

Biztonsági incidensek hatékony kezelése

Tartalom

Hálózatbiztonsági eszközök menedzsmentje,
avagy a nagy kihívás

A Cisco MARS termék család

CS-MARS

Hogyan látszik a Sasser a MARS-ról?



Hálózatbiztonsági eszközök menedzsmentje, avagy a nagy kihívás



Eszkalációs folyamat

Hálózati folyamatok

Mindig megkésve

Biztonsági folyamatok



A reakció lépései:

1. Riasztás
2. Felderítés
3. Elhárítás

Tűzfal

IDS/IPS

VPN

Sebezhetőség
vizsgálók

AAA

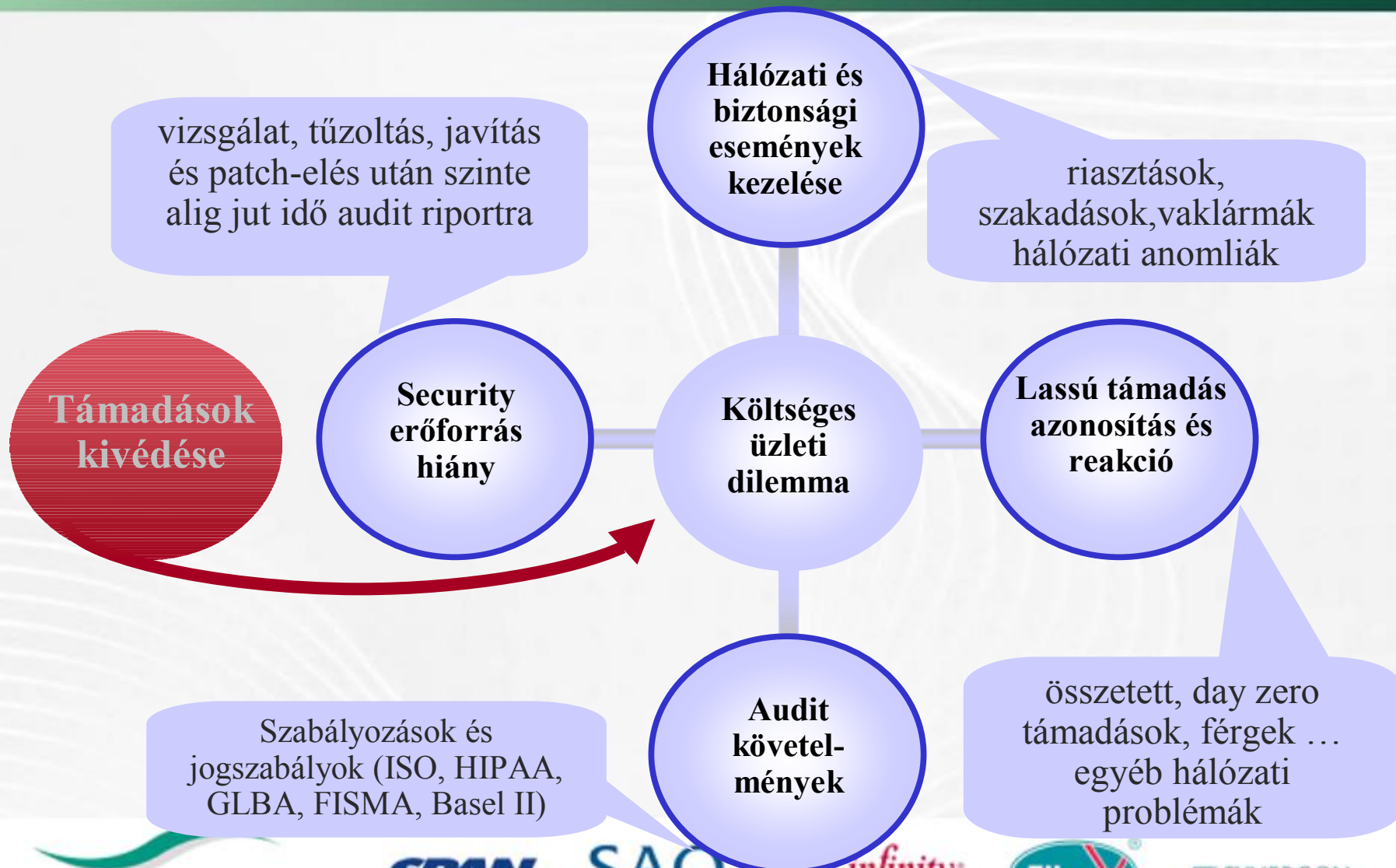
10K Win,
100s UNIX

Anti-virus

Router/Switch

Hálózati topológia felvázolása
Tonnányi log-adat
értelmezése
... és mindez naponta

Biztonsági kihívás – üzleti dilemma

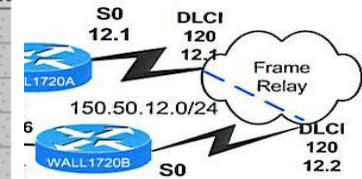


Komplex hálózat – bonyolult védelem



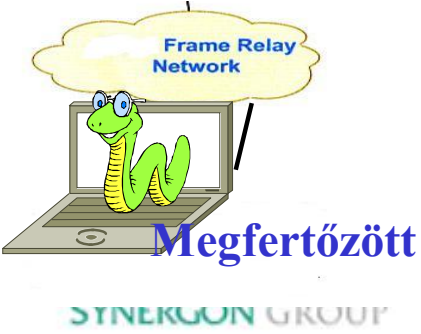
NAT SUBJECT: 10.01.30.0/24

Count	Sig Name	Source Address	Dest Address	Details	Source Protected	Dest Protected
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	+				



```

inside:192.168.1.3/1606 <67.82.225.18/1185>
inside:192.168.1.3/1607 <67.82.225.18/1185>
ation 0:00:01 bytes 5919 TCP Res
face outside
face inside
face outside
face outside
ation 0:00:01 bytes 53445 TCP F
.42 duration 0:00:35
inside:192.168.1.3/1610 <67.82.225.18/1185>
inside:192.168.1.3/1619 <67.82.225.18/1185>
inside:192.168.1.3/1619 <67.82.225.18/1185>
