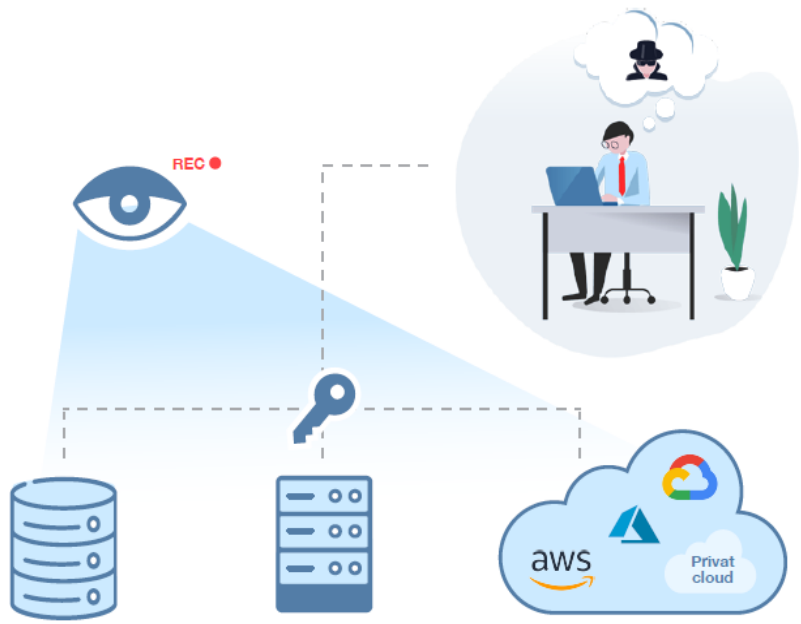
INSIDER THREAT MANAGEMENT – Cesta k bezpečnému IT

Pojem „Insider Threat" již nelze označit jako novinku na poli IT bezpečnosti, jedná se o zažitý výraz pro nebezpečí a hrozby způsobené externími či kmenovými zaměstnanci organizace. Celosvětově stojí Insider Threats až za 34% incidentů úniku dat (zdroj: Verizon report 2019). Vzhledem k těmto alarmujícím statistikám se řešení Insider Threat Management stalo nepostradatelným nástrojem pro moderní organizace, které kladou důraz na zabezpečení svých aktiv.

Řešení Insider Threat Management

Společnost Ekran System nabízí ucelené řešení pro správu tzv. vnitřních hrozeb. Jedná se kombinaci nástrojů pro audit a monitorování uživatelů doplněnou o správu privilegovaných uživatelských účtů a jejich hesel. Nástavbou těchto klíčových funkcionalit jsou nástroje pro aktivní vyšetřování bezpečnostních incidentů poskytující možnost reagovat na aktuálně probíhající bezpečnostní hrozby, nebo také UEBA modul (User and Entity Behavior Analytics) založený na algoritmech umělé inteligence.



Nahrávání uživatelských relací

Technologie Ekran umožňuje zaznamenávat všechny druhy uživatelských relací na koncových bodech, a to ve snadno interpretovatelném a srozumitelném formátu. Zaznamenávány jsou relace autorizované, kompromitované, nebo dokonce i tzv. **Backdoor relace** – nezáleží ani na výši nebo typu oprávnění, vždy je pořízena úplná nahrávka veškeré uživatelské aktivity a jejího kontextu.

Kvalitu videozáznamu lze nastavit jednotlivě i skupinově, navíc je možné sledovat dění na koncových bodech v reálném čase pomocí optimalizovaného videopřehrávače. V záznamech se lze jednoduše orientovat pomocí filtrování dle IP adresy, nebo například uživatelského jména.

Sběr logů a vyhledávání

Kromě nahrávání videozáznamu sbírá Ekran velké množství logů spojené s uživatelskou aktivitou, které jsou využity pro indexování. Díky tomu lze přímo ve videozáznamu vyhledávat například jména spuštěných aplikací, URL adresy, vložené příkazy, nebo dokonce i psaný text. Metadata usnadňují analýzu relace, neboli monitoringu uživatelské aktivity, alertingu, reportingu a vyhledávání.

Klíčové přínosy technologie

- ✓ **Navýšení efektivity** zaměstnanců
- ✓ **Vyhodnocování rizikovosti** uživatelů
- ✓ Cenný zdroj logů pro **SIEM**
- ✓ Určení **hmotné zodpovědnosti** administrátorů
- ✓ Integrace s **ticketovacím systémem**
- ✓ **Správa připojovaných USB** ze strany administrátorů
- ✓ Pokročilý **alerting a reporting**
- ✓ Možnost integrace **vícefaktorové autentizace**

