CISCO SECURITY

MONITORING, ANALYSIS AND RESPONSE SYSTEM

ÁCS GYÖRGY
GACS@CISCO.COM

„Madártávlattól a MAC címig!”

TARTALOM

A BIZTONSÁGI MENEDZSMENT KIHÍVÁSAI

Biztonsági kihívás = üzleti probléma

Biztonsági szolgáltatás üzeme – reakciók ma

Mindig túl késő

Hálózati operátorok

Reaktív lépések:
1. Fokozott riasztás
2. Vizsgálat
3. Koordináció
4. Elhárítás

Biztonsági operátorok

Routerek, Switch-ek

IDS/IPS-ek

VPN

Sérülékenységi letapogatók

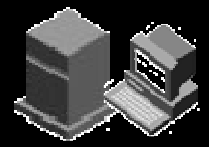
Authentikációs szerverek

Tűzfalak

Anti-vírusok

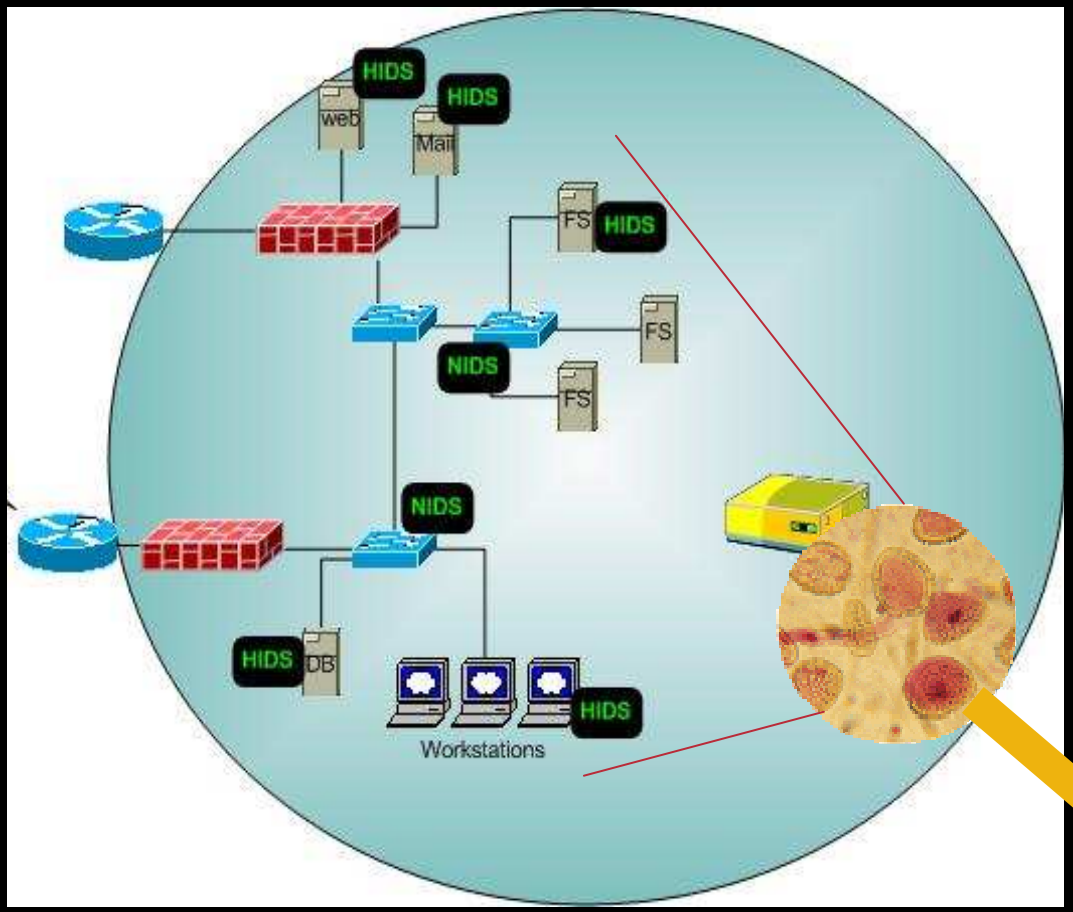
Több ezer Win, Több száz UNIX

A hálózati diagramm begyűjtése, több TONNA adat olvasása és analizálása… Ismét!



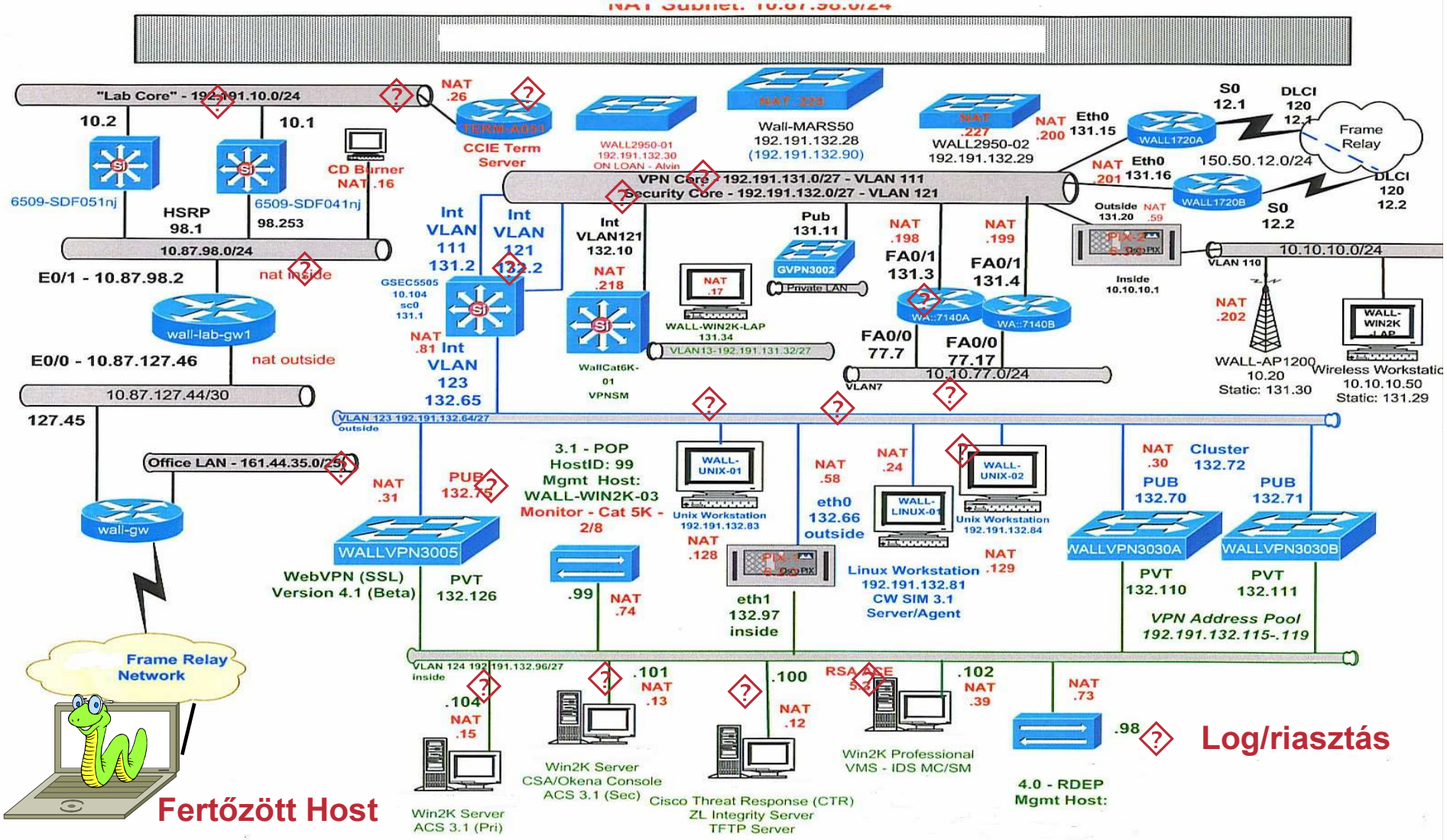
Biztonsági tudásbázis

Önvédő hálózati komponensek



- Tűzfalak
- Proxy-k
- VPN
- Anti-vírus
- Hálózati IDS/IPS
- Host alapú IDS/IPS
- Sérülékenységi kiértékelés
- Patch Management
- Policy megfelelés vizsgálat
- Router
- Switch

