

SECURITY 2013



21. ročník konference o bezpečnosti v ICT

Aby zo SOC nebol ŠOK

Ivan Masný

ALISON Slovakia s.r.o.





Vieme čo chceme ⁽¹⁾

- Očakávania zákazníka
 - Zber a vyhodnocovanie auditných záznamov z komponentov IS
 - Redukovanie objemu sledovaných udalostí
 - Rýchla a efektívna identifikácia bezpečnostných incidentov
 - Centralizovaná konsolidovaná platforma na riešenie bezpečnostných incidentov
 - Prehľad o prebiehajúcich útokoch a prevádzke v sieti



Vieme čo chceme ⁽²⁾

- Očakávania zákazníka (pokračovanie)
 - Detekcia bezpečnostných slabín komponentov IS
 - Zníženie nákladov na riešenie dopadov bezpečnostných incidentov
 - Uchovanie dôkazov pre prípadné úkony orgánov činných v trestnom konaní
 - Vytvorenie „mostu“ medzi Network Operations Centers (NOC) a Security Operations Centers (SOC)



Vieme kde to chceme

- Inštitúcia s celoštátnou pôsobnosťou
- Prevádzkované viaceré rozsiahle heterogénne IS
- Primárne platformy
 - Windows
 - Linux
 - UNIX
 - Cisco
- Primárne aplikácie
 - Webové
 - Intranetové
 - Finančné



Vieme ako by to malo vyzerat'



20. února 2013

SECURITY 2013



Vieme čomu sa vyvarovať

- Príliš vysokým očakávaniam a širokému záberu projektu
- Podhodnoteniu finančných a časových nárokov na projekt
- Nedostatočnej dokumentácii aktuálne prevádzkovaných informačných systémov, hlavne aplikácií a auditovacích funkcií
- Nedostatku kvalifikovaných interných ľudských zdrojov na implementáciu a prevádzku riešenia



Čo sme museli riešiť

- Nedostatok kvalifikovaných interných ľudských zdrojov na implementáciu a prevádzku riešenia
- Podhodnotenie časových nárokov na projekt na strane zákazníka
- Nedostatočnú dokumentáciu aktuálne prevádzkovaných informačných systémov, hlavne aplikácií a auditovacích funkcií
- „Štandardné“ projektové problémy



Pár praktických rád





Pár praktických rád

Motto: „Dvakrát merať a raz rezať!“

- Skôr ako začnete - papier, pero, ceruzka
- Prvotná konfigurácia
- Network Model
- SmartConnector a Connector Appliance
- Redukcia „False Positive“



Skôr ako začnete

- Majte aktuálny prehľad o monitorovaných komponentoch
- Získajte nasledujúce informácie
 - Koľko zariadení, aplikácií a používateľov bude monitorovaných
 - Typ monitorovaných zariadení
 - Operačné systémy a ich verzie
 - Aplikácie a ich verzie
 - Odhad EPS a objem udalostí GB / deň
- Nevyhýbajte sa „Proof of Concept“



Prvotná konfigurácia

- Je potrebné mať **jasné a pripravené**
 - Retenčnú politiku zaznamenávaných udalostí
 - Hostname zariadení
 - IP adresy pre zariadenia a manažment HW
 - Konektivitu medzi zariadeniami
 - Heslá a mená pre systémových používateľov (sú vyžadované počas inštalácie)
- Aktualizácia softvéru na posledné verzie
 - Download aktuálnych verzií
 - Upload softvéru na zariadenia
 - **Postup v zmysle dokumentácie výrobcu**
- Úprava úvodných hlásení na podmienky zákazníka



