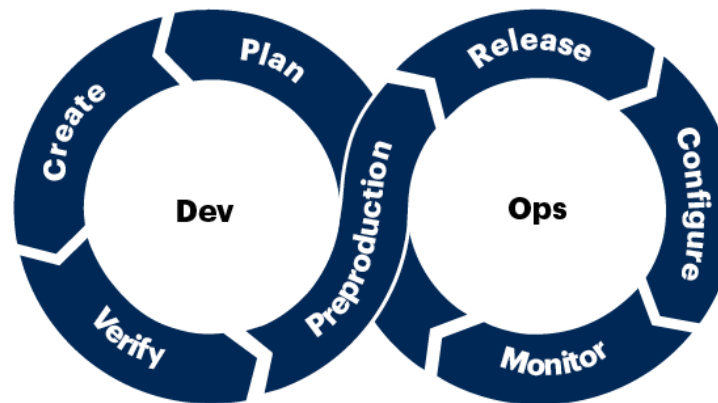
Viselkedés alapú elemzés a szokatlan tevékenységek azonosításához

automatizált reakciók a veszélyekre, például az érintett munkaterhelés izolálása

CWPP

Development Scanning

- Vulnerable components
- Cloud configuration
- Secrets
- Malware
- API discovery



Runtime Protection

- Workload vulnerability
- Workload configuration
- Workload segmentation
- Integrity monitoring
- Application control
- Behavioral monitoring
- Host IPS
- Anti-malware

Consistent Visibility and Control

- On-premises • Colocation • AWS • Bare metal • VMs • Azure • Containers • Alibaba Cloud • Serverless • Tencent • GCP • Kubernetes

Source: Gartner
725997_C



Cloud Security Posture Management (CSPM)

