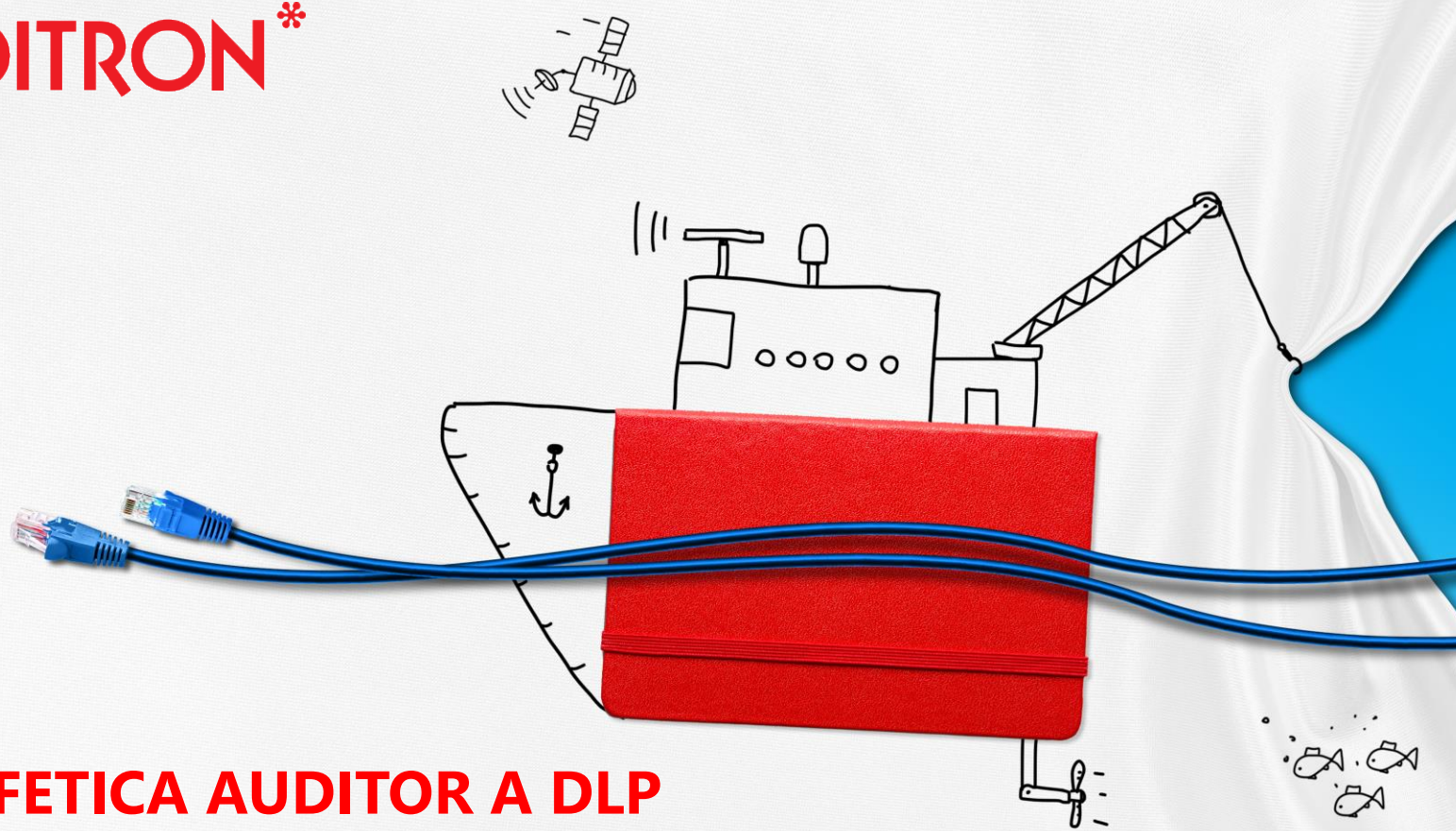
SOITRON



SAFETICA AUDITOR A DLP

Rýchly a prehľadný bezpečnostný audit na 1 klik

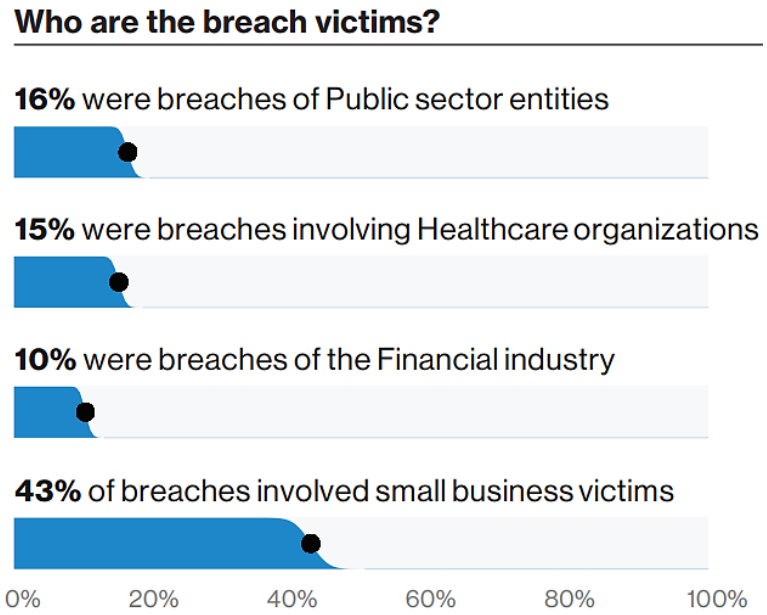
ČO BY SA STALO, KEBY STE STRATILI SVOJ LAPTOP?

- Viete aké sú Vaše citlivé dáta?
- Čo by sa stalo s citlivými dátami spoločnosti, ak by ste stratili firemný notebook?
- Máte prehľad o tom, ako Vaši zamestnanci fungujú vo vnútri organizácie?
- Dokážete zabrániť tomu, aby citlivé dáta neželane opustili priestory vašej firmy?

ČO SÚ TO CITLIVÉ DÁTA?

- **Dôverné informácie, ktorých únik môže ohroziť spoločnosť**
- **Čo sú Vaše citlivé dáta?**
  - Zmluvy
  - Strategické plány
  - Know-how
  - Databáza zákazníkov
  - Osobné údaje klientov a zákonom chránené informácie
  - Priemyselné nákresy a obchodné údaje
- **Najčastejšie príčiny úniku dát**
  - Ľudský faktor
  - Nesprávne nastavené procesy
  - Nespokojný zamestnanec

