



A biztonsági veszélyek  
monitorozása, analízálása  
és az erre adott válasz

Cisco Security-MARS



Ács György  
Konzultáns  
[gacs@cisco.com](mailto:gacs@cisco.com)

# Tartalom

- Biztonsági incidens menedzsment kihívásai
- MARS : “Monitoring, Analysis and Response”
- MARS Riportolás
- Esettanulmány
- Demonstráció
- Összefoglalás



# Biztonsági incidens menedzsment kihívásai



# Biztonsági szolgáltatás üzeme – reakciók ma

Hálózati operátorok



**Mindig túl késő**

Reaktív lépések:

1. Fokozott riasztás
2. Vizsgálat
3. Koordináció
4. Elhárítás

Biztonsági operátorok



Routerek,  
Switch-ek

IDS/IPS-ek

VPN

Sérülékeny-  
ségi letapogatók

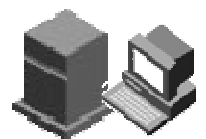
Authentikációs  
szerverek

A hálózati diagramm be-  
gyűjtése, több TONNA  
adat olvasása és  
analizálása... Ismét!

Több ezer Win,  
Több száz UNIX

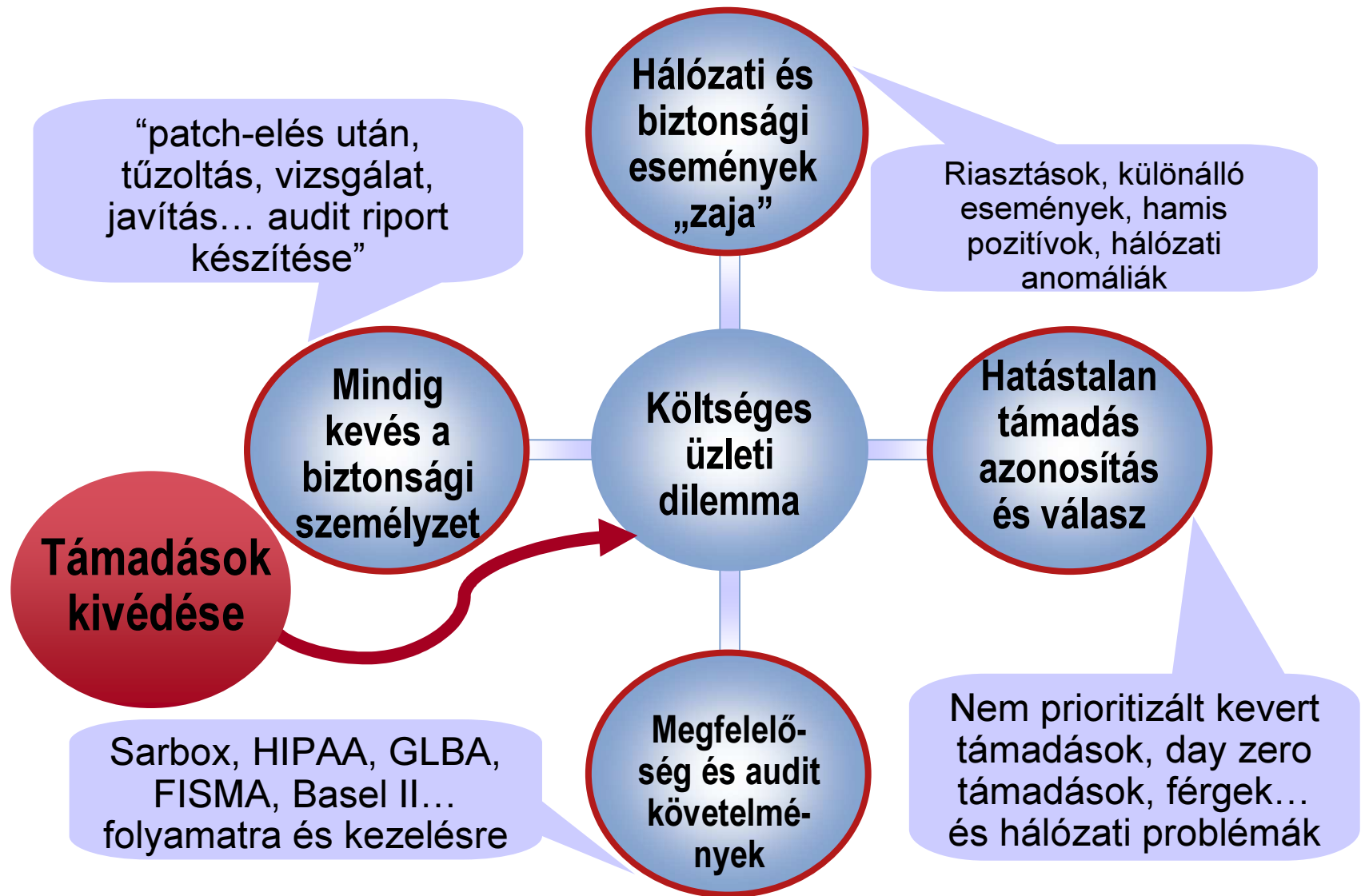
Anti-vírusok

Tűzfalak



Biztonsági  
tudásbázis

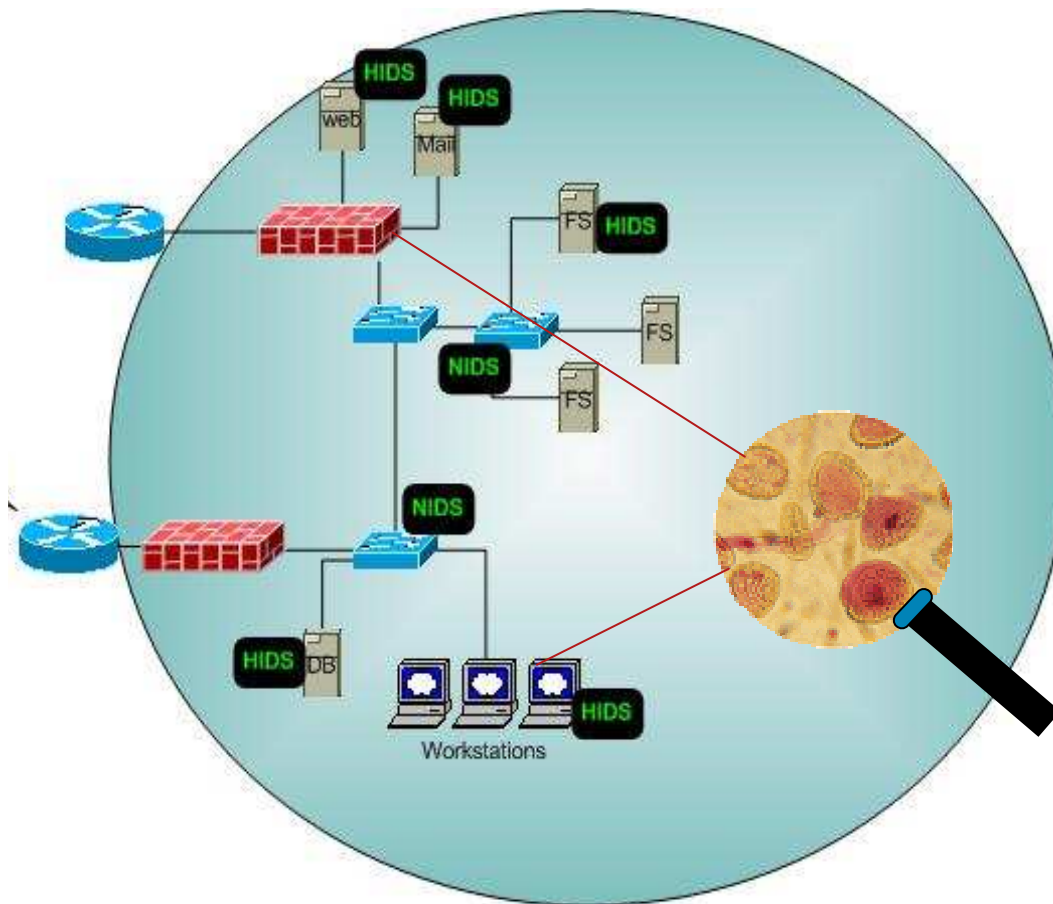
# Biztonsági kihívás = üzleti probléma



# Magyarország

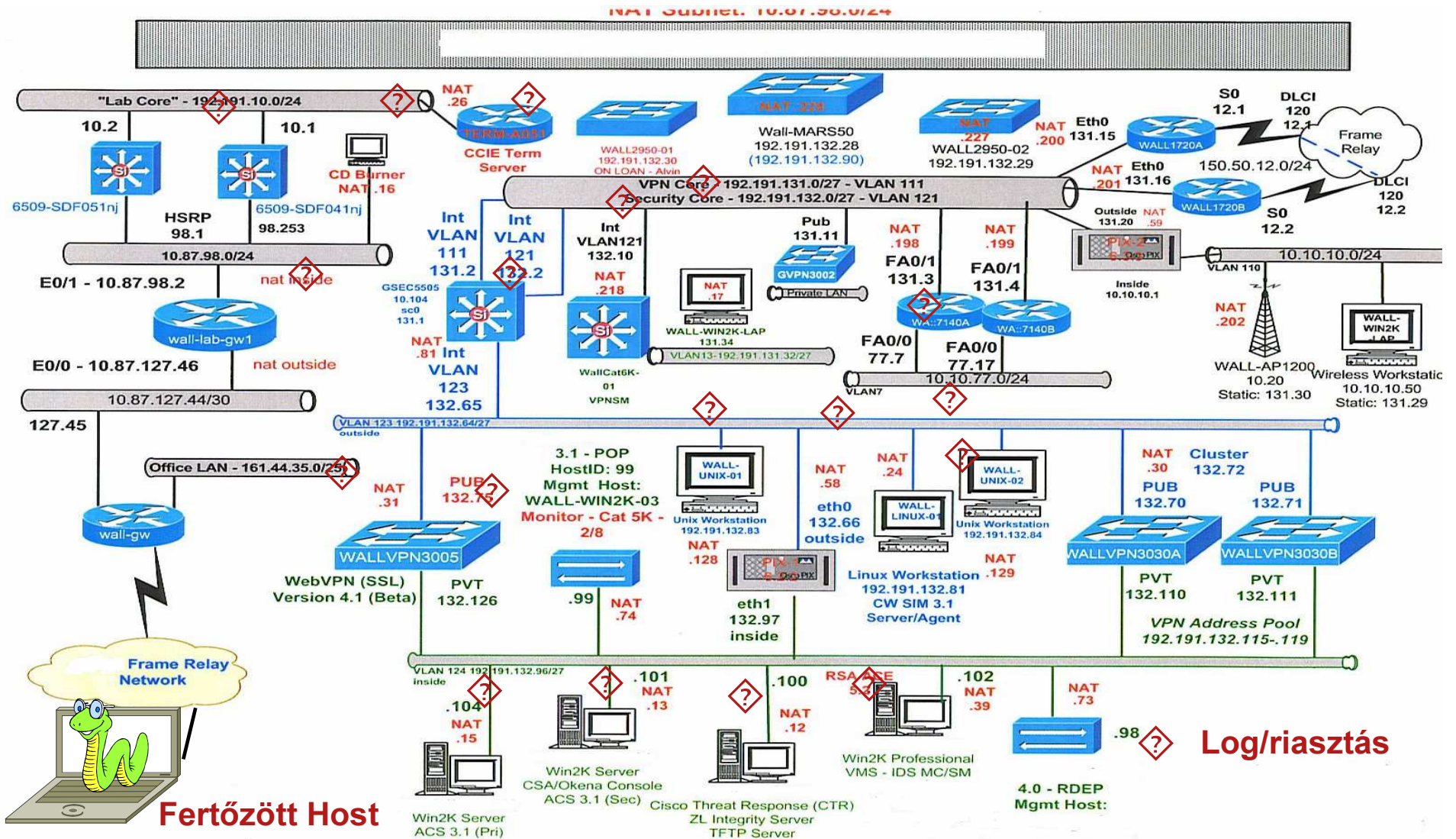
- . Az 1996. évi CXII. a hitelintézetekről és a pénzügyi vállalkozásokról szóló törvény (Hpt.) 13/B. § (5) d,-ben előírja az adott szervezet számára, hogy rendszeres, érdemi feldolgozást végezzen az informatikai eseményekkel kapcsolatban:
- *„... az informatikai rendszer működése szempontjából kritikus folyamatok eseményeit naplózza és alkalmas e naplózás rendszeres (esetleg önműködő) és érdemi értékelésre, illetve lehetőséget nyújt a nem rendszeres események kezelésére.”*
- Ezt a törvényt a 2004. évi XXII. törvényben (“A befektetők és a betétesek fokozott védelmével kapcsolatos egyes törvények módosításáról”) az 1. §-ban módosították, a tőkepiacról szóló 2001. évi CXX. törvénnyel együtt, amely a 101/A. § (5) d,-ben ugyanezeket a követelményeket fogalmazza meg.