Network model ⁽¹⁾

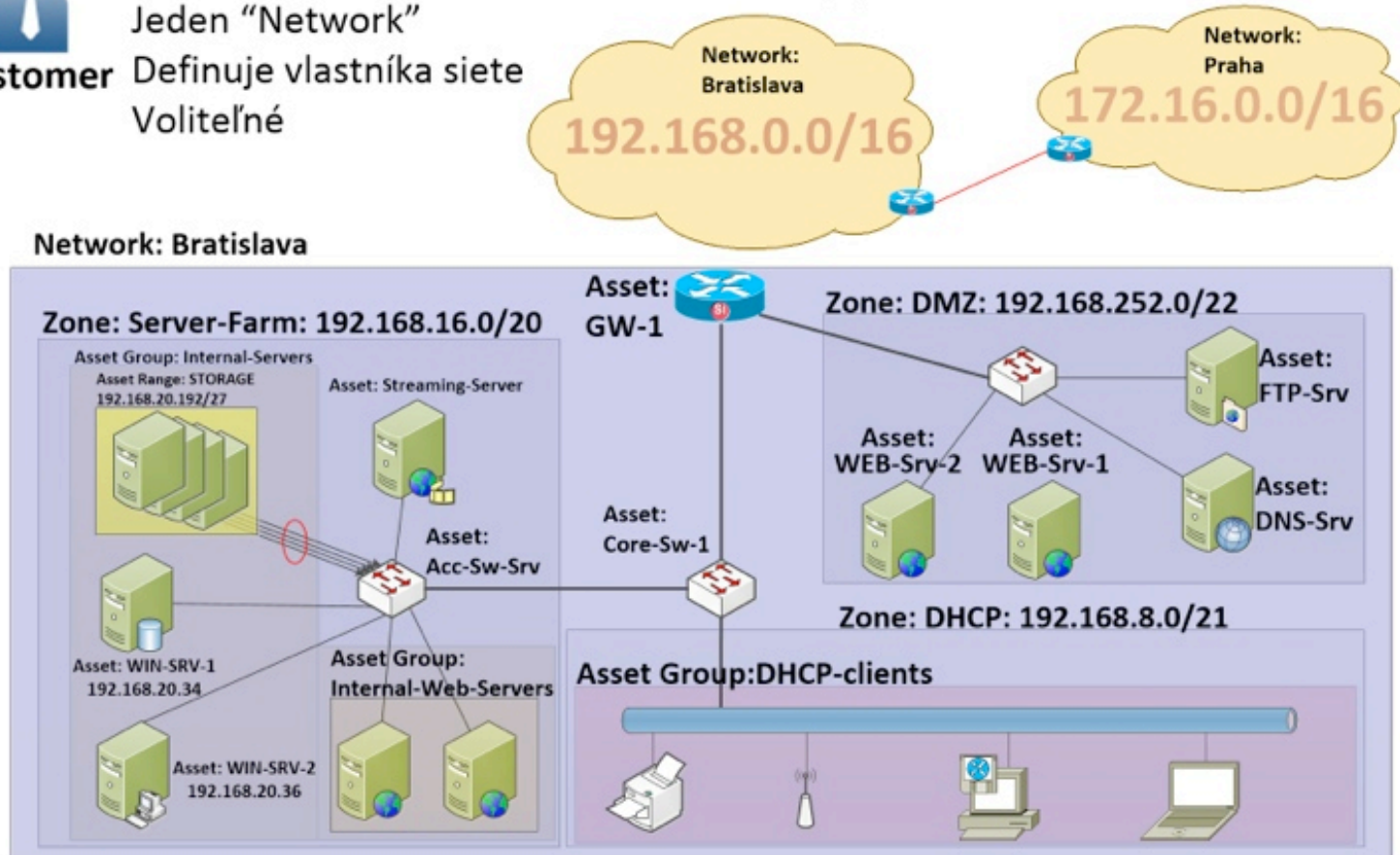
- Udržujte váš Network model
 - Jednoduchý
 - Presný
 - Manažovatelný
 - Maximalizujte vaše „return on investment“



