Aricoma Cyber Defense Center

Security Operations Center

Se službou Aricoma SOC získáte nepřetržitou viditelnost bezpečnostní situace nad celou infrastrukturou, rychlejší vyhodnocení bezpečnostních událostí a schopnost reagovat dříve, než incident přeroste v krizi.

Aricoma SOC v kostce

24x7 bezpečnostní dohled

Nepřetržité sledování a vyhodnocování bezpečnostních událostí.

Flexibilní napojení na vaše prostředí

Možnost využití vašich vlastních nástrojů (SIEM, Log Management) nebo dodání technologie jako součást služby. Umíme připojit i interní aplikace generující logy. Propojení dat z různých systémů umožňuje odhalit souvislosti, které by izolované nástroje nezachytily.

Špičkové technologie a expertíza

Aricoma SOC zahrnuje pokročilé aktivní i analytické nástroje, které v rukou našeho zkušeného týmu tvoří ochranný štít připravený nepřetržitě chránit váš provoz

Komplexní aktivní bezpečnost

Vaše investice chráníme aktivním řízením a plnou kontrolou celého kybernetického prostředí. Na hrozby nečekáme, aktivně jim předcházíme a jsme připraveni jim čelit.

Proč SOC

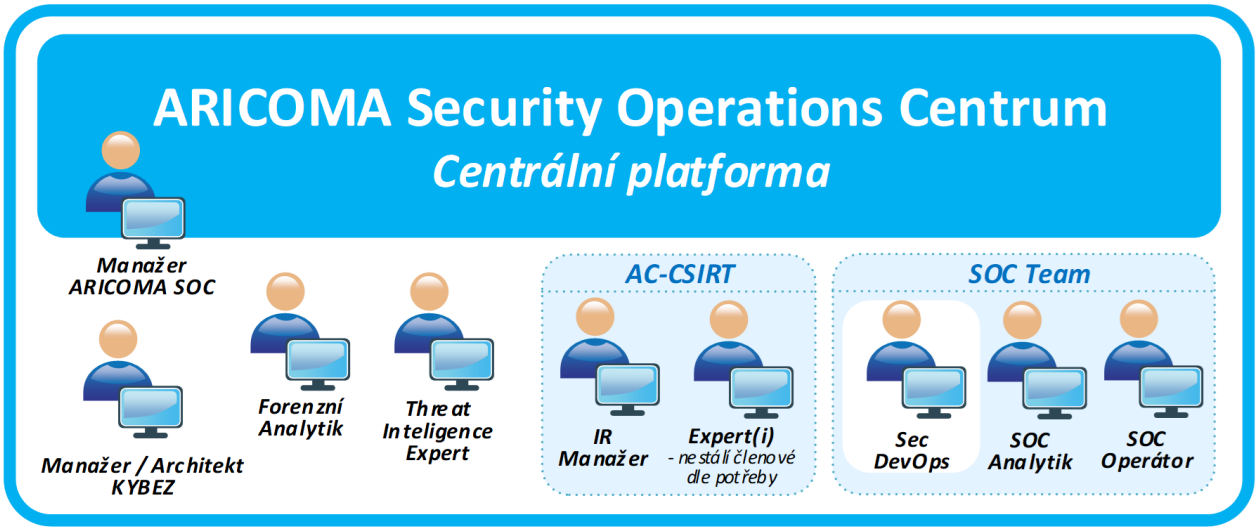
Propojit → Rozumět → Řídit

Rolí Aricoma Cyber Defense Center není pouze sledovat alarmy. Naší rolí je rozpoznat, které události jsou skutečně důležité, pochopit jejich kontext a včas reagovat. V prostředí, kde může být rozdíl mezi zvládnutým incidentem a krizí otázkou minut, je správné vyhodnocení stejně důležité jako samotná technologie.

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

Šest kroků k bezpečnější infrastruktuře

1. Kontinuální sběr, normalizace, kategorizace a korelace informací (nejen logů) prostřednictvím technologických řešení.
2. Převzetí detekovaných skutečností a postoupení procesu řízení bezpečnostních událostí a incidentů, zejména pak v první řadě Short Event Triage, ve které se validuje, zda se jedná o reálnou hrozbu.
3. Detailní analýza bezpečnostních událostí a jejich finální vyhodnocení, zda se jedná o bezpečnostní incidenty, nebo o falešné poplachy. V případě falešných poplachů jsou předávány podněty ke zlepšení bezpečnosti, a to zejména detekčních mechanismů jednotlivých bezpečnostních, ale i jiných prvků v infrastruktuře. V případě detekce bezpečnostního incidentu (potvrzení, že se nejedná o falešný poplach), je tento incident v rámci procesu řízení kybernetických bezpečnostních událostí a incidentů podroben investigaci.
4. Investigaci kybernetických bezpečnostních incidentů realizujeme s cílem stanovení vektoru útoku, dopadu a dalších informací nezbytných pro vyšetření bezpečnostních incidentů a stanovení adekvátní reakce.
5. Následně navrhneme reakci a kooperujeme při reakci. Zde můžeme i na vyžádání poskytnout koordinaci při řízení kybernetických bezpečnostních incidentů, poskytnutím role tzv. Incident koordinátora, případně vyžádat zásah reakčního CSIRT týmu.
6. Post incident aktivity, spočívající zejména v evidenci a doporučení pro další rozvoj bezpečnosti.



Komplexní dohledové služby s přidanou hodnotou

Vybudování vlastního bezpečnostního dohledového centra je pro mnoho organizací finančně i personálně náročné. Model SOC as a Service umožňuje využívat profesionální bezpečnostní dohled bez nutnosti budovat vlastní dohledovou infrastrukturu a tým.

Naše služba pokrývá široké spektrum aktivní bezpečnosti: Analýzu prostředí, pronájem sondy, software, sběr logů, definice procesů reakce, alerting v reálném čase a proaktivní komunikace, garance zahájení řešení dle SLA, Service Desk, měsíční reporting, post incident aktivity, konzultace s odborníky, rozvoj a doporučení pro další rozvoj bezpečnosti.