

The background of the slide is a dark blue overlay on a photograph. The photograph shows a large metal padlock in the foreground, slightly out of focus. Behind it, several credit cards are visible, also out of focus. One card clearly shows the number '3444' and the text 'MEMBER SINCE 1/5'.

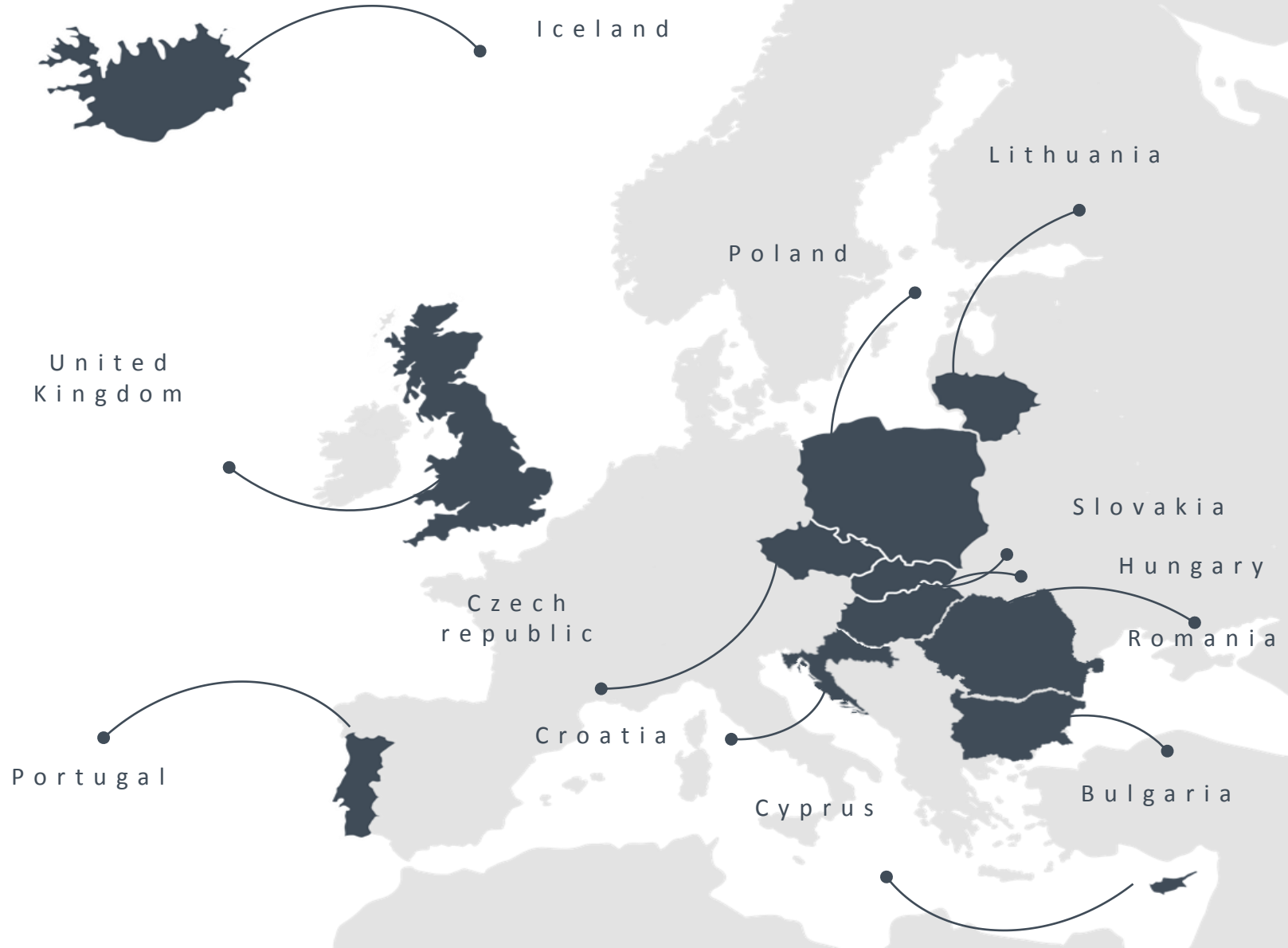
DanubePay

SIEM implementation : real case

≈

danubepay.com

DanubePay



Problém 1: Model aktív

„Konzultant neznalý IT prostredia zákazníka ho namodeluje podľa statickej tabuľky z IT. Tabuľka sa udržiava podľa potreby a obsahuje chyby. “

Výsledok:

Nesprávny model aktív → príliš veľa false positive a false negative

Název celku	Název zařízení nebo serveru	domain name	Celé DNS A jméno interface	noda	Standb	VLAN ID	Jméno VLAN	IP adresa síťe/maska (generováno)	t (host ID)	IP adresa celá (generováno)	ano/ne	(generováno)	PCI DSS	default	celá	rován
			FC switch port alias	WVI	y	VSAN	(generováno)									
46 c1	01V51	danubepay.local	c1-jira.danubepay.local													
47 c1	01V16	danubepay.local	c1-sanity-check.danubepay.local			699	C1_EXTRANET	10.197.62.192/26								
48 c1	03V06	danubepay.local	c1-Remoteapp.danubepay.local			644	C1_ATM-POS	10.197.64.128/28	201	10.197.62.201	ano	prod	yes	default	10.197.62.195	.195
49 c1	03V07	danubepay.local	c1-TS05-DMZ.danubepay.local			648	C1_TS05	10.197.64.224/28	135	10.197.64.135	ano	prod	yes	default	10.197.64.131	.131
50 c1	01v39	danubepay.local	c1-Haproxy01.danubepay.local			648	C1_TS05	10.197.64.224/28	235	10.197.64.235	ano	prod	yes	default	10.197.64.227	.227
51 c1	01v39	danubepay.local	c1-Haproxy01.danubepay.local			616	C1_PV_EXT	10.197.61.96/27	231	10.197.61.231	ano	prod	yes	default	10.197.61.227	.227
52 c1	01v39	danubepay.local	c1-Haproxy01.danubepay.local			616	C1_PV_EXT	10.197.61.96/27	123	10.197.61.123	ne	prod	yes	default	10.197.61.100	.100
53 c1	01v39	danubepay.local	c1-Haproxy01.danubepay.local			616	C1_PV_EXT	10.197.61.96/27	124	10.197.61.124	ne	prod	yes	default	10.197.61.100	.100
54 c1	01v40	danubepay.local	c1-Haproxy02.danubepay.local			617	C1_PV_INT	10.197.61.128/27	121	10.197.61.121	ne	prod	yes	default	10.197.61.100	.100
55 c1	01v40	danubepay.local	c1-Haproxy02.danubepay.local			616	C1_PV_EXT	10.197.61.96/27	141	10.197.61.141	ne	prod	yes	default	10.197.61.130	.130
56 c1	01V22	danubepay.local	c1-Haproxy02.danubepay.local			617	C1_PV_INT	10.197.61.128/27	122	10.197.61.122	ne	prod	yes	default	10.197.61.100	.100
57 c1	01V23	danubepay.local	c1-DP_frontend.danubepay.local			642	C1_DMZ	10.197.64.64/27	76	10.197.64.76	ano	prod	yes	default	10.197.64.67	.67
58 c1	01V38	danubepay.local	c1-CallCentrum.danubepay.local			642	C1_DMZ	10.197.64.64/27	77	10.197.64.77	ano	prod	yes	default	10.197.64.67	.67
59 c1	01V00	danubepay.local	c1-TMS.danubepay.local			644	C1_ATM-POS	10.197.64.128/28	142	10.197.64.142	ano	prod	yes	default	10.197.64.131	.131
60 c1	01V03	danubepay.local	c1-e-commerce-bkp.danubepay.local			#N/A	#N/A	#N/A	#N/A	#N/A	ne	bkp	yes	default	10.197.68.67	.67
61 c1	01V31	danubepay.local	c1-jira-bkp.danubepay.local			682	C1_DMZ_BKP	10.197.68.64/27	78	10.197.68.78	ne	bkp	yes	default	10.197.72.131	.131
62 c1	01V51	danubepay.local	c1-jira-bkp.danubepay.local			728	C1_EXTRANET_BKP	10.197.72.128/27	140	10.197.72.140	ne	bkp	yes	default	10.197.72.131	.131