Mély védelem = komplexitás



Amikkel foglalkozni kell: NIDS/NIPS riasztások

Count	Sig Name	Source Address	Dest Address	Details	Source Protected	Dest Prote
1	FTP SYST	172.21.163.168	172.21.163.167	SYST	0	
18	ICMP Echo Req	+				
18	ICMP Echo Rply	+				
388	ICMP Unreachable	64.101.182.237	172.21.163.170	+		
2487		172.21.163.163	161.44.137.214	+		
2		172.21.163.168	3.3.3.3	+		
12		172.21.163.189	+			
8		172.21.163.190	+			
4630	NET FLOOD Icmp Any	+				
2	NET FLOOD Icmp Reply	172.21.163.163	161.44.137.214	MaxPPS=1	0	
2	NET FLOOD Icmp Request	172.21.163.163	161.44.137.214	MaxPPS=1	0	
113	NET FLOOD TCP	+				
5003	NET FLOOD UDP	+				
21	SMB Authorization Failure	+				
2	TCP High Port Sweep	172.21.163.189	+			
279	Windows Null Account Name	+				
21	Windows SRVSVC Access	+				

Amikkel foglalkozni kell: tűzfal Log

Telnet 192.168.1.1

```
302013: Built outbound TCP connection 207 for outside:198.133.219.25/80 (198.133.219.25/80) to inside:192.168.1.3/1606 (67.82.22
.18/1182)
305011: Built dynamic TCP translation from inside:192.168.1.3/1607 to outside:67.82.225.18/1183
302013: Built outbound TCP connection 208 for outside:198.133.219.25/80 (198.133.219.25/80) to inside:192.168.1.3/1607 (67.82.22
.18/1183)
304001: 192.168.1.3 Accessed URL 198.133.219.25:/favicon.ico
304001: 192.168.1.3 Accessed URL 198.133.219.25:/swa/j/cisco_detect.js
302014: Teardown TCP connection 207 for outside:198.133.219.25/80 to inside:192.168.1.3/1606 duration 0:00:01 bytes 5919 TCP Res
t-I
106015: Deny TCP (no connection) from 198.133.219.25/80 to 67.82.225.18/1182 flags ACK  on interface outside
106015: Deny TCP (no connection) from 192.168.1.3/1606 to 198.133.219.25/80 flags RST  on interface inside
106015: Deny TCP (no connection) from 198.133.219.25/80 to 67.82.225.18/1182 flags ACK  on interface outside
106015: Deny TCP (no connection) from 198.133.219.25/80 to 67.82.225.18/1182 flags ACK  on interface outside
302014: Teardown TCP connection 206 for outside:198.133.219.25/80 to inside:192.168.1.3/1602 duration 0:00:01 bytes 53445 TCP FI
s
305012: Teardown dynamic TCP translation from inside:192.168.1.3/1427 to outside:67.82.225.18/1142 duration 0:00:35
305011: Built dynamic TCP translation from inside:192.168.1.3/1610 to outside:67.82.225.18/1184
302013: Built outbound TCP connection 209 for outside:198.133.219.25/80 (198.133.219.25/80) to inside:192.168.1.3/1610 (67.82.22
.18/1184)
Jesus-Christ# sh log
Syslog logging: enabled
    Facility: 20
    Timestamp logging: enabled
    Standby logging: disabled
    Console logging: level informational, 919 messages logged
    Monitor logging: disabled
    Buffer logging: level informational, 915 messages logged
    Trap logging: disabled
    History logging: disabled
nslation from inside:192.168.1.3/1618 to outside:67.82.225.18/1052
305011: Built dynamic UDP translation from inside:192.168.1.3/29 to outside:67.82.225.18/42
302015: Built outbound UDP connection 210 for outside:167.206.3.158/53 (167.206.3.158/53) to inside:192.168.1.3/29 (67.82.225.18
42)
302016: Teardown UDP connection 210 for outside:167.206.3.158/53 to inside:192.168.1.3/1618 duration 0:00:01 bytes 158
305011: Built dynamic TCP translation from inside:192.168.1.3/1619 to outside:67.82.225.18/1185
302013: Built outbound TCP connection 211 for outside:64.154.80.250/80 (64.154.80.250/80) to inside:192.168.1.3/1619 (67.82.225.
8/1185)
304001: 192.168.1.3 Accessed URL 64.154.80.250:/HG?hc=we69&hb=DM5401281KAA%3BDM54012890CV&cd=1&hv=6&n=/Cisco.com+Public&con=&vc
=/%3B/Public&bn=Netscape&ce=y&ss=1024*768&sc=32&sv=13&cmp=&gp=&dcmp=&cy=u&hp=u&ln=en-US&cp=null&fnl=&pec=&vpc=090101r&vjs=09010
07r&seg=*;1&epg=n&ja=y&dt=5&zo=240&lm=0&cv=&gn=&ld=&la=&c1=&c2=&c3=&c4=&customerid=&ra=&rf=bookmark&pl=CDT%20Plug-in%3AQuickTime
20Plug-in%205.0.1%3AQuickTime%20Plug-in%205.0.1%3AQuickTime%20Plug-in%205.0.1%3AQuickTime%20Plug-in%205.0.1%3AQuickTime%20Plug-
%205.0.1%3AMozilla%20Default%20Plug-in%3AShockwave%20Flash%3AMicrosoft%AE%20DRM%3AMicrosoft%AE%20DRM%3AMetaStream%203%20Plugin%3
Java%20Plug-in%3AJava%20Plug-in%3AJava%20Plug-in%3AJava%20Plug-in%3AJava%20Plug-in%3AHP%20Peripheral%20Interrogator%3AWindows%20
edia%20Player%20Plug-in%20Dynamic%20Link%20Library%3AAdobe%20Acrobat%3A&tt=auto_pos
305011: Built dynamic TCP translation from inside:192.168.1.3/1620 to outside:67.82.225.18/1186
302013: Built outbound TCP connection 212 for outside:64.154.80.250/80 (64.154.80.250/80) to inside:192.168.1.3/1620 (67.82.225.
8/1186)
305012: Teardown dynamic UDP translation from inside:192.168.1.3/1454 to outside:67.82.225.18/1040 duration 0:00:31
305012: Teardown dynamic UDP translation from inside:192.168.1.3/17 to outside:67.82.225.18/30 duration 0:00:31
302014: Teardown TCP connection 211 for outside:64.154.80.250/80 to inside:192.168.1.3/1619 duration 0:00:01 bytes 2652 TCP FINs
304001: 192.168.1.3 Accessed URL 64.154.80.250:/HGct?hc=we69&hb=DM5401281KAA%3BDM54012890CV&cd=1&hv=6&n=/Cisco.com+Public&con=&v
on=/%3B/Public&bn=Netscape&ce=y&ss=1024*768&sc=32&sv=13&cmp=&gp=&dcmp=&cy=u&hp=u&ln=en-US&cp=null&fnl=&pec=&vpc=090101r&vjs=0901
1.07r&seg=*;1&epg=n&ja=y&dt=5&zo=240&lm=0&cv=&gn=&ld=&la=&c1=&c2=&c3=&c4=&customerid=&ra=&rf=bookmark&pl=CDT%20Plug-in%3AQuickT
e%20Plug-in%205.0.1%3AQuickTime%20Plug-in%205.0.1%3AQuickTime%20Plug-in%205.0.1%3AQuickTime%20Plug-in%205.0.1%3AQuickTime%20Plug
in%205.0.1%3AMozilla%20Default%20Plug-in%3AShockwave%20Flash%3AMicrosoft%AE%20DRM%3AMicrosoft%AE%20DRM%3AMetaStream%203%20Plugin
3AJava%20Plug-in%3AJava%20Plug-in%3AJava%20Plug-in%3AJava%20Plug-in%3AJava%20Plug-in%3AHP%20Peripheral%20Interrogator%3AWindows%
0Media%20Player%20Plug-in%20Dynamic%20Link%20Library%3AAdobe%20Acrobat%3A&tt=auto_pos
305012: Teardown dynamic UDP translation from inside:192.168.1.3/1462 to outside:67.82.225.18/1041 duration 0:00:31
305012: Teardown dynamic UDP translation from inside:192.168.1.3/18 to outside:67.82.225.18/31 duration 0:00:31
305012: Teardown dynamic UDP translation from inside:192.168.1.3/1463 to outside:67.82.225.18/1042 duration 0:00:31
305012: Teardown dynamic UDP translation from inside:192.168.1.3/19 to outside:67.82.225.18/32 duration 0:00:31
```

