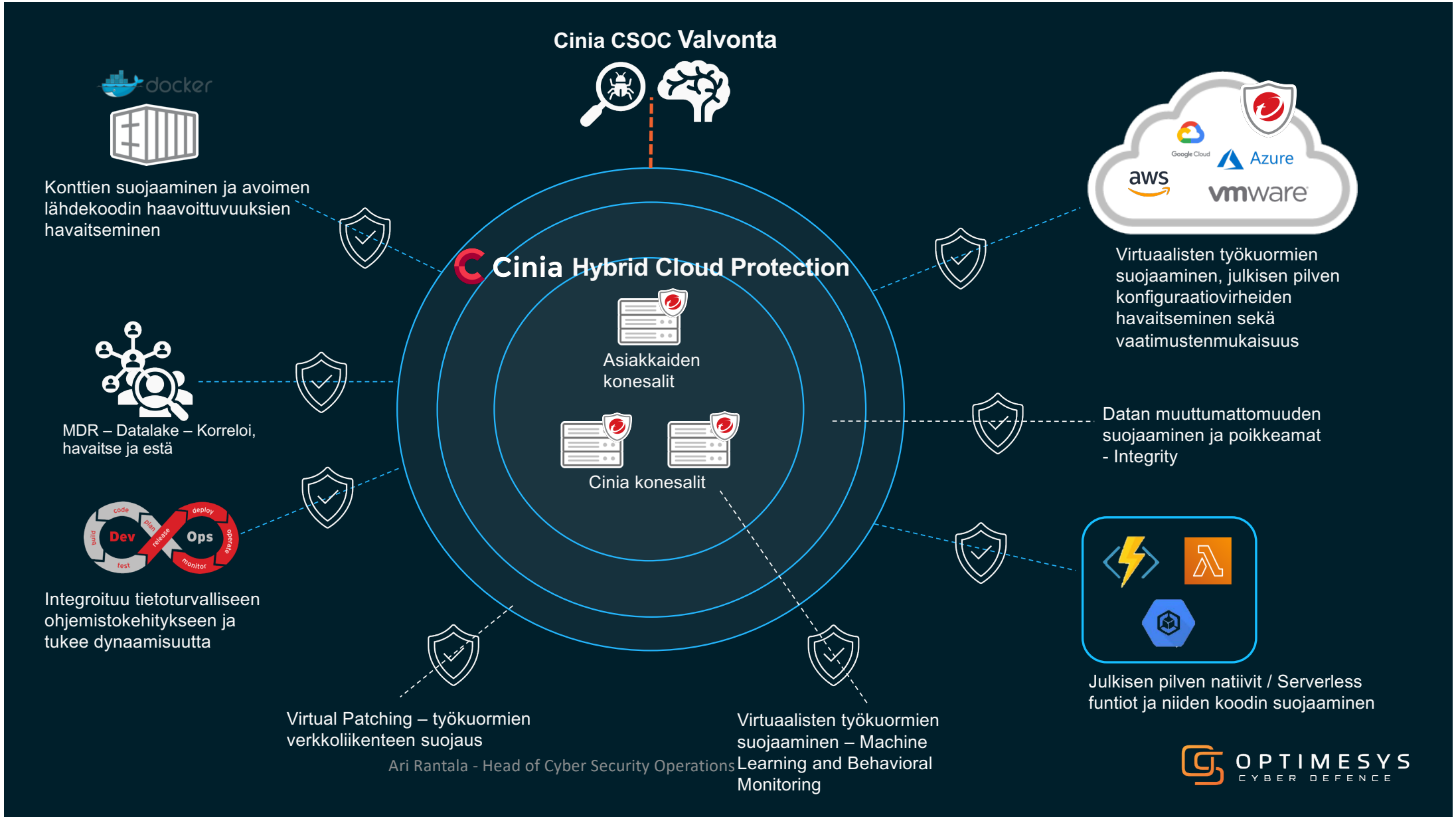
Part of Cinia

Ota haltuun ja reagoi– Hybridipilven suojaus kokonaispalveluna

Ari Rantala – Head of Cyber Security Operations

OPTIMESYS
CYBER DEFENCE


Cinia CSOC Valvonta
Cinia Hybrid Cloud Protection
Asiakkaiden konesalit
Cinia konesalit
Konttien suojaaminen ja avoimen lähdekoodin haavoittuvuuksien havaitseminen
MDR – Datalake – Korreloi, havaitse ja estä
Integroituu tietoturvalliseen ohjemistokehitykseen ja tukee dynaamisuutta
Virtual Patching – työkuormien verkkoliikenteen suojaus
Virtuaalisten työkuormien suojaaminen – Machine Learning and Behavioral Monitoring
Virtuaalisten työkuormien suojaaminen, julkisen pilven konfiguraatiovirheiden havaitseminen sekä vaatimustenmukaisuus