63 c1	01V16	danubepay.local	c1-sanity-check-bkp.danubepay.local			728	C1_EXTRANET_BKP	10.197.72.128/27	141	10.197.72.141	ne	bkp	yes	default	10.197.68.131	.131
64 c1	03V06	danubepay.local	c1-Remoteapp-bkp.danubepay.local			684	C1_ATM-POS_BKP	10.197.68.128/28	135	10.197.68.135	ne	bkp	yes	default	10.197.69.3	.3
65 c1	03V07	danubepay.local	c1-TS05-DMZ-bkp.danubepay.local			690	C1_TS5_DMZ_BKP	10.197.69.0/28	10	10.197.69.10	ne	bkp	yes	default	10.197.69.3	.3
66 c1	01V22	danubepay.local	c1-DP_FRONTEND-bkp.danubepay.local			690	C1_TS5_DMZ_BKP	10.197.69.0/28	6	10.197.69.6	ne	bkp	yes	default	10.197.68.67	.67
67 c1	01V23	danubepay.local	c1-CallCentrum-bkp.danubepay.local			682	C1_DMZ_BKP	10.197.68.64/27	76	10.197.68.76	ne	bkp	yes	default	10.197.68.67	.67
68 c1	01V38	danubepay.local	c1-TMS-bkp.danubepay.local			77	10.197.68.77	10.197.68.77	77	10.197.68.77	ne	bkp	yes	default	10.197.68.67	.67
69 c1	01V39	danubepay.local	c1-TMS-bkp.danubepay.local			682	C1_DMZ_BKP	10.197.68.64/27	142	10.197.68.142	ne	bkp	yes	default	10.197.68.67	.67
70 c1	01V39	danubepay.local	c1-TMS-bkp.danubepay.local			682	C1_DMZ_BKP	10.197.68.64/27	142	10.197.68.142	ne	bkp	yes	default	10.197.68.67	.67
71 c1	01V39	danubepay.local	c1-TMS-bkp.danubepay.local			682	C1_DMZ_BKP	10.197.68.64/27	142	10.197.68.142	ne	bkp	yes	default	10.197.68.67	.67
72 c1	01V39	danubepay.local	c1-TMS-bkp.danubepay.local			682	C1_DMZ_BKP	10.197.68.64/27	142	10.197.68.142	ne	bkp	yes	default	10.197.68.67	.67
73 c1	01V39	danubepay.local	c1-TMS-bkp.danubepay.local			682	C1_DMZ_BKP	10.197.68.64/27	142	10.197.68.142	ne	bkp	yes	default	10.197.68.67	.67
74 c1	01V39	danubepay.local	c1-TMS-bkp.danubepay.local			682	C1_DMZ_BKP	10.197.68.64/27	142	10.197.68.142	ne	bkp	yes	default	10.197.68.67	.67
75 c1	01V39	danubepay.local	c1-TMS-bkp.danubepay.local			682	C1_DMZ_BKP	10.197.68.64/27	142	10.197.68.142	ne	bkp	yes	default	10.197.68.67	.67
76 c1	01V39	danubepay.local	c1-TMS-bkp.danubepay.local			682	C1_DMZ_BKP	10.197.68.64/27	142	10.197.68.142	ne	bkp	yes	default	10.197.68.67	.67
77 c1	01V39	danubepay.local	c1-TMS-bkp.danubepay.local			682	C1_DMZ_BKP	10.197.68.64/27	142	10.197.68.142	ne	bkp	yes	default	10.197.68.67	.67
78 c1	01V39	danubepay.local	c1-TMS-bkp.danubepay.local			682	C1_DMZ_BKP	10.197.68.64/27	142	10.197.68.142	ne	bkp	yes	default	10.197.68.67	.67
79 c1	01V39	danubepay.local	c1-TMS-bkp.danubepay.local			682	C1_DMZ_BKP	10.197.68.64/27	142	10.197.68.142	ne	bkp	yes	default	10.197.68.67	.67
80 c1	01V39	danubepay.local	c1-TMS-bkp.danubepay.local			682	C1_DMZ_BKP	10.197.68.64/27	142	10.197.68.142	ne	bkp	yes	default	10.197.68.67	.67
81 c1	01V39	danubepay.local	c1-TMS-bkp.danubepay.local			682	C1_DMZ_BKP	10.197.68.64/27	142	10.197.68.142	ne	bkp	yes	default	10.197.68.67	.67