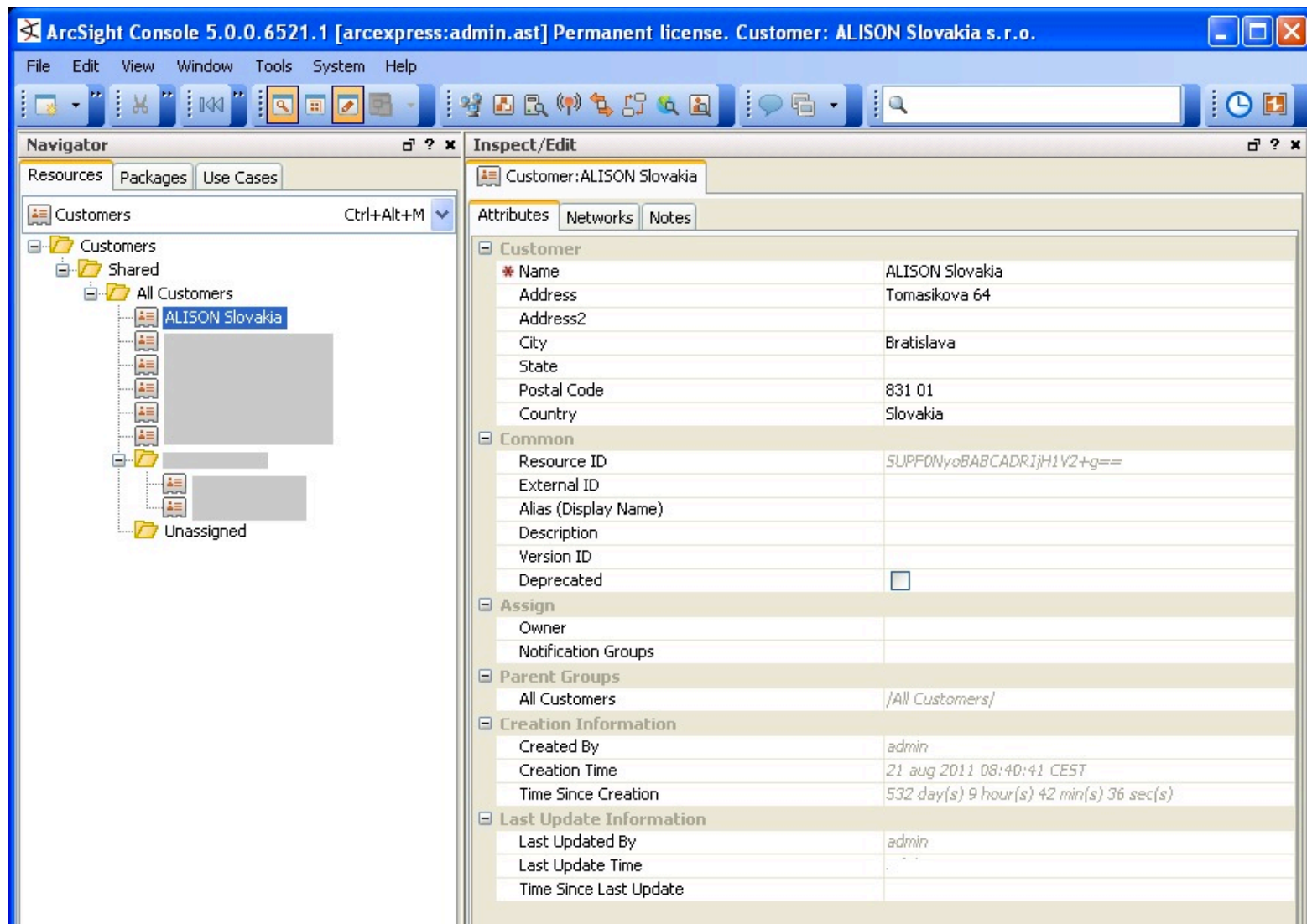
Network model (2)


Customer =
Jeden "Customer"
Jeden "Network"
Definuje vlastníka siete
Voliteľné

Network Definuje globálne logickú sieť
Sú užitočné pri dvoch neprekrývajúcich sa
privátnych adresných priestoroch
Vytvára väzbu medzi konektorom a sieťou
Obsahuje jednu alebo viac zón



Network model - Customer



ArcSight Console 5.0.0.6521.1 [arcexpress:admin.ast] Permanent license. Customer: ALISON Slovakia s.r.o.