Datan muuttumattomuuden suojaaminen ja poikkeamat - Integrity
Julkisen pilven natiivit / Serverless funtiot ja niiden koodin suojaaminen
Ari Rantala - Head of Cyber Security Operations
OPTIMESYS
CYBER DEFENCE

Part of Cinia

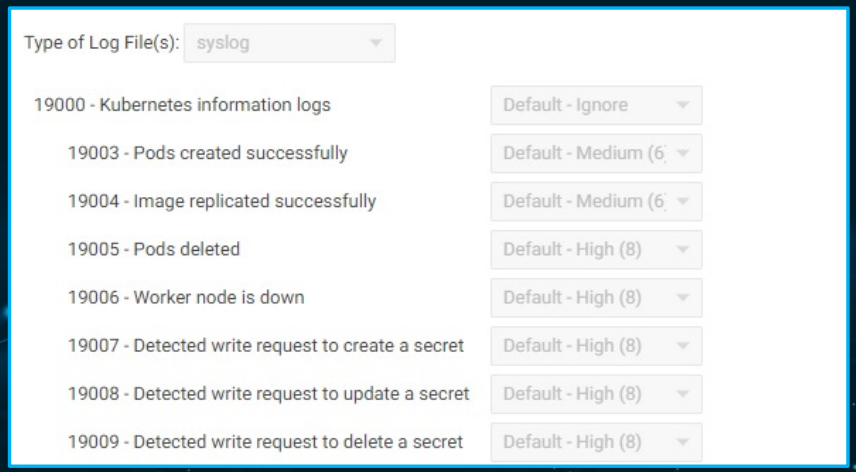
Hybridipilven suojaus kokonaispalveluna

- ✓ Demottavat teknologiat
  - ✓ Cloud One – Workload Security
    - ✓ Virtuaalikoneille ja konteille – Windows / Linux
    - ✓ Legacy tuki – WIN2000 :O
    - ✓ Enemmän kuin pelkkä AV
    - ✓ Palveluiden valvontaan
    - ✓ Palvelimien kovettamiseen
      - ✓ Sekä kovetettujen palvelimien valvontaan
    - ✓ Suojaa haavoittuvuuksilta ennen kuin ehdit päivittää

OPTIMESYS CYBER DEFENCE

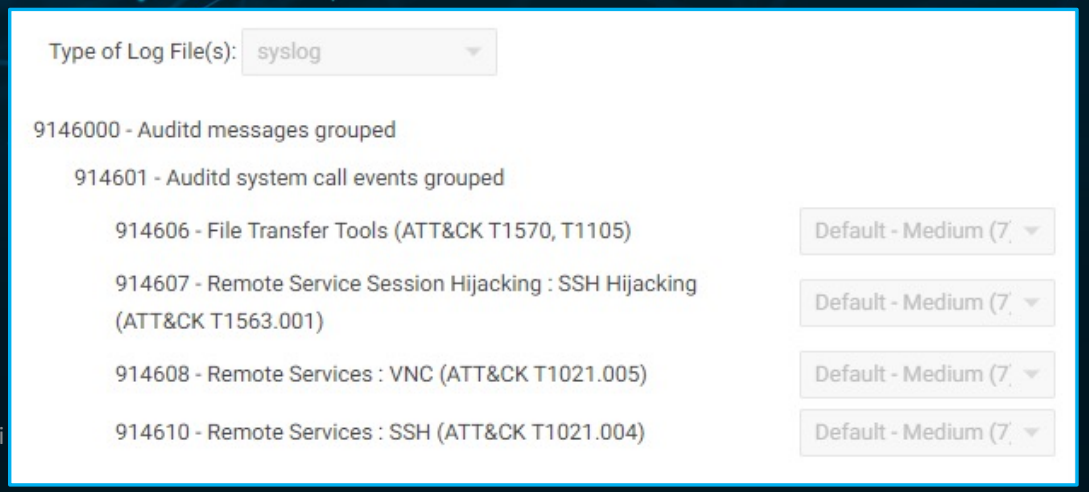
Log Inspection – eihän tämä SIEM ole??