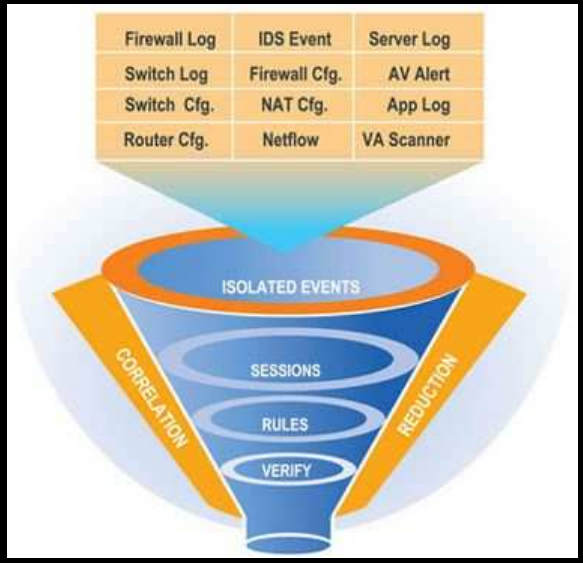
MARS: A MEGOLDÁS ÁTTEKINTÉSE

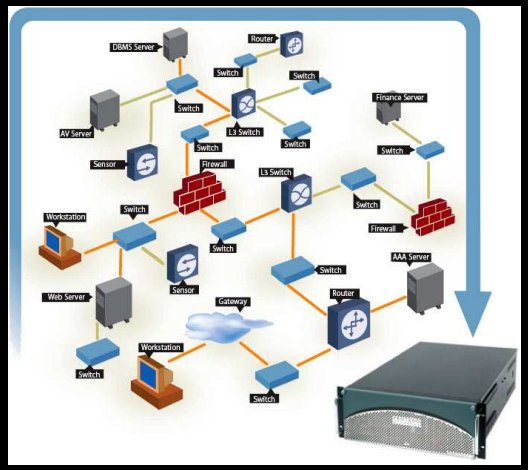
Monitoring, Analysis, and Response System (MARS)
Új generációs SIM/STM

- A hálózatban **már meglévő** minden eszközben jelenlévő biztonsági szolgáltatásokat használja ki
- A vállalat egészén keletkező adatokat **korrelálja**

  NIDS, tűzfalak, routerek, switch-ek, CSA

  Syslog, SNMP, RDEP, SDEE, NetFlow, végpont esemény logok, több gyártó támogatása
- Gyorsan **lokalizálja és enyhíti** a támadásokat





- **Főbb jellemzők**

  Meghatározza az ***incidenseket*** az üzenetek, események és a kapcsolatok alapján

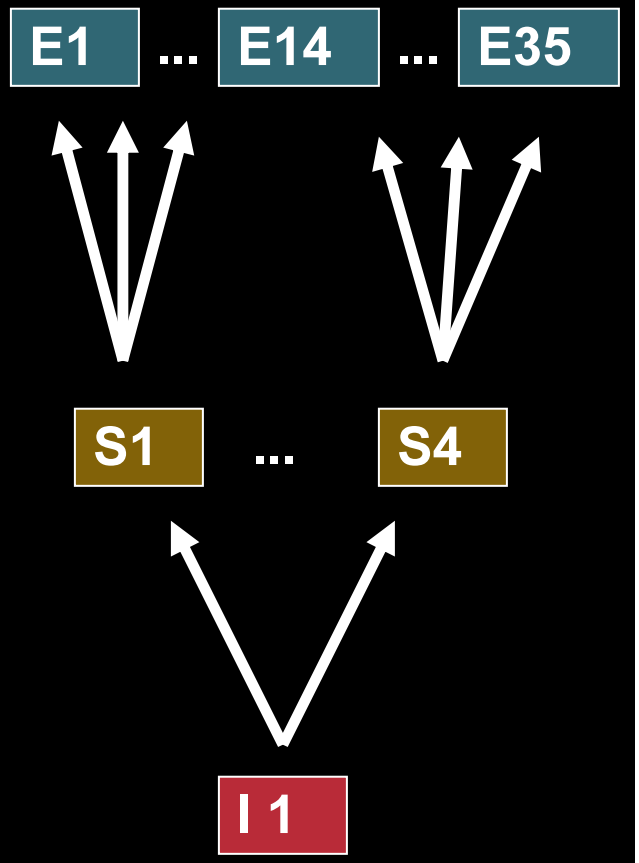
  Az incidens ***topológiájának birtokában*** lehetőség van ábrázolásra és visszajátszásra

  Enyhítés L2 és L3 „lezárópontokon”

  A teljes vállalaton keresztüli hatékony **skálázhatóság** a valós idejű használatra

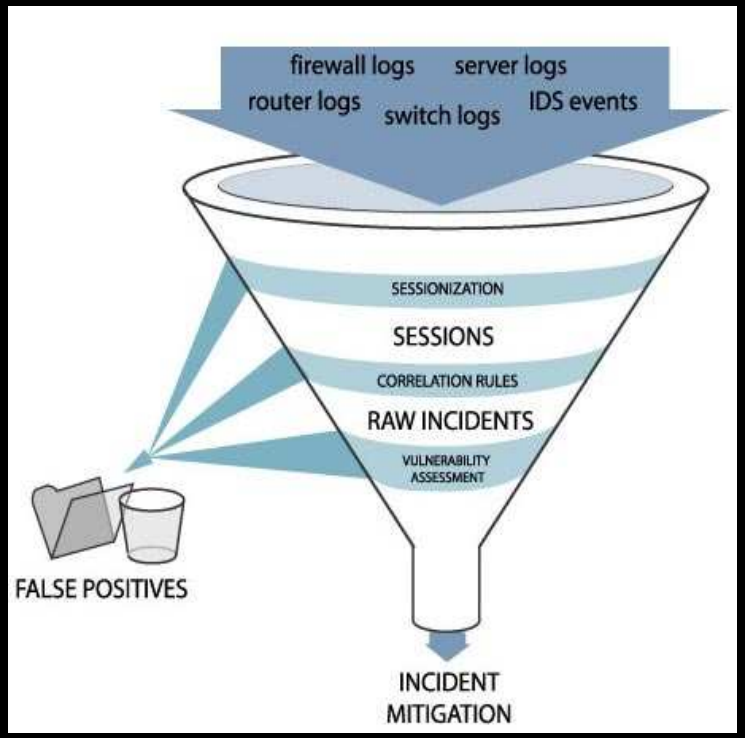
CS-MARS terminológiák

Események	Nyers üzenetek (pl.: IDS és tűzfal naplók), amelyeket a CS-MARS-nak küldenek a riportoló eszközök
Session-ök (kapcsolatok)	Olyan eseményből álló sorozat, melyeknek a végponti információi megegyeznek: Cél/Forrás IP cím Cél/Forrás Port és protokoll
Incidensek	Olyan kapcsolatokból álló sorozat, melyek egy definiált szabályra egyeznek

