ELISA SECURITY MANAGER

DATA SYS

UPOZORNĚNÍ NA CHYBY APLIKACÍ NEBO SYSTÉMŮ

SOFISTIKOVANÉ VYHODNOCOVÁNÍ KORELACEMI
- Detekce bezpečnostních incidentů
- Potlačení falešných alarmů a notifikací

KONKRÉTNÍ JEDNOTLIVÉ CHYBY
- Pružněji než běžný provozní monitoring (Nagios, Zabbix, ...)

SROZUMITELNOST
- Překlad chybových kódů
- Překlad IP adres na DNS jména

BEZPEČNOSTNÍ MONITORING

CENTRÁLNÍ KONZOLE ALARMŮ
- Antivirový systém
- Systém prevence průniku (IPS)
- Systém prevence ztráty dat (DLP)

ANALÝZA DOPADŮ
- Komu byla doručena infikovaná příloha e-mailu?
- Jaké stanice vykazují příznaky virové nákazy?
- Které uživatelské účty byly při útoku kompromitovány?

PROVOZNÍ MONITORING

INTEGROVANÝ SYSTÉM ZABBIX
- Grafické znázornění dostupnosti a zatížení sítě
- Plně automatizovaný monitoring VMware infrastruktury
- End-user monitoring webových aplikací
- Vyhodnocování plnění SLA dodavateli

ANALÝZA PROVOZU V SÍTI

WEBOVÁ PROXY
- Nejvíce navštěvované weby
- Největší stahovači dat

WEBOVÝ SERVER
- Z jakých měst lidé přistupují?
- Detekce nefunkčních odkazů na firemním webu

FIREWALL, ROUTER
- Detekce skenování portů útočníkem
- Detekce DoS a DDoS útoků

INTERNÍ PŘEPÍNAČ
- Jaké aplikace nejvíce zatěžují síť
- Která zařízení generují nejvíc provozu v síti?
- Kontrola řízení přístupu zařízení k síti dle 802.1x

AUDITOVÁNÍ ZMĚN A ČINNOSTÍ

DATABÁZE
- Kdo změnil číslo bankovního účtu?
- Kdo si prohlíží osobní údaje zaměstnanců?

DOKUMENTY A SOUBOROVÉ SYSTÉMY
- Kdo smazal nabídkové dokumenty?
- Kdo si kopíruje neobvyklé množství výkresů?

ZMĚNY KONFIGURACE
- Síťových prvků a bezpečnostních zařízení
- Adresářových služeb a operačních systémů
- Aplikací a databází

SOULAD S NORMAMI
- ČSN ISO 27001
- Zákon o kybernetické bezpečnosti
- PCI, SOX a další