Defined	1010141 - Microsoft Windows - Export Certificate and Private Key	December 1, ...
Defined	1010349 - Docker Daemon Remote API Calls	August 4, 2020
Defined	1010390 - Microsoft Windows User Logon Events	July 21, 2020
Defined	1010421 - Trend Micro Deep Security Agent Removal Attempt	August 4, 2020
Defined	1010465 - Auditd - Mitre ATT&CK TA0007: Discovery	November 24,...
Defined	1010489 - Auditd - Mitre ATT&CK TA0003: Persistence	November 10,...
Defined	1010528 - Auditd - Mitre ATT&CK TA0004: Privilege Escalation	November 10,...
Defined	1010536 - Auditd - Mitre ATT&CK TA0006: Credential Access	November 10,...
Defined	1010541 - Netlogon Elevation Of Privilege Vulnerability (Zerologon) (CVE-2020-1472)	December 8, ...
Defined	1010558 - Auditd - Mitre ATT&CK TA0005: Defense Evasion	November 10,...
Defined	1010582 - Auditd - Mitre ATT&CK TA0008: Lateral Movement	November 24,...
Defined	1010595 - Microsoft LDAP Query Execution	November 24,...



Type of Log File(s): syslog

19000 - Kubernetes information logs	Default - Ignore
19003 - Pods created successfully	Default - Medium (6
19004 - Image replicated successfully	Default - Medium (6
19005 - Pods deleted	Default - High (8)
19006 - Worker node is down	Default - High (8)
19007 - Detected write request to create a secret	Default - High (8)
19008 - Detected write request to update a secret	Default - High (8)
19009 - Detected write request to delete a secret	Default - High (8)



Type of Log File(s): syslog

9146000 - Auditd messages grouped	
914601 - Auditd system call events grouped	
914606 - File Transfer Tools (ATT&CK T1570, T1105)	Default - Medium (7
914607 - Remote Service Session Hijacking : SSH Hijacking (ATT&CK T1563.001)	Default - Medium (7
914608 - Remote Services : VNC (ATT&CK T1021.005)	Default - Medium (7
914610 - Remote Services : SSH (ATT&CK T1021.004)	Default - Medium (7

Ari

Part of Cinia

OPTIMESYS CYBER DEFENCE

Datan muuttumattomuuden suojaaminen

1006683 - TMTR-0016: Suspicious Running Processes Detected	High
1010855 - Microsoft Exchange - HAFNIUM Targeted Vulnerabilities	High
1009626 - Windows Accessibility Features - ImageFileExecution (ATT&CK T1015,T1183)	Medium
1010055 - AntiVirus - Trend Micro ApexOne Server	Medium
1003744 - AntiVirus - Trend Micro OfficeScan Server	Medium
1002776 - Microsoft Windows - Startup Programs Modified (ATT&CK T1112, T1060)	High
1010515 - Trend Micro ServerProtect For Linux Command Execution Vulnerability (CVE-2020-24561)	Medium
1010422 - SCP - Remote File Copy (ATT&CK T1105, T1048.001)	Medium
1003019 - Trend Micro Deep Security Agent / Relay	Medium
1002999 - Database Server - Microsoft SQL Server	Medium
1003020 - Trend Micro Deep Security Manager	Medium
1008271 - Application - Docker	Medium
1010389 - Unix - Monitor Processes Running From '/tmp' Directories (ATT&CK T1059)	Medium
1002779 - Microsoft Windows - System File Modified	High
1010382 - CommandLine (ATT&CK T1059)	Medium
1009618 - PowerShell (ATT&CK T1086)	Medium
1010373 - Systemd Service (ATT&CK T1501)	Medium
1010353 - Local Security Authority (LSA) Notification Packages modified (ATT&CK T1131)	Medium