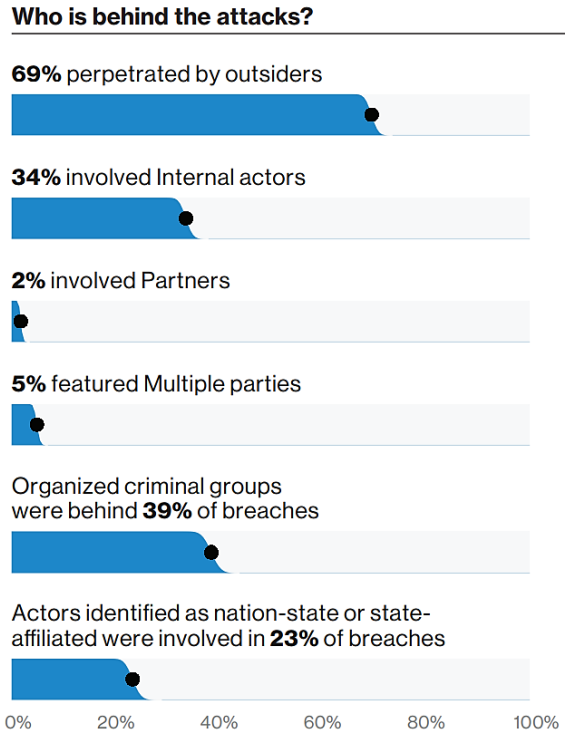
ČO HOVORÍ ŠTATISTIKA

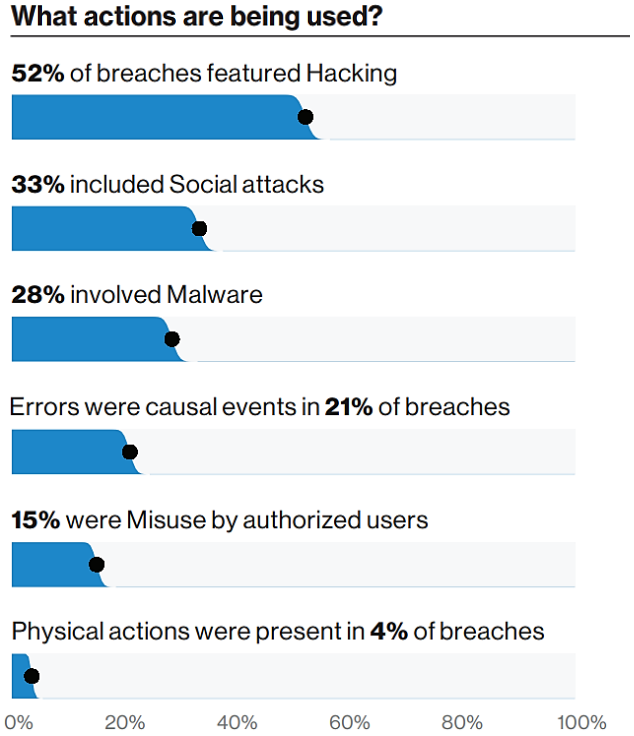


Verizon Data Breach Investigations Report (DBIR) 2019

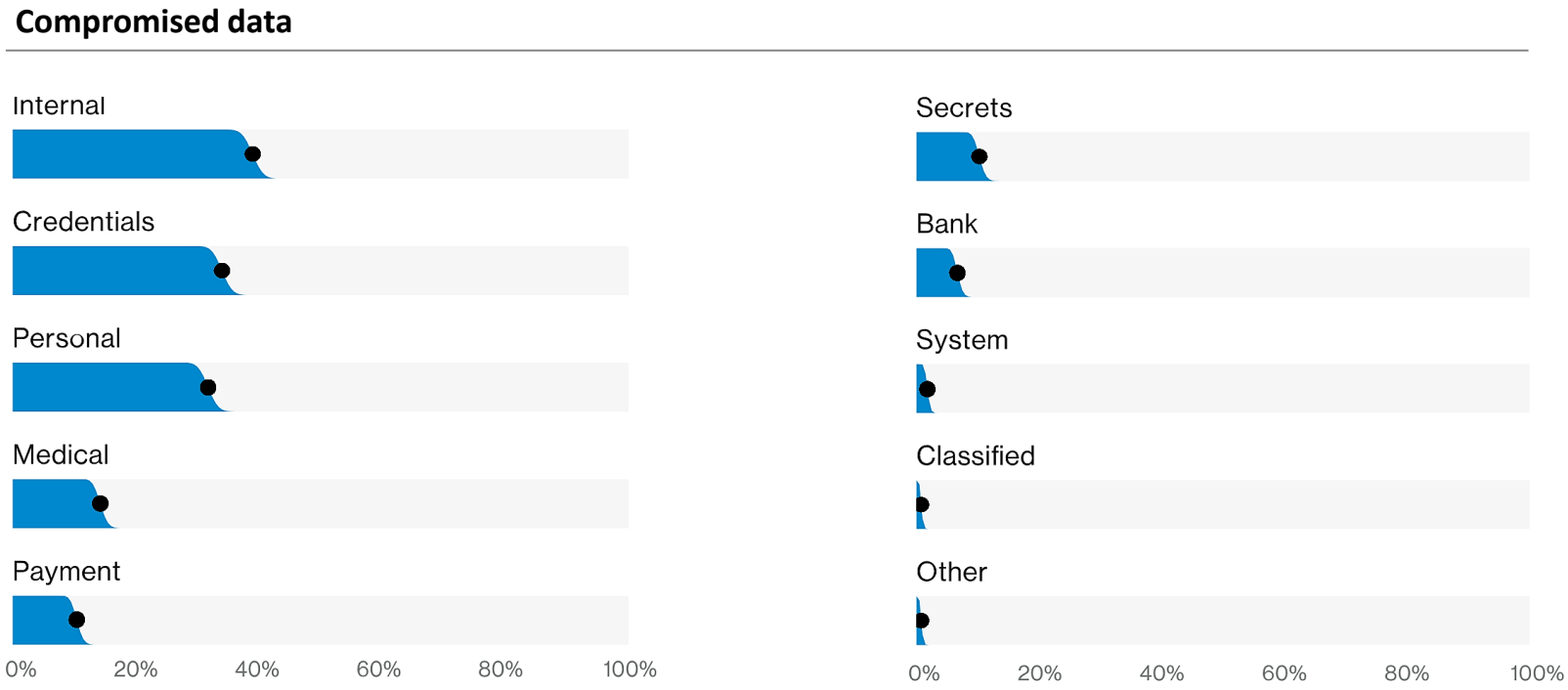
Dáta boli zozbierané a vyhodnotené zo 41 686 bezpečnostných incidentov a 2 013 prípadov únikov dát zo 73 zdrojov verejného aj privátneho sektora z 86 krajín celého sveta

