

ARICOMMA

Služby bezpečnostního dohledu

Jiří Chalota, Petr Vejmělek

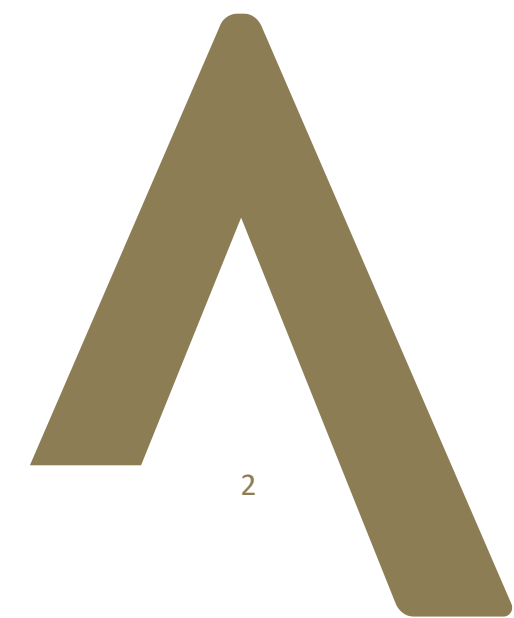
02.12.2024

Aricoma Managed Services - bezpečnostní dohled

klíčové služby

Služba Aricoma MDR

Služba Aricoma SOC



Aricoma Managed Services - bezpečnostní dohled

klíčové služby

Služba Aricoma MDR

- ▲ Služba „**REAKTIVÍHO**“ charakteru
- ▲ Detekce a reakce na kybernetické hrozby primárně ve formě útoků
- ▲ Pokročilá detekce díky **automatizované** platformě a technologii ve více vrstvách (**XDR**)
- ▲ Zrychlené reakce na incidenty díky nasazení odborníků zvolené platformy **Cynet CyOps** týmu i bezpečnostního týmu **Aricoma CSIRT**
- ▲ Služba v režimu **24x7**



Služba Aricoma MDR

... možné varianty

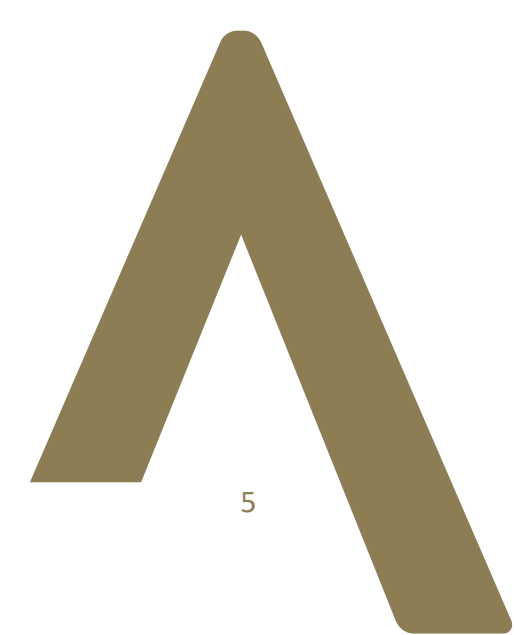
**Aricoma MDR
„Standard“**

**Aricoma MDR
„All-in-One“**

Služba Aricoma MDR

... co obsahuje varianta „Standard“

- ^ Endpoint Protection Platform (EPP = antivir)
- ^ Endpoint Detection and Response (EDR)
- ^ Network Detection and Response (NDR)
- ^ User Behavior Analytics (UBA)
- ^ Deception (Decoy)
- ^ Security Orchestration, Automation and Response (SOAR)



Služba Aricoma MDR

... co obsahuje varianta „All-in-One“

- ^ ... vše co varianta „Standard“
- ^ Endpoint Security Posture Management (ESPM)
- ^ Mobile Threat Detection (MTD)
- ^ Email Security
- ^ SaaS & Cloud Security Posture Management (SSPM & CSPM)
- ^ Centralized Log Management (CLM) and Open XDR