# 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	+				


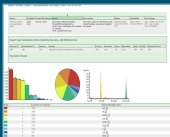
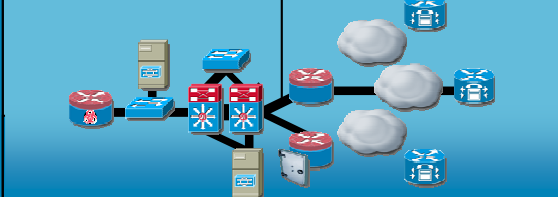
# Amikkel foglalkozni kell: tűzfal Log

```
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 (67.82.225.18/1182)
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 (67.82.225.18/1183)
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 Reset-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 Reset-I
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 (67.82.225.18/1184)
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
305011: Built dynamic UDP translation from inside:192.168.1.3/1618 to outside:67.82.225.18/1052
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 (67.82.225.18/1185)
304001: 192.168.1.3 Accessed URL 64.154.80.250:/HG?hc=we69&hb=DM5401281KAA%3BDM54012890CU&cd=1&hv=6&n=/Cisco.com+Public&con=&vcd=&w=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=09010107r&seg=*;1&epg=n&ja=y&dt=5&zo=240&lm=0&cu=&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%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%20Media%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 (67.82.225.18/1186)
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 FIN
304001: 192.168.1.3 Accessed URL 64.154.80.250:/HG?hc=we69&hb=DM5401281KAA%3BDM54012890CU&cd=1&hv=6&n=/Cisco.com+Public&con=&vcd=&w=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=09010107r&seg=*;1&epg=n&ja=y&dt=5&zo=240&lm=0&cu=&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%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%3AHP%20Peripheral%20Interrogator%3AWindows%20Media%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
```

# CS-MARS



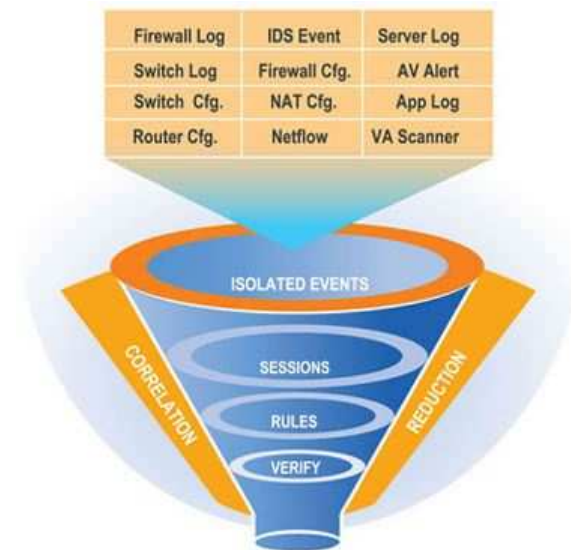
# Cisco Security menedzsment készlet

<h2>Cisco Security Manager</h2> 	<h2>Cisco Security Mars</h2> 	
<p>Egyszerűsített Policy Adminisztráció</p> <p>Végponttól végpontig konfiguráció</p> <p>Hálózatszintű vagy eszköz specifikus</p>	<p>Konfiguráció Megvalósítás</p> <p>Monitoring Analysis Mitigation</p>  <p>Self-Defending Network</p>	<p>Gyors <b>veszély azonosítás</b> és enyhítés</p> <p>Topológia ismeret</p> <p>Adat korreláció</p>

- Integrált biztonsági menedzsment és monitorozás
- ACS

# 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



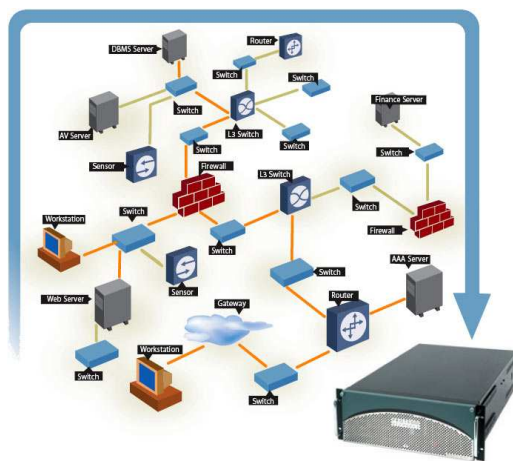
- Főbb jellemzők

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

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

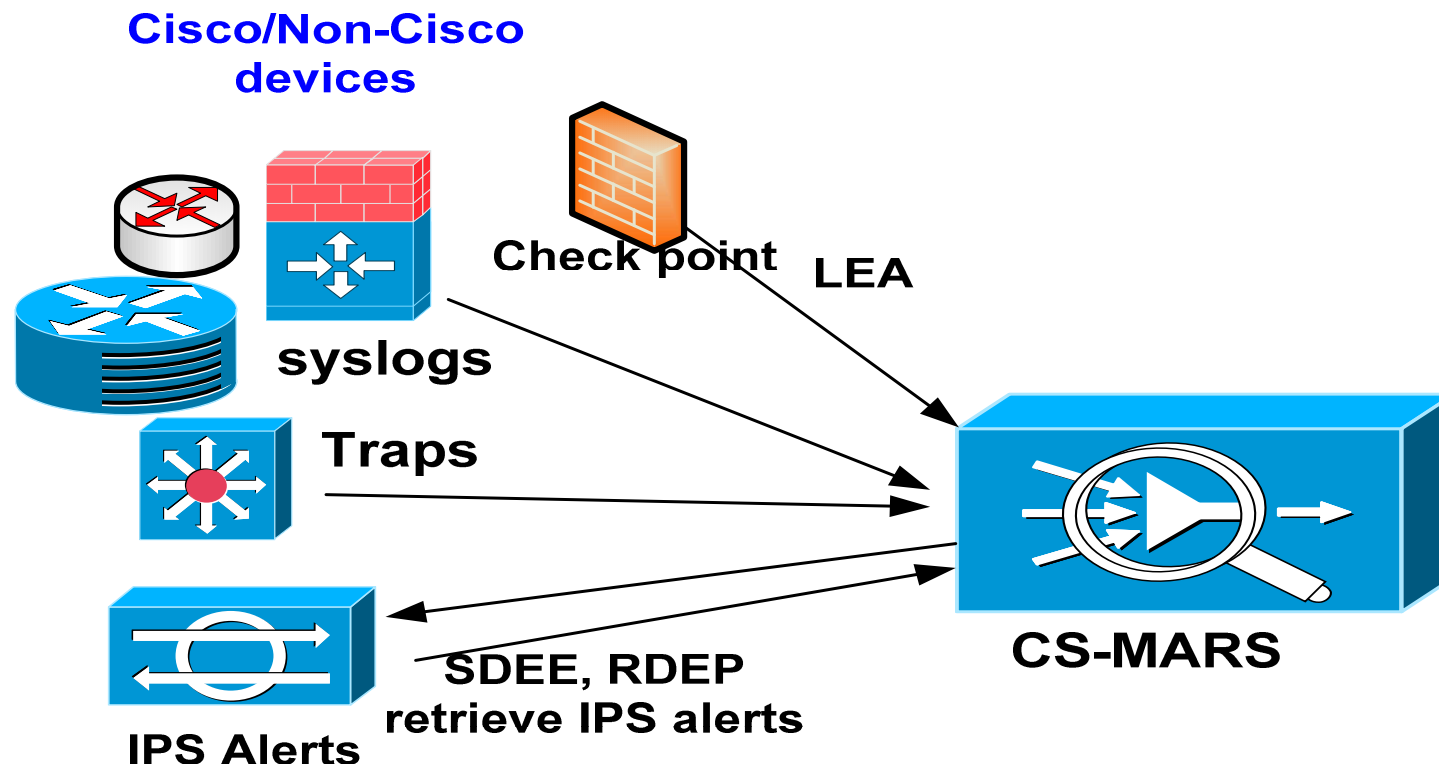
**Enyhítés** L2 és L3 „lezáráspontokon”

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



# Alapfogalmak – Események Events

- **Események**— A monitorozott riportoló eszközök (syslog, trap...) MARS-nak küldött üzenetei, <VAGY> a monitorozott riportoló eszközökről (IPS alerts, Windows log....) a MARS által “leszedett” (“pull”) események



# Rendszer logok: a kételű kard



- Nem elégséges logolás nem ad igazi eredményt, értéket
- Túl sok a jóból -> rosszává válhat

## Események - syslog

Dec 5, 2007 1:06:34 [10.1.2.2] %FWSM-6-302015: Built  
outbound UDP connection 219025352 for  
inside: 10.10.21.108/4664 (10.61.1.1/25572) to  
outside: 144.254.6.144/1029 (144.254.6.144/1029)

Dec 5, 2007 1:07:38 [10.1.2.2] %FWSM-6-302016:  
Teardown UDP connection 219025322 for  
inside: 10.10.21.108/4660 to  
outside: 144.254.6.144/1029 duration 0:02:03 bytes 64

Dec 5, 2007 1:08:34 [10.1.2.2] %FWSM-6-302015: Built  
outbound UDP connection 219025330 for  
inside: 10.10.21.108/4673 (10.61.1.1/25597) to  
outside: 144.254.6.144/1029 (144.254.6.144/1029)



# Cisco ASA 5580 tűzfal család

Nagy teljesítményű tűzfal és skálázható távoli hozzáférés VPN szolgáltatás

- **Piacvezető teljesítmény**

A legmagasabb kapcsolat arány a piacon

Adatközpont szintű teljesítmény (10/ 20 Gbps), ultra kicsi késleltetéssel

- **Nagy sebességű auditálás és esemény monitorozás**

NetFlow alapú monitorozás gyűjtés

- **Skálázható távoli hozzáférés**

10,000 párhuzamos felhasználó



Mind tűzfal, mind VPN képességekben piacvezető

# Cisco ASA 5580 újdonsága: NetFlow biztonsági esemény naplózása

- Biztonsági esemény korreláció és adatcsökkentés (több gigabites forgalom)

A NetFlow v9 támogatása az ASA5580 platformon

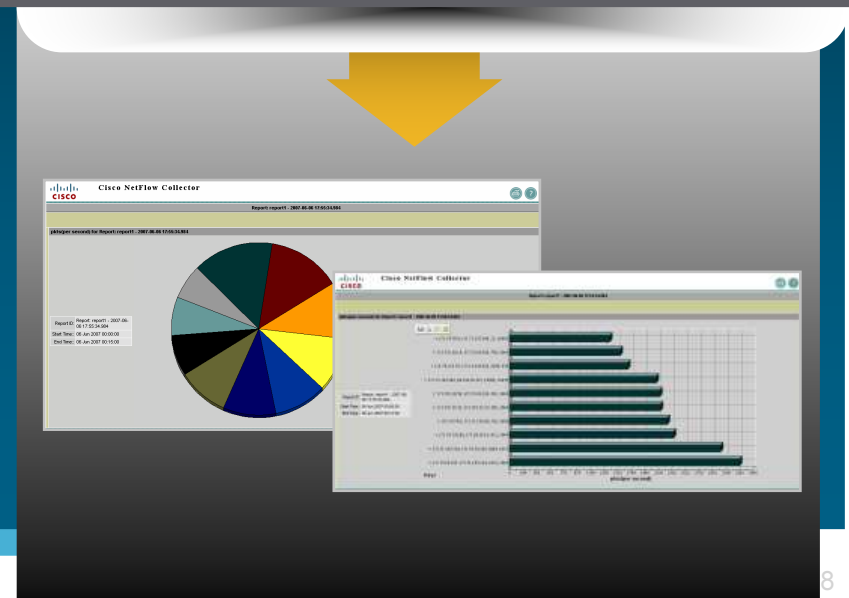
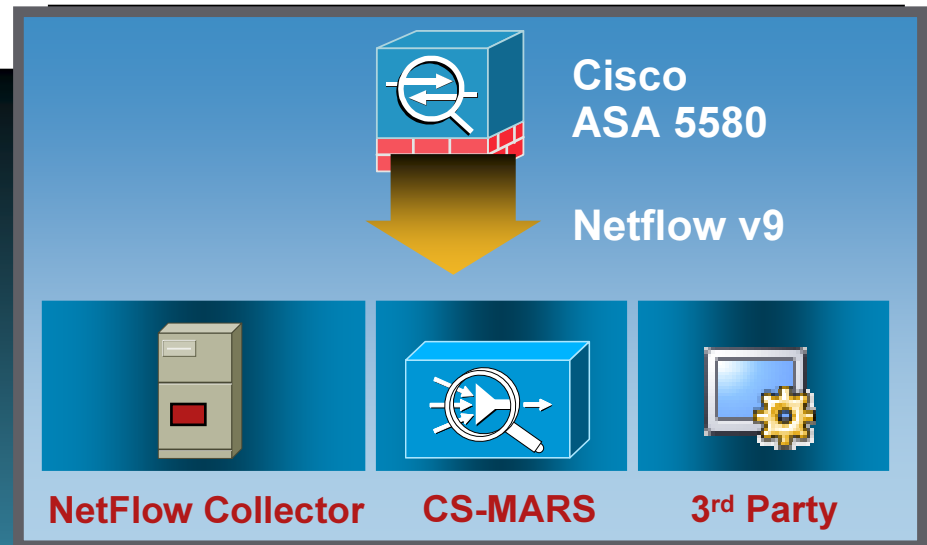
A több, mint **10 éves** NetFlow fejlesztés újítása

