
VARONIS
DATALERT SUITE

VARONIS DATALERT SUITE

Odhalte podezřelou činnost ve svém souborovém a e-mailovém systému a nechte se na ni upozornit.

DATALERT:

- Sleduje důležitá aktiva a odhaluje v nich podezřelé aktivity a neobvyklé chování
- Umožňuje meziplatformové monitorování v systémech Windows, UNIX/Linux, NAS, Active Directory, SharePoint a Exchange
- Umožňuje spouštět upozornění napříč různými platformami, a pomáhá tak odhalovat potenciální narušení bezpečnosti, chyby v konfiguraci a další problémy
- Odhaluje kritické události a napadená aktiva
- Zkracuje dobu potřebnou k odhalení a posouzení skutečného problému

DATALERT ANALYTICS:

- Automatizuje odhalování hrozeb pomocí jejich prediktivního modelování založeného na pokročilé analýze, chování uživatelů a strojovém učení
- Umožňuje profilovat uživatelské role a účty služeb a stanovit základní úroveň toho, jak využívají souborové a e-mailové systémy a systém Active Directory
- Poskytne vám užitečné informace o vzorcích chování uživatelů a dat, bezpečnostních rizicích a o sociálních vazbách
- Chrání před hrozbami zevnitř, vyděračským softwarem a potenciálními úniky dat

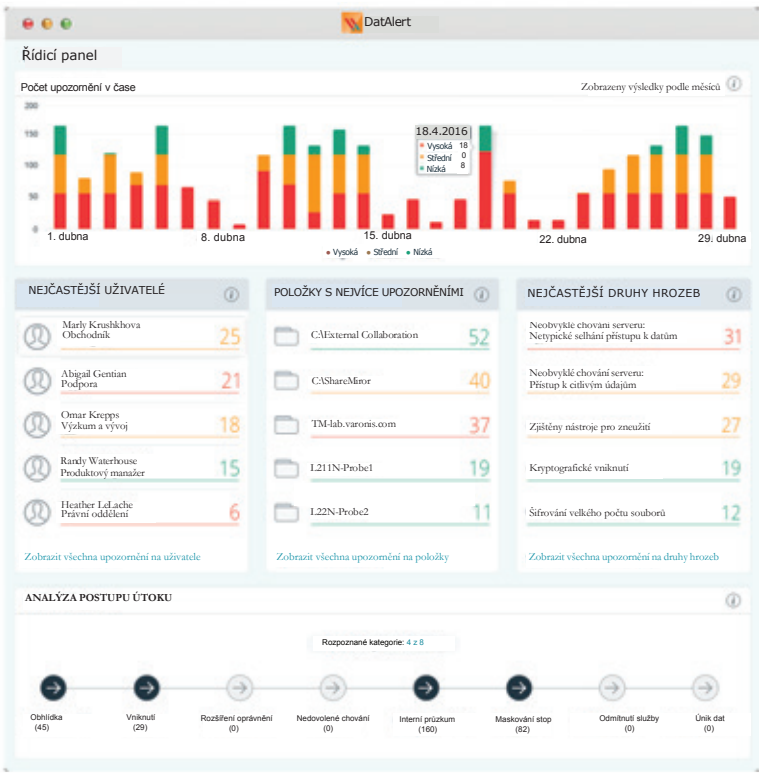
VIZUALIZUJE, INTERPRETUJE A ANALYZUJE DATA:

- Pomocí webových řídicích panelů aplikace DatAlert můžete přijímat, třídit a analyzovat upozornění, určovat jejich priority a zjištěné problémy řešit
- Podmínky pro upozornění a výstupy lze nastavit tak, jak potřebujete
- Můžete spouštět vlastní akce prováděné z příkazové řádky
- Umožňuje snadnou integraci se SIEM a s řešeními pro správu sítě

LABORATOŘ VÝZKUMU CHOVÁNÍ VARONIS:

- Vyhrazený tým expertů na bezpečnost a data ze společnosti Varonis průběžně zavádí nové behaviorální modely hrozeb
- Udržujte si přehled o nejnovějších bezpečnostních hrozbách, vážných trvalých hrozbách a hrozbách zevnitř i o tom, jak se proti nim bránit

FREEDIVISION
for safety reasons



MONITORUJE, ANALYZUJE A ODHALUJE

- Software umožňující vydírání
- Neobvyklou aktivitu týkající se souborů
- Neobvyklou aktivitu týkající se poštovních schránek a e-mailů
- Přístup k citlivým datům
- Pokusy o neoprávněný přístup
- Neobvyklou šifrovací aktivitu
- Kumulativně analyzuje nevy-užívaná a citlivá data
- Neobvyklé přístupy k systémovým souborům
- Neoprávněné přístupy k souborům
- Maskovaná vniknutí
- Chyby v konfiguraci
- Vniknutí do systému
- Nepovolená rozšíření oprávnění
- Hromadná mazání
- Neobvyklá uzamčení
- Pokusy o poškození a zničení provozních souborů
- Škodlivé nástroje
- Změny členství
- Změny kriticky důležitých souborů a jednotek
- Změny kriticky důležitých objektů skupinových zásad
- Podezřelé přístupy
- Změny oprávnění
- Útoky hrubou silou
- Pokusy o úniky dat