Služba Aricoma MDR

... orientační ceny

- začínáme na **172,- Kč/asset**

25 zařízení

Zřizovací poplatek 8.000 Kč

- ^ **4.300 Kč / 1 měsíc**
- ^ 51.600 Kč / 1 rok
- ^ 154.800 Kč / 3 roky

- ^ **9.200 Kč / 1 měsíc**
- ^ 110.400 Kč / 1 rok
- ^ 331.200 Kč / 3 roky

50 zařízení

Zřizovací poplatek 15.000 Kč

- ^ **8.300 Kč / 1 měsíc**
- ^ 99.600 Kč / 1 rok
- ^ 298.800 Kč / 3 roky

- ^ **15.700 Kč / 1 měsíc**
- ^ 188.400 Kč / 1 rok
- ^ 565.200 Kč / 3 roky

100 zařízení

Zřizovací poplatek 20.000 Kč

- ^ **16.200 Kč / 1 měsíc**
- ^ 194.400 Kč / 1 rok
- ^ 583.200 Kč / 3 roky

- ^ **29.100 Kč / 1 měsíc**
- ^ 349.200 Kč / 1 rok
- ^ 1.047.600 Kč / 3 roky

Aricoma MDR – podpora Cynet CyOps týmu 24x7

o koho se v oblasti nabízených služeb můžete opřít

^ Analýza souborů

Můžeme posílat podezřelé soubory k analýze přímo z konzole Cynet a získat okamžité verdikty.

^ Okamžitý přístup a podpora

Po souhlasu zákazníka můžeme zapojit CyOps jediným kliknutím na aplikaci Cynet Dashboard

^ Vyšetřování útoku

Podrobná analýza, úplný přehled o rozsahu a dopadu a poskytnutí aktualizovaných IOC

^ Výjimky, whitelisting a ladění

Přizpůsobení výstražných mechanismů společnosti Cynet s cílem snížit počet falešných poplachů a zvýšit přesnost.

^ Pokyny k nápravě

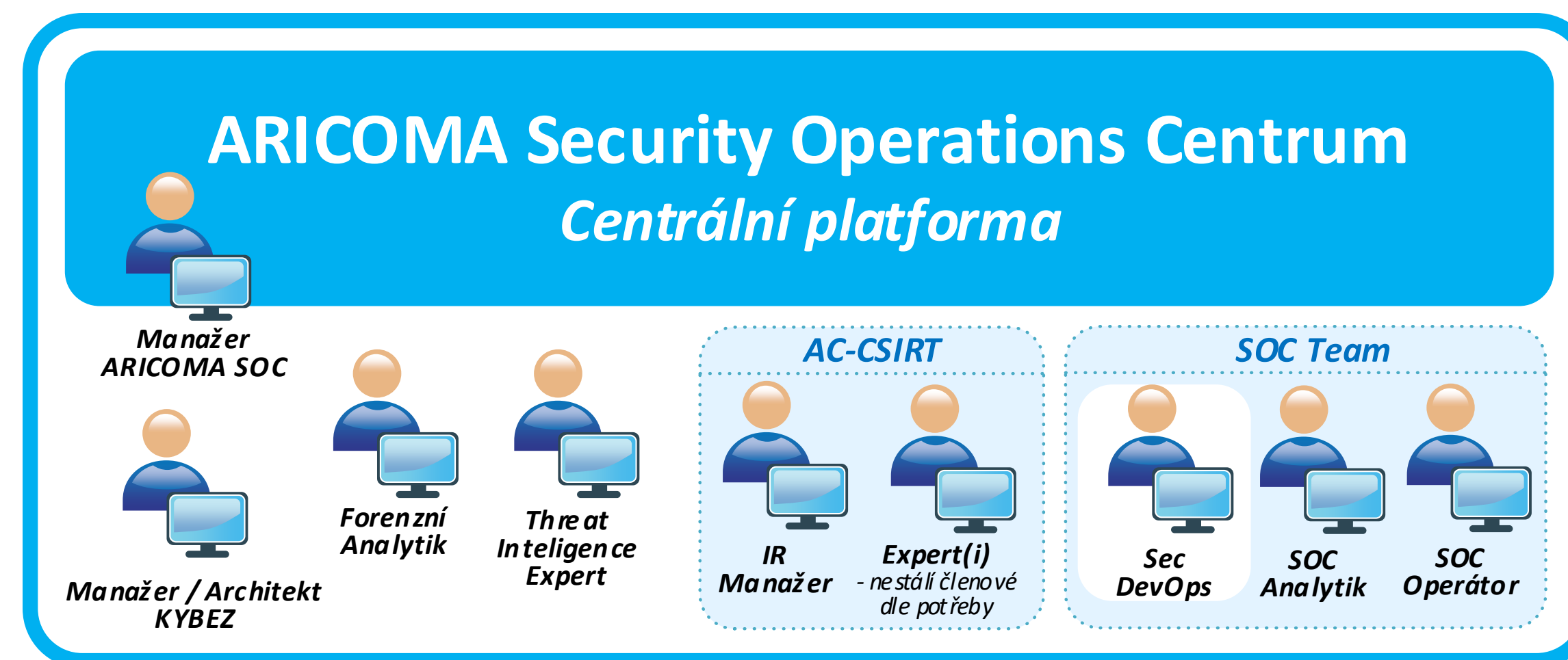
Závěr vyšetřovaných útoků zahrnuje konkrétní pokyny pro uživatele, které koncové body, soubory, uživatelský a síťový provoz by měly být napraveny.