ČO HOVORÍ ŠTATISTIKA





ČO HOVORÍ ŠTATISTIKA



TOP 3 PRÍPADY ÚNIKOV DÁT ZA ROK 2019

- **Toyota** zaznamenala niekoľko útokov na pobočky po celom svete – napr. Japonsko, Austrália, Vietnam – pričom útočníkom sa podarilo vyniesť údaje približne 3,1 milióna zákazníkov a zamestnancov.

- **Walmart** – jeho hlavný dodávateľ a technologický partner Compucom neoprávnene monitoroval vnútrofiremnú komunikáciu zamestnancov, pričom s najväčšou pravdepodobnosťou prišlo aj k úniku dát citlivej povahy smerom ku konkurencii.

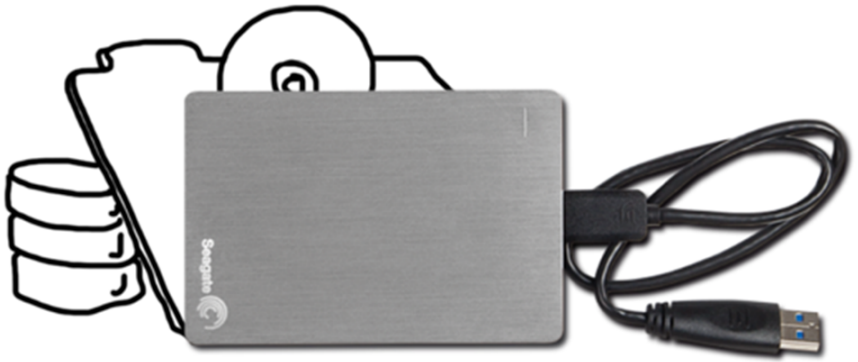
- **Citrix** – Iránska skupina hackerov s názvom IRIDIUM napadla firemnú sieť a počas približne 5 mesiacov odcudzila cca. 6 TB dát ako napr. citlivé súbory, emaily, množstvo dokumentov rôznej povahy, osobné údaje zamestnancov, finančné informácie, technologické plány a návrhy.

RIEŠENÍM JE SYSTÉM DLP

Data Leak Prevention
Prevencia pred únikom dát

Cieľ DLP
Minimalizácia rizika úniku dát

Safetica DLP



S ČÍM SAFETICA POMÔŽE

- Úmyselný únik citlivých informácií
- Omyly zamestnancov
- Nízka produktivita zamestnancov a neefektívne využitie IT zdrojov
- Chyby v procesoch
- Naplnenie legislatívnych požiadaviek

VÝHODY RIEŠENIA SAFETICA

- Efektívna prevencia úniku akýchkoľvek dát
- Pokrýva všetky potenciálne cesty úniku
- Riešenie nezasahuje do obsahu dát
- Dokáže identifikovať podozrivé pohyby citlivých informácií
- Dohľaduje využívanie firemných zdrojov – tlačiarne, aplikácie, externé zariadenia, a pod.
- Ponúka manažment šifrovania diskov a periférií
- Identifikuje zmeny v produktivite a ponúka široké auditné možnosti
- Pomáha plniť legislatívne požiadavky ako napr. GDPR a iné
- Integruje MDM - Mobile Device Management

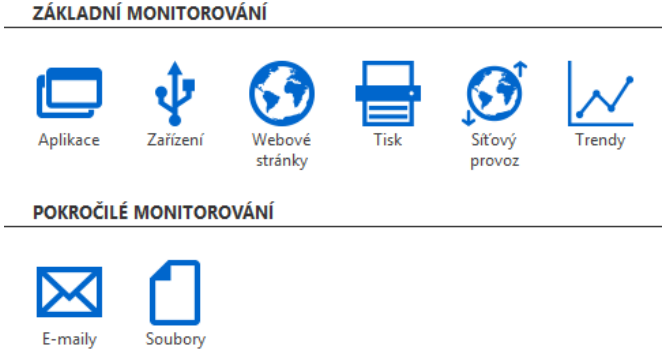
SAFETICA MODULY

SAFETICA AUDITOR

Slúži na audit a vyhodnocovanie aktivít koncových užívateľov, pričom ponúka dve prostredia na prácu so systémom. Webové prostredie napr. umožňuje vygenerovať bezpečnostný audit na jeden klik. Konzolové rozhranie je určené skôr pre správcov systému – predstavuje kompletný manažment riešenia.

