Part of Cinia

Riko siilot ja havaitse tehokkaasti – MDR-palvelun keskeiset hyödyt

Ari Rantala – Head of Cyber Security Operations

OPTIMESYS CYBER DEFENCE

Cinia CSOC Valvonta

Konttien suojaaminen ja avoimen lähdekoodin haavoittuvuuksien havaitseminen

Cinia Hybrid Cloud Protection

Asiakkaiden konesalit

Cinia konesalit

Virtuaalisten työkuormien suojaaminen, julkisen pilven konfiguraatiovirheiden havaitseminen sekä vaatimustenmukaisuus

MDR – Datalake – Korreloi, havaitse ja estä

Datan muuttumattomuuden suojaaminen ja poikkeamat - Integrity

Integroituu tietoturvalliseen ohjemistokehitykseen ja tukee dynaamisuutta

Julkisen pilven natiivit / Serverless funtiot ja niiden koodin suojaaminen

Virtual Patching – työkuormien verkkoliikenteen suojaus

Virtuaalisten työkuormien suojaaminen – Machine Learning and Behavioral Monitoring

Ari Rantala - Head of Cyber Security Operations

OPTIMESYS CYBER DEFENCE

Part of Cinia

Mitä on Managed Detection & Response?

- ✓ Uhkien havaintaan ja reagointiin, ei vaatimusten mukaisuuteen (Compliance)
- ✓ Nojautuu automatiikkaan, näkyvyyteen, telemetriikkaan ja sitä kautta nopeampaan reagointikykyyn
- ✓ Vaikka automatiikkaa hyödynnetään, takana on kuitenkin aina ihminen
- ✓ Human + automation => Better together!
- ✓ Ei vain havaintaa, vaan myös välineet ja prosessit uhkien nopeaan torjumiseen
- ✓ MDR ei korvaa SIEMiä / logienhallintaa – tuo ’rikkaita’ hälytyksiä joissa on kontekstia ja tukee muita teknologioita

OPTIMESYS CYBER DEFENCE

Part of Cinia

Käyttäjät

Työasemat

Verkko

Palvelimet ja pilvi

Sähköposti

Jatkuva sensorien tuottama data

Automatiikka

Threat Hunting

Prosessit

CSOC analyytikot

Koneoppiminen

Big data – analytiikka

Nopea tietoturvapoikkeamien korjaus ja juurisyy!

Hälytykset ja näkyvyys joka sisältää kontekstin tarvittaviin jatkotoimenpiteisiin

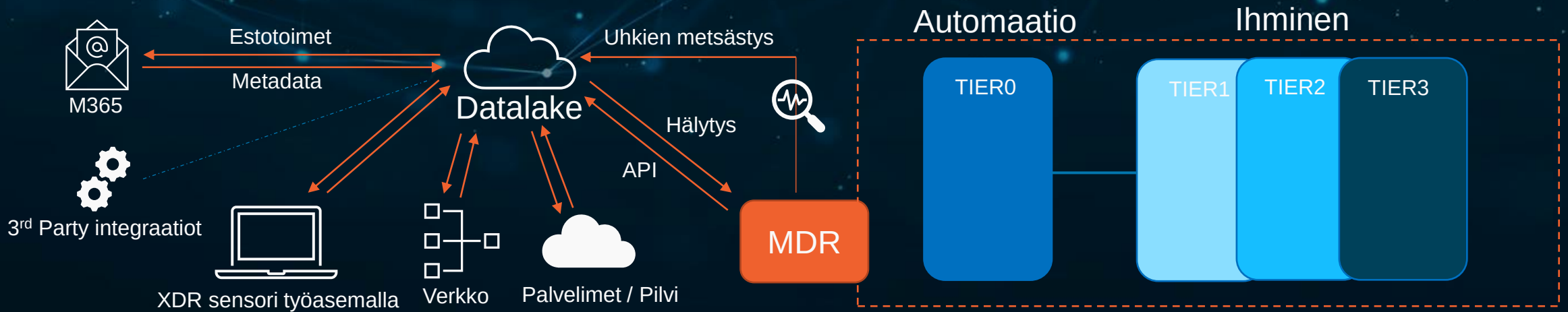
Ari Rantala - Head of Cyber Security Operations

OPTIMESYS CYBER DEFENCE

Part of Cinia

Mitä on Managed Detection & Response?

