OCHRAŇUJTE KRITICKÁ DATA A USMĚRŇUJTE ŘEŠENÍ INCIDENTŮ V RÁMCI SPRÁVY UDÁLOSTÍ S INTEGROVANÝMI BEZPEČNOSTNÍMI INFORMACEMI.

Řešení SIEM poskytuje monitoring systémových změn a uživatelských aktivit v reálném čase, je schopen objevit hrozby a neoprávněné vniknutí, poskytuje správu bezpečnostních událostí a jejich vzájemné propojení, nabízí správu logů a automatizaci odpovědí na incidenty - to vše v rámci jedné, integrované a škálovatelné infrastruktury. Je schopen uspokojit nároky na ty nejnáročnější standardy tím, že automatizuje revize bezpečnostních aktivit, aby byla zajištěna integrita souborových systémů. Provádí také audit změn a správu reakcí na incidenty.

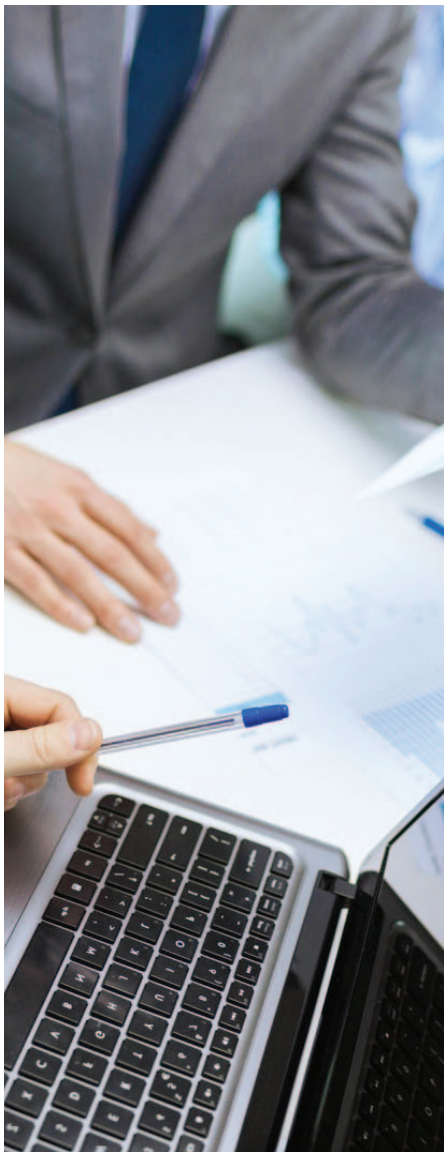
Inovativní řešení

Jaký smysl má centralizované sbírání a ukládání logů? Pro splnění bezpečnostních předpisů a požadavků na dostupnost, jak požaduje např. kybernetický zákon nebo nařízení EU na ochranu osobních údajů, známé pod zkratkou GDPR, investují organizace nadále do velké škály bezpečnostních řešení, jako jsou firewally, antivirové produkty a produkty na detekci průniků. Ty produkují neuvěřitelně vysoké objemy bezpečnostních dat, která představují obrovskou výzvu pro jejich zpracování v reálném čase. Více protokolů z více zařízení je potřeba sjednotit do společné, snadno srozumitelné formy, která může být reprezentovaná grafy, schémata apod. Pravidelné reporty na vyžádání mohou administrátorům značně usnadnit cestu k požadovaným informacím. Přednastavené GUI (Graphical user interface) zobrazuje jen informace, které budou v danou chvíli potřeba. Je jasné, že SIEM řešení nemá potlačovat síťové hrozby samo o sobě, ale pomáhat správcům tyto hrozby včasně identifikovat. Za pomoci korelace dat z více zařízení jsou schopni pracovat s anomáliemi z tisíců zařízení v reálném čase tak, aby mohla být definována vhodná opatření, která zabrání dalším škodám.

Klíčové výhody

Redukuje čas ohrožení - optimalizuje reakční časy, díky monitoringu bezpečnostních incidentů, podrobných hlášení, informačních schopností a automatických odpovědí, to vše v reálném čase.

Zlepšuje povědomí o bezpečnosti - poskytuje komplexní znalostní bázi, která automaticky vytváří aktivní bezpečnostní nástroje a vstřebává nové a aktualizované informace. To vede k získání znalosti potřebné k vyřešení problému v aktuálním okamžiku.



Zvyšuje úroveň zabezpečení - integruje a slaďuje archivovaná i ”živá“ (data v reálném čase) data ze všech bezpečnostních procesů a systémů. Sleduje incidenty, aby bylo zřejmé, zda byly zpracovány správně a včas. Tím vám dává možnost dosáhnout skutečně účinné správy životních cyklů bezpečnostních incidentů, abyste měli zajištěnou optimální ochranu.

Zvyšuje operační výkon - zvyšuje návratnost investice pomocí konsolidace bezpečnostních informací z celé organizace do centrálního místa, přičemž filtruje falešné a rušivé skutečnosti a předkládá k vyhodnocení skutečné incidenty. To zajišťuje možnost provádět soustředěný monitoring a dává k dispozici rozšířenou schopnost reakce.

Zajišťuje kompatibilitu - napomáhá pravidelným revizím a přezkoumání bezpečnostních informací z celé organizace, monitoruje bezpečnostní mechanismy k zhodnocení jejich efektivity a poskytuje nástroj na vynucování politik a ”best practices“ v reálném čase. Což napomáhá uspokojit bezpečnostní požadavky současné doby.

Pomáhá naplnit některé z konkrétních požadavků GDPR na zavedení odpo-vídajících technických a organizačních opatření na ochranu OÚ, jako je:

- schopnost obnovit dostupnost OÚ a přístup k nim včas v případě fyzických či technických incidentů
- zohlednění rizik zpracování OÚ, jako např. neoprávněný přístup k OÚ
- prokazatelnost, tj. schopnost správce doložit, že zpracování je prováděno v souladu s GDPR
- vedení záznamů o činnostech zpracování OÚ
- ohlašování případů porušení zabezpečení OÚ atd.