Lehetővé teszi a megfelelőségi riportok készítését

- Az ipari szabvány kialakítása

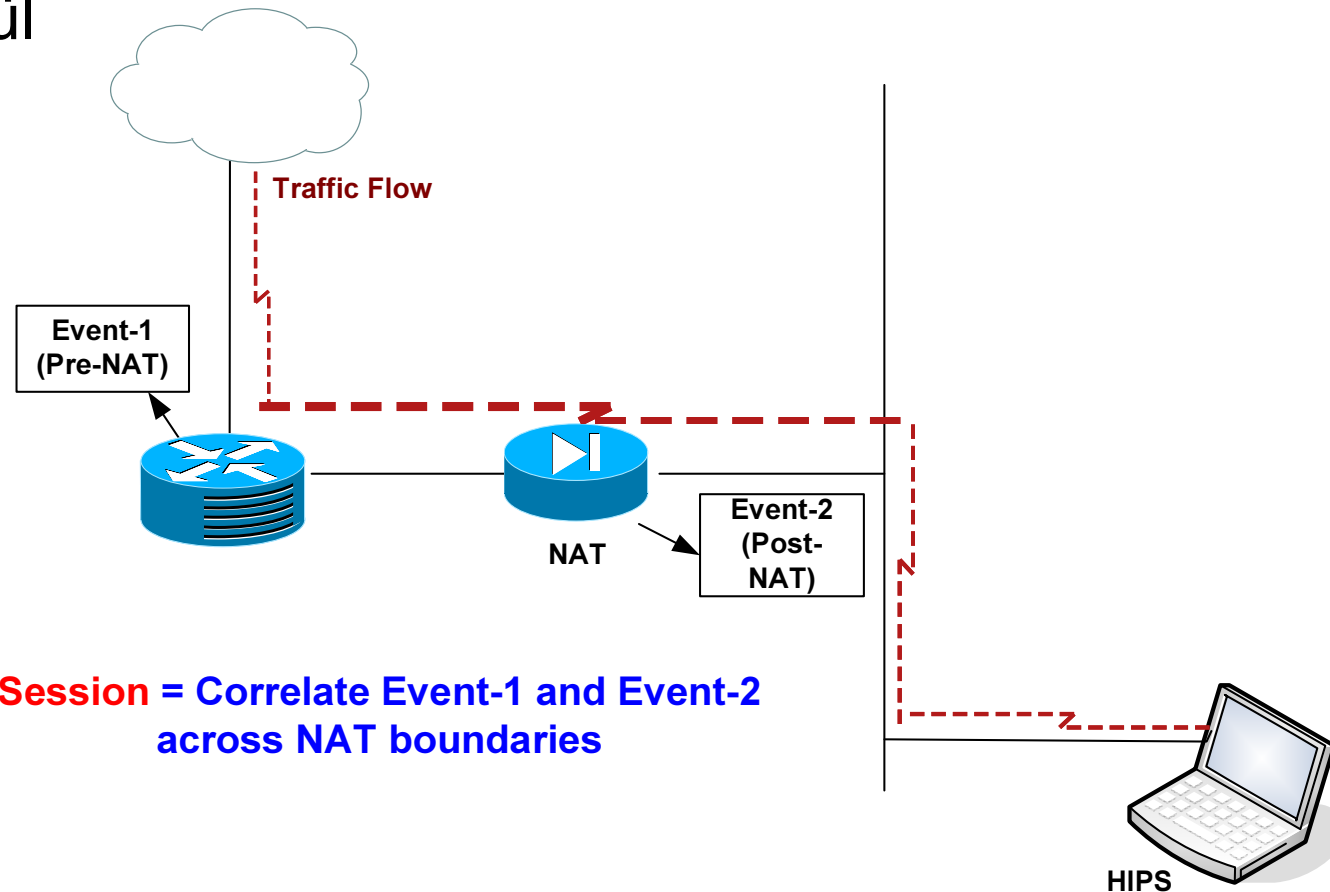
A szabványosítási munkálatok **vezetése** az IETF IPFIX Working Group

A vezető **NetFlow monitoring szállítókkal** történő egyeztetés

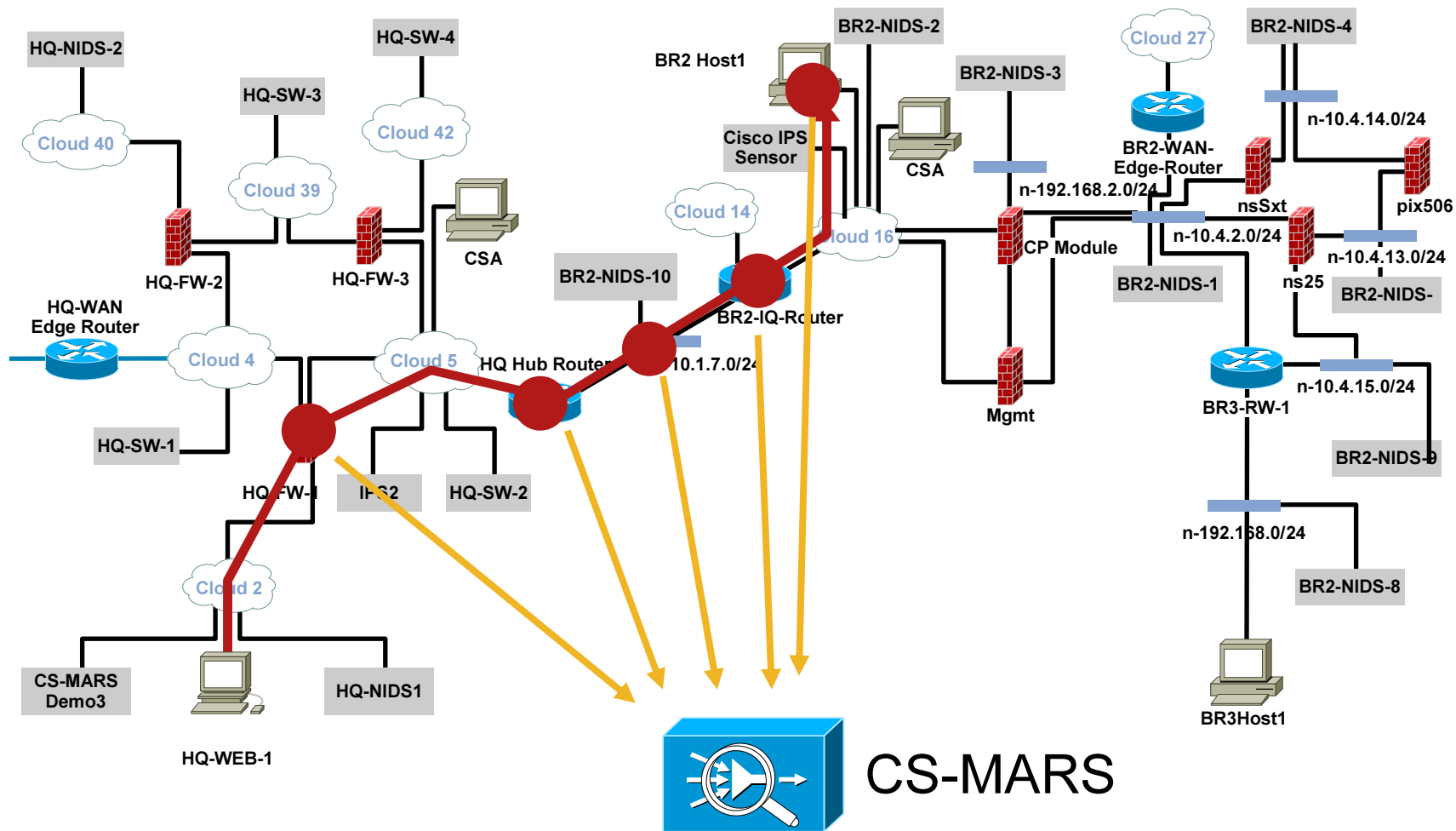


# Alapfogalmak - Sessionization

- **Sessions**— üzenetek (események) halmaza, melyet (melyeket) a MARS korrelált MARS a NAT határokon keresztül

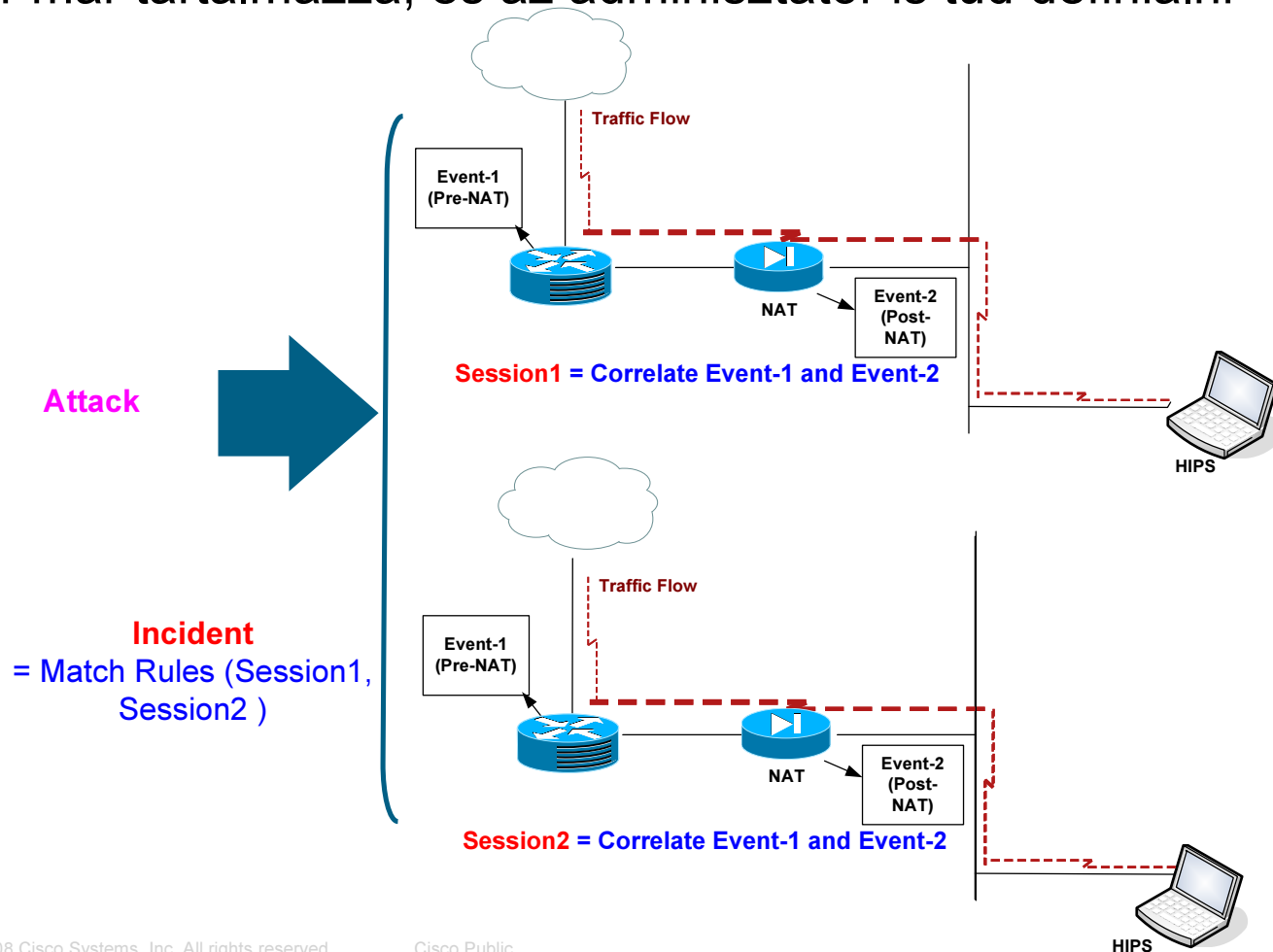


# Miből lesz egy session ?



# Alapfogalmak - Incidensek

- **Incidensek** — a session-ok halmaza, mely(ek) illeszkednek egy előre meghatározott vizsgálati szabályra. A szabályokat (Rule) a MARS rendszer már tartalmazza, és az adminisztrátor is tud definiálni

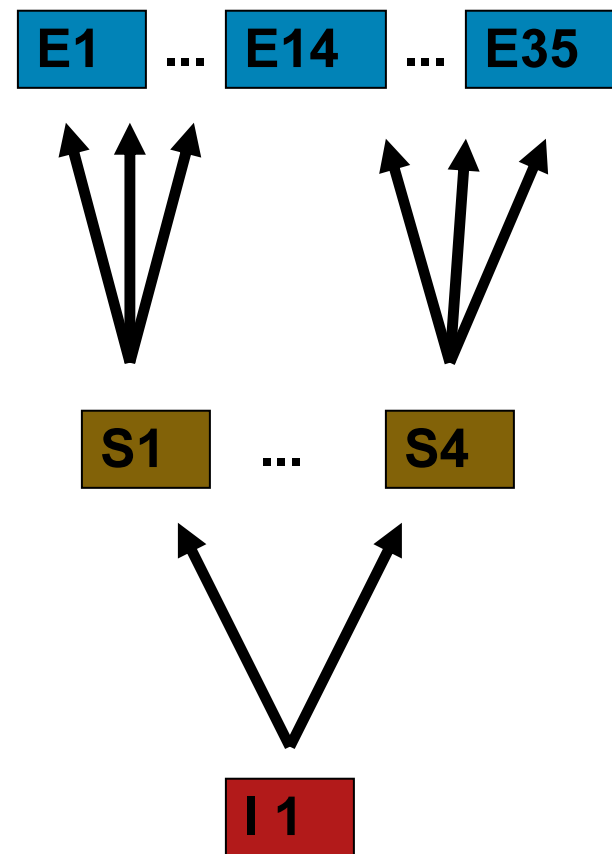


# Szabályból incidens...

<b>Rule Name:</b>	System Rule: Worm Propagation - Attempt	<b>Status:</b>	Active
<b>Action:</b>	None	<b>Time Range:</b>	0m:10s
<b>Description:</b>	This correlation rule detects worm propagation via means such as SMTP, TFTP, and network shares.		