004001: 192.168.1.3 Accessed URL 64.154.80.250:/HG?hc=we69&hb=DMS401281KAA%3BDMS4012890CU&cd=1&hv=6&n=/Cisco.com+Public&con=8&vcd
=//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=090101
07r&seg=*;i&epg=n&ja=y&dt=5&zo=240&ln=0&cu=0&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-in%
205.0.1%3AMozilla%20Default%20Plug-in%3AShockwave%20Flash%3AMicrosoft%20DRM%3AMicrosoft%20DRM%3AMetaStream%203%20Plug-in%3
Java%20Plug-in%3AJava%20Plug-in%3AJava%20Plug-in%3AJava%20Plug-in%3AJava%20Plug-in%3AJava%20Plug-in%3AHP%20Peripheral%20Interrogator%3AWindows%2
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 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
304001: 192.168.1.3 Accessed URL 64.154.80.250:/HG?hc=we69&hb=DMS401281KAA%3BDMS4012890CU&cd=1&hv=6&n=/Cisco.com+Public&con=8&vcd
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=090101
1.07r&seg=*;i&epg=n&ja=y&dt=5&zo=240&ln=0&cu=0&gn=&ld=&la=&c1=&c2=&c3=&c4=&customerid=&ra=&rf=bookmark&pl=CDT%20Plug-in%3AQuickTime
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%
in%205.0.1%3AMozilla%20Default%20Plug-in%3AShockwave%20Flash%3AMicrosoft%20DRM%3AMicrosoft%20DRM%3AMetaStream%203%20Plug-in%3
AJava%20Plug-in%3AJava%20Plug-in%3AJava%20Plug-in%3AJava%20Plug-in%3AJava%20Plug-in%3AHP%20Peripheral%20Interrogator%3AWindows%2
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
    
```