Detailed Description

Description	Object Monitored
Install Software Monitored for standard attribute changes	kubelet
Binary files monitored for standard attribute changes under following directory Looking in → /usr/local/bin/ → /usr/bin/ → /usr/share/bash-completion/completions/	Application Binary: kubelet docker
Processes monitored for standard attribute changes	Processes: kubelet kube-proxy
Files monitored for standard attribute changes in following directories looking in → /var/lib/kubelet → /etc/sysconfig/ → /etc/cni/net.d → /opt/cni/bin/	Files: Certificate File (*.crt)* Key file (*.key) PEM File (*.pem) Yaml file (*.yaml) kubelet
Directory monitored for owner, permission and group attribute changes	Directory: /var/lib/kubelet/ /var/lib/docker/

OK Cancel Apply

Part of Cinia

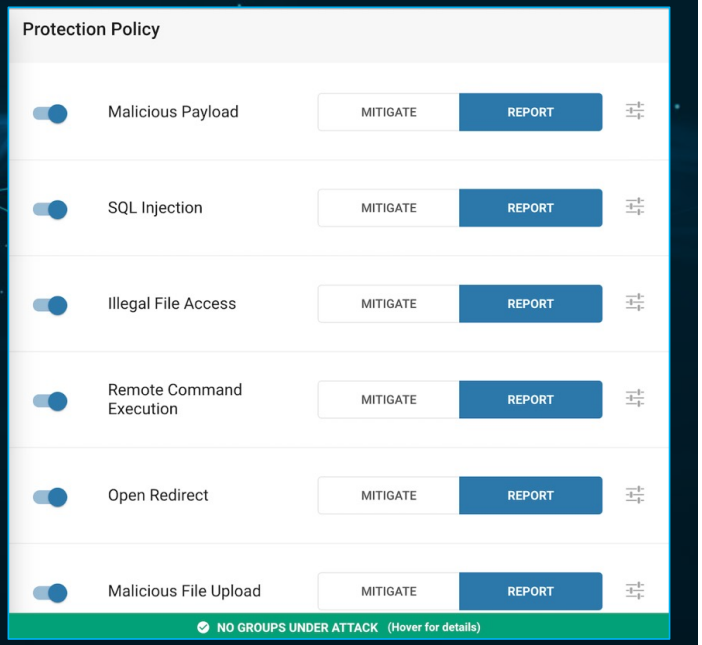
Ari Rantala - Head of Cyber Security Operations

