SODAT Protection & Analytics

SODAT Protection & Analytics je silný softwarový nástroj pro detekci bezpečnostních incidentů a prevenci ztráty informací. Je postaven na využití behaviorální analýzy a strojového učení. Průběžně analyzuje sesbíraná data o chování uživatelů na koncových stanicích. Primárně je určen pro detekci potenciálních hrozeb, a nalezená fakta o činnosti uživatelů dokáže přehledně vizualizovat.

Hlavní přínosy

1. Zaznamenání bezpečnostních incidentů
2. Rychlé detekce a efektivní opatření
3. Snížení negativních dopadů a finančních ztrát
4. Detailní podklady pro efektivní řešení incidentů

Klíčové vlastnosti

☐ Analýza pohybu dat

přináší přehled o tom, kdo a jak s vašimi citlivými daty pracuje. Můžeme tak odhalit potenciálně nebezpečné aktivity.

☐ Pokročilá UEBA

aneb „User and Entity Behavior Analytics“ průběžně sleduje chování uživatelů a porovnává je vůči uživateli samotnému nebo celé skupině.

☐ Snadná implementace

s minimem nastavení je jednou z hlavních výhod našeho produktu. Ušetříte tak hodiny strávené nastavováním, kontrolou a rekonfiguracemi.

☐ Detekce anomálií

automaticky upozorňuje na nestandardní chování díky strojovému učení. Díky tomu tak můžete na potenciální hrozby reagovat skutečně rychle.

☐ Definice citlivých oblastí

vám dá možnost určit místa, kde se nacházejí vaše citlivá data a to na úrovni sdílených úložišť a URL adres. Víte tak, kdo k datům přistupuje a kdo je odesílá.

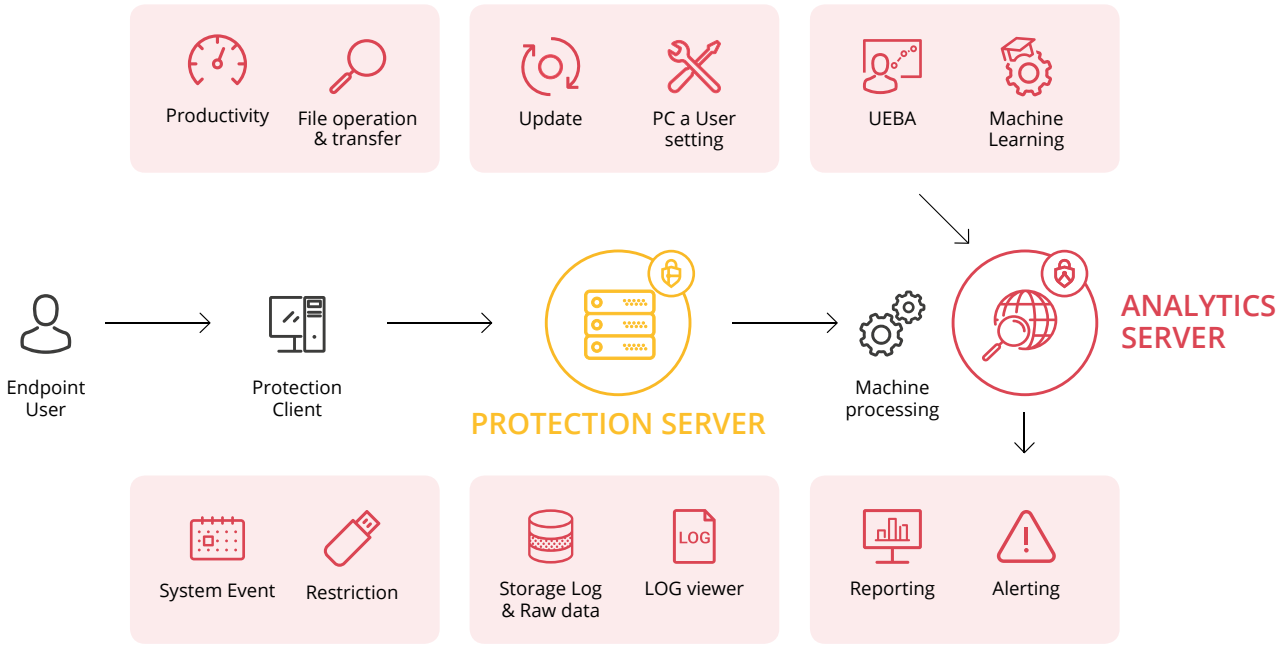
☐ Alertový systém

shromažďuje veškeré nalezené incidenty na jednom místě včetně jejich automatické prioritizace. Incidenty tak vidíte pěkně pohromadě.

SODAT

Jak SODAT Protection & Analytics funguje?

Řešení je postavené na architektuře klient-server, a to včetně centrální správy a pokročilé analytiky.



Veškeré uživatelské aktivity jsou logovány a přenášeny na Protection Server v desetiminutových intervalech (near-time). V centrální správě Protection Serveru jsou veškeré potřebné nástroje pro aktualizaci a distribuci klientů, správu monitorovacích a restriktivních politik, provozní stavy systému a další.

Tato data jsou opět v near-time režimu předávána do Analytics serveru, kde dochází k analýze uživatelského chování, pohybu citlivých souborů atd. Nad veškerými výstupy je postavena Správa upozornění (Alertový systém), která na jednom místě shromažďuje a prioritizuje vzniklé incidenty dle jejich závažnosti.

Vyzkoušejte SODAT Protection & Analytics zdarma

www.sodat.com/online-demo

SODAT

+420 543 236 177
sales@sodat.com

www.sodat.com