- Webové rozhranie

- Konzolové rozhranie



SAFETICA AUDITOR

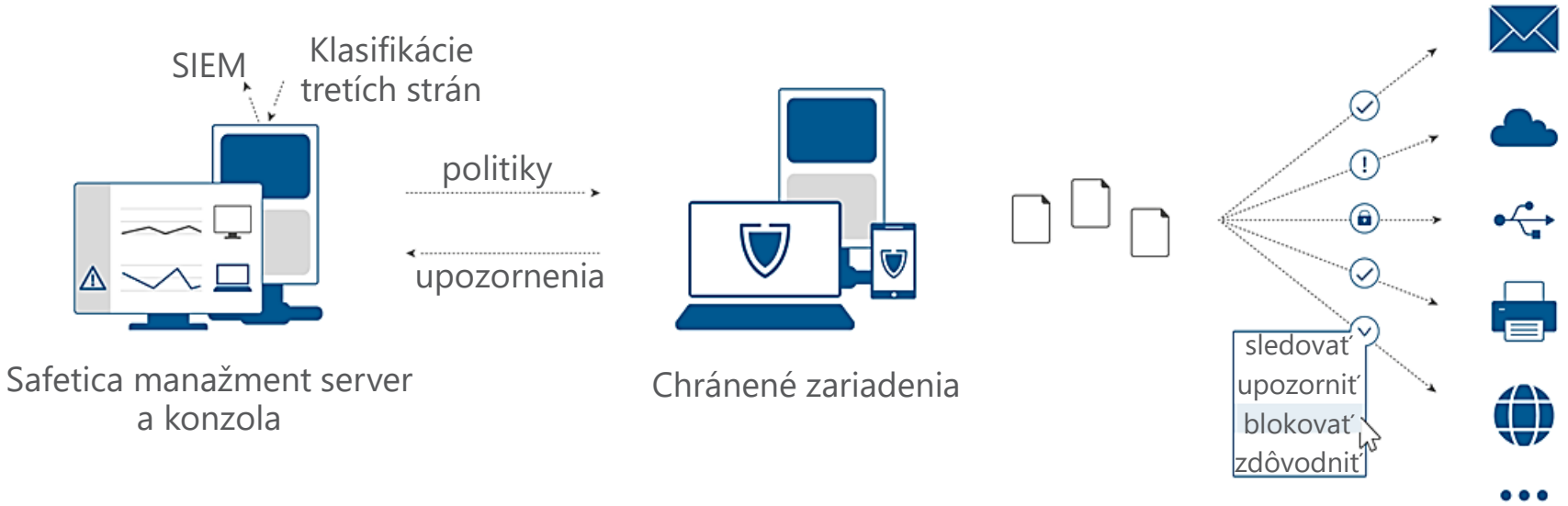
Sledované oblasti a udalosti

- Všetky súborové operácie
- Dlhodobé trendy, krátkodobé fluktuácie aktivity
- Webové stránky (podpora všetkých prehliadačov vrátane komunikácie HTTPS) – aktívny a neaktívny čas
- Emaily a webmailové služby – podpora najpoužívanejších mailových klientov
- Využívanie instant messaging platforiem
- Používanie aplikácií vrátane aktívneho a neaktívneho času
- Utilizácia tlačiarní - virtuálne, lokálne a sieťové tlačiarne
- Pripájanie externých zariadení - Bluetooth, IR/LPT/COM/paralelné porty
- Prehľady o sieťovej komunikácii na pracovných staniciach