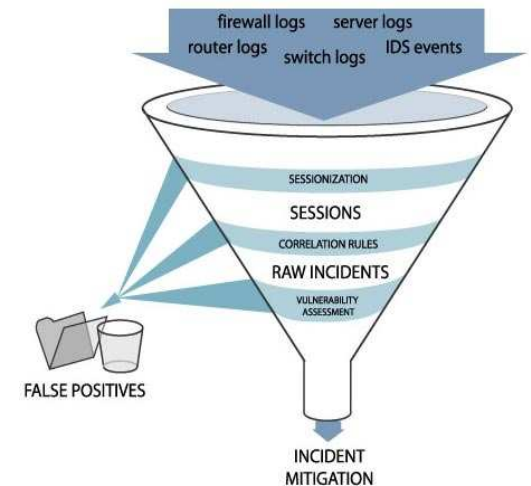
# CS-MARS terminológiák

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




# Ahogy a CS-MARS működik

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





# CS-MARS – analízis egy lapon



SUMMARY INCIDENTS QUERY / REPORTS RULES MANAGEMENT ADMIN HELP

Dashboard | Network Status | My Reports
May 13, 2006 3:20:25 AM PDT

SUMMARY | CS-MARS Standalone: demo1 v4.1
Login: Administrator (padmin) :: [Logout](#) :: [Activate](#)

Select Case: No Case Selected... [View Cases](#) [New Case](#)

**Page Refresh Rate**

15 minutes

---

**24 Hour Events**

Netflow 0

Events 2,694,083

Sessions 992,511

Data Reduction 63%

---

**24 Hour Incidents**

High 61 24%

Medium 0 0%

Low 188 75%

Total 249 100%

---

**All False Positives**

To be confirmed 57,507 75%

System determined 0 0%

Logged 0 0%

Dropped 19,080 24%

User confirmed 0 0%

Total 76,587 100%

---

**To-do List**

C:1429647 (Assigned) Please investigate [🔗](#)

C:1429362 (Assigned) New Case [🔗](#)

C:1428976 (Resolved) Attack 101 [🔗](#)

C:1428556 (New) Test Case [🔗](#)

C:1428550 (New) CS-MARS is untouchable [🔗](#)

C:1428544 (New) Cisco Press Rocks [🔗](#)

C:1428395 (New) New Case [🔗](#)


**Recent Incidents**

All Severities
All Rules
All Case Statuses

Incident ID	Event Type	Matched Rule	Action	Time	Path	Cases
I:109840	Deny packet due to security policy <a href="#">🔗</a>	NetworkConfigError, Copied: 06.03.12/23:05:28 <a href="#">🔗</a>		May 13, 2006 3:05:36 AM PDT	<a href="#">🔗</a> <a href="#">🔗</a>	
I:109841	Deny packet due to security policy <a href="#">🔗</a>	NetworkConfigError, Copied: 06.04.20/09:23:56 <a href="#">🔗</a>		May 13, 2006 3:05:36 AM PDT	<a href="#">🔗</a> <a href="#">🔗</a>	
I:109842	Built/teardown/permitted IP connection <a href="#">🔗</a>	test Rule1 <a href="#">🔗</a>	Email Admin	May 13, 2006 3:05:17 AM PDT - May 13, 2006 3:05:34 AM PDT	<a href="#">🔗</a> <a href="#">🔗</a>	
I:109838	Built/teardown/permitted IP connection <a href="#">🔗</a>	System Rule: Client Exploit - Sasser Worm <a href="#">🔗</a>	Email Admin, admin email	May 13, 2006 3:04:11 AM PDT	<a href="#">🔗</a> <a href="#">🔗</a>	
I:109837	IIS Dot Dot Crash <a href="#">🔗</a> , WWW WinNT cmd.exe Exec <a href="#">🔗</a> , WWW IIS Unicode Directory traversal <a href="#">🔗</a> , IIS CGI Double Decode <a href="#">🔗</a>	System Rule: Server Attack: Web - Attempt <a href="#">🔗</a>		May 13, 2006 3:03:15 AM PDT	<a href="#">🔗</a> <a href="#">🔗</a>	

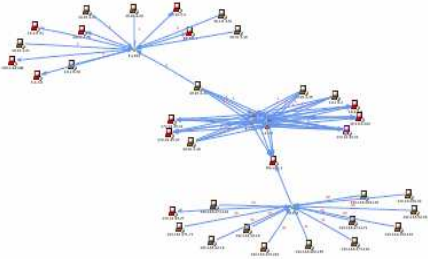
**HotSpot Graph**

[Full Topo Graph](#) [Large Graph](#) [Help](#)

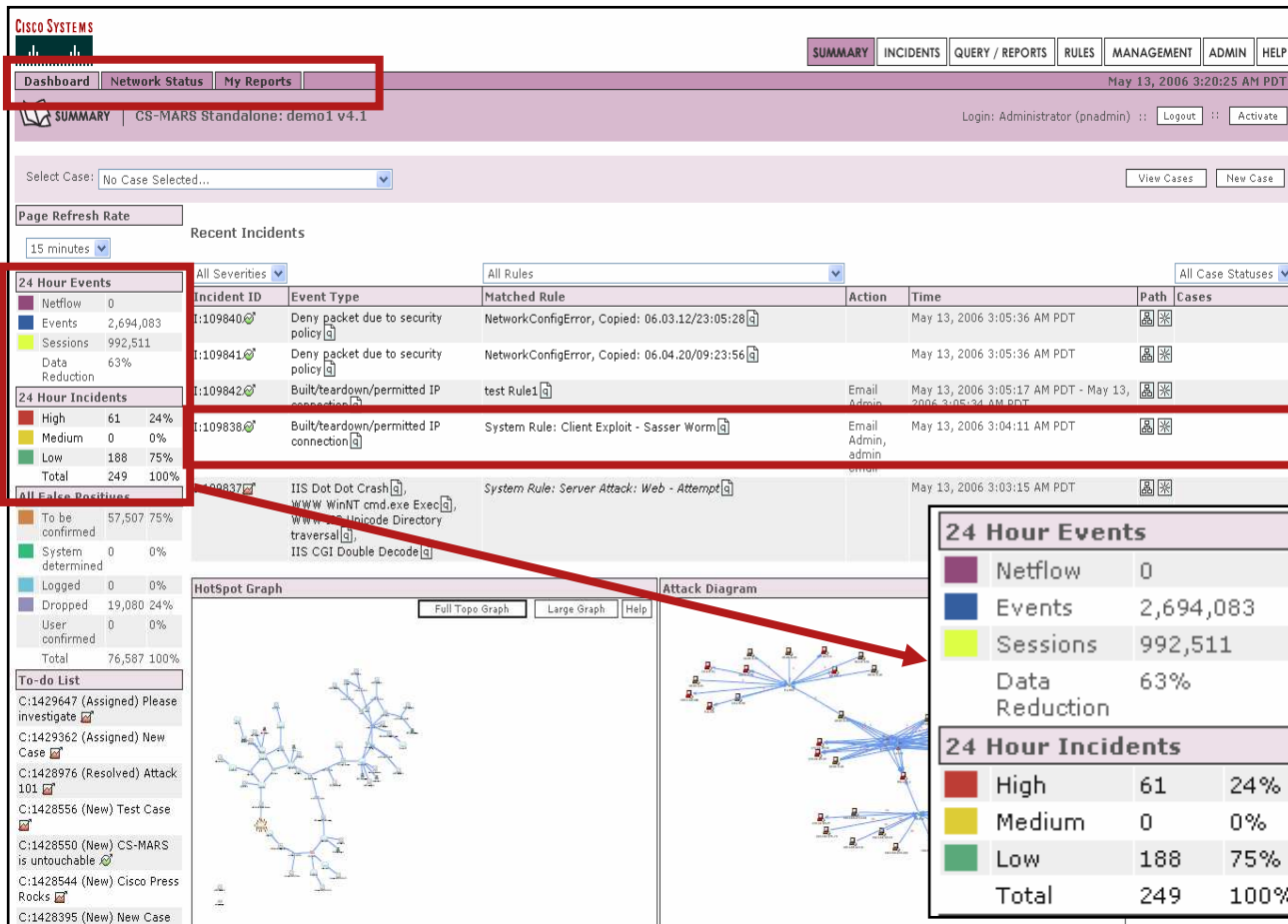


**Attack Diagram**

[Large Graph](#) [Help](#)



# Jelentős adat csökkenés



## Incident Dashboard

- Aggregate
- Correlate
- Summarize

2,694,083 Events



992,511 Sessions



249 Incidents



61 High Severity Incidents



**Hatásos adatcsökkenés, az adminisztrátornak csak a magas prioritású incidensekkel kell foglalkoznia**

# CS-MARS korreláció és egyszerűsítés

**Részletes szabály keretrendszer és incidens részletezés**

**Jelentős egyszerűsítés**

Incidents: **False** Nov 22, 2004 4:36:40 PM PST

INCIDENTS | PN-MARS Standalone: demo2 v3.2 Login: Gordon, Scott (sgordon) :: Logout :: Activate

Incident ID: 59235282 Show  
Session ID: Show

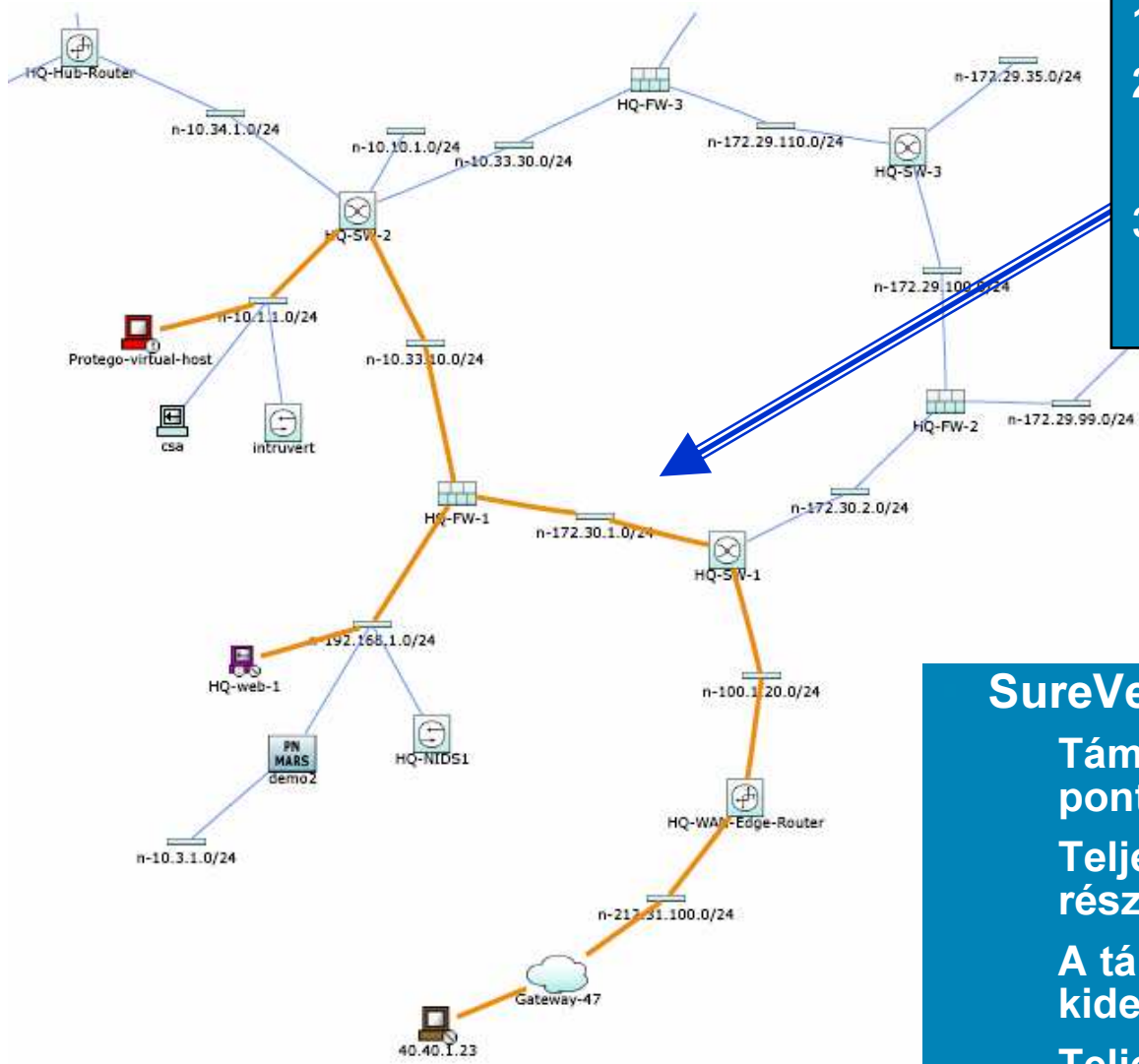
Matched Rule: Successful Recon and Buffer Overflow  
Description: Successful Recon and Buffer Overflow