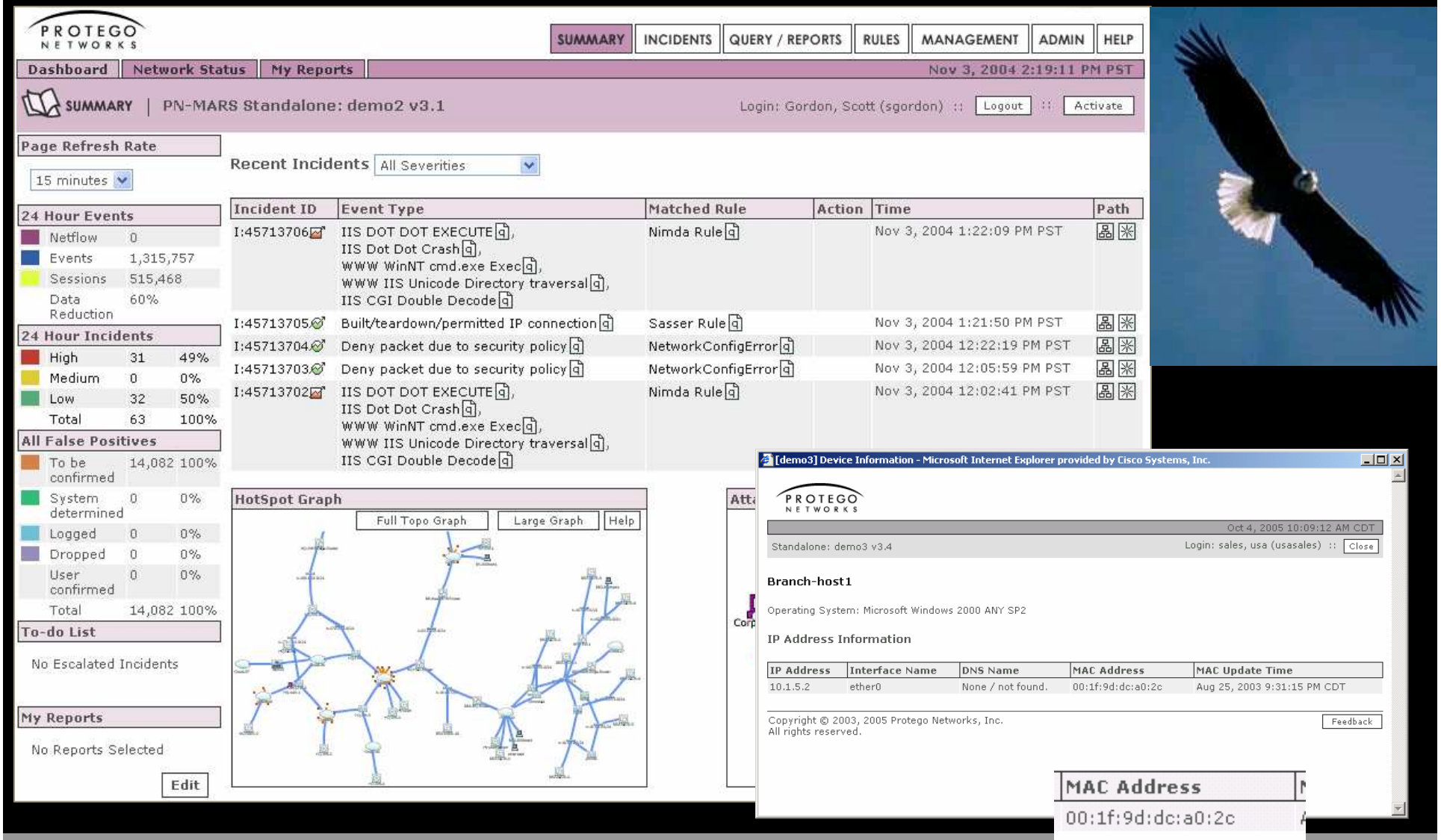


Ahogyan a CS-MARS működik

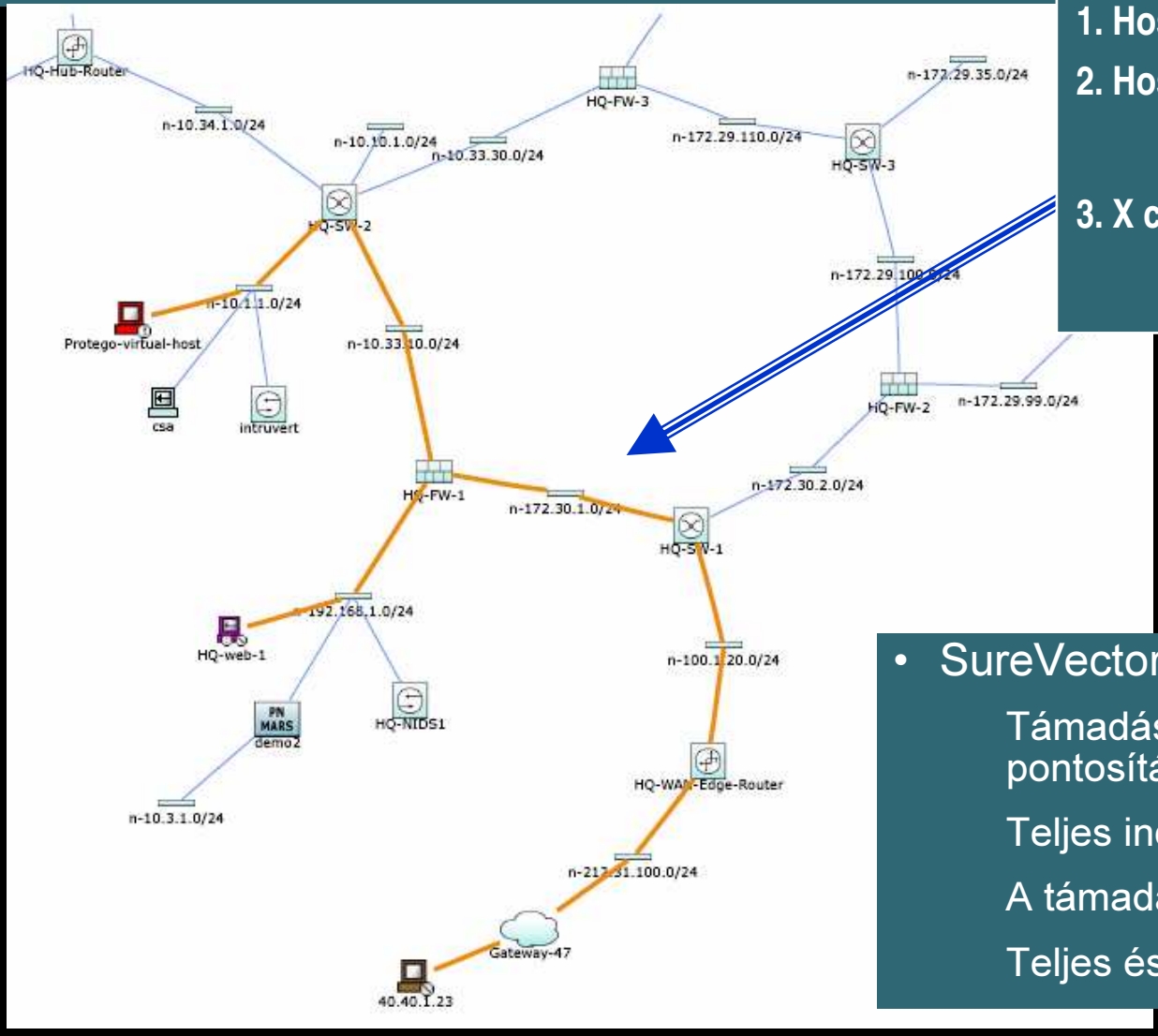
1. A hálózati eszközből megérkeznek az események a CS-MARS-ba
2. Az eseményeket „értelmezi”
3. Az eseményeket “normalizálja”
4. Sessionized/NAT korreláció
5. Rule Engine (szabály motor) futtatása
   - Eldobási szabályok
   - A rendszerben lévő előre definiált szabályok
   - Felhasználó által definiált szabályok
6. Hamis pozítiv analízis
7. Sérülékenységi kiértékelés a gyanús host-ok ellen
8. Forgalom elemzése és statisztikai anomalália detektálás