82 c1	01V39	danubepay.local	c1-TMS-bkp.danubepay.local			682	C1_DMZ_BKP	10.197.68.64/27	142	10.197.68.142	ne	bkp	yes	default	10.197.68.67	.67
83 c1	01V39	danubepay.local	c1-TMS-bkp.danubepay.local			682	C1_DMZ_BKP	10.197.68.64/27	142	10.197.68.142	ne	bkp	yes	default	10.197.68.67	.67
84 c1	01V39	danubepay.local	c1-TMS-bkp.danubepay.local			682	C1_DMZ_BKP	10.197.68.64/27	142	10.197.68.142	ne	bkp	yes	default	10.197.68.67	.67
85 c1	01V39	danubepay.local	c1-TMS-bkp.danubepay.local			682	C1_DMZ_BKP	10.197.68.64/27	142	10.197.68.142	ne	bkp	yes	default	10.197.68.67	.67
86 c1	01V39	danubepay.local	c1-TMS-bkp.danubepay.local			682	C1_DMZ_BKP	10.197.68.64/27	142	10.197.68.142	ne	bkp	yes	default	10.197.68.67	.67
87 c1	01V39	danubepay.local	c1-TMS-bkp.danubepay.local			682	C1_DMZ_BKP	10.197.68.64/27	142	10.197.68.142	ne	bkp	yes	default	10.197.68.67	.67
88 c1	01V39	danubepay.local	c1-TMS-bkp.danubepay.local			682	C1_DMZ_BKP	10.197.68.64/27	142	10.197.68.142	ne	bkp	yes	default	10.197.68.67	.67
89 c1	01V39	danubepay.local	c1-TMS-bkp.danubepay.local			682	C1_DMZ_BKP	10.197.68.64/27	142	10.197.68.142	ne	bkp	yes	default	10.197.68.67	.67
90 c1	01V39	danubepay.local	c1-TMS-bkp.danubepay.local			682	C1_DMZ_BKP	10.197.68.64/27	142	10.197.68.142	ne	bkp	yes	default	10.197.68.67	.67
91 c1	01V39	danubepay.local	c1-TMS-bkp.danubepay.local			682	C1_DMZ_BKP	10.197.68.64/27	142	10.197.68.142	ne	bkp	yes	default	10.197.68.67	.67
92 c1	01V39	danubepay.local	c1-TMS-bkp.danubepay.local			682	C1_DMZ_BKP	10.197.68.64/27	142	10.197.68.142	ne	bkp	yes	default	10.197.68.67	.67
93 c1	01V39	danubepay.local	c1-TMS-bkp.danubepay.local			682	C1_DMZ_BKP	10.197.68.64/27	142	10.197.68.142	ne	bkp	yes	default	10.197.68.67	.67
94 c1	01V39	danubepay.local	c1-TMS-bkp.danubepay.local			682	C1_DMZ_BKP	10.197.68.64/27	142	10.197.68.142	ne	bkp	yes	default	10.197.68.67	.67
95 c1	01V39	danubepay.local	c1-TMS-bkp.danubepay.local			682	C1_DMZ_BKP	10.197.68.64/27	142	10.197.68.142	ne	bkp	yes	default	10.197.68.67	.67
96 c1	01V39	danubepay.local	c1-TMS-bkp.danubepay.local			682	C1_DMZ_BKP	10.197.68.64/27	142	10.197.68.142	ne	bkp	yes	default	10.197.68.67	.67
97 c1	01V39	danubepay.local	c1-TMS-bkp.danubepay.local			682	C1_DMZ_BKP	10.197.68.64/27	142	10.197.68.142	ne	bkp	yes	default	10.197.68.67	.67
98 c1	01V39	danubepay.local	c1-TMS-bkp.danubepay.local			682	C1_DMZ_BKP	10.197.68.64/27	142	10.197.68.142	ne	bkp	yes	default	10.197.68.67	.67
99 c1	01V39	danubepay.local	c1-TMS-bkp.danubepay.local			682	C1_DMZ_BKP	10.197.68.64/27	142	10.197.68.142	ne	bkp	yes	default	10.197.68.67	.67
100 c1	01V39	danubepay.local	c1-TMS-bkp.danubepay.local			682	C1_DMZ_BKP	10.197.68.64/27	142	10.197.68.142	ne	bkp	yes	default	10.197.68.67	.67





