

Rozvoj SIEM systému v organizaci

*e*FOCUS



Rozvoj SIEM systému v organizaci

*e*FOCUS



Svoboda Jan, AEC spol. s.r.o.

Proč chceme či potřebujeme rozvoj

- Protože původní implementace se věnovala zajištění monitoringu v oblasti infrastruktury
- Protože regulativní požadavky na monitoring jsou přesnější
- Protože organizace prodělala v minulosti bezpečnostní incident
- Potřeba posunout bezpečnost a povědomí o jejím stavu dále

Rozvoj SIEM systému



Cíle



- Obecné požadavky na monitorování
- Změny nad uživatelskými účty
- Monitorování akcí uživatelů s administrátorským oprávněním
- Operace s citlivými daty
 - Zákaznická data
 - Firemní tajemství
 - a další.

Cíle

- Obecné požadavky na výstupy
- Reporty
 - Změny nad uživatelskými účty
 - Akce uživatelů s administrátorským oprávněním (počty a typy událostí)
 - Operace s citlivými daty
 - Počty a typy alertů
 - Proces nakládání s výstupy a proces nápravy – nutná definice zodpovědností
- Alerty
 - Neřízené změny ve sledovaném systému (bez změnového požadavku, z nesprávných segmentů infrastruktury...)
 - Vytvoření a smazání administrátorských účtů
 - Nestandardní operace s citlivými daty (nadměrné využití, z nesprávných segmentů infrastruktury, v nestandardních pracovních hodinách)
 - Proces nakládání s výstupy a proces nápravy – nutná definice zodpovědností

Výběr zdrojů



- Core aplikace
- Aplikace/slужby obsahující citlivá data

Analýza

- Obecné a technické informace

- Jaké typy systémů (OS, DB, App)
- Umístění citlivých
- Vlastník aplikace

- Aktuální logování

- Existence a typ akt
- Ukázky logů s přihl
- Porovnání požadav
- Sumarizace požada
- výstupů (včetně m
- Návrhy finálního sc

Analýza se provádí pro každou vybranou aplikaci, tak aby došlo k jejímu preciznímu popsání

	A	B	C	D
1	Vlastník služby			
2	Dpovedný administrátor			
3				
4	Výrobce			
5				
6	Dodavatel			
7				
8	Functional Description:			
9				
10	Standard CRM systém			
11				
12		Oracle DB		
13	List of component (SW +OS)	Windows 2008 SP2 64		
14	IP address			
15	System location			
16	access to application			
17				
18	obsahuje user db?	Yes		
19	obsahuje sensitive data?	No		
20	kde jsou uložena sensitive data?	NT system		
21	Vytváří vlastní log?			
22	Typu logu (syslog,file,DB,event_log)?			
23		User login/logout?		
24		Creation/deletion user acc?		
25		Change user rights (roles, access to...)		
26		Change user params (passwd, lockouts)		
27	typy událostí	Search sensitive data		

Revize požadavků

- Porovnání rizik oproti nákladům na případné změny v logování
 - Přihlédnutí k doporučení z analytické části
- Revize naplnění všech požadovaných parametrů
 - Definované v úvodní fázi definice cílů
- Odsouhlasení implementace ve schváleném rozsahu
- Definice finálních termínů

Realizace

- Realizace změn na úrovni aplikací
 - Definovaných v analytické části
- Zajištění transportu událostí do SIEM systému
 - Způsobem definovaným v analytické části
- Zajištění parsování/normalizace, ukládání a zálohování událostí
- Definice výstupů
 - Definovaných v analytické části
 - Testování výstupů

Rozvoj SIEM systému



Problémy

- Součinnost
 - Na projektu spolupracuje mnoho složek IT včetně dodavatelů
 - Je tedy nutné definovat procesy eskalace a pravidelné kontroly
- Zodpovědnost
 - V rámci projektu je nutné provést určitá rozhodnutí o financích
 - alokaci lidských zdrojů
 - případné akceptaci rizik
- Roční období
 - Léto a dovolené (podobně vánoce a nový rok)

Přínosy

- Zvýšení bezpečnosti a povědomí o bezpečnosti
- Naplnění auditních požadavků
- Definice požadavků a parametrů pro nové aplikace

Ďakujeme za pozornost

AEC

DATA SECURITY

eFOCUS