CS-MARS – analízis egy lapon



CS-MARS - a végpontok összekötése



1. Host A <u>port szkenneli</u> X célt
2. Host A <u>Buffer Overflow támadja</u> X-et, ahol X NAT eszköz mögött van és X <u>sérülékeny</u> az adott támadásra
3. X cél <u>jelszó támadást</u> hajt végre Y cél ellen, ami egy NAT mögött lévő eszköz

- SureVector™ analízis
  - Támadási útvonal bemutatása és pontosítása
  - Teljes incidens és esemény részletezés
  - A támadás pontos forrásának kiderítése
  - Teljes és pontos történet

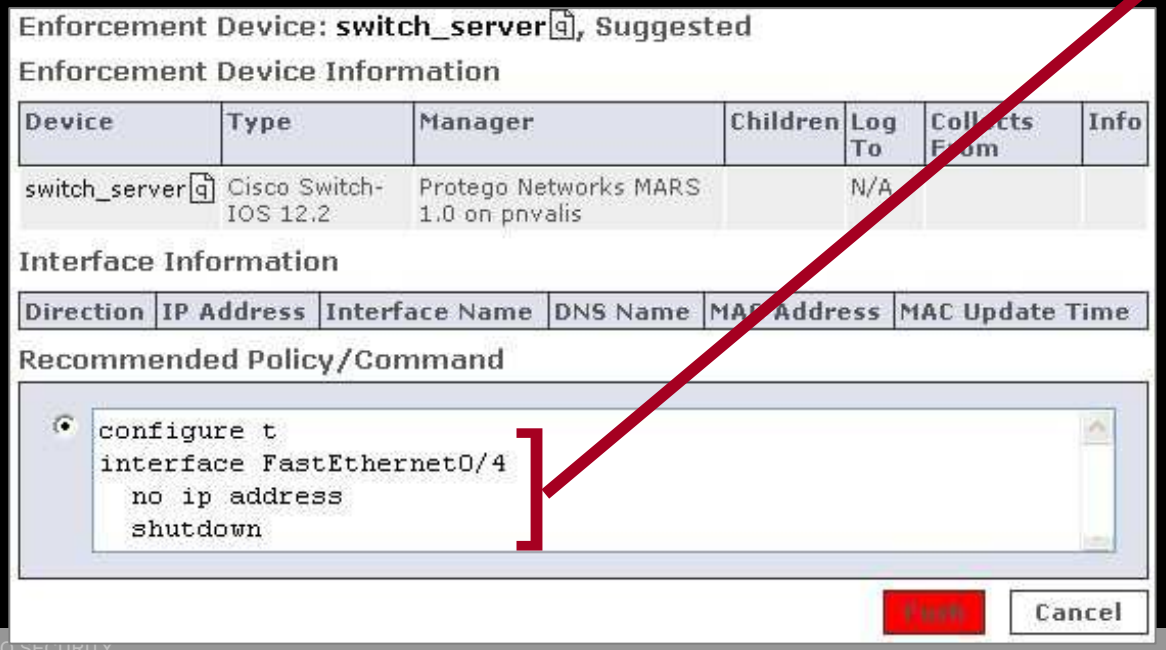
CS-MARS korreláció és egyszerűsítés

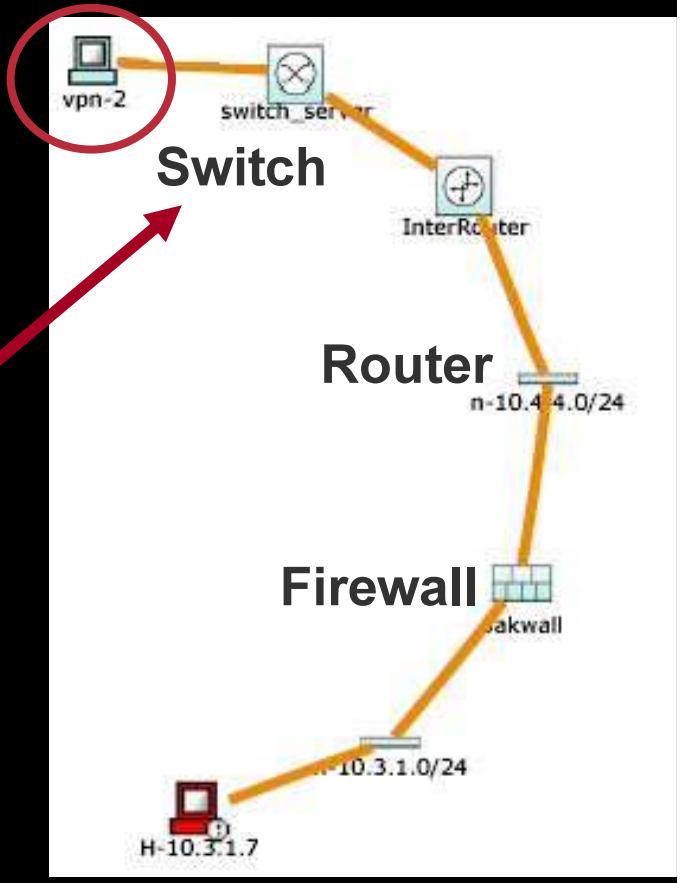
Részletes szabály keretrendszer és incidens részletezés

Jelentős egyszerűsítés

CS-MARS - alkalmazott védelem

- **Vezérlési lehetőségek**
  - **Layer 2/3 támadási út világosan látható**
  - **A kivédési eszközök definiálhatók**
  - **A pontos kivédési parancs megadható**





CS-MARS megfelelőségi riportok

A leggyakrabban használt riportok (beépített) – testreszabási lehetőség
Intuitív keretrendszer (nincs SQL konfigurálási igény)

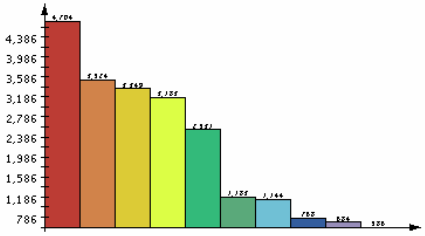
Report: Activity: Denies - Top Destination Ports Sep 8, 2004 1:07:45 PM PDT

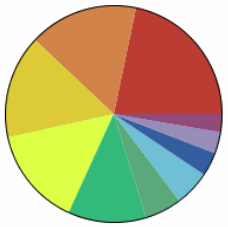
Name	Schedule	Format	Recipients	Query	Description	Status	Submitted	Time Range
Activity: Denies - Top Destination Ports	*Every hour*	*Normal*	None	*Event type: AttacksProtected, FirewallPolicyViolation/ACL, Query Type: Destination Ports ranked by Sessions Time: 1dd:0hh:0mm:0ss*	This report ranks the destination ports to which attacks have been targetted but denied.	Finished: Sep 8, 2004 1:07:43 PM PDT	Sep 8, 2004 1:07:39 PM PDT	Sep 7, 2004 1:07:39 PM PDT - Sep 8, 2004 1:07:39 PM PDT

