SIEM
Security Information and Event Managment

Trustwave®
Security begins with Trust℠

Trustwave SIEM

V každé organizaci jsou denně generovány tisíce, někdy i miliony, log záznamů z různých typů zařízení. Tyto log záznamy obsahují klíčové informace o provozní kondici veškerých komponent informačního systému a také informace o vykonaných aktivitách všech uživatelů. Pro mnoho organizací se stává, vzhledem k objemu a rozmanitosti generovaných dat, stále větší výzvou udržovat kontrolu nad těmito informacemi, především z důvodů preventivní, detekční a korekční schopnosti. Proto Trustwave přichází s řešením, které dovoluje realizovat sběr logů, řídit a vyhodnocovat nejrůznější události (tzv. event management), a to z více zařízení různých typů.

Trustwave SIEM appliance

Představuje hardwarovou variantu SIEM řešení, která umožňuje organizacím spravovat různé typy logů sesbírané z různých zařízení a interpretovat je uživateli ve srozumitelné podobě. SIEM appliance optimalizuje investice do jiných bezpečnostních produktů a do lidských zdrojů.

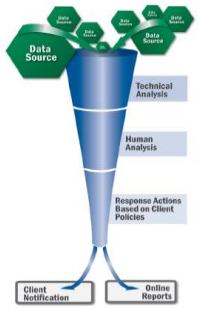
Modelová řada	LC	LMO/LME2	LMO/LME3	LMO/LME4	LMO/LME5
CPU	Quad Core Xeon 2.53 GHz	Quad Core 2.83 GHz	Hexa Core Xeon 2.66 GHz	Dual Hexa Core Xeon 2.66 GHz	Dual Hexa Core Xeon 2.66 GHz
RAM	8 GB	12 GB	16 GB	24 GB	48 GB
Disk	1T / RAID 5	2T / RAID 5	4T / RAID 5	6T / RAID 5	12T / RAID 5
Velikost racku	1U	1U	1U	1U	1U

Efektivní a jednoduché řešení

⇒ Nasazení celého řešení je velice jednoduché díky applianci typu „Plug and Play". Po zapojení zařízení a nastavení základních funkcí přes intuitivní rozhraní, SIEM appliance již automaticky monitoruje, sbírá a uchovává logy, čímž se výrazně snižují náklady na management. Získané informace jsou vyhodnoceny a zobrazeny uživateli ve srozumitelné podobě.

⇒ Efektivita celého řešení spočívá v tom, že záznamy jsou sbírány na jednotlivých síťových segmentech, kde jsou „zabaleny", zašifrovány a zaslány na další SIEM řešení, kde dochází k jejich zpracování.

⇒ Veškerá komunikace je potvrzována tak, aby nedošlo k vymazání dat, která nebyla druhou stranou přijata nebo byla přijata poškozená. Díky využití této architektury lze získat přehled o vysoce distribuovaných sítích, kde by byl jinak sběr dat komplikovaný.



Trustwave Real-time Analysis

SIEM Operations Edition

Toto řešení představuje škálovatelné a snadno nasaditelné softwarové SIEM řešení. Velkou výhodou celého řešení je automatický převod log záznamů do jednotné taxonomizované podoby (nezávislé na typu vstupního zařízení), při které ohodnotí událost dle jejich závažnosti (priority). Pro správce a analytiky je potom jednoduché dohledat, co se v jejich infrastruktuře děje a na vzniklé události rychle a efektivně reagovat.

Stálá shoda se standardy

⇒ SIEM OE automaticky koreluje události z různých zařízení a na základě výsledků přiděluje událostem skóre pro jednodušší orientaci správců/analytiků. Samozřejmostí je možnost automatické notifikace při překročení určité meze bezpečnosti.

⇒ Součástí SIEM OE je sada reportů, které lze využít pro audit. Tyto reporty lze kombinovat s vlastními, vytvořenými reporty pomocí „report wizardu".

⇒ Velká část procesů je automatizovaná, což zvyšuje efektivitu práce pověřených zaměstnanců.

⇒ Splňuje nejnáročnější požadavky compliance v ČR.

Managed SIEM

Monitorování a sběr systémových dat se může zdát jako jednoduchá věc. Ale po nasazení řešení a při snaze o splňování standardů, může být uživatel překvapen náročností celé správy. Často se měnící standardy a požadavky na správu řešení se mohou stát pro laika poměrně složitými a časově náročnými úkoly. Trustwave proto přichází s řešením, které Vám formou služby zajistí sběr, analýzu logů a správu rizik.

Varianty řešení	Self-Service	Daily Analysis	Real-Time Analysis
Real-time alerting a analýzy			Ano
Denní bilance a analýzy		Ano	Ano
24x7 Telephon support		Ano	Ano
24x7 Email/IM support	Ano	Ano	Ano
Automatické aletry	Ano	Ano	Ano
Vlastní aletry		Ano	Ano
Online reporting portal	Ano	Ano	Ano
Denní a měsíční reporty	Ano	Ano	Ano
Roční offline archiv	Ano	Ano	Ano
PCI Logging Guides	Ano	Ano	Ano

COMGUARD
security & networking

COMGUARD s.r.o.
Sochorova 38, CZ 616 00 Brno
tel. +420 513 035 400
info@comguard.cz | www.comguard.cz

WAF
Web Application Firewall

Trustwave®
Security begins with Trust℠

WebDefend

WebDefend od společnosti Trustwave je robustní webový aplikační firewall (WAF), který poskytuje webovým aplikacím v reálném čase neustálou ochranu před útoky a krádežemi dat. Zajišťuje jejich bezproblémový chod a pomáhá upevnit shodu s oborovými standardy, jako je např. PCI (Payment Card Industry) DSS (Data Security Standard). Využitím obousměrné analýzy provozu, automatizované profilace chování a vícenásobných detekčních mechanismů identifikuje WebDefend také události mající potenciální vliv na bezpečnost, funkci a dostupnost webové aplikace.

