



COMGUARD je Value Added Distributor (B2B) se specializací na IT bezpečnost. Působíme v České republice a na Slovensku. Naše komplexní řešení plně odpovídají potřebám velkých firem, včetně datových center, ale i menších a středních podniků. Zaměřujeme se na bezpečnost koncových stanic, ochranu perimetru, ochranu citlivých dat, vyhodnocování potencionálních rizik, kybernetické bezpečnosti v průmyslovém prostředí a dalších oblastí. Navíc poskytujeme expertní služby jako je například penetrační testování a Security Operation Center (SOC).

Jsme hrdými partnery značek jako Trellix, Sophos, Barracuda, Skyhigh Security, Rapid7, Wallix, Honeywell ScadaFence, Gypol, LogRhythm, Ekran, SecurEnvoy, Whalebone a Labyrinth.

COMGUARD pro ochranu operačních technologií nabízí OT Guard, který spojuje několik technologií, které působí synergicky a dokážou pokrýt nejdůležitější oblasti v OT bezpečnosti.



Cyber Insights je systém pro monitorování průmyslových sítí, který poskytuje jejich kompletní viditelnost. Automaticky monitoruje, jaká zařízení se nachází v síti, detekuje hrozby a zranitelnosti. Využívá širokou škálu algoritmů strojového učení a umělé inteligence a díky tomu dokáže detekovat anomálie v síti, které mohou ohrozit dostupnost systémů a jejich bezpečnost.

### Přehled o OT sítích, komunikačních vzorcích, odhalení potencionálních útoků

Úplné pokrytí **monitorování síťového provozu** (bez vzorkování, bez filtrování)

**Monitoruje aktivitu** vzdáleně připojených uživatelů

**Proaktivně upozorňuje na zranitelnosti a rizika v OT síti**

### Nejmenší false positive nálezy

#### Asset Management

#### Žádný zásah do kontinuity výroby

Neintruzivní řešení, lze přidat do stávající fungující sítě

**Risk Reduction** – Pasivně detekuje IoC (Indicators of Compromise) v reálném čase a poskytuje tak včasné informace o náznacích útoku



Barracuda Next Generation Firewall se postará o ochranu proti různým kybernetickým hrozbám, zajistí segmentaci sítě a umožňuje sledovat a analyzovat veškerý síťový provoz v OT síti. Pomocí firewallu můžeme striktně kontrolovat přístup k OT zařízením a systémům.

### Ochrana před externími hrozbami

Barracuda firewall umožňuje monitorování a filtrování veškerého síťového provozu, což pomáhá chránit OT síť před externími hrozbami, jako jsou malware, botnets, phishingové útoky a další.

### Segmentace sítě

Firewall umožňuje segmentaci sítě. Rozdělí síť do logických částí, aby se omezila možnost šíření útoku v případě, že dojde k prolomení bezpečnostních opatření v jedné části sítě.

### Kontrola přístupů

S pomocí Barracuda firewallu lze definovat a uplatňovat přesná pravidla pro přístup k zařízením a systémům v OT síti. Pouze oprávněné osoby nebo zařízení budou mít povolený přístup, což snižuje riziko neoprávněného přístupu.



Wallix PAM4OT je platforma pro správu přístupů a hesel (PAM), která je speciálně přizpůsobena pro operační technologie. Umožňuje organizacím centralizovaně spravovat a řídit přístup k OT zařízením a systémům, což je klíčové pro zajištění bezpečnosti v průmyslovém prostředí. Navíc poskytuje nástroje pro audit všech aktivit a přístupů k OT zařízením.

Umožňuje **centralizovanou správu** privilegovaných účtů a přístupů v organizaci.

### Řízení připojení k externímu přístupu a správa hesel

**Bezproblémová integrace** do infrastruktury zákazníka s dostatečnou flexibilitou, aby se předešlo odporu uživatelů

**Snížení interní pracovní zátěže** díky schvalovacím pracovním postupům

**Bez agentské řešení**

**Podpora průmyslových protokolů**