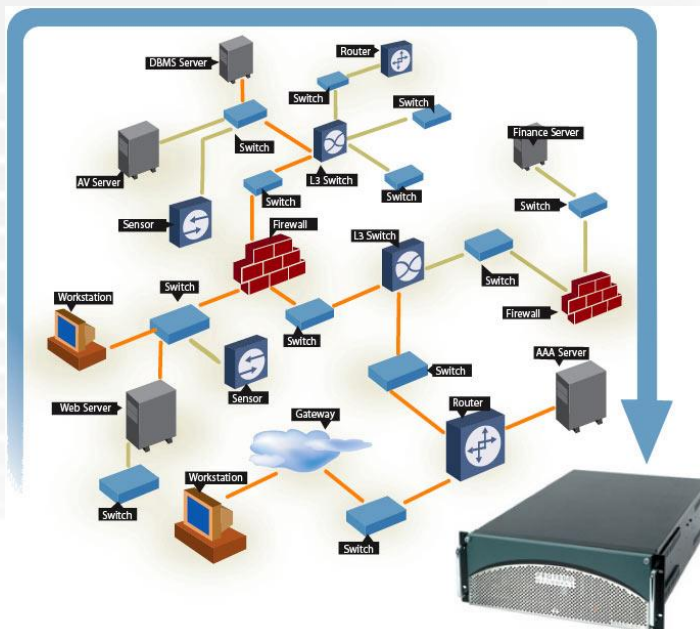
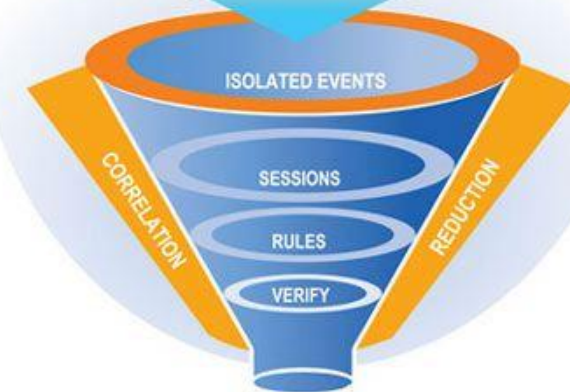
MARS termékcsalád



Cisco Security Monitoring, Analysis, and Response System (CS-MARS)

- MEGLÉVŐ hálózati biztonsági infrastruktúra elemeiből átható biztonság
- A teljes vállalati eseményhalmaz korrelációja
 - NIDS, tűzfalak, routerek, switchek, CSA
 - Syslog, SNMP, RDEP, SDEE, NetFlow, Endpoint event logs, Multi-Vendor
- Támadások gyors lokalizálása és kivédése

Firewall Log	IDS Event	Server Log
Switch Log	Firewall Cfg.	AV Alert
Switch Cfg.	NAT Cfg.	App Log
Router Cfg.	Netflow	VA Scanner

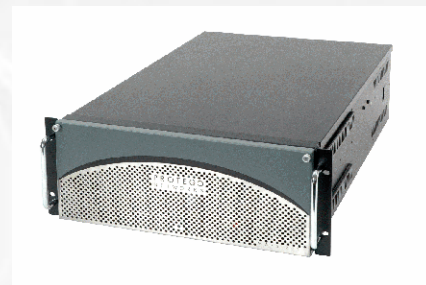
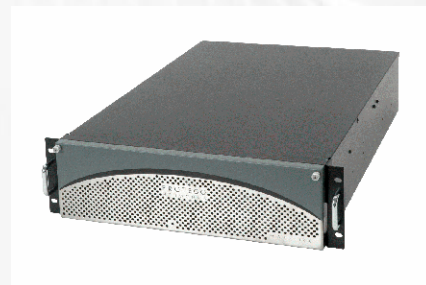
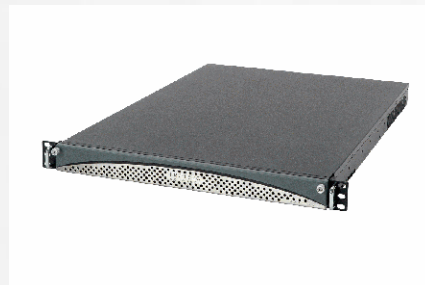