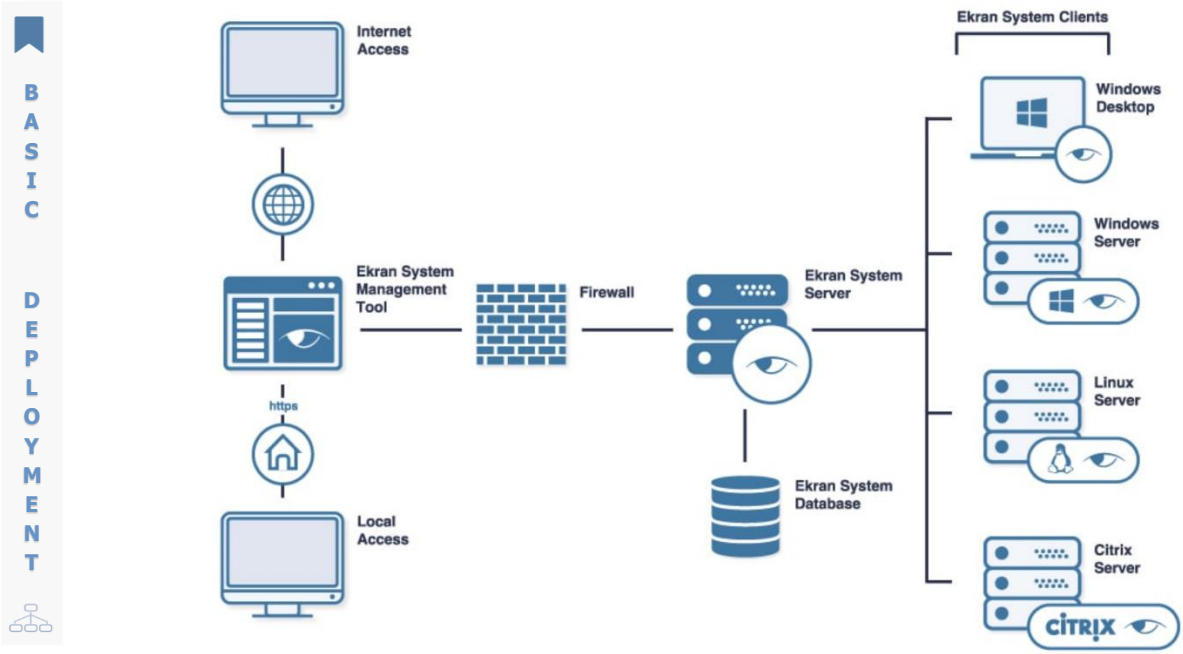
COMGUARD security & networking

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

EKRAN

Analýza uživatelského chování

Insider Threat Platform společnosti Ekran obsahuje sofistikovaný systém pro zasílání alertů, který lze velmi detailně konfigurovat dle potřeb konkrétního prostředí. Pravidla lze upravit buď na základě generických ukazatelů potenciálního nekalého chování uživatele, nebo využitím modulu UEBA, který využívá algoritmů umělé inteligence díky čemuž dokáže vyhodnotit anomálie nastalé v běžné rutině konkrétního uživatele.



Automatizované reakce na bezpečnostní incidenty

Pomocí technologie Ekran lze také nastavit automatizované reakce na bezpečnostní incidenty. Tím se výrazně sníží čas vyhrazený pro realizaci nekalých úmyslů, čímž lze předejít hmotné škodě. Příklady automatizovaných reakcí:

- Blokace uživatele, které spustil bezpečnostní alert (odhlášení ze všech jeho současných relací a nastavení restrikcí na další možnosti přihlášení)
- Blokace připojeného USB zařízení neodpovídajícího korporátní politice
- Ukončení škodlivé aplikace nebo procesu

Správa privilegovaných přístupů

Díky technologii Ekran získají administrátoři nástroje pro tzv. Privileged Access Management (PAM). Pomocí těchto nástrojů lze definovat konkrétní politiky pro privilegované uživatele – například schvalovat přístupy na servery (třeba i jen na předem definovaný časový interval), poskytovat dočasné přístupové údaje nebo řídit přístupy do AD. Pomocí modulu Password Management jsou spravována hesla privilegovaných účtů a to pomocí šifrovaného virtuální trezoru jehož zabezpečení odpovídá armádním standardům

SEOUL NATIONAL UNIVERSITY · Česká pošta · Deloitte. · SAMSUNG · CBCG Central Bank of Montenegro · tvn · UPS

Podporované platformy a nasazení

Ekran umožňuje monitorovat širokou paletu zařízení: Windows, Linux, macOS, UNIX, X Window System, Citrix nebo také VMware. Díky různým druhům agentů přizpůsobeným konkrétnímu typu koncového zařízení je dosaženo maximální viditelnosti a kontroly. Ekran tedy nabízí řadu možností nasazení, a to od základního až po multi-tenantní architekturu. Jednoduché nasazení a výhodné licencování poskytuje skvělý poměr investovaných prostředků k navýšení celkové bezpečnosti organizace a to ve velmi krátkém čase.

COMGUARD security & networking

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