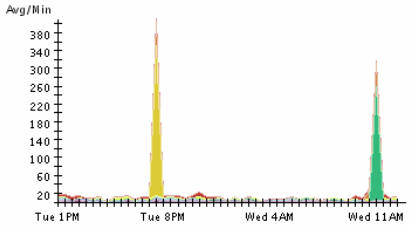
Report type: Destination Ports ranked by Sessions, 1dd:0hh:0mm:0ss

Source IP	Destination IP	Service	Events	Device	Severity	Zone	Operation	Rule	Action	Reported User
ANY	ANY	ANY	AttacksProtected, FirewallPolicyViolation/ACL	ANY	ANY	CA	None	ANY	ANY	ANY

Keywords: [None]







Rank		Count (# of sessions)	Raw Destination Port
	1	4704	445
	2	3524	80
	3	3349	26686
	4	3183	135
	5	2531	47683
	6	1183	1026
	7	1144	0
	8	768	139
	9	684	9898

CS-MARS eszköz támogatás

- Hálózat
  - Cisco IOS 11.x and 12.x, Catalyst OS 6.x
  - NetFlow v5/v7
  - NAC ACS 3.x
  - Extreme Extremeware 6.x
- Tűzfal/VPN
  - Cisco PIX 6.x, 7.x, ASA, IOS Firewall/IPS, FWSM 1.x, 2.3, VPN Concentrator 4.x
  - CheckPoint Firewall-1 NG FPx, VPN-1
  - NetScreen Firewall 4.x, 5.x
  - Nokia Firewall
- IDS/IPS
  - Cisco NIDS 4.x, 5.x, IDSM 4.x, 5.x
  - Enterasys Dragon NIDS 6.x
  - ISS RealSecure Network Sensor 6.5, 7.0
  - Snort NIDS 2.x
  - McAfee Intrushield NIDS 1.x
  - NetScreen IDP 2.x
  - Symantec ManHunt 3.x
- Sérülékenységi kiértékelés (VA)
  - eEye REM 1.x
  - Foundstone FoundScan 3.x
  - Qualys Guard
- Host biztonság
  - Cisco Security Agent (CSA) 4.x
  - McAfee Entercept 2.5, 4.x
  - ISS RealSecure Host Sensor 6.5, 7.0
  - Symantec AnitVirus 9.x
- Host Log
  - Windows NT, 2000, 2003 (agent/agent-less)
  - Solaris
  - Linux
- Syslog
  - Universal device support
- Alkalmazások
  - Web servers (IIS, iPlanet, Apache)
  - Oracle 9i, 10i database audit logs
  - Network Appliance NetCache

CS-MARS megoldás

Modell	CS-MARS 20	CS-MARS 50	CS-MARS 100e	CS-MARS 100	CS-MARS 200	CS-MARS GC
Esemény / Sec.	500	1,000	3,000	5,000	10,000	na
Flow / Sec.	10,000	25,000	75,000	150,000	300,000	na
RAID Storage	120GB+	240GB	750GB	750GB	1TB	1TB

+nem RAID

- **Egyedülálló funkcionalitás, legkisebb TCO**
- **Kész megoldás (appliance)**
  - **Teljes integrált rendszer; nincs szükség egyéb hardverre, platformra, adatbázisra, vagy „ügynök” szoftverre – sem megvásárolni, sem installálni, sem karbantartani**
  - **Nincs szükség állomások, adminisztrátorok, illetve egyéb licenszekre**
  - **Keményített OS, szerep alapú adminisztráció és biztonságos kommunikáció**
- **Egyszerű telepítés, nem Java alapú GUI, (szerver oldali script), RAID 1+0, nincs külső adatbázis igény, Layer 2/3 topológia ismeret és „kárelhárítás”**

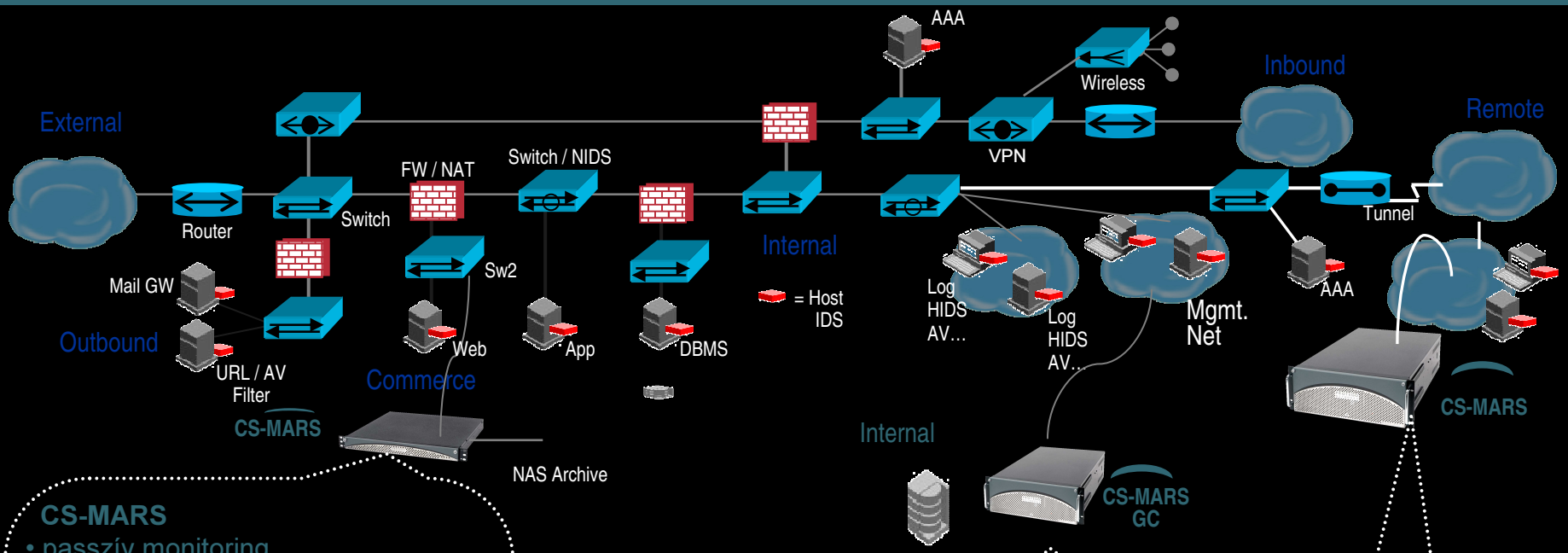
Esemény per másodperc (Event Per Second, EPS) példa

- 1 x CheckPoint NG
- 1 x ISS RealSecure 6.5 & 7.0
- 1 x NetApp Netcache 4 x Pix 525
- 5 x Cisco 12.x
- 4 x Cisco 12.x with ACL’s
- 1 x CSA MC 4.0
- 50 x MS Windows Generic

= 10.650 EPS (ÁTLAGBAN)

MARS: MEGVALÓSÍTÁSI PÉLDÁK

CS-MARS
Global Controller megvalósítás



CS-MARS
- passzív monitoring
- hálózati topológia tudást szerez
- A NAT-ot kezeli, Netflow határértékeket figyel
- A logok, riasztások, és a Netflow között korrelációt végez
- Azonosítja a valódi incidenseket, nincsenek hamis pozitív események
- Valós idejű ábrázolás, visszajátszás és lekérdezés
- Részletekbe menő vizsgálat, kivédés
- Konszolidálja, tárolja az incidensek nyers adatait