- Főbb funkciók
 - Biztonsági *incidensek* észlelése üzenetek, események és session információk alapján
 - *Incidensek* topológiai megjelenítése és visszajátszása
 - L2 és L3 védekezési mechanizmusok

MARS termékcsalád



CS-MARS Model	20	50	100e	100	200	Global Controller
Esemény/sec	500	1,000	3,000	5,000	10,000	N/A
NetFlow folyam /Sec	15,000	25,000	75,000	150,000	300,000	N/A
RAID Storage	120GB	120GB	750GB	750GB	1TB	1TB
Rack Size	1 RU	1 RU	3 RU	3 RU	4 RU	4 RU



- Gyors telepítés
- Raid 1+0
- Nem kell külön adatbázis licenc (Oracle adatbázis)

- Agent-nélküli esemény gyűjtés
- Layer 2/3 hálózati topológia és védekezés
 - NetFlow



Támogatott eszközök (MARS 4.1)

- 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
 - eEye REM 1.x
 - Foundstone FoundScan 3.x
 - Qualys Guard
- Hoszt oldali védelem
 - Cisco Security Agent (CSA) 4.x
 - McAfee Enterecept 2.5, 4.x
 - ISS RealSecure Host Sensor 6.5, 7.0
 - Symantec AnitVirus 9.x
- Hoszt log
 - Windows NT, 2000, 2003 (agent/agent-less)
 - Solaris
 - Linux
- Syslog
 - Tetszőleges eszköz támogatás
- Alkalmazások
 - Web servers (IIS, iPlanet, Apache)
 - Oracle 9i, 10i database audit logs
 - Network Appliance NetCache

CS-MARS



A keletkezett, nagy mennyiségű biztonsági és hálózati események átalakítása értelmezhető és kezelhető támadási jelentésekként

- hálózati-intelligenciával támogatott korreláció
- incidens érvényesség ellenőrzés
- támadás megjelenítés
- automatikus hálózat felderítés
- beavatkozás támogatás
- megfelelőség kezelés
- nagy teljesítmény
- hibajegy kezelés

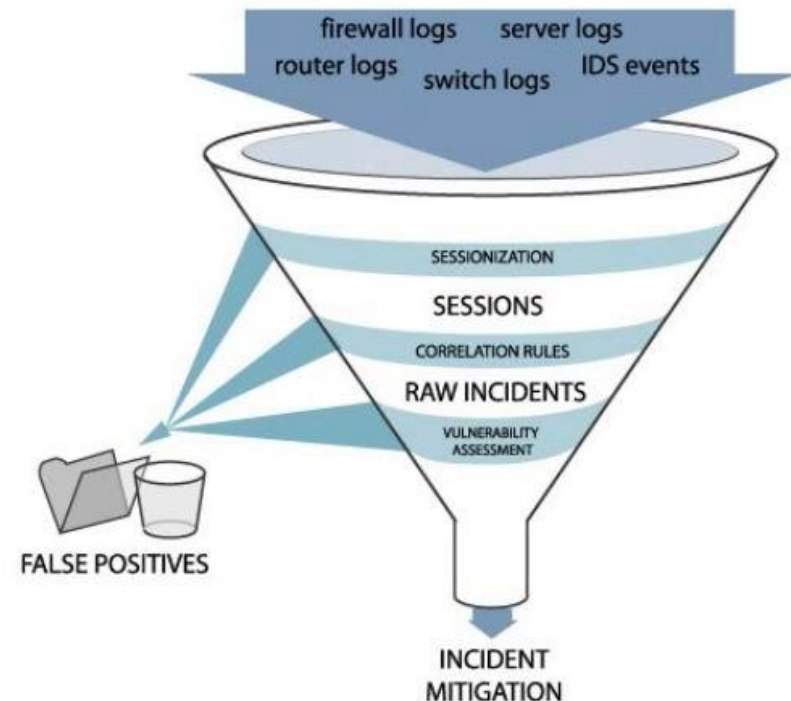


- Esemény korreláció a hálózati topológia ismeretében
 - beépített hálózat felderítés (SNMP, Telnet, SSH, CPMI)
 - konfiguráció, security policy letöltése, routing
 - session azonosítás (NAT-on keresztül is)
 - ellenlépés pontjának meghatározása (a támadóhoz legközelebb)
 - támadási útvonal megjelenítése