Riešenie:

- SPOT pre IT aktíva
- Životný cyklus modelu
- Riadenie zmien **vždy** zahŕňa napojenie na bezpečnostné systémy
- Monitoring – SIEM odhaľuje neznáme (nenamodelované) aktíva

Assets

Shared

All Assets

ArcSight Solutions

ArcSight System Administration

DanubePay

C1

Administrative

Backup

Card System

C1 Back Office #1 Member01

C1 Back Office #1 Member02

C1 Back Office #2 Member01

C1 Back Office #2 Member02

C1 Back Office Cluster

C1 CD EP New

C1 CD EP Old

C1 DP BackEnd

C1 DP FrontEnd

C1 HAProxy #1

C1 HAProxy #2

C1 InACT Application

C1 InACT Engine

C1 JMS

C1 Merchant Portal

C1 Online #1 Member01

C1 Online #1 Member02

C1 Online #2 Member01

C1 Online #2 Member02

C1 Online Cluster

C1 Sanity Check

C1 SCP MP CC

C1 sFTP (clients)

C1 TMS

C1 VISA EA server

C1 VISA EA server01

C1 VISA EA server02

C1 Weblogic #1

C1 Weblogic #2

Other Systems

Security

TS

C2

C3

C4

Inspect/Edit

Asset: C1 Sanity Check

Attributes

Categories

Alternate Interfaces

Vulnerabilities

Notes

Asset

Name

C1 Sanity Check

IP Address

10.197.64.135

MAC Address

00:00:00:00:00:00

Host Name

C1-01V16

Location

Datacube

Zone

C1_ATM-POS

Static Addressing

☒

Asset Disabled

☐

Common

Resource ID

4ctWC5kkBABDDqXlxiwe25A ==

External ID

Alias (Display Name)

Description

Version ID

AAAACTH89SmIEOyI

Assign

Owner

Notification Groups

Parent Groups

Card System

/All Assets/DanubePay/C1/Card System/

Creation Information

Created By

dp_kvocka

Creation Time

24 10 2016 10:26:04 CEST

Time Since Creation

206 day(s) 5 hour(s) 4 min(s) 28 sec(s)

Last Update Information

Last Updated By

dp_kvocka

Last Update Time

24 10 2016 10:26:05 CEST

Time Since Last Update

206 day(s) 5 hour(s) 4 min(s) 27 sec(s)

