Aricoma Cyber Defense Center

Aktivní bezpečnostní služby

Bezpečnost zajišťujeme jak malým firmám, tak největším organizacím na trhu. S týmem expertů v našem centru chráníme to, na čem záleží nejvíce. Dohledové centrum nepřetržitě sleduje váš provoz, rychle reaguje na incidenty, nabízí široké spektrum bezpečnostních služeb.

8 analytiků L1 - průběžný dohled
První linie bezpečnostního dohledu. Nepřetržitě monitoruje bezpečnostní události, jako první reaguje.

8 analytiků L2 - analýza událostí
Od L1 přebírají potvrzené události a detailně analyzují příčinu i dopady, jsou s vámi v aktivním kontaktu.

5 specialistů L3/DevOps - CSIRT
V případě bezpečnostního incidentu koordinují další postup, minimalizují dopady a pomáhají rychle obnovit provoz.

ACDC Team Manager - od začátku s vámi
Více jak 13 let se také úspěšně věnuje problematice dohledových systémů, instalacím SIEMů a řešení incidentů jako zkušený Incident Response Manager.

Certifikovaná zkušenost a kontinuální rozvoj
Naši specialisté disponují certifikacemi CompTIA CySA+, CompTIA Security+, CEH, BTL1, BTL2 a CSOM, další rozvoj pak pokračuje i k pokročilým certifikacím ECIH, GCIH a dalším.

Trusted Introducer
Jsme držiteli stupně accredited, již brzy budeme plně certifikovaní stupněm Certified.

Široká servisní síť
V rámci rodiny Aricoma se můžete opřít o širokou síť servisních míst a více než 120 technických garantů a expertů.

Governance, Risk and Compliance
Nezapomínáme ani na jednání s úřady, vyšetřovateli i Váš soulad se směrnicemi jako NIS2, DORA, GDPR a další.

Komplexní dohledové služby s přidanou hodnotou

Kybernetické útoky nečekají na pracovní dobu. Přicházejí skrytě, zkoušejí obranu z různých směrů a využívají každé prodlení a zaváhání. Útočníkům často stačí jeden kompromitovaný účet, jedno neaktualizované zařízení, jedna škodlivá příloha nebo jeden špatně zabezpečený vzdálený přístup.

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.

Aricoma MDR

Vidět → Vyhodnotit → Reagovat

Managed Detection & Response propojuje pokročilou platformu Cynet, expertní dohled a jasně řízenou reakci na bezpečnostní incidenty.

- **EDR/XDR a 24x7 reaktivní dohled**
  Kompletní služba včetně licence a instalace EDR/XDR Cynet360, monitoringu, expertů i zásahů s transparentními, předvídatelnými náklady.
- **Okamžité nasazení bez nutnosti HW**
  Technologie Cynet360 nevyžaduje použití dalšího HW, je tak připravena k okamžitému nasazení do provozu.
- **Precizní nastavení a správa technologie**
  Správné nastavení korelace událostí a automatizace zajistí minimální počet falešných poplachů. Zajistíme tak dohled společně s efektivním provozem nástrojů.

Aricoma SOC

Propojit → Rozumět → Řídit

Služba Security Operations Center zajišťuje komplexní dohled nad bezpečností IT prostředí napříč technologiemi, systémy i sítěmi.

- **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.
- **Korelace a kontext bezpečnostních událostí**
  Propojení dat z různých systémů umožňuje odhalit souvislosti, které by izolované nástroje nezachytily.
- **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.

Aricoma Advanced Response

Tato služba rozšiřuje bezpečnostní dohled o aktivní reakci na incidenty nad EDR a XDR technologiemi, které již ve své infrastruktuře provozujete.

Zvýšení efektivity bezpečnostních nástrojů

Zajistíme maximální využití Vašich EDR či XDR nástrojů a tím snížíme provozní zátěž IT týmu

Odborný dohled a reakce týmu ACDC

Rychlá identifikace a vyhodnocení bezpečnostních incidentů s okamžitým aktivním zásahem