

DLP



alebo ako Vám už nikdy neunikne citlivý údaj

AKÉ SÚ RIZIKÁ?

Strata zariadenia	Externý útočník	Zamestnanci a dodávatelia
 Okolo 40% všetkých incidentov straty dát bolo reportovaných na základe straty alebo krádeže zariadenia – notebook, mobilné zariadenia, externé pamäťové média	 Okolo 59% reportovaných incidentov spôsobených malware alebo zneužitím zraniteľnosti aplikácie externými útočníkmi, obsahovali citlivé dáta	 Okolo 57% reportovaných incidentov, ktoré majú na svedomí interní zamestnanci, ak už vedome alebo nevedome, obsahovali citlivé dáta

Viac ako **50% incidentov**
straty dát bolo
publikovaných externe

TYPY DÁT

VEKTORY ÚNIKU DÁT

DATA IN MOTION



WEB



EMAIL



NETWORK & TRAFFIC



IM CHAT

DATA IN REST



FILE SHARE



DATABASE



DESKTOP



LAPTOP

DATA IN USE



REMOVABLE DEVICES



EMAIL



CLOUD



CLIPBOARD



TYPY DÁT

VEKTORY ÚNIKU DÁT



AKO NA TO?

- **ANALÝZA INTERNEJ INFRAŠTRUKTÚRY A CITLIVÝCH DÁT**

- ANALÝZA VYTVÁRANÝCH DÁT
- ANALÝZA UKLÁDANÝCH DÁT
- ANALÝZA DATOVÝCH TOKOV
- KLASIFIKÁCIA ÚDAJOV

- **NÁVRH KLASIFIKÁCIE A KLASIFIKÁCIA CITLIVÝCH DÁT**

FILE CONDITIONS

- DOCUMENT PROPERTIES
- FILE ENCRYPTION
- FILE EXTENSION
- FILE INFORMATION
- THIRD PARTY TAGS
- TRUE FILE TYPE

DATA CONDITIONS

- ADVANCED PATTERN
- DICTIONARY
- KEYWORD
- PROXIMITY

- **NÁVRH BEZPEČNOSTNEJ POLITIKY DLP**

- VYHĽADÁVANIE - LOCAL DISCOVERY - CITLIVÝCH DÁT NA UŽIVATEĽSKÉ STANICI
- VYHĽADÁVANIE - NETWORK DISCOVERY - CITLIVÝCH DÁT NA SIEŤOVÝCH ÚLOŽISKÁCH
- VYHĽADÁVANIE CITLIVÝCH DÁT NA DISKOVOM ÚLOŽISKU
- KOPÍROVANIE CITLIVÝCH DÁT MEDZI SIEŤOVÝMI ÚLOŽISKAMI
- MONITORING KOMUNIKÁCIE NA SIEŤOVEJ INFRAŠTRUKTÚRE



- APPLICATION
- LOCATION
- WEB APPLICATION

DOBRÉ VEDIEŤ

Vždy je potrebné zvážiť všetky kroky pri definícií klasifikácií a pravidiel a všetko dôkladne otestovať

Nesprávna definícia vedie k false positives, generovaniu veľkého množstva udalostí, blokovaniu štandardnej komunikácie, nespokojnosti používateľov,

Čím menej klasifikačných a reakčných pravidiel, tým lepšie – znižuje sa tak záťaž systémov, ktoré musia s týmito pravidlami pracovať.

THE END ?



DISKUSIA

Otázky môžete klásť aj cez **sli.do**
Zadajte slido.com do Vášho prehliadača
Zadajte kód eventu **#EMMBB**