Offset	Open	Source IP	Destination IP	Service Name	Event	Device	Severity	Counts	Action/Operation	Time-range
1		\$TARGET02	\$TARGET01	ANY	Probe/HostSweep/Non-stealth	ANY	ANY	1	OR	
2		\$TARGET02	\$TARGET01	ANY	Probe/PortSweep/Stealth	ANY	ANY	1	FOLLOWED-BY	
3		\$TARGET02	\$TARGET01	ANY	Penetrate/BufferOverflow/DNS, Penetrate/BufferOverflow/FTP, Penetrate/BufferOverflow/Mail, Penetrate/BufferOverflow/RPC, Penetrate/BufferOverflow/Login, Penetrate/BufferOverflow/Web	ANY	ANY	1	FOLLOWED-BY	
4		\$TARGET01	ANY	ANY	Info/AllSession	ANY	ANY	1		0h:05m

Incident ID: 59235282 Escalate Expand All Collapse All

Offset	Session / Incident ID	Event Type	Source IP/Port	Destination IP/Port	Protocol	Time	Reporting Device	Path / Mitigation	Tune
1		ICMP Ping Network Sweep	40.40.1.23	192.168.1.10		Total: 2			
1	S:73993850, I:59235282	ICMP Ping Network Sweep	40.40.1.23	192.168.1.10	ICMP	Nov 22, 2004 7:02:52 AM PST	HQ-SW-1-idsm		False Positive
1	S:73993851, I:59235282	ICMP Ping Network Sweep	40.40.1.23	192.168.1.10	ICMP	Nov 22, 2004 7:02:52 AM PST	HQ-NIDS1		False Positive
3	S:73993900, I:59235282	WWW IIS_ida Indexing Service Overflow	40.40.1.23	192.168.1.10	TCP	Nov 22, 2004 7:02:52 AM PST	HQ-FW-1, HQ-NIDS1, HQ-SW-1-idsm		False Positive
4		Built/teardown/permitted IP connection	192.168.1.10	10.1.1.10		Total: 3			
4	S:73993871, I:59235282	Built/teardown/permitted IP connection	192.168.1.10	10.1.1.10	TCP	Nov 22, 2004 7:02:52 AM PST	HQ-FW-1		False Positive
4	S:73993872, I:59235282	Built/teardown/permitted IP connection	192.168.1.10	10.1.1.10	TCP	Nov 22, 2004 7:02:52 AM PST	HQ-FW-1		False Positive
4	S:73993873, I:59235282	Built/teardown/permitted IP connection	192.168.1.10	10.1.1.10	TCP	Nov 22, 2004 7:02:52 AM PST	HQ-FW-1		False Positive

# CS-MARS - a végpontok összekötése



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

## SureVector™ analízis

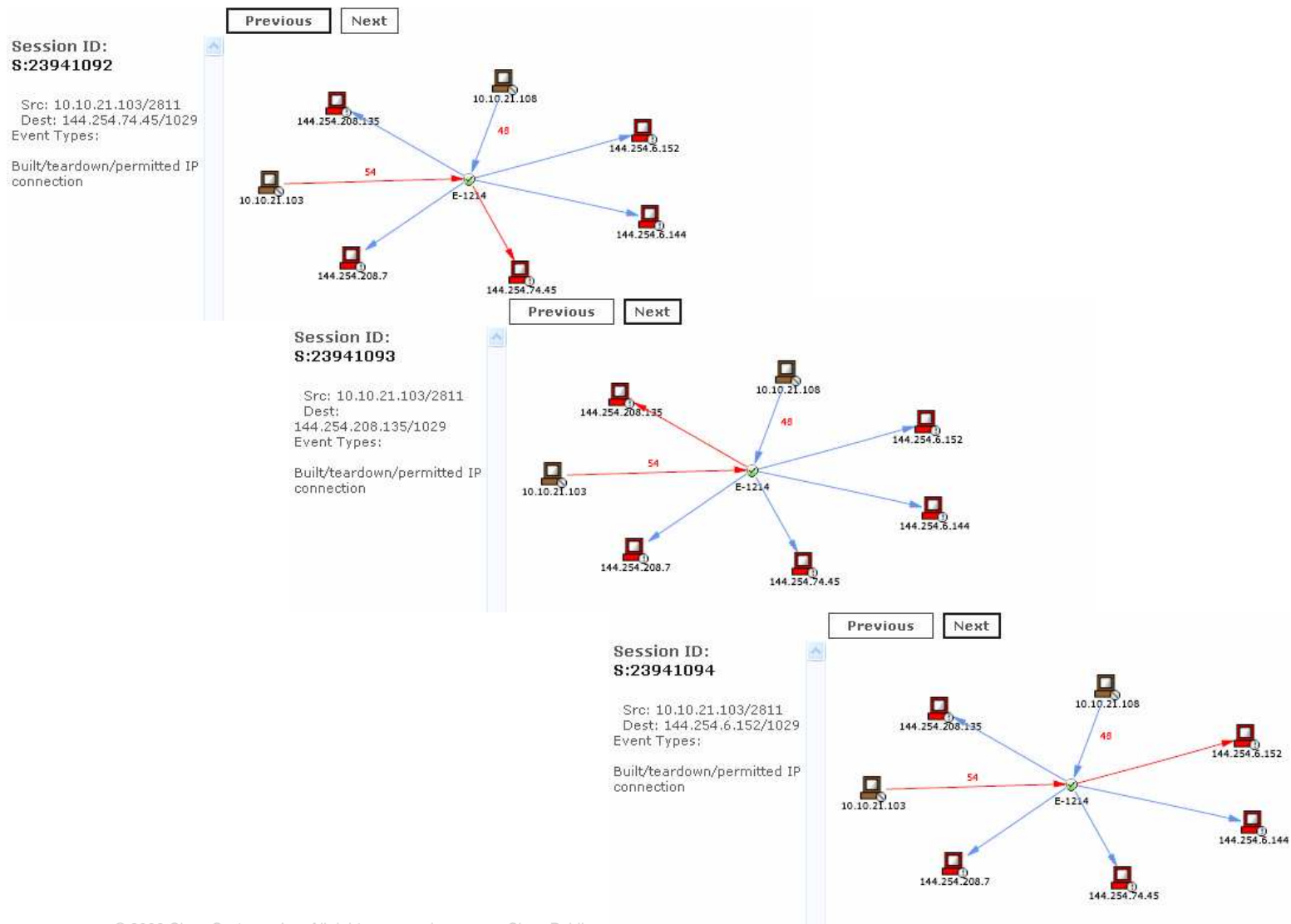
Támadási útvonal bemutatása és pontosítása

Teljes incidens és esemény részletezés

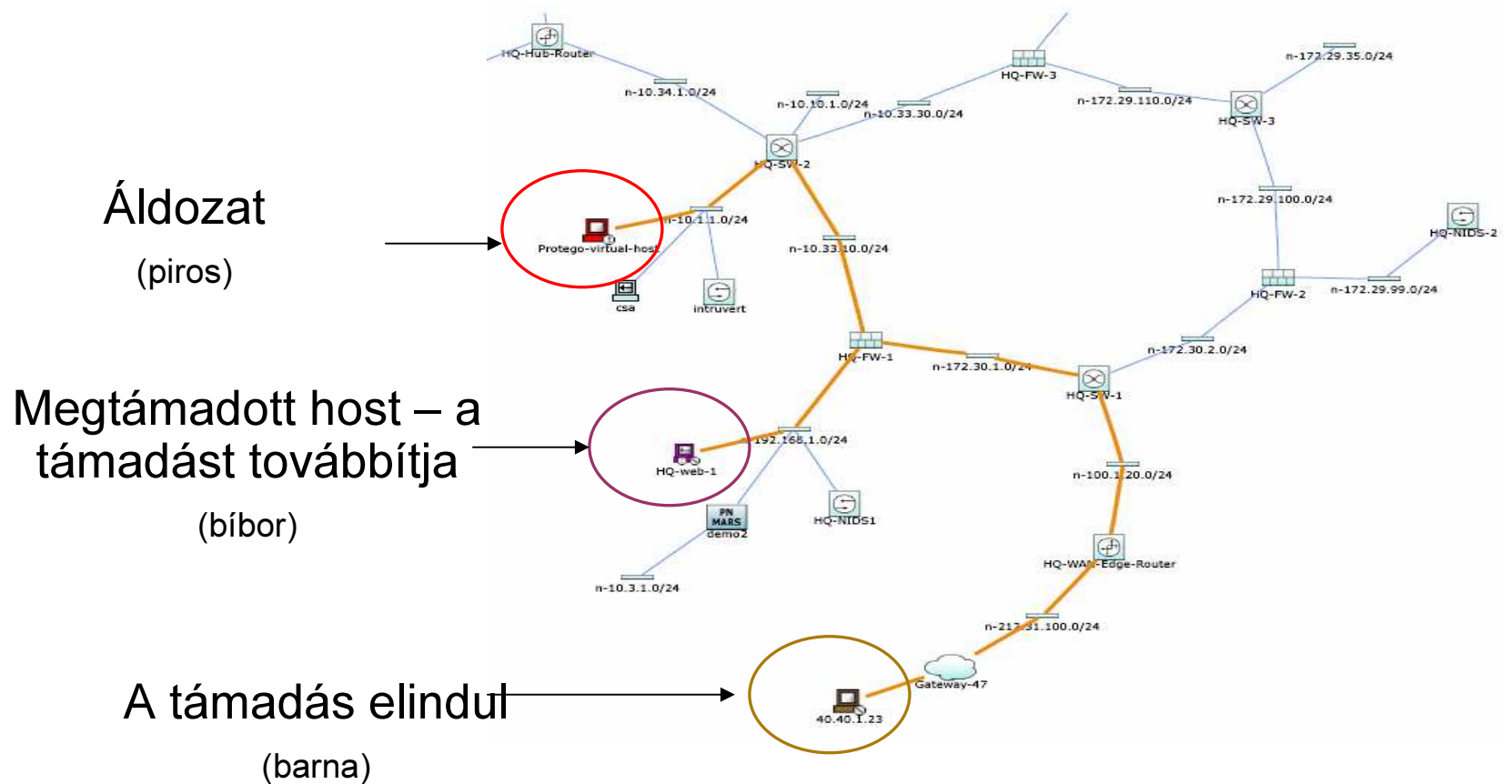
A támadás pontos forrásának kiderítése

Teljes és pontos történet

# Bizonyíték Információ - támadás visszajátszás



# Támadási útvonal és topológia ismeret



# Most már teljes képünk van...

Previous    Next    Toggle Topology

**Session ID:**  
**S:23941092**

Src: 10.10.21.103/2811  
Dest: 144.254.74.45/1029  
Event Types:

Built/teardown/permitted IP connection

**Session ID:**  
**S:23941093**

Src: 10.10.21.103/2811  
Dest: 144.254.208.135/1029  
Event Types:

Built/teardown/permitted IP connection

**Session ID:**  
**S:23941094**

Src: 10.10.21.103/2811  
Dest: 144.254.6.152/1029  
Event Types:

# És most állítsuk meg! – Támadás enyhítés

**Enforcement Devices**

**Suggested**

amslab-6509a.cisco.com

**Alternate**

FWSM-amslab.cisco.com

**S:23961224 Path**

Layer 3 Path

```
graph TD; H1[10.53.230.133] --- G15[Gateway 15]; G15 --- S1[n-10.61.1.0/24]; S1 --- SW[amslab-6509a]; SW --- S2[n-10.1.2.0/24]; SW --- S3[n-10.10.1.0/24]; S3 --- G2[Gateway 2]; G2 --- H2[10.10.10.21];
```

**L3 Enforcement Device Information**

Device	Type	Manager
amslab-6509a.cisco.com	Cisco Switch-IOS 12.2	PN-MARS on pnmars

**Interface Information**

Direction	Interface Name	MAC Address
Inbound	FastEthernet1/24	00:d0:00:0e:c0:00
Outbound	Vlan2	00:d0:00:0e:c0:00

**Recommended L3 Policies/Commands**

ip access-list extended <aclname\_on\_FastEthernet1/24>  
deny tcp host 10.10.10.21 host 10.53.230.133 eq 139

Or

ip access-list extended <aclname\_on\_FastEthernet1/24>  
deny tcp host 10.10.10.21 any



# CS-MARS - alkalmazott védelem

- Vezérlési lehetőségek

  - Layer 2/3 támadási út világosan látható

  - A kivédési eszközök definiálhatók

  - A pontos kivédési parancs megadható

Enforcement Device: **switch\_server**, Suggested

Enforcement Device Information

Device	Type	Manager	Children	Log To	Collects From	Info
switch_server	Cisco Switch- IOS 12.2	Protego Networks MARS 1.0 on p-nvalis		N/A		

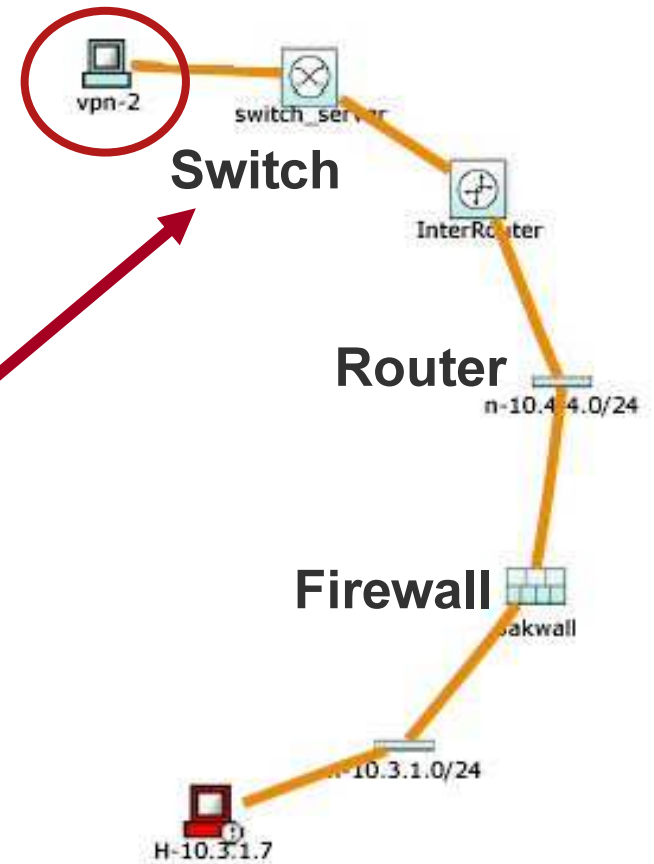
Interface Information

Direction	IP Address	Interface Name	DNS Name	MAC Address	MAC Update Time
-----------	------------	----------------	----------	-------------	-----------------

Recommended Policy/Command

```
• configure t
  interface FastEthernet0/4
    no ip address
    shutdown
```

Push Cancel



# Command and Control Dashboard

24 Hour Events		All Severities	All Rules			
Netflow	137,156					
Events	444,954					
Sessions	428,573					
Data Reduction	3%					
24 Hour Incidents						
High	4 36%					
Medium	3 27%					
Low	4 36%					
Total	11 100%					
Incident ID	Event Type	Matched Rule	Action	Time	Path	
I:260285295	Sudden increase of traffic to a port, Denied packet - no translation group	System Rule: DoS: Network - Success Likely		Nov 22, 2005 10:06:11 AM CET - Nov 22, 2005 10:11:05 AM CET		
I:260285294	Sudden increase of traffic to a port, Built/teardown/permitted IP connection	System Rule: Sudden Traffic Increase To Port	e-mail notify	Nov 22, 2005 10:11:05 AM CET		
I:260285292	Denied packet - no translation group	System Rule: Worm Propagation - Attempt		Nov 22, 2005 10:08:33 AM CET - Nov 22, 2005 10:08:34 AM CET		

<b>Rule Name:</b>	System Rule: Worm Propagation - Attempt	<b>Status:</b>	Active									
<b>Action:</b>	None	<b>Time Range:</b>	0m:10s									
<b>Description:</b> This correlation rule detects worm propagation via means such as SMTP, TFTP, and network shares:												
Offset	Open (	Source IP	Destination IP	Service Name	Event	Device	Reported User	Keyword	Severity	Count	Close	Operation

5		SAME, \$TARGET02, ANY	ANY	icmp (code: ANY, type: ANY, proto: ICMP)	ANY	ANY	None	ANY	ANY	100	)	OR
---	--	-----------------------	-----	--	-----	-----	------	-----	-----	-----	---	----

Denied packet - no translation group	10.1.1.246	0	10.1.61.1
Denied packet - no translation group	10.1.1.246	0	10.1.61.2
Denied packet - no translation group	10.1.1.246	0	10.1.61.3
Denied packet - no translation group	10.1.1.246	0	10.1.61.4

- 100 ICMP üzenet ugyanabból a forrásból 10 másodpercen belül valami gyanúsra utal

# Testreszabható rendszer definiált szabályok

## Szabály definíció

Rule Name: Sasser Rule											Status:	Active	
Action:											Time Range:		0h:05m
Description:											This rule matches the traffic pattern of the Sasser worm.		
Offset	Open (	Source IP	Destination IP	Service Name	Event	Device	Reported User	Keyword	Severity	Count	) Close	Operation	
1		\$TARGET01	\$TARGET02	User Defined (src port: ANY, dst port: 445, proto: TCP)	ANY	ANY	None	ANY	ANY	1		AND	
2		\$TARGET01	\$TARGET02	User Defined (src port: ANY, dst port: 9996, proto: TCP)	ANY	ANY	None	ANY	ANY	1		AND	
3		\$TARGET02	\$TARGET01	User Defined (src port: ANY, dst port: 5554, proto: TCP)	ANY	ANY	None	ANY	ANY	1		FOLLOWED-BY	
4		\$TARGET02	DISTINCT	User Defined (src port: ANY, dst port: 445, proto: TCP)	ANY	ANY	None	ANY	ANY	20			

- Az előfordulás számosságának megadása
- Idő keret megadása

A rule használható riport generálásra is

# Custom Parser

A **Custom Parser** segítségével bármilyen eszköz hozzáadható, mely **Syslog** vagy **SNMP Trap-et** küld

1. Új **eszköz / alkalmazás** típus hozzáadása
2. Egy **“esemény”** típus megadása az új eszközre vagy alkalmazásra
3. Mintázat megadása az adott esemény típusra
4. Új eszköz / alkalmazás felvétele a MARS-ba

Device/Application Type Definition

→ \*Type:  Appliance  Software

→ \*Vendor:

→ \*Model:

→ \*Version:

System  Get Search

deny  All Severity  Red Severity  Yellow Severity  Green Severity

ACL log deny-flows reached limit

Deny connection - no xlate

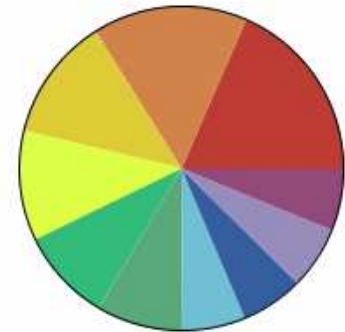
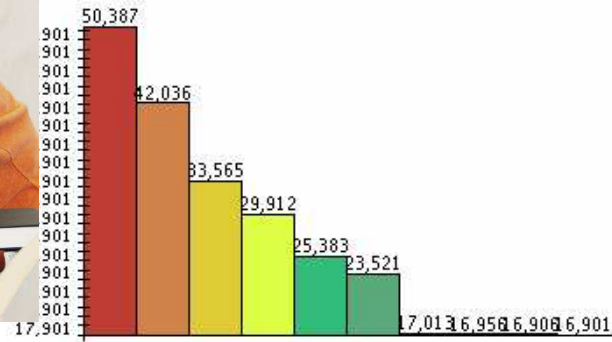
Deny packet due to security policy

Deny policy alarm

Megjegyzés:

MARS 6.0 Device Support Framework

# Riportolás



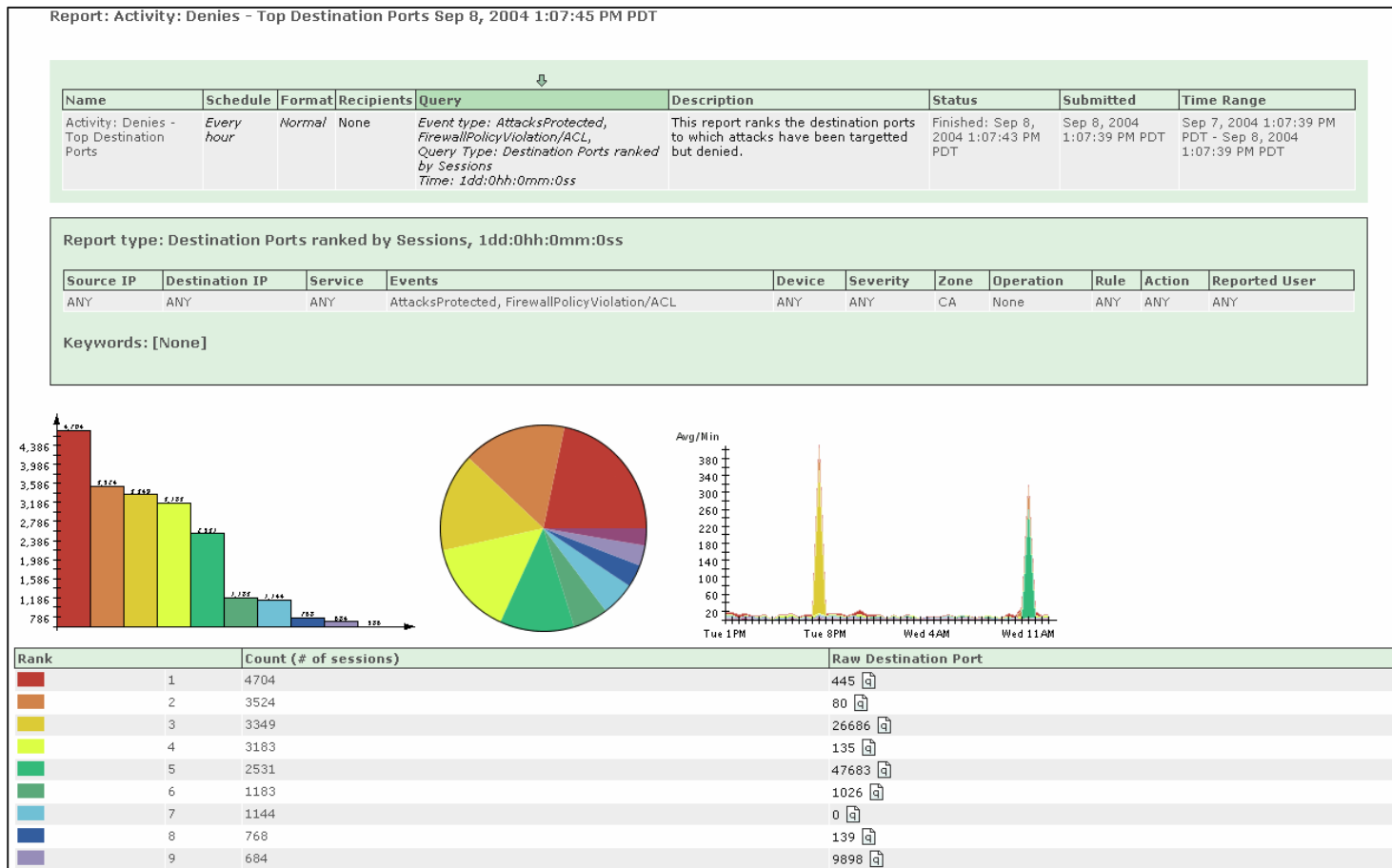
Apr 3, 2007 3:50:00 PM PDT - Apr 3, 2007 4:00:00 PM PDT