The screenshot displays the ArcSight console interface. On the left, the 'Assets' tree is expanded, showing a hierarchy from 'Shared' to 'All Assets' to 'DanubePay' to 'C1'. The 'C1' folder contains subfolders like 'Administrative', 'Backup', and 'Card System'. The 'Card System' folder is expanded, showing a list of assets including 'C1 Back Office #1 Member01', 'C1 Back Office #1 Member02', 'C1 Back Office #2 Member01', 'C1 Back Office #2 Member02', 'C1 Back Office Cluster', 'C1 CD EP New', 'C1 CD EP Old', 'C1 DP BackEnd', 'C1 DP FrontEnd', 'C1 HAProxy #1', 'C1 HAProxy #2', 'C1 InACT Application', 'C1 InACT Engine', 'C1 JMS', 'C1 Merchant Portal', 'C1 Online #1 Member01', 'C1 Online #1 Member02', 'C1 Online #2 Member01', 'C1 Online #2 Member02', 'C1 Online Cluster', 'C1 Sanity Check' (highlighted), 'C1 SCP MP CC', 'C1 sFTP (clients)', 'C1 TMS', 'C1 VISA EA server', 'C1 VISA EA server01', 'C1 VISA EA server02', 'C1 Weblogic #1', and 'C1 Weblogic #2'. Other folders like 'Other Systems', 'Security', and 'TS' are also visible.

On the right, the 'Inspect/Edit' window is open, showing the 'Asset: C1 Sanity Check'. The window has tabs for 'Attributes', 'Categories', 'Alternate Interfaces', 'Vulnerabilities', and 'Notes'. The 'Categories' tab is selected, showing a list of categories. The 'Local Asset Categories' section lists several categories, including '/All Asset Categories/System Asset Categories/Criticality/Very High', '/All Asset Categories/Site Asset Categories/Business Impact Analysis/Data Role/Reporting Requirement/PCI/Cardholder Data', '/All Asset Categories/Site Asset Categories/Application/Vendor/RedHat', '/All Asset Categories/Site Asset Categories/Business Impact Analysis/Business Role/Operations', '/All Asset Categories/Site Asset Categories/Business Impact Analysis/Data Role/Reporting Requirement/PCI/DMZ', '/All Asset Categories/Investigations/Unsuccessfully Attacked Assets', and '/All Asset Categories/Site Asset Categories/Operating System/Linux'. The 'Inherited Asset Categories' section lists one category: '/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Production'.

Problém 2: Log Management

- SIEM != Log Management
- Žiaden log management, iba SIEM
- Logovanie podľa CIS benchmarkov
- Zbytočne vysoká SIEM licencia
- Väčšina logov je odpad

Riešenie:

- Log management oddelený od SIEMu (syslog-ng PE, ArcSight Loggre...)
- Agregácia logov
- Do SIEMu len vybraná časť logov
- Logovanie systémov nastavené „na mieru“

Výsledok:

- Rádové zníženie počtu logov
- Kvalita logov
- Obohatenie logov
 - Chýba hostname? Lookup ID->String? Tag? syslog-ng opraví
- Vyťaženie SIEM licencie z $\frac{3}{4}$ na $\frac{1}{4}$

C2 RHEL auditd config

Linux auditd ▼

Add tag...

Tahoma ▼

10 ▼

a ▼

B

I

U

±

🖌

{ }

☰

|

event count pred nasadenim:

4.4. 00:00:00 - 5.4. 23:59:59

10.197.74.110	1980171
---------------	---------

10.197.74.173	1598091
---------------	---------

10.197.74.76	1586868
--------------	---------

event count po nasadeni:

\$now-24h - \$now

10.197.74.110	4491
---------------	------

10.197.74.173	4458
---------------	------

10.197.74.76	7131
--------------	------

```
147 -a always,exit -F arch=b32 -S mount -S umount -S umount2 -F auid>=500 -F auid!=4294967295
148
149 ### monitor process ID changes/sudoers changes
150 -w /bin/su -p x -k priv_esc
151 -w /usr/bin/sudo -p x -k priv_esc
152 -w /etc/sudoers -p wa -k priv_esc
153
154 ### kernel module (un)loading
155 -w /sbin/insmod -p x -k modules
156 -w /sbin/rmmod -p x -k modules
157 -w /sbin/modprobe -p x -k modules
158 # 64-bit
159 -a always,exit -F arch=b64 -S init_module -S delete_module -k modules
160
161 ### all root file actions, but exclude non-user and daemon accounts
162 -a always,exit -F euid=0 -F auid>=500 -F auid!=4294967295 -F perm=wxa -k root
163
164 ### all executables run by root, but exclude non-user and daemon accounts
165 -a exit,always -F arch=b64 -F euid=0 -F auid>=500 -F auid!=4294967295 -S execve -k root
166 -a exit,always -F arch=b32 -F euid=0 -F auid>=500 -F auid!=4294967295 -S execve -k root
167
168 ### special files
169 -a exit,always -F arch=b32 -S mknod -S mknodat -k specialfiles
170 -a exit,always -F arch=b64 -S mknod -S mknodat -k specialfiles
171
172 ### user/group tools
173 -w /usr/sbin/groupadd -p x -k accounts
174 -w /usr/sbin/groupmod -p x -k accounts
175 -w /usr/sbin/addgroup -p x -k accounts
```

Problém 3: Use case

Množstvo vágne definovaných scenárov, napr. copy-paste z compliance požiadaviek.

One-liners.

Príklady zlých scenárov:

„Čítal som o tom v časopise. Mali by sme s tým niečo robiť.“

„Windows nie je bezpečný, mali by sme detekovať či niekto nerobí niečo čo nemá.“

„Monitorujte kritické súbory a objekty (PCI DSS).“

„SOC dostane alert XXX a vyrieši ho.“

Riešenie:

Každý scenár exaktne definovaný. Miniprojekt:

- Akú udalosť chcem detekovať?
- Na základe čoho? (mám logy?)
- Na základe akých kritérií určím že udalosť nastala?
- A čo s ňou potom?

Triviálny príklad dobrého scenára:

- Vzorka logov z každého systému – prihlásenia
- Tabuľka zamestnancov po výpovedi
- Pravidlo – ak sa na ľubovoľný systém prihlási niekto kontom, ktoré obsahuje priezvisko z tabuľky, generuj alert
- SOC zanalyzuje kedy, kto, kam, odkiaľ...ale nevyrieši príčinu

Problém 4: Pluginy

- PCI DSS Compliance Insight Package
- Po konfigurácii...nepoužiteľný
- Plugin nerozumie zložitému IT prostrediu service providera
- Čiastočné riešenie: výnimky v pravidlách a reportoch
- Počet výnimiek po roku >> počet pravidiel

Riešenie:

- PCI plugin ako tutoriál, vzor
- Scenáre na monitoring vlastné, na mieru
- Minimum výnimiek
- ArcSight Activate Framework

Súčasný stav

- Funkčný in-house SIEM
- SOC as a Service
 - Multiinštitučná architektúra
 - Licencie (MSSP)
 - Ľudia (L1, L2)

Rady na záver: Ak rozmýšľate nad SIEM-om

- Zvážiť či naozaj potrebujete SIEM
- In-house vs. SOC as a Service
 - Náklady
 - IT zázemie
 - Personálne zabezpečenie
 - SLA a jej vymáhateľnosť
 - Poskytnutie logov 3. strane
- Honeypoty / honeytokens

ĎAKUJEME ZA POZORNOSŤ!



DanubePay

Marián Žilinec

SECURITY MANAGER

marian.zilinec@danubepay.com

Martin Kvočka

SECURITY SPECIALIST

martin.kvocka@danubepay.com

?

?

?

?