DEMO

SAFETICA DLP

Ako to funguje – architektúra riešenia



Safetica manažment server a konzola

Chránené zariadenia

SAFETICA DLP

Prevencia straty údajov

- Všetky pevné disky, zariadenia USB a FireWire, karty SD/MMC/CF a jednotky SCSI
- Mechaniky CD/DVD/BluRay na čítanie aj zápis
- Sieťový prenos súborov (nezabezpečený, zabezpečený)
- Emaily (protokoly SMTP, POP, IMAP, Microsoft Outlook/MAPI)
- Virtuálne, lokálne a sieťové tlačiarne
- Bluetooth, IR/LPT/COM/paralelné porty
- Kontrola prístupu k súborom aplikácií
- Kopírovanie a vkladanie, schránka, presúvanie súborov pomocou myši
- SSL/HTTPS (prehliadače a aplikácie so štandardnou správou certifikátov)

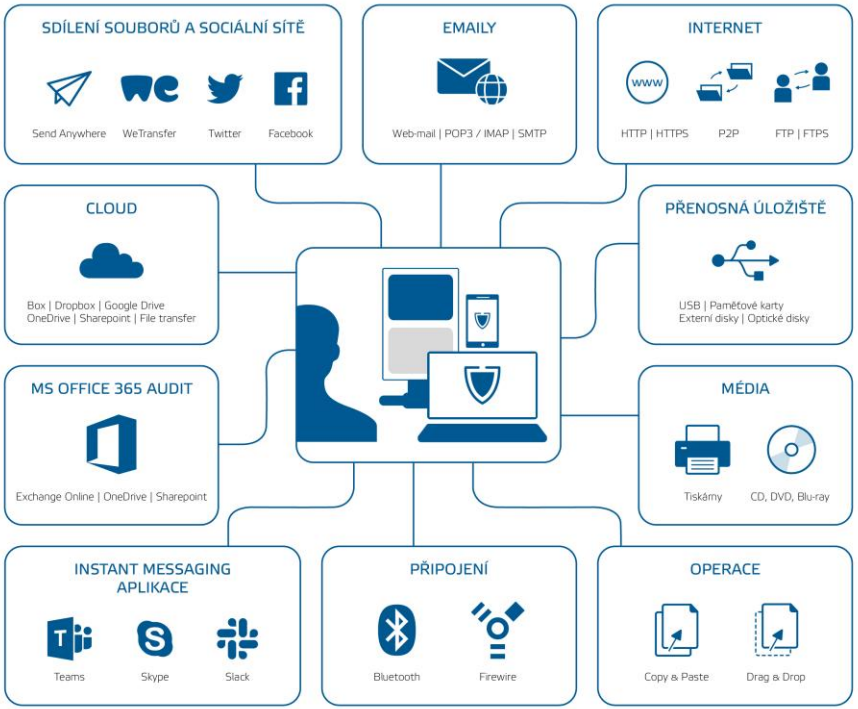
SAFETICA DLP

Prevencia straty údajov

- Detekcia a obmedzenie cloudových úložísk
- Tvorba snímok obrazovky
- Sťahovanie a upload vo webových prehliadačoch

SAFETICA DLP

Riadenie toku dát



DEMO

NOVINKY V NADCHÁDZAJÚCEJ VERZII

Safetica 9.3

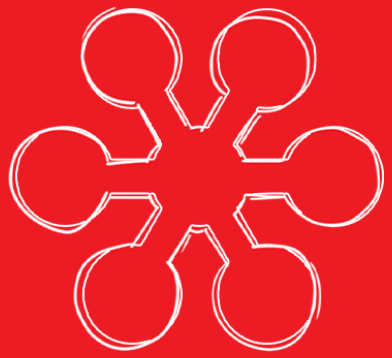
- Integrácia s FortiGate sieťovými prvkami
- macOS klient s auditnou funkcionalitou
- Možnosť importu vlastného slovníka na detekciu citlivého obsahu
- Možnosť stiahnuť predmetný súbor v prípade incidentu
- Nové DLP kumulatívne upozornenia
- Možnosť využiť alternatívny kontextový spôsob označovania dát
- Safetica Mobile: Nové auditné funkcie na platforme Android
- Rozšírené možnosti integrácie so SIEM systémami

LEGISLATÍVA VS. SAFETICA

Safetica pomáha pri riešení legislatívnych požiadaviek typu:

- GDPR
- PCI DSS
- HIPAA
- ISO 27001
- spoločnosť Safetica je certifikovaná pre ISO 9001, 27001

OTÁZKY A ODPOVEDE



ĎAKUJEME