File Edit View Window Tools System Help

Navigator

Resources Packages Use Cases

Customers Ctrl+Alt+M

Customers

Shared

All Customers

ALISON Slovakia

Unassigned

Inspect/Edit

Customer:ALISON Slovakia

Attributes Networks Notes

Customer

Name	ALISON Slovakia
Address	Tomasikova 64
Address2	
City	Bratislava
State	
Postal Code	831 01
Country	Slovakia

Common

Resource ID	SUPF0NyoBABCADRIjH1V2+g==
External ID	
Alias (Display Name)	
Description	
Version ID	
Deprecated	☐

Assign

Owner	
Notification Groups	

Parent Groups

All Customers	/All Customers/
---------------	-----------------

Creation Information

Created By	admin
Creation Time	21 aug 2011 08:40:41 CEST
Time Since Creation	532 day(s) 9 hour(s) 42 min(s) 36 sec(s)

Last Update Information

Last Updated By	admin
Last Update Time	
Time Since Last Update	

Network model - Networks

The screenshot displays the ArcSight Console 5.0.0.6521.1 interface. The title bar indicates a permanent license for ALISON Slovakia s.r.o. The interface is divided into several panes:

- Navigator:** Shows a tree view of the network model. The 'Networks' folder is expanded, showing 'Shared' and 'All Networks'. Under 'All Networks', there is an 'ArcSight System' folder containing the 'ALISON' network. Other folders include 'Core', 'Public', and 'Unassigned'.
- Inspect/Edit:** Displays the details for the selected 'Network:ALISON'. It includes tabs for 'Attributes', 'Connectors', 'Zones', and 'Notes'.

The 'Attributes' tab shows the following information:

Category	Attribute	Value
Network	Name	ALISON
	Customer	ALISON Slovakia
	Location	BAHQ - Bratislava - BSK - SVK
Common	Resource ID	XdFUFQAEBABCAKaxkp9ga2g==
	External ID	Local
	Alias (Display Name)	
	Description	Add Custom Zones to this network. Zone Mappings in th
	Version ID	
	Deprecated	☐
Assign	Owner	
	Notification Groups	
Parent Groups	ArcSight System	/All Networks/ArcSight System/
Creation Information	Created By	
	Creation Time	18 aug 2011 23:06:12 CEST
	Time Since Creation	534 day(s) 19 hour(s) 19 min(s) 10 sec(s)
Last Update Information	Last Updated By	admin
	Last Update Time	
	Time Since Last Update	1 sec(s)

Network model- Zones

ArcSight Console 5.0.0.6521.1 [arcexpress:admin.ast] Permanent license. Customer: ALISON Slovakia s.r.o.

File Edit View Window Tools System Help

Navigator

Resources Packages Use Cases

Assets Ctrl+Alt+S

Assets Zones Networks Categories Vulnerabilities Locations

Zones

Shared

All Zones

ALISON Slovakia

BAHQ - Bratislava - BSK - SVK

BAHQ-Bratislava 03. poschodie - DHCP 10.41. - 10.41.

BAHQ-Bratislava 10. poschodie - DHCP 10.41. - 10.41.

BAHQ-Bratislava LAB - DHCP 10.41. - 10.41.

BAHQ-Bratislava MGMT a FIN - DHCP 10.41. - 10.41.

BAHQ-Bratislava servre - DHCP 10.41. - 10.41.

BAHQ-Bratislava VoIP - DHCP 10.41. - 10.41.

BAHQ-Bratislava VPN RAS - DHCP 10.66. - 10.66.