Peak	Rank	Number of Sessions at Peak
Peak	1	50,387
Peak	2	42,036
Peak	3	33,565
Peak	4	29,912
Peak	5	25,383
Peak	6	23,521
Peak	7	17,013
Peak	8	16,956
Peak	9	16,906
Peak	10	16,901

# CS-MARS megfelelőségi riportok

A leggyakrabban használt riportok – testreszabási lehetőség

A lekérdezéseket szabályként vagy riportként menti el. - intuitív keretrendszer (nincs SQL konfigurálási igény)



# A rendszer által definiált/ saját készítésű riportok

Példa: A tűzfal által letiltott legtöbbször előforduló portok riportja

Óránként időzített riport

Több, mint 24 órás riport

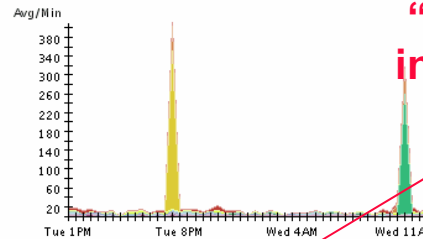
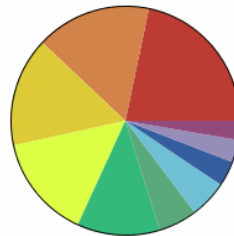
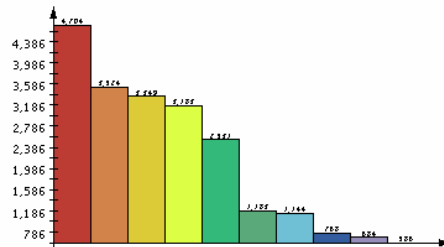
Report: Activity: Denies - Top Destination Ports Sep 8, 2004 1:07:45 PM PDT

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 targeted 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

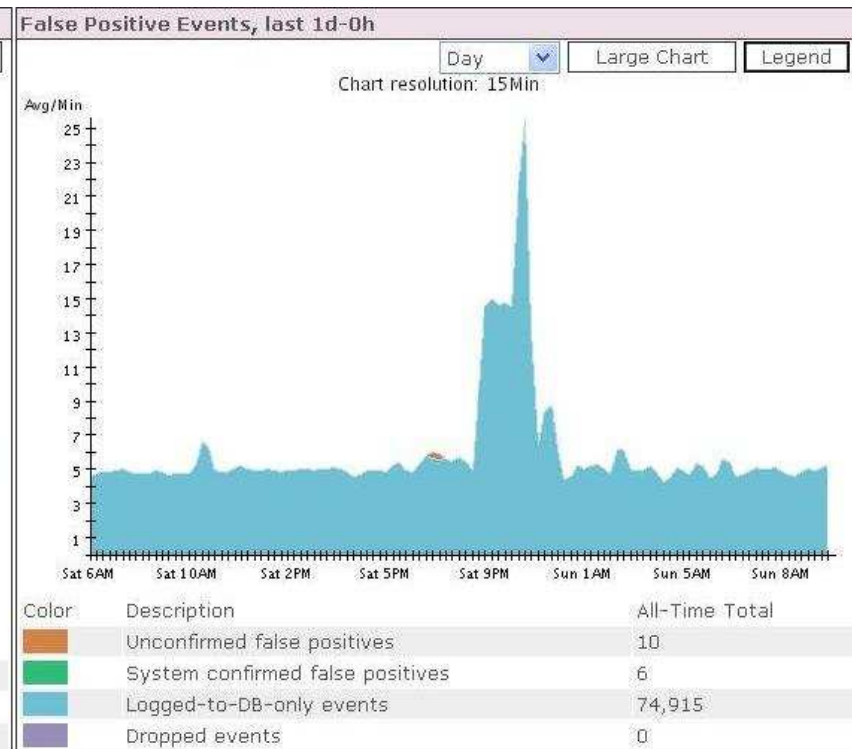
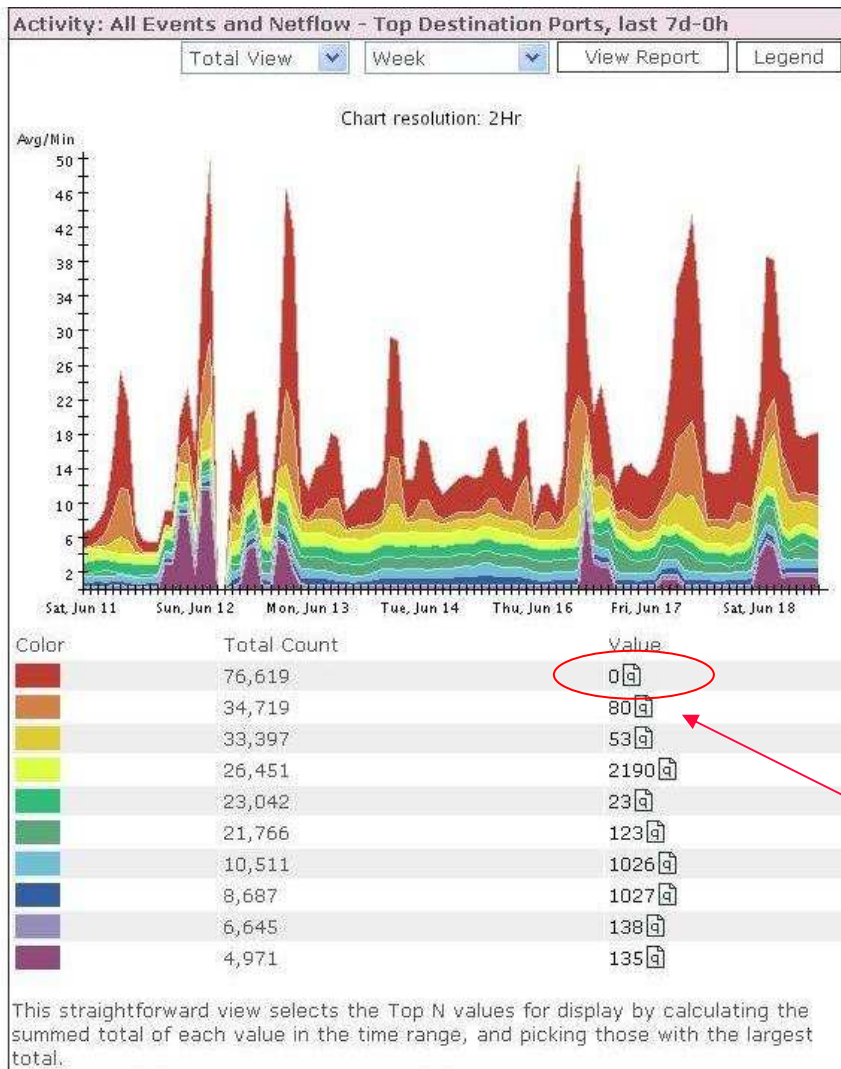
Keywords: [None]



