SIEM jako služba

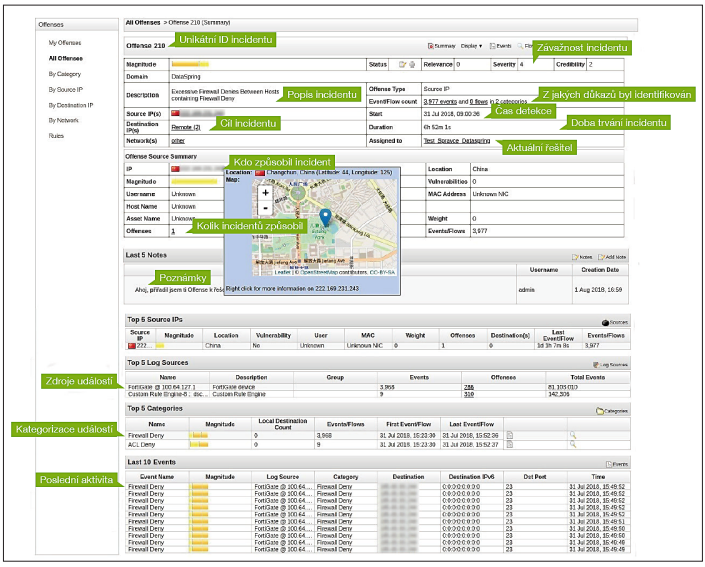
LogDock Advanced

Kategorie:
Bezpečnostní řešení
Iseco.cz, *www.iseco.cz*

Přihlašovatel:
DataSpring, *www.dataspring.cz*
služba vytvořená na softwaru Iseco Security Monitor

Použití produktu: Služba LogDock je cloudové enterprise řešení pro zákazníky, kteří řeší potřebu správy logů, toků a událostí. Nadstavbou nad těmito sesbíranými daty je funkcionalita SIEM (Security Information and Event Management), která zákazníkovi poskytne kompletní pohled na jeho IT infrastrukturu z hlediska bezpečnostních událostí, nalézání vzájemných vztahů, upozorňování na jednotlivé bezpečnostní incidenty a vytváření přehledných reportů. Služba je provozovaná z bezpečného datového centra Tier III v České republice.

Popis produktu: Služba je provozovaná ve virtuálním datovém centru, ve kterém – podle konfigurace služby – zákazník nalezne přidělené kolektory, které se starají o příjem logů a toků jak ze všech zařízení nacházejících se v zákaznickém segmentu v datovém centru, tak i z prostředí zákazníka. Tím se zajistí oddělení od ostatních klientů a logy i toky jsou přístupné pouze tomu, komu patří. Všechny logy se zpracovávají centrálním zařízením, které nad těmito uloženými daty vykonává klasifikaci, agregaci, normalizaci, korelaci a alerting.

Zajímavé vlastnosti produktu:
- Cloudová služba
- Management logů, toků a událostí
- Podpora SIEM
- Alerting
- Forenzní analýza
- Splnění podmínek GDPR, zákona o kybernetické bezpečnosti a ISO 27001
- Dlouhodobé ukládání

Cena (bez DPH): projektově, od 8 400 Kč měsíčně