Aricoma Cyber Defense Center

Managed Detection & Response

Služba Aricoma MDR představuje pokročilou bezpečnostní službu, která kombinuje moderní XDR technologie, automatizovanou detekci hrozeb a reaktivní dohled expertního bezpečnostního týmu.

Aricoma MDR v kostce

24x7 bezpečnostní dohled
Nepřetržité sledování a vyhodnocování bezpečnostních událostí

EDR/XDR Platforma Cynet
Technologická vrstva pro detekci, ochranu, korelaci a reakci, licence součástí služby

Expertní tým Aricoma Cyber Defense Center
Tým poskytující služby SOC, MDR, CSIRT a další specializované bezpečnostní služby

Rychlá eskalace incidentů
Kritické události jsou převzaty, klasifikovány a eskalovány podle závažnosti

Reakční rámec od 30 minut
U kritických incidentů začíná příjem a zahájení nejpozději do 30 minut

Podpora CyOps týmu
Expertní tým výrobce Cynet, který doplňuje náš interní tým o hluboké know-how produktu.

Proč MDR

Útok už dávno nemíří jen na endpoint
Moderní útoky procházejí napříč celým prostředím. Útočník může začít phishingovým e-mailem, pokračovat přes kompromitovaný účet, využít vzdálený přístup, spustit škodlivý skript nebo se pokusit o laterální pohyb v síti

Aktivní obranná vrstva nad vaším prostředím
Platforma Cynet dodává viditelnost a reakční schopnosti, ACDC přidává lidskou expertizu, kontext, eskalaci a podporu při řešení incidentů

Bezpečnostní dohled = lidé, čas a režim 24×7
Vaše interní IT týmy se mohou plně věnovat provozu, podpoře uživatelů a projektům pro rozvoj a tím přinášet užitnou hodnotu pro váš business.

Transparentní náklady bez příplatků
Služba Aricoma MDR nezná dovolenou, nemocenskou, OČR a jiné absence, které jsou u interního týmu vaším nákladem

Dvě úrovně obrany dle Vašich skutečných potřeb

Aricoma MDR Standard

Základní obranná linie s vysokou schopností detekce a reakce

Tato verze je vhodná pro organizace, které chtějí silnou ochranu koncových zařízení, dohled 24×7 a řízenou reakci bez nutnosti budovat vlastní MDR tým.

Hlavní funkce verze Standard:

- Ochranu koncových zařízení (EPP)
- Detekci a reakci na endpointu (EDR)
- Detekci síťových hrozeb (NDR)
- Analýzu chování uživatelů (UBA)
- Deception prvky / návnady pro útočníka
- Automatizovanou reakci (SOAR)
- Dohled a analýzu událostí týmem ACDC
- Eskalaci incidentů

Vhodné pro:

- Firmy bez vlastního SOC
- Organizace s důrazem na endpoint security
- Všechny, kdo požaduje rychlé posílení detekce a reakce

Aricoma MDR All-in-One

Rozšířený obranný perimetr pro komplexní prostředí

Verze určená pro organizace, které potřebují širší bezpečnostní pokrytí napříč endpointy, identitami, e-mailem, cloudem, SaaS službami, mobilními zařízeními a logy.

Hlavní funkce verze All-in-One:

- Vše z verze Standard
- Kontrolu bezpečnostního nastavení endpointů (ESPM)
- Ochranu mobilních zařízení (MTD)
- E-mailovou bezpečnost
- Bezpečnost SaaS a cloudu (SSPM / CSPM)
- Centralizovaný log management (CLM)
- Open XDR korelaci
- Širší korelaci událostí napříč více zdroji
- Komplexnější pohled na bezpečnostní stav

Vhodné pro:

- Komplexní IT prostředí
- Cloudové a SaaS organizace
- Splnění auditních požadavků

MDR od Aricoma Cyber Defense Center není pouze technologie, je to služba aktivní obrany.

Platforma Cynet poskytuje viditelnost, detekci a reakční schopnosti. ACDC tým přidává dohled, expertízu, vyhodnocení a schopnost koordinovat další kroky. Společně vytváříme obrannou vrstvu, která vám pomůže čelit moderním útokům s vyšší jistotou, rychlostí a kontrolou.