Riasztások, javítási javaslatok

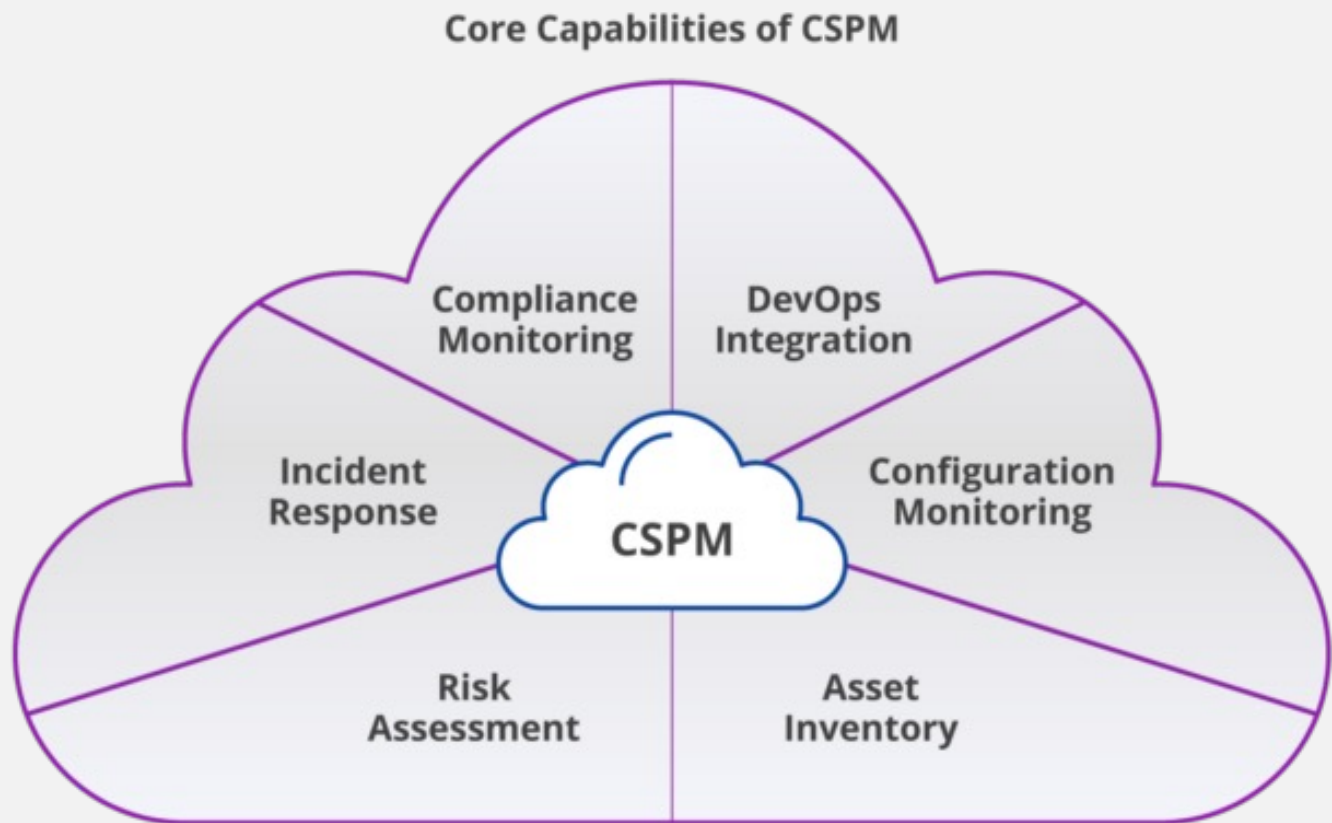
Konfigurációk automatizált ellenőrzése

Incidens prioritizálás

Biztonsági ajánlások, gdpr + iso27001 követelmények betartása

Változások naplózása

Hibrid (felhő)környezetekhez is használható



Cloud Infrastructure Entitlement Management (CIEM)

Jogosultságkezelés

Key Challenges Managing Cloud Infrastructure Entitlements

Privileged Access Management

Akit kifejezetten az
indentitáskezelés érdekel, az
jöjjön el az Identity Day
konferenciánkra szeptember 14-
én. Részletek:
<https://identityday.hu>

Célja
hozzáfér-
jogosultság-szintek
elkerülése

defined
across cloud
infrastructures

Source: Gartner



 Security  Networking  Management

Cloud Native Application Protection Platform (CNAPP)

Védelmet biztosít a felhőben futtatott alkalmazások teljes életciklusára (kódtól termelésig)

Egy platformon belül helyettesíti a CSPM, CWPP, CIEM eszközöket

Teljeskörű lefedettséget biztosít

Shift-left beépített képesség

Detailed CNAPP Capabilities

Artifact Scanning

- SAST/DAST
- API Scanning
- Software Composition Analysis
- Exposure Scanning
 - CVEs
 - Secrets
 - Sensitive Data
 - Malware
 - Attack Path Analysis

Security



Cloud Configuration

- Infrastructure as Code Scanning
- Network Configuration and Security Policy
- Cloud Infrastructure Entitlements Management
- Kubernetes Security Posture Management
- Cloud Security Posture Management

Runtime Protection

- Web Application and API Protection
- Application Monitoring
- Cloud Workload Protection Platform
- Network Segmentation
- Exposure Scanning
 - CVEs
 - Secrets
 - Sensitive Data
 - Malware
 - Attack Path Analysis

Source: Gartner
742828_C



Gartner



Security



Networking



Management

A biztonságos felhőkörnyezet alkotóelemei

- CWPP (Cloud Workload Protection Platform) – munkafolyamatok védelme “IaC” – VM-ek, konténerkörnyezetek, szerverek
- CSPM (Cloud Security Posture Management) – hibás konfigurációk és megfelelőségi (compliance) kockázatok felismerésében segít
- CIEM (Cloud Infrastructure Entitlement Management) – engedélyek/hozzáférések szabályozása és kezelése az infrastruktúrában
- CNAPP (Cloud Native Application Protection Platform) – biztosítja az alkalmazások biztonságát kódtól termelésig egyetlen platformon belül

ARISTA

ARMIS®

Cryptshare®

CLOUDIAN®

CYBERARK®

DIGI®

ENTRUST

exabeam

Fidelis
Cybersecurity

Forcepoint

FORESCOUT.

GREYCORTEX

illumio

imperva

Infinera®

IronNet

ivanti®

JUNIPER
driven by Mist AI

MICROSENS

netskope

nextsense

opengear
A DIGI® COMPANY

paloalto®
NETWORKS

radware

RAPID7

Recorded Future®

rubrik

COMMScope®
RUCKUS®

SailPoint

SCIRGE

SentinelOne™

THALES

tufin

VECTRA®

Letölthető whitepaper:



 Security  Networking  Management

Save the date: Clico Cloud Control (C3) konferencia nov. 9 délután, KEG Sörművház



Security Networking Management