- MDR-palvelu tuotetaan CSOC-resurssien voimin
  - Osaavaa ja ketterää palvelua - tietoturvakumppanuus
- Hälytykset tuodaan keskitettyyn MDR-valvontaan
- Mahdollistaa uhkien metsästämisen ja estotoimenpiteet

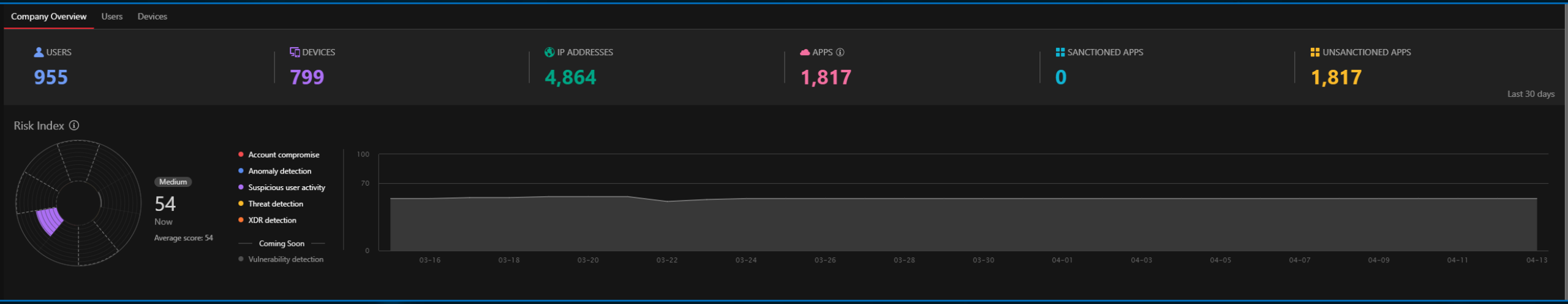


OPTIMESYS CYBER DEFENCE

Part of Cinia

Mitä on Managed Detection & Response

Riskikäyttäjät ja sovellukset



Ari Rantala - Head of Cyber Security Operations

OPTIMESYS CYBER DEFENCE

Part of Cinia

Mitä on Managed Detection & Response

Kolmannen osapuolen integroinnit

Integration ↓	Vendor
Azure AD	Microsoft
Azure AD (Mobile Security) *Preview*	Microsoft
Check Point Open Platform for Security (OPSEC) *Preview*	Check Point
Intelligence Feeds	-
Microsoft Endpoint Manager (Intune) *Preview*	Microsoft
Palo Alto Panorama *Preview*	Palo Alto
ProxySG and Advanced Secure Gateway *Preview*	Broadcom (Symantec)
QRadar on Cloud: STIX-Shifter connector *Preview*	IBM
Trend Micro Risk Insights for Splunk *Preview*	Splunk
Trend Micro XDR Splunk Add-On	Splunk

OPTIMESYS CYBER DEFENCE

Part of Cinia

MDR DEMO

Ari Rantala - Head of Cyber Security Operations

OPTIMESYS
CYBER DEFENCE

Part of Cinia

Hälytysketjujen esimerkkejä

Cryptocurrency Mining Malware - HIGH

Script Execution via Misnamed Executable - MEDIUM

Hacking Tool Detection - MEDIUM

Possible Spear Phishing Attack on High-profile User via Link - HIGH

Unknown Threat Detection and Mitigation via Predictive Machine Learning - LOW

Threat Intelligence Sweeping - HIGH

Case 1 – Epäilyttävä tiedostopolku

- ✓ **Hälytys:** Uncommon File Path of Executable File
- ✓ **Mitre ATT&CK:** TA0005, T1036
- ✓ **Riski:** Kohtalainen (Medium)
- ✓ **MDR-palvelu:** Havaitaan hälytys, käydään läpi FP/TP, tehdään tarvittavia lisähakuja, eristetään päätelaite tarvittaessa ja kontaktoidaan asiakas

Case 2 – Ulkoinen uhkatietohälytys

- ✓ **Hälytys:** **Threat Intelligence Sweeping**
- ✓ **Mitre ATT&CK:** **-**
- ✓ **Campaign:** Analyzing attacks taking advantage of the Exchange Server vulnerabilities (Hafnium)
- ✓ **MDR-palvelu:** Havaitaan hälytys, käydään läpi FP/TP, käydään läpi Auto Sweeping sääntöön osuneet artifaktit, eristetään päätelaite(et) tarvittaessa sekä viedään havainnot integroinnin kautta esim. Palomuurille sekä kerätään tiedostot tutkintaan ja avataan SIRT-toimenpiteet.

Part of Cinia

MDR-palvelun sisältö

Ominaisuus	MDR
Vision One -alusta (Saas)	x
Hälytyksien reagointi	x
Säännölliset laatu- ja kehityspalaverit	x
Tietovarasto / Big Data analytiikka (Datalake)	x
Palveluaika arkisin 08 - 18	x
Uhkatieto	x
Palvelun tuottaminen erillisestä CSOC-valvomosta (ISO27001)	x
Kuukausittainen raportointi	x
Automaattiset päivittyvät havaintamallit	x
Incident Response – Team käytettävissä	x
Näkyvyys tietoturvan eri kerroksiin (Sähköposti, työasemat, palvelimet, verkko, pilvi)	x
Threat Hunting	x
Tietoturvakumppanuus	x

Add-on Ominaisuus	MDR
24/7 palvelut	x

XDR tietoturvakerrokset	MDR
Työasemat ja sähköposti	x
Palvelimet ja pilven työkuormat	x
Verkko	x

OPTIMESYS CYBER DEFENCE

Part of Cinia

Kiitos!

ari.rantala@optimesys.fi

Ari Rantala - Head of Cyber Security Operations

OPTIMESYS
CYBER DEFENCE