OPTIMESYS
CYBER DEFENCE

Part of Cinia

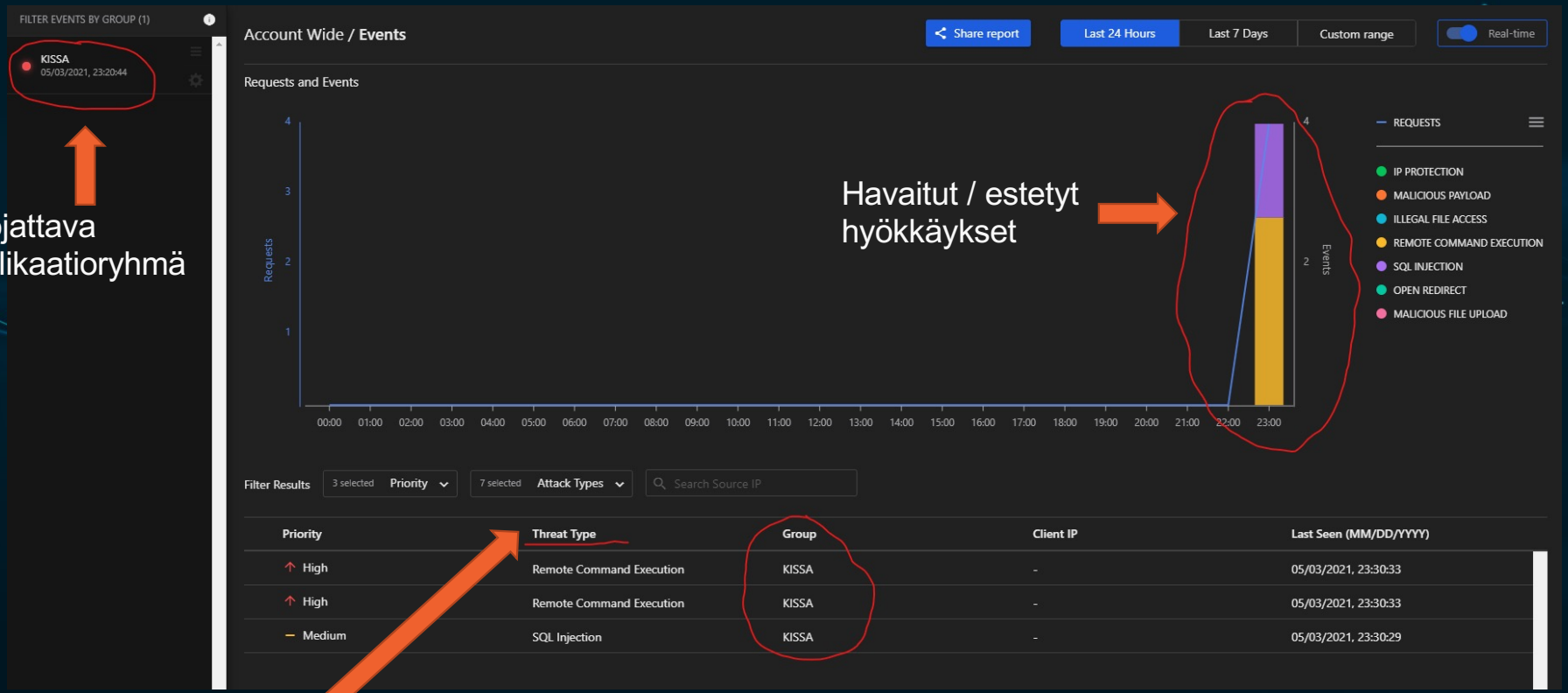
Hybridipilven suojaus kokonaispalveluna

- ✓ Demottavat teknologiat
  - ✓ Cloud One – Application Security (Serverless, API and application security)
    - ✓ RASP? Mikä häh? -> Runtime Application Self-protection
    - ✓ Suomeksi: Suojaa applikaation aina kun sitä ajetaan
    - ✓ Tuki usealle kielelle sekä esim. AWS Lambdalle
      - ✓ Java, node.JS, .NET, Python, Docker jne.
    - ✓ Suojaa useilta eri hyökkäysvektoreilta



