FortiSIEM®

Zlúčenie korelácie udalostí a manažmentu rizika pre moderné siete

» Dnes už aj na Slovensku začínajú spoločnosti vnímať potrebu zvýšenia bezpečnosti v ich podnikovej IT infraštruktúre. Takisto aj výrobcovia sa prispôsobujú trendom ochrany naprieč celému modelu ISO/OSI. Okrem špecializovaných zariadení, ako sú IPS/IDS, vznikajú zariadenia, ktoré zahŕňajú celú škálu bezpečnostných funkcionalít, ako napr. aplikačný firewall, integrované IPS, antispamové riešenie a mnoho ďalších funkcionalít.

Čo je SIEM – FortiSIEM

Každé zariadenie produkuje určité množstvo informačných správ – logov na diagnostiku problému, ktoré sa ukladajú lokálne na zariadenie alebo ich možno posielať na externú entitu. Týchto správ môže byť z jednotlivých zariadení od 10 do 1000 za minútu. Prehľadávanie a prehľadnosť týchto správ alebo udalostí môže byť v momente prebiehajúceho útoku dôležitá.

FortiSIEM je práve ten správny nástroj na prijímanie a ukladanie takýchto logov alebo udalostí. Umožňuje s týmito informáciami ďalej pracovať, správne ich čítať, rozkúskovať, priraďovať ich do skupín pomocou pravidiel a vyhodnocovať. Dať tomu celému správnu logiku. Následne na základe pravidiel a nastavení vyhodnotiť bezpečnostný incident a informovať zainteresovaných.

Implementácia systému FortiSIEM

Pred implementáciou je dôležité usporiadať si jednotlivé faktory, pretože pokiaľ vykonáte iba inštaláciu, môžete mať len veľmi drahý logovací nástroj. Preto je dôležité už v prvom kroku nastaviť hodnotenie aktív a počet udalostí, ktoré pri bežnom pohľade nemusia mať s IT nijaký súvis, ale pri priblížení ukážu, ako všetky tieto veci s ním súvisia. Hodnotenie aktív je významné z hľadiska prehľadnosti a určenia dôležitosti, ktoré zariadenia a takisto ich rozhrania a ktoré aplikácie a procesy budú mať aké hodnoty dôležitosti, následne treba zistiť celkový súčet počtu udalostí, ktoré sa budú posielať na nástroj FortiSIEM.

Posledný bod pred zadovážením a implementáciou FortiSIEM je určiť, či celý systém bude distribuovaný alebo pôjde len o centralizovaný počet a typ konektorov, ktoré daný nástroj SIEM podporuje. Následne možno pristúpiť k implementácii. Implementácia sa uskutočňuje viacerými spôsobmi. FortiSIEM má možnosť dynamického skenovania aktív pomocou vopred pripravených konektorov a prihlasovacích údajov. Aktíva, ktoré nebudú naskenované alebo nemajú možnosť byť naskenované štandardným spôsobom, by sa mali dať pridať manuálne.

Len čo sú všetky aktíva pripojené a monitorované, treba určiť, či už na strane zdroja informácií (logov), alebo na FortiSIEM, čo všetko je relevantná informácia a čo nie je. Posledný a hlavne nikdy nekončiaci úkon je analýza a písanie pravidiel, za pomoci ktorých nás bude FortiSIEM informovať o potenciálnych bezpečnostných incidentoch. Tieto úkony treba vykonávať pri každom incidente a pri každom pridanom aktíve. Preto sa proces bezpečnosti nikdy nekončí.

Fortinet je líder na globálnom trhu sieťovej bezpečnosti. Veracomp je výhradný distribútor technológie Fortinet už viac ako deväť rokov. Okrem technológií z oblasti bezpečnosti IT, Veracomp Slovakia s.r.o. zastrešuje aj ďalšie okruhy, ako sú siete a infraštruktúra, dátové centrá, mobilita a komunikácie a open source softvér..

FORTINET®

veracomp

we inspire IT

Jaroslav Remeň je zakladateľ spoločnosti ReFoMa, s.r.o., študoval na Pedagogickej fakulte Trnavskej univerzity v Trnave, neskôr pôsobil ako pedagóg, po čase sa priklonil k sfére IT a začal pracovať v súkromných spoločnostiach ako správca siete. Svoju kariéru rozvíjal na pozícii senior security inžiniera v spoločnostiach ako Hewlett-Packard Company alebo Siemens. Dnes je konateľom spoločnosti ReFoMa, s.r.o., ktorá pôsobí v oblasti bezpečnosti počítačových sietí a systémovej integrácie už od roku 2008.