Aricoma Managed Services - bezpečnostní dohled

o koho se v oblasti nabízených služeb můžete opřít

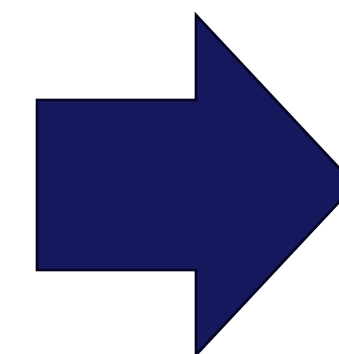
- Λ Zkušený tým Aricoma specialistů, který využívá popsané procesy a je akreditovaným členem komunity CERT/CSIRT týmů Trusted Introducer (TI)
- Λ Tým řeší více jak 30.000 alarmů měsíčně
- Λ Služby bezpečnostního dohledu poskytuje desítkám zákazníků mezi kterými jsou Kofola, Tescoma, Česká zbrojovka Uherský Brod, nemocnice a další...



Co už služby „MDR“ neumí?

příklady

- ^ Proč se mi blokují účty v AD?
- ^ Mám vlastní nebo specifické aplikace?
- ^ Potřebuji detekovat vlastní korelaci událostí z více zdrojů?
- ^ Potřebuji konkrétní vizualizaci (vlastní dashboardy)?
- ^ Chci mít přehled o zranitelnostech aktivních prvků LAN?
- ^ Potřebuji detailní reporting ?



**Služba
Aricoma
SOC**



Aricoma Managed Services - bezpečnostní dohled

klíčové služby

Služba Aricoma MDR

- ^ Služba „**REAKTIVÍHO**“ charakteru
- ^ Detekce a reakce na kybernetické hrozby primárně ve formě útoků
- ^ Pokročilá detekce díky **automatizované** platformě a technologii ve více vrstvách (**XDR**)
- ^ Zrychlené reakce na incidenty díky nasazení odborníků dodavatele platformy Cynet CyOps týmu i Aricoma CSIRT týmu
- ^ Služba v režimu **24x7**

Služba Aricoma SOC

- ^ Služba „**PROAKTIVNÍHO**“ charakteru
- ^ Komplexní služby bezpečnostního dohledu pro celé IT prostředí (**SIEM + SOAR**)
- ^ Analýza prostředí, pronájem sondy, sběr logů, definice procesů reakce, alerting v reálném čase a proaktivní komunikace, garance zahájení řešení do 4 hodin, service desk, měsíční reporting
- ^ Zajišťuje Aricoma CSIRT tým
- ^ Služba možná v režimech 8x5 i 24x7

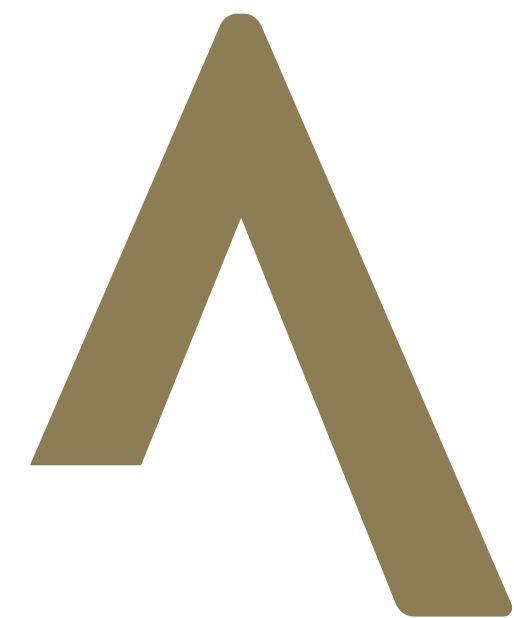
Služba „Aricoma SOC“

^ Co obsahuje základní služba:

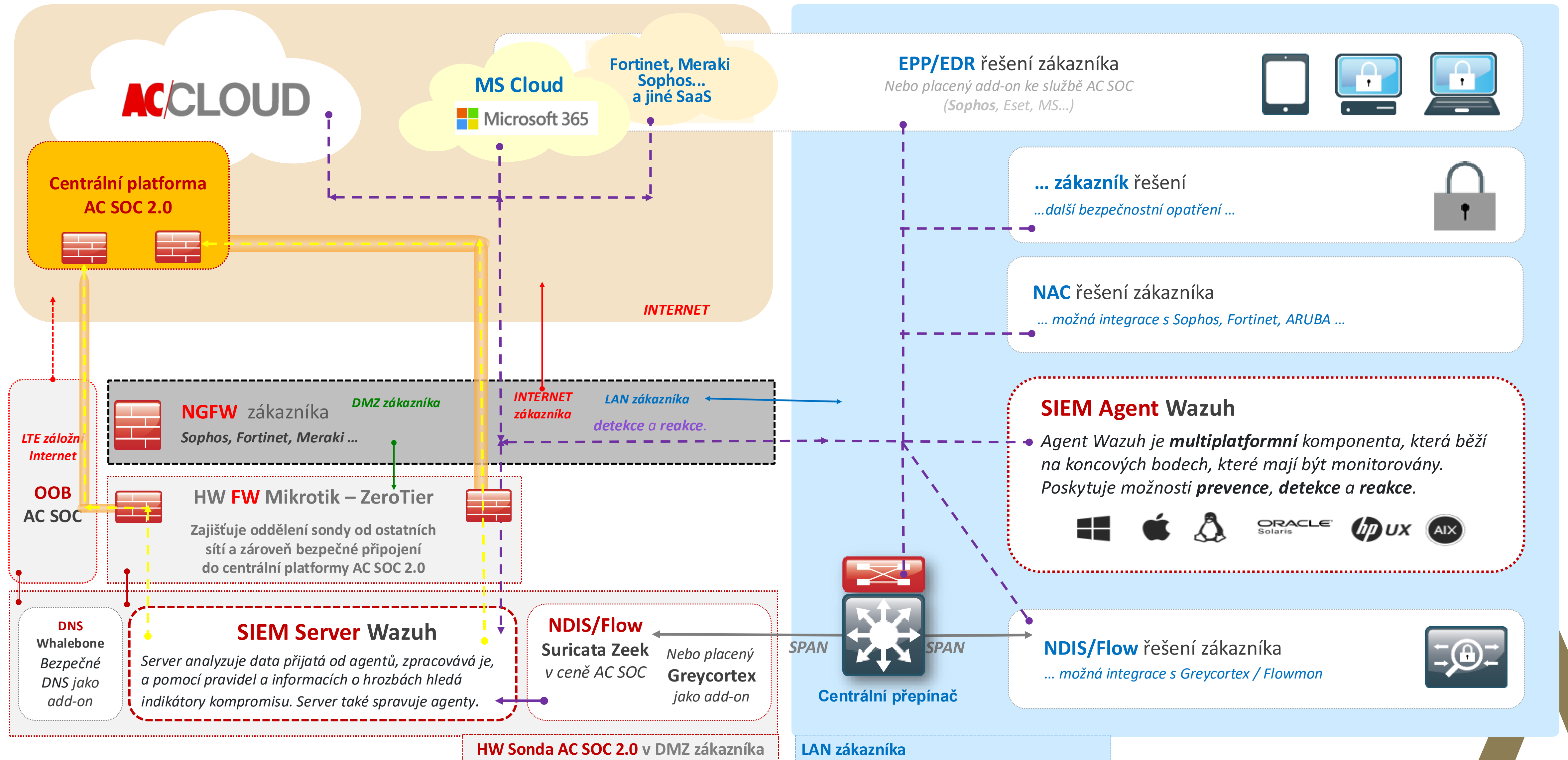
- ^ Analýza prostředí, identifikace technických aktiv
- ^ Pronájem HW sondy včetně profylaxe HW a SW
- ^ Nastavení sběru a uložení logů
- ^ Definice procesů reakce
- ^ Analýza a korelace událostí v reálném čase
- ^ Analýza a identifikace možných incidentů
- ^ **Threat Hunting**
- ^ Základní scénáře reakce
- ^ **Audit konfigurace dle CIS Security Controls**
(sada „Best Practis“ konfigurací)
- ^ **Host-based audit zranitelností**
- ^ **DarkWeb Monitoring**
- ^ Alerting v reálném čase a proaktivní komunikace
- ^ Reporting - měsíční report o událostech a incidentech

- ^ Garance technického specialisty pro zahájení řešení kybernetického incidentu do 4 hodin
- ^ Service Desk
- ^ Komunikace s třetími stranami (*NUKIB, ÚOOÚ...*)
... i s agresory (*jazyky, agresivní vyjednávání...*)
- ^ 30 min. Teams meeting se specialisty SOC tzv. Lessons Learned (*ponaučení, systémová doporučení...*)

Hlídáme všem stejně !



BEZPEČNOSTNÍ PLATFORMA „WAZUH“ - GLOBÁLNÍ POHLED



ARICOMA

Jiří Chalota

Team Leader

Aricoma SOC

jiri.chalota@aricoma.com

+420 724 175 915

aricoma.com

Petr Vejmělek

Manažer oblasti nabídky

Kybernetická bezpečnost

petr.vejmelek@aricoma.com

+420 724 263 249

aricoma.com