BAHQ-Bratislava WIFI - DHCP 10.41. - 10.41.

BARP - Bratislava - BSK - SVK

ArcSight System

System Disabled

Unassigned

Inspect/Edit

Zone:BAHQ-Bratislava 03. posch...

Attributes Assets Categories Notes

Zone

Name BAHQ-Bratislava 03. poschodie - DHCP 10.41. - 10.41.

Start Address 10.41.

End Address 10.41.

Dynamic Addressing ☒

Location BAHQ - Bratislava - BSK - SVK

Network ALISON

Common

Resource ID MKhgfrzyoBABCawy3Jxdj7pw==

External ID

Alias (Display Name)

Description

Version ID AAAAAI3XzjU1SRd

Deprecated ☐

Assign

Owner

Notification Groups

Parent Groups

BAHQ - Bratislava - BSK - SVK /All Zones/ALISON Slovakia/BAHQ - Bratislava - BSK - SVK/

Creation Information

Created By admin

Creation Time 21 aug 2011 08:40:42 CEST

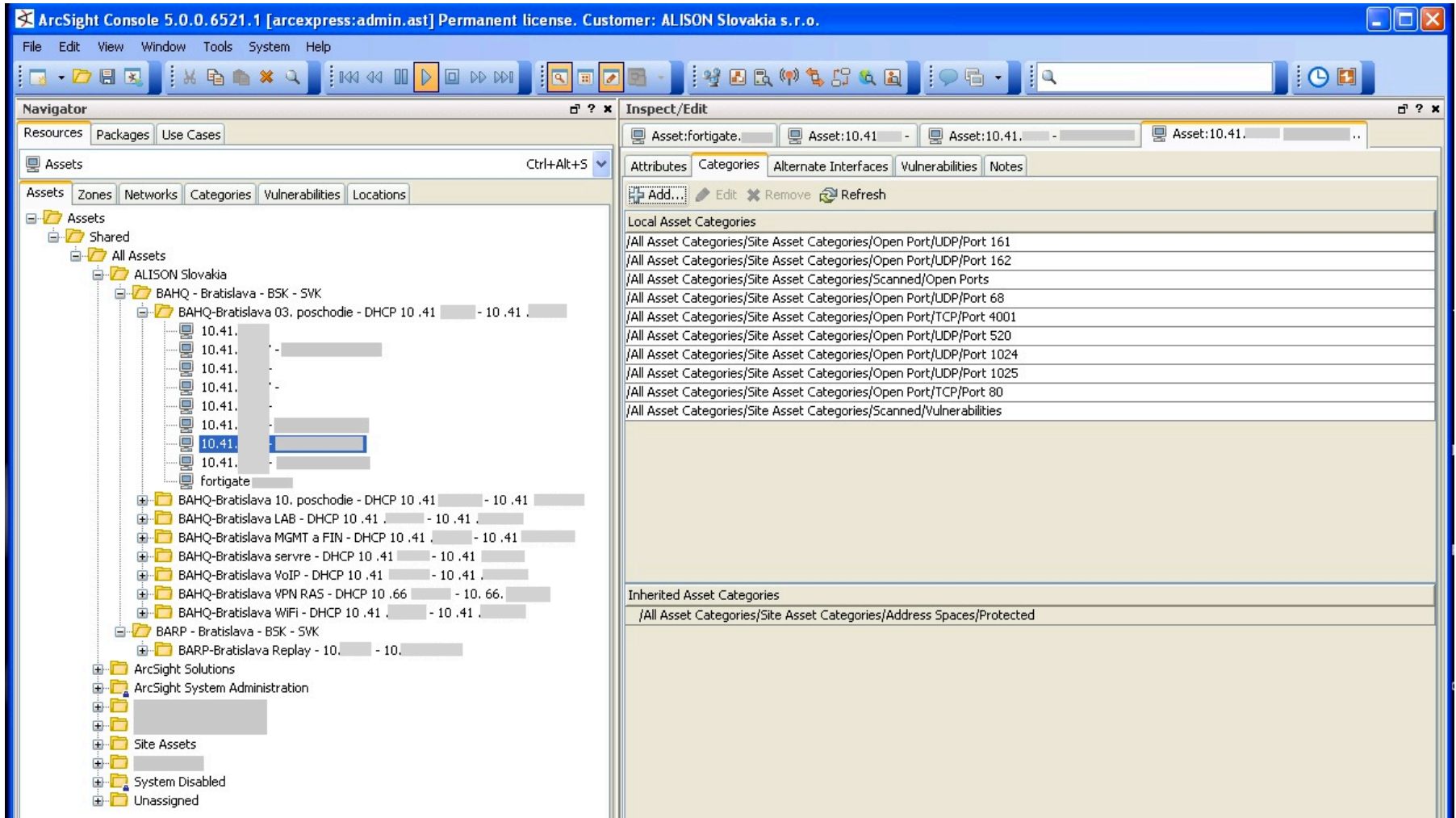
Time Since Creation 532 day(s) 9 hour(s) 47 min(s) 10 sec(s)