OPTIMESYS CYBER DEFENCE

Serverless – Hyökkäyksien havaitseminen



Suojattava applikaatioryhmä

Havaitut / estetyt hyökkäykset

Hyökkäyksen tyyppi

Ari Rantala - Head of Cyber Security Operations

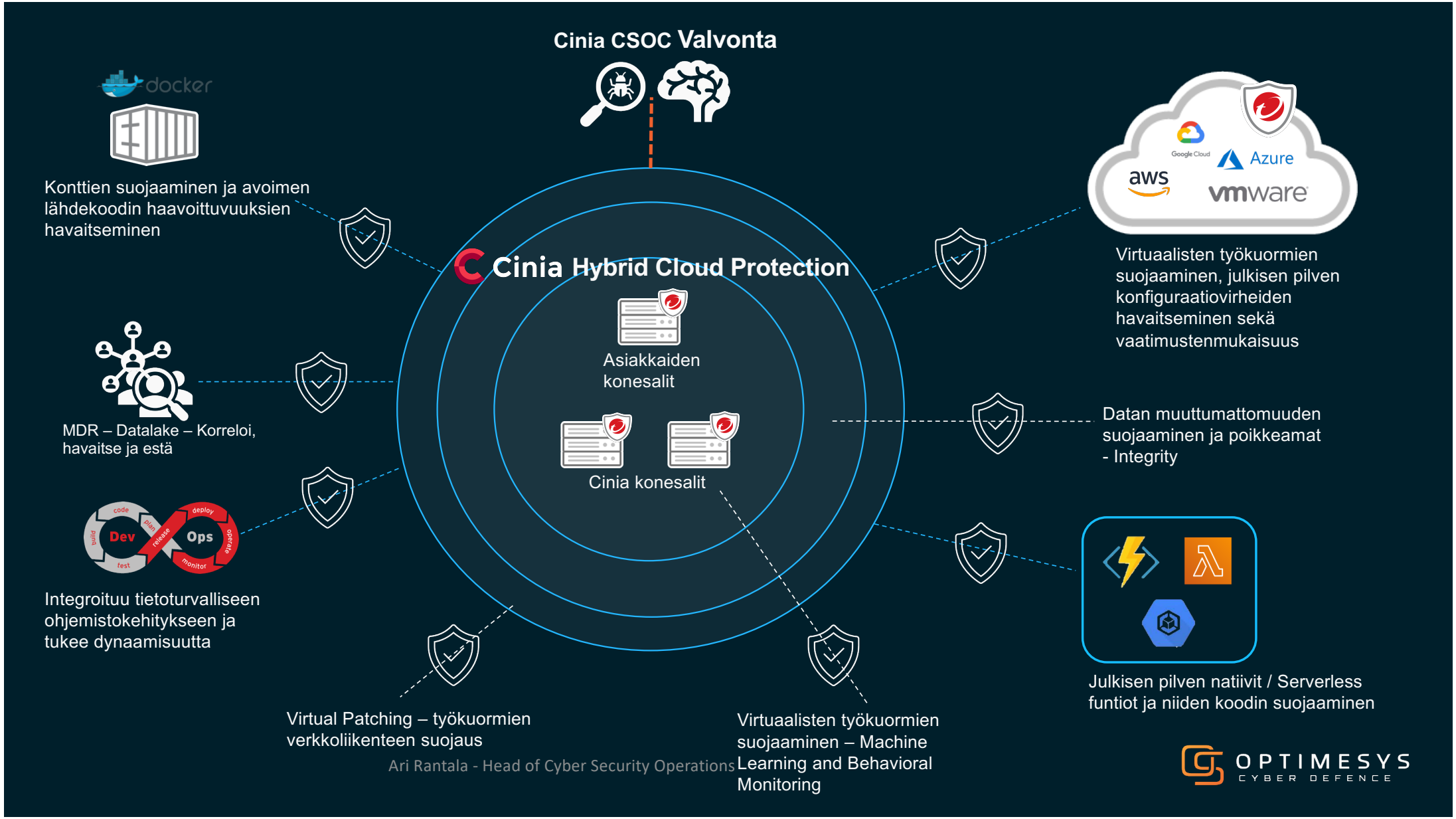
Part of Cinia

OPTIMESYS CYBER DEFENCE

Part of Cinia

Ari Rantala - Head of Cyber Security Operations

OPTIMESYS
CYBER DEFENCE


Cinia CSOC Valvonta
Cinia Hybrid Cloud Protection
Asiakkaiden konesalit
Cinia konesalit
Konttien suojaaminen ja avoimen lähdekoodin haavoittuvuuksien havaitseminen
MDR – Datalake – Korreloi, havaitse ja estä
Integroituu tietoturvalliseen ohjemistokehitykseen ja tukee dynaamisuutta
Virtual Patching – työkuormien verkkoliikenteen suojaus
Virtuaalisten työkuormien suojaaminen – Machine Learning and Behavioral Monitoring
Virtuaalisten työkuormien suojaaminen, julkisen pilven konfiguraatiovirheiden havaitseminen sekä vaatimustenmukaisuus
Datan muuttumattomuuden suojaaminen ja poikkeamat - Integrity
Julkisen pilven natiivit / Serverless funtiot ja niiden koodin suojaaminen
Ari Rantala - Head of Cyber Security Operations
OPTIMESYS
CYBER DEFENCE

Part of Cinia

Kiitos!

ari.rantala@optimesys.fi

Ari Rantala - Head of Cyber Security Operations

OPTIMESYS
CYBER DEFENCE