Klíčové přínosy:

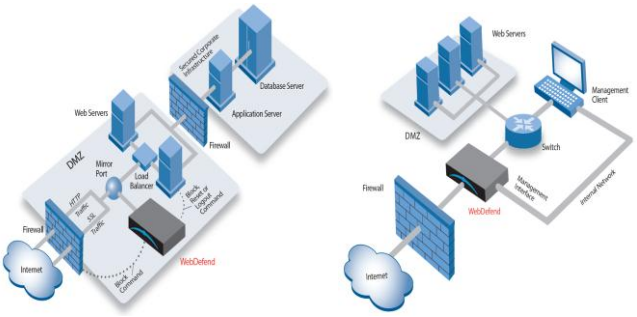
- ⇒ Poskytuje bezkonkurenční ochranu citlivých a důvěrných dat.
- ⇒ Možnost nasazení virtuální appliance do prostředí VMware.
- ⇒ Flexibilní nasazení: IN-LINE / **OUT- OF-LINE.**
- ⇒ Umožňuje organizacím identifikovat aplikační události, které ohrožují zisk, snižují důvěru zákazníků a v neposlední řadě představují riziko pro datová aktiva.
- ⇒ replikuje a dešifruje SSL streamy bez terminace původních šifrovaných spojení.
- ⇒ Výrazně napomáhá udržovat shodu s oborovým standardem PCI DSS.

Trustwave je celosvětovým lídrem v oblasti ochrany webových aplikací.

Nejlepší dostupná detekce a prevence útoků

WebDefend poskytuje bezkonkurenčně nejlepší detekci a ochranu proti zranitelnostem a nebezpečným útokům, jako je např. „site scraping", „malicious bots", „Google™ hacking", útokům v čase nule a cíleným útokům. Pro dosažení komplexní a přesné ochrany analyzuje WebDefend příchozí i odchozí provoz z webové aplikace, přičemž koreluje data z různých detekčních systémů, např.:

- ⇒ Adaptivní aplikační profilovací systém kontinuálně buduje dynamický bezpečnostní model každé chráněné webové aplikace, který zaručuje, že pouze validní provoz je povolen.
- ⇒ Systém „ExitControl" analyzuje odchozí provoz z hlediska potenciálního úniku citlivých dat, maskování dat a získávání informací pro řízení bezpečnosti.
- ⇒ Signatury vyvinuté laboratořemi Trustwave poskytují bezkonkurenčně nejaktuálnější zdroj aplikačních signatur a informací o známých zranitelnostech webových aplikací.



Robustní provedení – snadná instalace

WebDefend je vyvinut pro velké organizace. Jeho architektura umožňuje řídit a chránit více data center najednou. Kterýkoli senzor je možné zapojit v páru pro zajištění vysoké dostupnosti. K dispozici je také centrální správa „WebDefend Manager". **Pro zajištění neintruzivního nasazení v celé distribuované architektuře, může být instalován „out-of-line"** nebo transparentně „in-line", bez potřeby jakéhokoli přenastavení sítě – viz následující obrázky.

Out-of-the-Box shoda se standardem PCI

WebDefend obsahuje přednastavené „PCI" politiky a reporty pro organizace, které chtějí vyhovět požadavkům standardu PCI DSS. Tyto politiky zaručují správnou konfiguraci pro prevenci útoků a logování v souvislosti s užíváním systémů pro platební katy. Specifické reporty poskytují okamžitý přehled o shodě a používání citlivých dat pro auditní účely.

Okamžitá detekce bezpečnostních událostí

WebDefend provádí kontinuální vyhodnocování každé chráněné aplikace tak, aby identifikoval události, které mohou ovlivnit bezpečnost aplikace, její funkčnost a dostupnost. Události zahrnují programátorské chyby, selhání aplikace a nebezpečné kódování. Když je taková událost zjištěna, WebDefend zajistí všechny požadavky a reakce stejně jako náhled události skrz prohlížeč tak, aby mohl být problém jednoduše pochopen a rychle vyřešen.

Modelová řada WebDefend	TX30i System	TX60i System	TX110i System	TX120i System
CPU	1 x Quad Core 2.4 GHz	1 x Quad Core 2.0 GHz	2 x Quad Core 2.0 GHz	2 x Quad Core 2.4 GHz
Síť	Silicon Dual Port Copper Bypass	Silicon Dual Port Copper Bypass	Silicon Quad Port Copper Bypass	Silicon Quad Port Copper Bypass
Počet transakcí / sec	7000	9000	13000	20000
Max počet webových stránek (unikátní IP & Port combo)	30	60	200	200
Propustnost (všechny prvky aktivní)	50Mb/s (40% SSL)	100Mb/s (50% SSL)	600Mb/s (50% SSL)	1000+Mb/s (50% SSL)
Možnosti nasazení	In-line / Out-of-Line	In-line / Out-of-Line	In-line / Out-of-Line	In-line / Out-of-Line

COMGUARD
security & networking

COMGUARD s.r.o.
Sochorova 38, CZ 616 00 Brno
tel. +420 513 035 400
info@comguard.cz | www.comguard.cz