Last Update Information

Last Updated By admin

Last Update Time 21 aug 2011 08:40:51 CEST

Time Since Last Update 532 day(s) 9 hour(s) 47 min(s) 1 sec(s)





Network model

- Najčastejšou chybou pri používaní „Customer“ je nepriradenie zodpovedajúceho „Connector“ (hlavne pri novonainštalovaných konektoroch)
- „Locations“ definujte len pre „Private Address Space“
- Viac ako jednu „Local“ sieť („Network“) potrebujete len vtedy, ak sa prekrývajú „Private Address Space“ v rámci organizácie
- „Zone“ je logická reprezentácia súvislého adresného priestoru, ktorá identifikuje, či je alebo nie je v „Protected“ priestore
- Je odporúčané priradiť kategóriu („Category“) „Protected“ v najvyššej úrovni „Zone“
- **NIKDY** nerobte zmeny v „Default Zones“
- Použite rovnakú názvoslovnú konvenciu pre „Asset“ rozsahy, ako ste použili pre „Zone“



SmartConnector a Connector App

- V časti siete bol identifikovaný problém s preposielaním udalostí vzhľadom na firewall politiku organizácie
- Riešením bolo vytvorenie „SmartConnector Servera“
- SmartConnector Server
 - Virtualizovaný
 - Platforma Linux
 - Výkonnostne postačoval pre danú časť monitorovaných zariadení
 - Napojený na Connector Appliance pre potreby manažmentu udalostí



Redukcia „False Positive“

- Identifikovaný problém s vysokým počtom „False Positive“
- Udalosti prezentované systémom boli dôsledkom neošetrených operačných systémov a zákazník o nich vedel
- Riešenie na elimináciu
 - Upravenie „Threat Level Formula“
 - Použitie filtra pre "False Positive" => relevancia udalosti sa vždy znížila na "0"
 - Dôsledok - znížená priorita udalosti
 - Výsledok - dobrá vizualizácia, čo je a čo nie je „False Positive“ udalosť
 - Celé riešenie je alternatíva k úplnému filtrovaniu na úrovni SmartConnector – zákazník požadoval záznam všetkých udalostí z monitorovaných systémov



Čo povedať na záver?

- Pri budovaní SOC alebo implementovaní SIEM nezabudnite
 - Stanoviť si požiadavky na logovanie
 - Spracovať stratégiu analýzy udalostí
 - Určiť merateľné hodnoty
 - Definovať workflow bezpečnostných incidentov
 - Integrovať incident manažment do externých nástrojov

SECURITY 2013

21. ročník konference o bezpečnosti v ICT

Děkujeme za pozornost.

Ivan Masný

ALISON Slovakia s.r.o.

ivan.masny@alison-group.sk



PROSTOR
PRO OTÁZKY