“q” ikon – részletes információ a 445 portról

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

# Hálózati forgalom vizsgálat



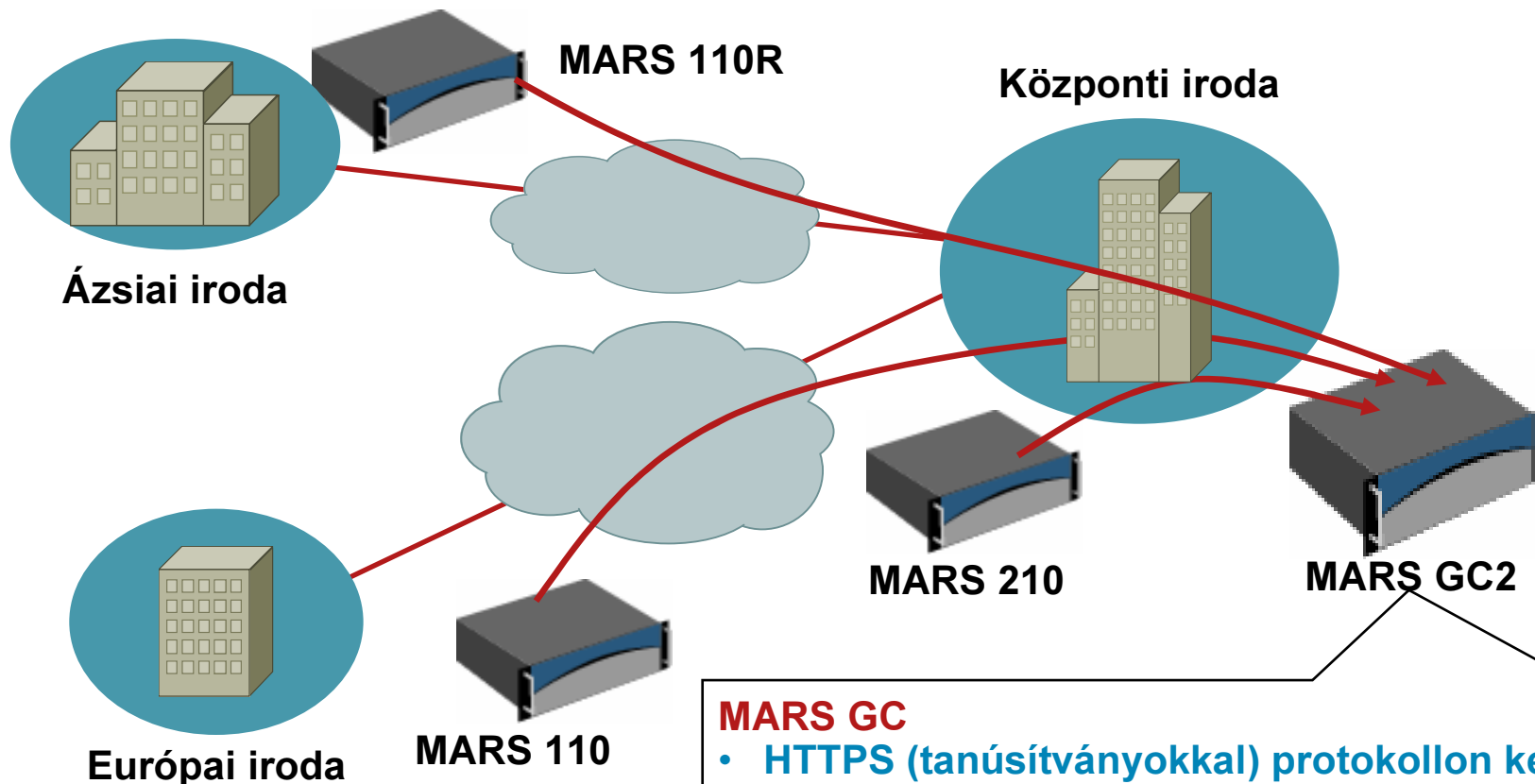
**Miért a "Port 0" forgalom ?**

**Valóban Port0 támadás vagy ez egy esemény, melynek nincs port információja?**

**További vizsgálat szükséges**



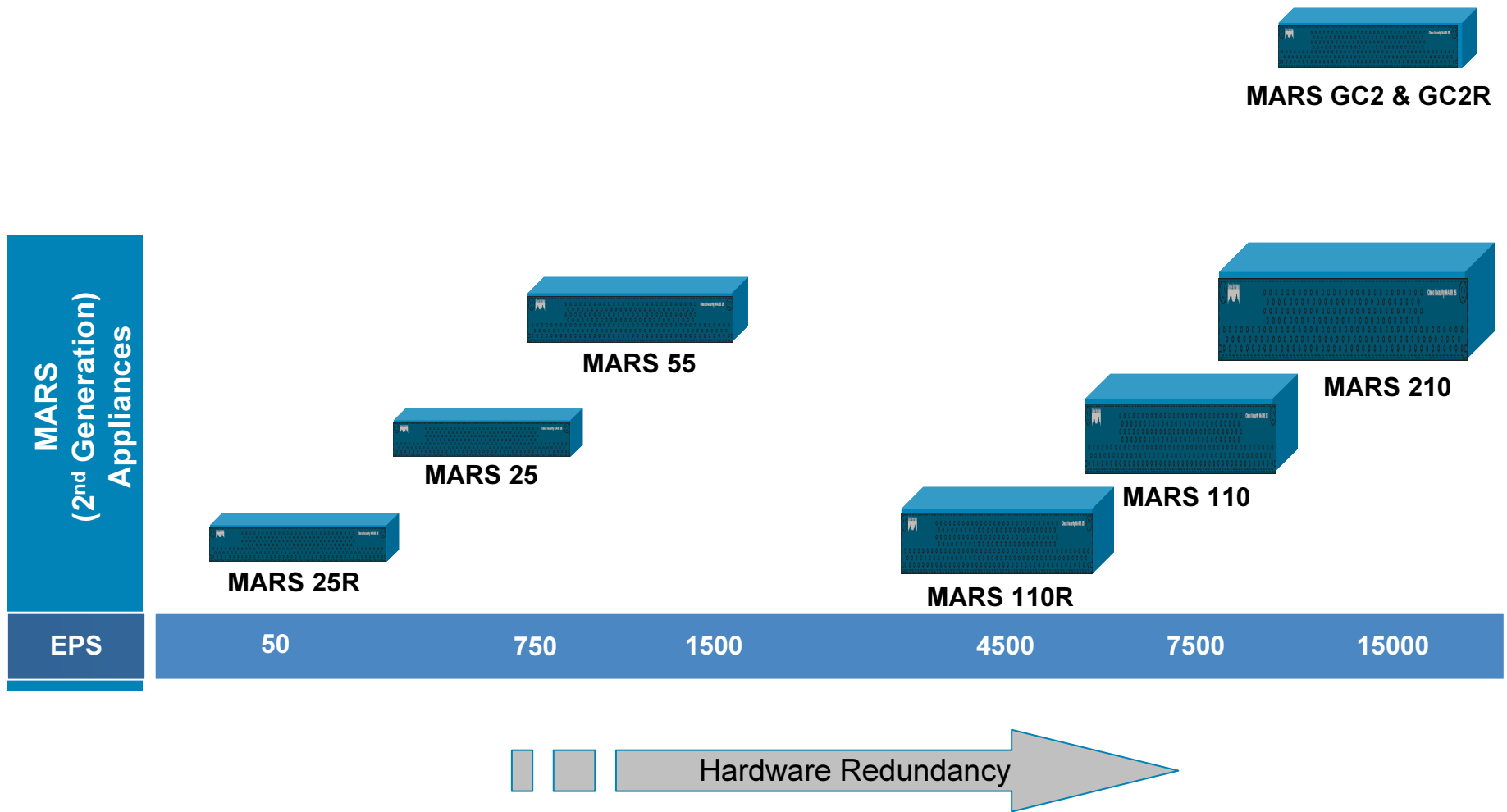
# MARS megvalósítási opciók



## MARS GC

- HTTPS (tanúsítványokkal) protokollon keresztül kommunikál
- Csak a globális szabályokból keletkező incidenseket továbbítják a helyi elemek (LC)
- GC frissítéseket, szabályokat, riport sablonokat, hozzáférési szabályokat és lekérdezéseket tud szétosztani az LC-k felé

# Cisco Security MARS Appliance Overview



# MARS: SASSER-D DAY ZERO TANULMÁNY



# Incidens, mely a Dashboard-on megjelenik

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

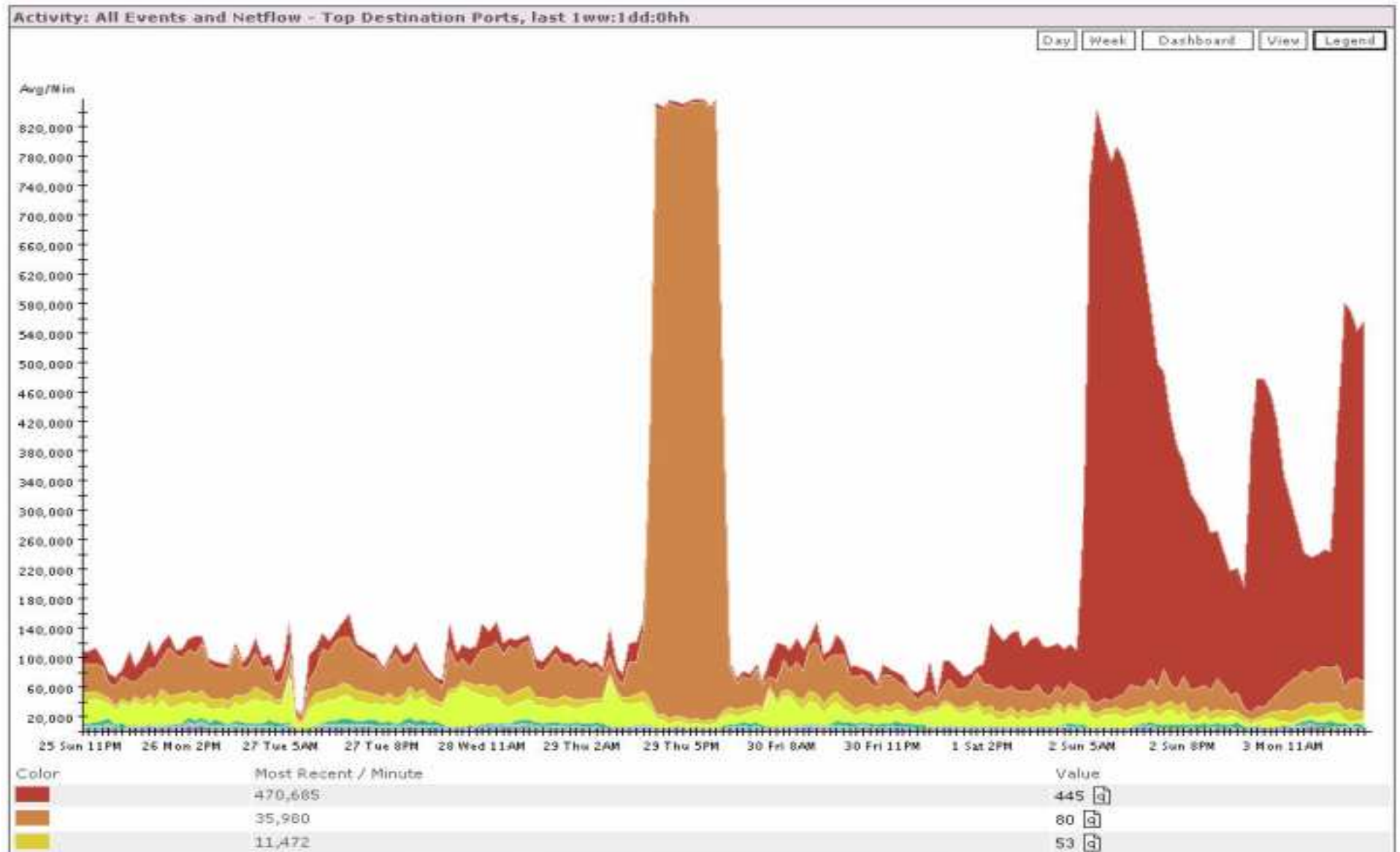
Open	Source IP	Destination IP	Service Name	Event	Device	Severity	Counts	Zone	Close	Action/Operation	Time-range
	ANY	ANY	ANY	System Rule: Sudden Traffic Increase To Port	ANY	ANY	1	NIJT			0hh:10mm:0ss

1473601390   

[Escalate](#) [Expand All](#) [Collapse All](#)

ID	Event Type	Source IP/Port	Destination IP/Port	Protocol	Time	Zone	Reporting Device	Graph	False Positive	Mitigate		
10316, 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		
16544, 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].5.136.132								[+] Total: 2		
	AAA authorization denied due to no prior authentication	[redacted].5.138.174								[+] 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		
16538, 1390	Built/teardown/permitted IP connection	[redacted].25.93.70	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										
16547, 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 [a]	
2	40339	[REDACTED].132.44 [a]	
3	36881	[REDACTED].203.82 [a]	dhcp-203-82 [a]
4	36595	[REDACTED].202.66 [a]	dhcp-202-66 [a]
5	35827	[REDACTED].134.196 [a]	
6	35622	[REDACTED].134.75 [a]	
7	35428	[REDACTED].133.80 [a]	
8	35307	[REDACTED].134.199 [a]	
9	35167	[REDACTED].138.196 [a]	
10	34070	[REDACTED].136.118 [a]	
11	33376	[REDACTED].136.205 [a]	
12	32931	[REDACTED].203.42 [a]	dhcp-203-42 [a]
13	30390	[REDACTED].133.16 [a]	
14	27682	[REDACTED].90.120 [a]	
15	22031	[REDACTED].138.166 [a]	
16	19681	[REDACTED].140.154 [a]	
17	19135	[REDACTED].130.82 [a]	
18	18229	[REDACTED].140.5 [a]	

# Támadási útvonal Layer 2 kivedéssel

The screenshot displays the Protego Networks web interface, split into two main panels. The left panel, titled "[pnguard] Topology Path Graph - Microsoft Internet Explorer", shows a network topology diagram. It features a path graph with nodes including "cherryWall", "switch3", "PN MARS pnguard", "wanRouter1", "mngt", and "H-10.4.17.". The path is highlighted in orange. The right panel, titled "[pnguard] Mitigation Information - Microsoft Internet Explorer", provides details for an incident. It includes a header with "INCIDENTS" and a login status: "Login: Chiu, Phil (pchiu) :: Mar 29, 2004 4:51:57 AM PST". The main content is "Mitigation Information", which lists "Enforcement Devices" (switch3 (L2) (suggested), cherryWall (alternate), wanRouter1 (alternate), mngt (alternate)) and "Enforcement Device - Suggested" (switch3). The suggested device details are: Name: switch3, Device type: Cisco Switch-CatOS ANY, Zone: ProtegoHQ, Managed by: pnguard, Status: Active, Default gateway: 0.0.0.0. Below this, the "Recommended Policy/Command" section shows the command "set port disable 4/6". A "Push" button is visible at the bottom right of the mitigation information panel.

**Topology Path Graph**

Layer 3 Path | **Layer 2 Path** | Full Topo

**Mitigation Information**

**Enforcement Devices**

- switch3 (L2) (suggested)
- cherryWall (alternate)
- wanRouter1 (alternate)
- mngt (alternate)

**Enforcement Device - Suggested**

Name: switch3  
Device type: Cisco Switch-CatOS ANY  
Zone: ProtegoHQ  
Managed by: pnguard  
Status: Active  
Default gateway: 0.0.0.0

**Recommended Policy/Command**

```
set port disable 4/6
```

Push

For Help, click Help Topics on the Help Menu.

# Demonstráció





# Összefoglalás



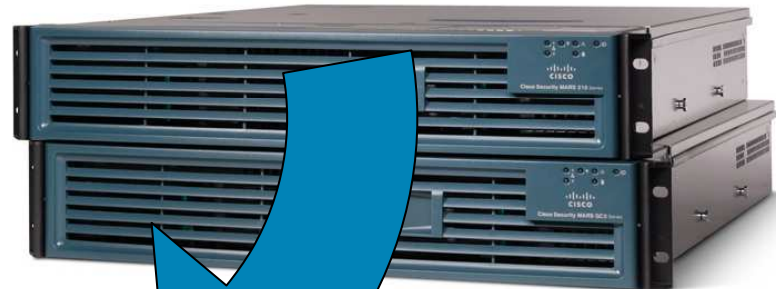
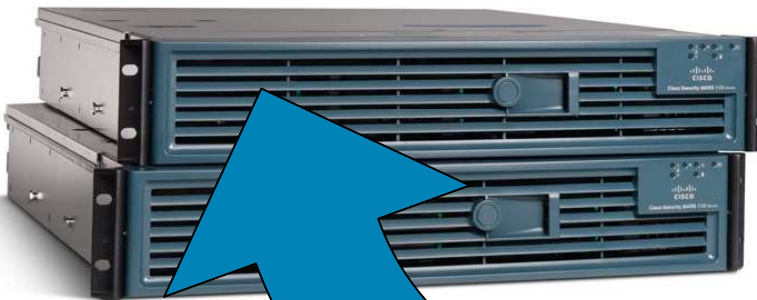
# MARS Összefoglalás

## Jobb

Integrált hálózati tudás  
Célhardver, redundáns tervezés

## Gyorsabb

15,000 EPS teljes korrelációval  
(3-10x, mint a egyéb gyártók)  
Skálázható, elosztott esemény analízis



## Költséghatékony

Appliance kivitel  
A legjobb ár/teljesítmény  
Nincs rejtett szoftver/ testreszabási költség

## Mit szeretne ma tudni?

- Melyik a legutóbbi férget a hálózaton?
- Milyen információk van a 192.168.16.2 IP című gépről az elmúlt 30 napban?
- Mennyi account letiltva az Active Directory-ben?
- Mennyi (szándéktalanul) kapcsolódni a WiFi hálózatra?

# További információ

- **Cisco Security MARS**  
[www.cisco.com/go/mars](http://www.cisco.com/go/mars)
- **Cisco Self Defending Network Strategy**  
[www.cisco.com/go/selfdefend](http://www.cisco.com/go/selfdefend)
- **Cisco Security and VPN Solutions**  
[www.cisco.com/go/security](http://www.cisco.com/go/security)
- **Cisco SAFE Blueprints**  
[www.cisco.com/go/safe](http://www.cisco.com/go/safe)
- **Netflow v9**  
[http://www.cisco.com/en/US/docs/ios/12\\_3/feature/gde/nfv9expf.html](http://www.cisco.com/en/US/docs/ios/12_3/feature/gde/nfv9expf.html)
- **CS-M**  
<http://www.cisco.com/en/US/products/ps6498/index.html>
- **CS-MARS**  
<http://www.cisco.com/en/US/products/ps6241/index.html>
- **CS-MARS blog**  
<http://ciscomars.blogspot.com/>
- **CS-MARS Google Group**  
<http://groups.google.com/group/cs-mars-ug?hl=en-GB>

# További információk