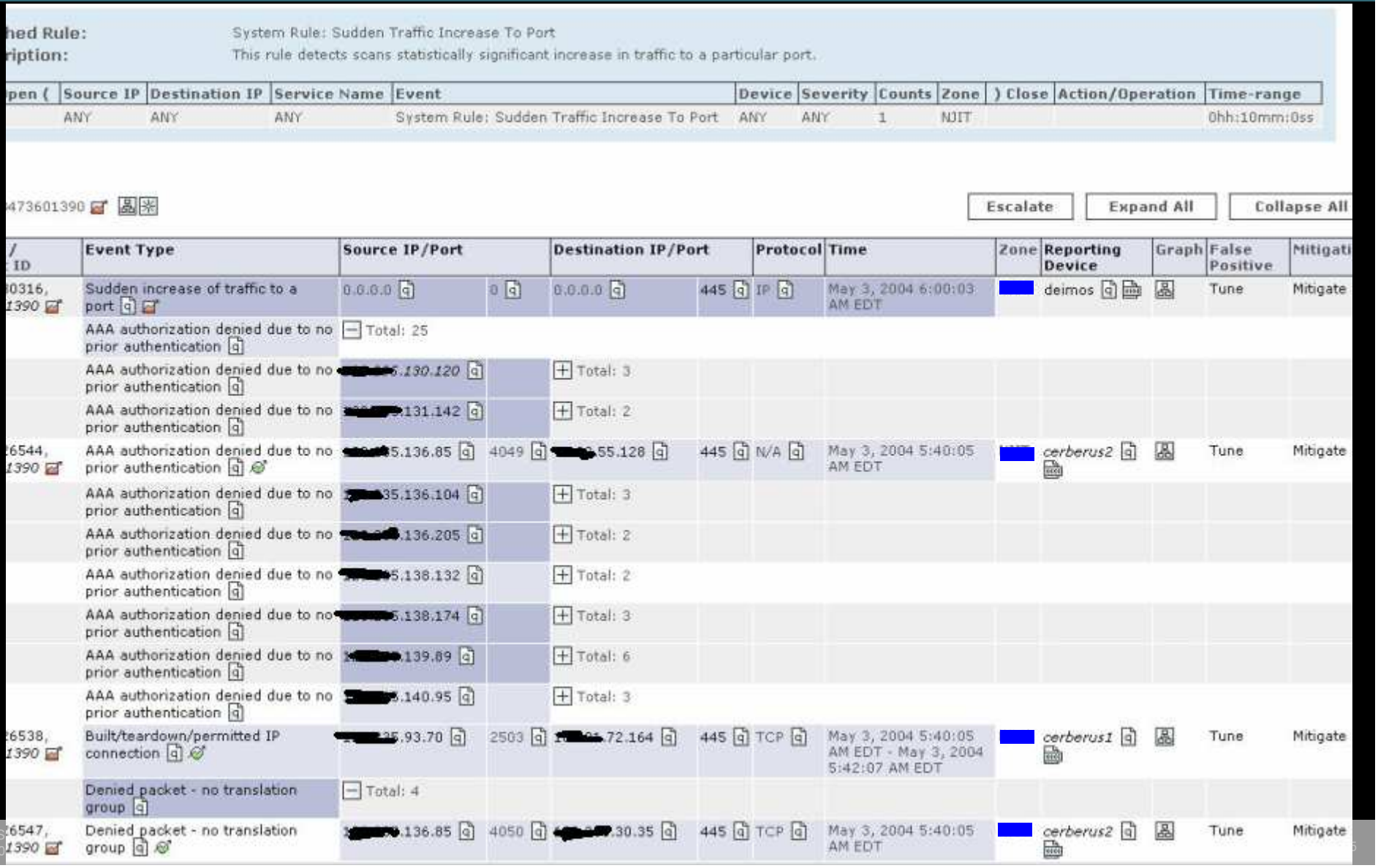
CS-MARS GC, melyet a menedzsment hálózatba kötjük globális nézetet, menedzsmentet és riportolást biztosít. Minden CS-MARS biztonságosan és hatékonyan kommunikál a GC felé. GC az update-eket, szabályokat, a riport sémákat, a hozzáférési szabályokat szétosztja és a lekérdezéseket a teljes MARS hálózaton végzi el.

CS-MARS a távoli állomásokra helyezhető, melyet a CS-MARS GC menedzsel

Elosztott architektúra -> zóna

MARS: SASSER-D DAY ZERO TANULMÁNY

Incidens, mely a Dashboard-on megjelenik



hed Rule: System Rule: Sudden Traffic Increase To Port
ription: This rule detects scans statistically significant increase in traffic to a particular port.

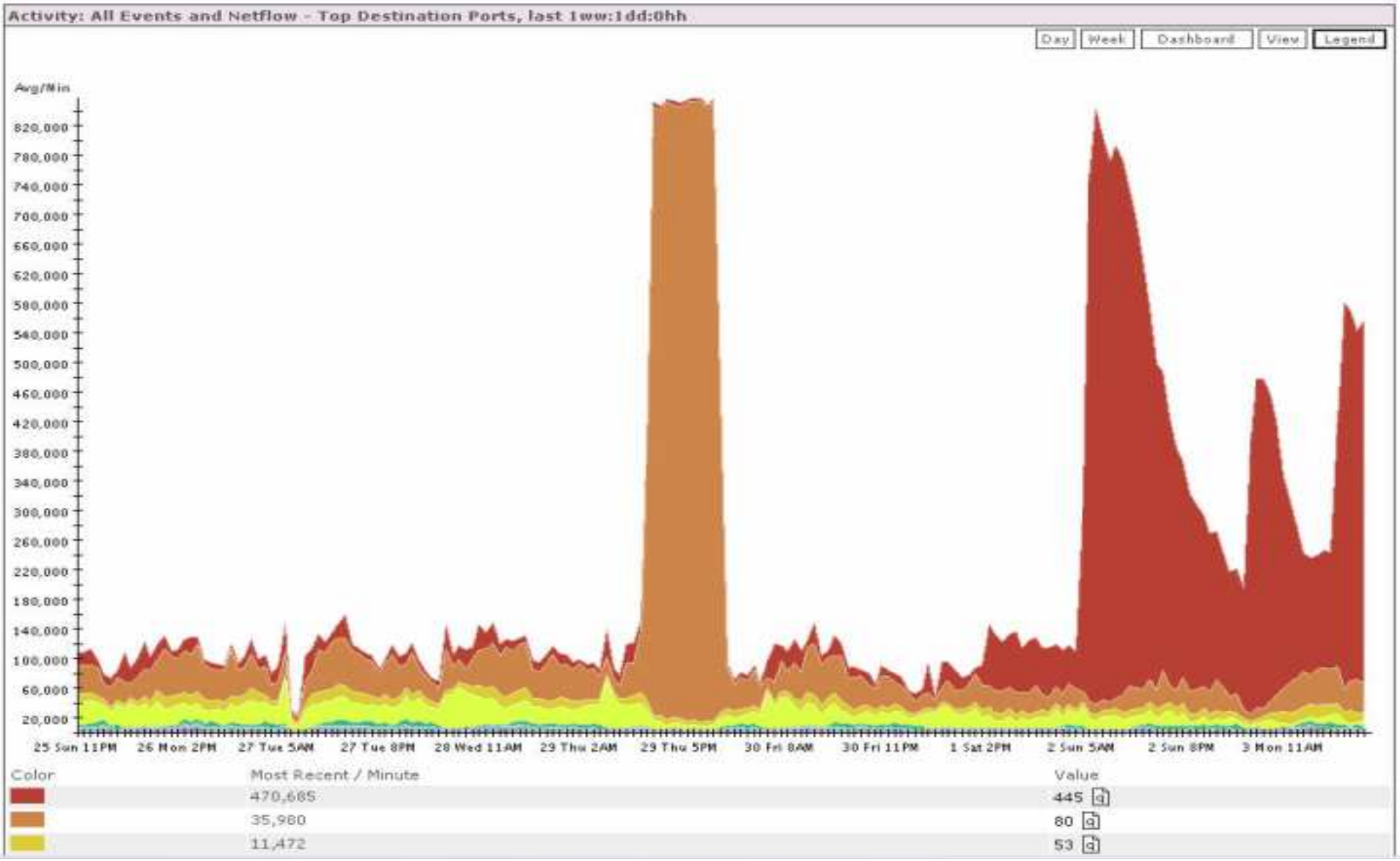
pen (	Source IP	Destination IP	Service Name	Event	Device	Severity	Counts	Zone	) Close	Action/Operation	Time-range
	ANY	ANY	ANY	System Rule: Sudden Traffic Increase To Port	ANY	ANY	1	NJIT			0hh:10mm:0ss