- Esemény (Event)
 - Riportoló eszközöktől (tűzfal, IPS, router) kapott nyers formátumú üzenet
- Kapcsolat (Session)
 - Korrelált esemény halmaz (NAT figyelembevételével)
- Incidens (Incident)
 - Kapcsolatok korrelációs szabályok alapján azonosított sorozata

A MARS működése

1. Hálózati eszközökből új esemény érkezik
2. Esemény értelmezése
3. Normalizálás
4. Session kialakítás / NAT korreláció
5. Szabályok futtatása
 - eldobási szabályok
 - beépített/definiálható szabályok
6. Téves riasztások kiszűrése
7. Sérülékenység elemzés
8. Forgalom elemzés és statisztikai anomália detektálás



A MARS felszíne



CISCO SYSTEMS

SUMMARY INCIDENTS QUERY / REPORTS RULES MANAGEMENT ADMIN HELP

Dashboard Network Status My Reports Nov 28, 2005 2:16:13 PM PST

SUMMARY CS-MARS Standalone: demo2 v4.1 Login: Sales, USA (usasales) :: Logout :: Activate

Select Case: No Case Selected...

View Cases New Case

Page Refresh Rate

15 minutes

24 Hour Events

Netflow	0
Events	2,663,025
Sessions	985,895
Data Reduction	62%

24 Hour Incidents

High	35	49%
Medium	0	0%
Low	36	50%
Total	71	100%

All False Positives

To be confirmed	112,531	96%
System determined	0	0%
Logged	2,534	2%
Dropped	0	0%
User confirmed	1,568	1%
Total	116,633	100%

To-do List

- C:1659860 (Assigned) Nimba Case
- C:1658999 (Assigned) Test
- C:1658541 (New) New Case

My Reports

- Activity: All - Top Destination Ports (Peak View)
- Activity: All - Top Destinations (Peak View)
- Activity: All - Top Reporting Devices (Total View)
- Activity: All - Top Sources (Peak View)

Edit

Recent Incidents

Incident ID	Event Type	Matched Rule	Action	Time	Path	Case
I:790062007	Built/teardown/permitted IP connection [a], ICMP Ping Network Sweep [a], WWW IIS .ida Indexing Service Overflow [a]	Successful Recon and Buffer Overflow [a]		Nov 28, 2005 2:06:16 PM PST		
I:790062006	Deny packet due to security policy [a]	NetworkConfigError [a]		Nov 28, 2005 2:04:01 PM PST		
I:790062005	IIS DOT DOT EXECUTE [a], IIS Dot Dot Crash [a], WWW WinNT cmd.exe Exec [a], WWW IIS Unicode Directory traversal [a], IIS CGI Double Decode [a]	Nimda Rule [a]		Nov 28, 2005 2:03:06 PM PST		
I:790062004	Built/teardown/permitted IP connection [a]	Sasser Rule [a]		Nov 28, 2005 2:00:02 PM PST - Nov 28, 2005 2:00:03 PM PST		
I:790062003	Built/teardown/permitted IP connection [a], ICMP Ping Network Sweep [a], WWW IIS .ida Indexing Service Overflow [a]	Successful Recon and Buffer Overflow [a]		Nov 28, 2005 1:43:32 PM PST		

