Extended Detection and Response System

SecureX

Kategorie:
Bezpečnostní řešení
Cisco Systems, *www.cisco.com/*

Přihlašovatel:
Alef Nula, *www.alef.com*
konzultační partner

Použití produktu: Cloudová XDR (eXtended Detection and Response system) platforma pro dohled bezpečnostní infrastruktury a detekci hrozeb. Produkt využijí zejména bezpečnostní analytici pro zefektivnění a automatizaci procesů při detekci a investigaci bezpečnostních incidentů. Další možností je proaktivní prohledávání hrozeb napříč infrastrukturou – threat hunting.

Popis produktu: SecureX je cloudová XDR platforma poskytující dohled nad bezpečnostní infrastrukturou, která je doplněná o funkce pro řešení bezpečnostních incidentů. Spravuje se z unifikovaného dashboardu, do něhož je přes REST API propojena Cisco bezpečnostní infrastruktura s možností připojit produkty třetích stran. Mezi základní funkce patří threat hunting a investigace bezpečnostních incidentů napříč infrastrukturou či automatizace procesů pro detekci a reakci na bezpečnostní incident. Nabízí také prostředí pro dohledový tým ke sběru indikátorů a vytváření incident tiketů.

Zajímavé vlastnosti produktu:
- Cloudová platforma
- Orchestrace – vytváření vlastních workflow, díky kterým je možné automatizovat procesy
- Threat hunting – proaktivní prohledávání hrozeb na základě IOC (Indication of Compromise)
- Možnost instalace plug-inu do webového prohlížeče pro efektivní a rychlé sbírání indikátorů a následné vytváření incidentů
- Propojení s produkty třetích stran
- K dispozici zdarma

Cena (bez DPH): zdarma