473601390

Escalate | Expand All | Collapse All

/ ID	Event Type	Source IP/Port		Destination IP/Port		Protocol	Time	Zone	Reporting Device	Graph	False Positive	Mitigati
0316, 1390	Sudden increase of traffic to a port	0.0.0.0	0	0.0.0.0	445	IP	May 3, 2004 6:00:03 AM EDT		deimos		Tune	Mitigate
	AAA authorization denied due to no prior authentication	Total: 25										
	AAA authorization denied due to no prior authentication	[redacted].130.120		Total: 3								
	AAA authorization denied due to no prior authentication	[redacted].131.142		Total: 2								
6544, 1390	AAA authorization denied due to no prior authentication	[redacted]5.136.85	4049	[redacted]55.128	445	N/A	May 3, 2004 5:40:05 AM EDT		cerberus2		Tune	Mitigate
	AAA authorization denied due to no prior authentication	[redacted]35.136.104		Total: 3								
	AAA authorization denied due to no prior authentication	[redacted].136.205		Total: 2								
	AAA authorization denied due to no prior authentication	[redacted]5.138.132		Total: 2								
	AAA authorization denied due to no prior authentication	[redacted].138.174		Total: 3								
	AAA authorization denied due to no prior authentication	[redacted].139.89		Total: 6								
	AAA authorization denied due to no prior authentication	[redacted].140.95		Total: 3								
6538, 1390	Built/teardown/permitted IP connection	[redacted].93.70	2503	[redacted].72.164	445	TCP	May 3, 2004 5:40:05 AM EDT - May 3, 2004 5:42:07 AM EDT		cerberus1		Tune	Mitigate
	Denied packet - no translation group	Total: 4										
6547, 1390	Denied packet - no translation group	[redacted].136.85	4050	[redacted].30.35	445	TCP	May 3, 2004 5:40:05 AM EDT		cerberus2		Tune	Mitigate

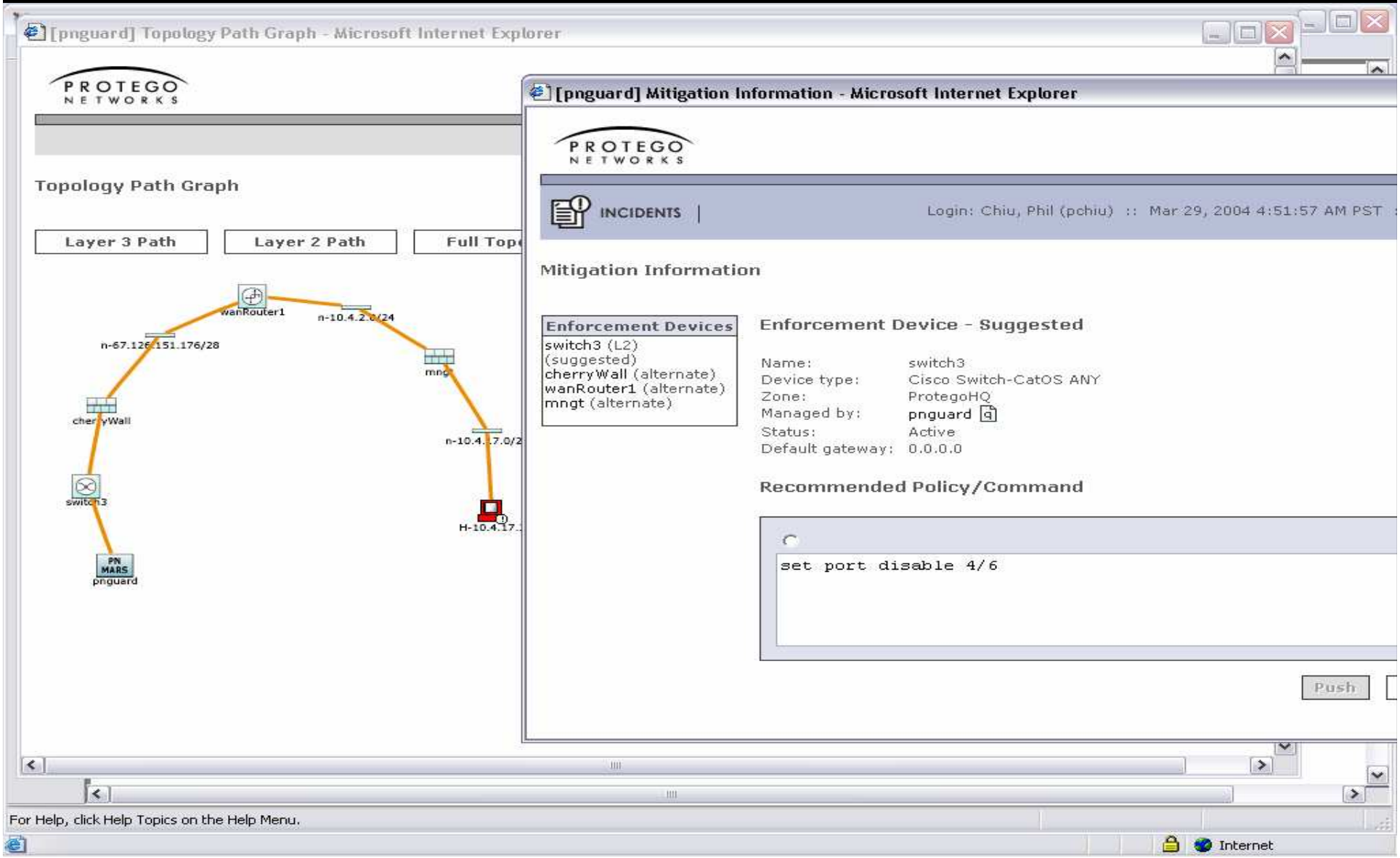
A grafikon önmagáért beszél



A fertőzött host-ok

Rank	Count (# of Sessions)	Raw Source IP	Defined Hosts
1	102572	[redacted].130.160	
2	40339	[redacted].132.44	
3	36881	[redacted].203.82	dhcp-203-82
4	36595	[redacted].202.66	dhcp-202-66
5	35827	[redacted].134.196	
6	35622	[redacted].134.75	
7	35428	[redacted].133.80	
8	35307	[redacted].134.199	
9	35167	[redacted].138.196	
10	34070	[redacted].136.118	
11	33376	[redacted].136.205	
12	32931	[redacted].203.42	dhcp-203-42
13	30390	[redacted].133.16	
14	27682	[redacted].30.120	
15	22031	[redacted].136.166	
16	19681	[redacted].140.154	
17	19135	[redacted].130.82	
18	18229	[redacted].140.5	

Támadási útvonal Layer 2 kivédéssel



DEMONSTRÁCIÓ

ÖSSZEFOGLALÁS

CS-MARS Előnyök

Jobb
- Integrált hálózati tudás
- MAC cím, switch port szerinti támadó izoláció
- A folyamatban lévő támadások megakadályozása
- Támadási útvonal megjelenítése
- Keményített OS és rendszer
- Cél hardver redundáns tervezés

Gyorsabb
- Gyorsított esemény analízis a memóriában
- Szabadalmaztatott algoritmusok
- 10,000 EPS teljes korrelációval
- Skálázható, elosztott esemény analízis architektúra a CS-MARS Global Controller-el

Költséghatékonyabb
- Appliance kivitel
- Nincs rejtett szoftver/testreszabási költség
- Egyszerű licenszezés – nincs szoftver ügynök

CISCO SECURITY

MONITORING, ANALYSIS AND RESPONSE SYSTEM

ÁCS GYÖRGY
GACS@CISCO.COM

„Madártávlattól a MAC címig!”