HotSpot Graph

Full Topo Graph Large Graph Help



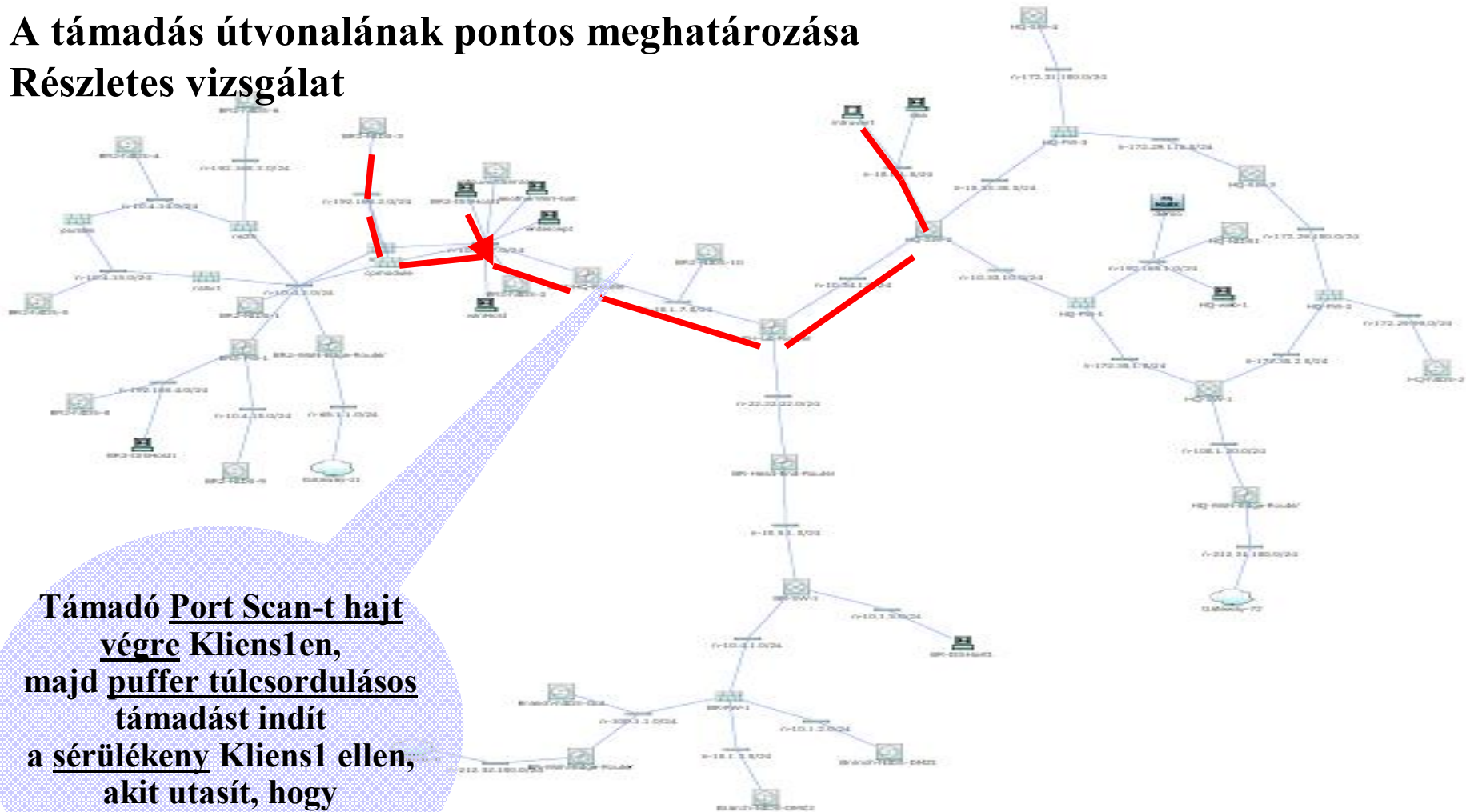
Attack Diagram

Large Graph Help



Támadási útvonal meghatározás

A támadás útvonalának pontos meghatározása Részletes vizsgálat



**Támadó Port Scan-t hajt
vége Kliens1en,
majd puffer túlcsordulásos
támadást indít
a sérülékeny Kliens1 ellen,
akit utasít, hogy
jelszó támadást végezzen
Célpont ellen**

Riport csoportok

- beépített és testreszabható riportok

Report Selection

Group: All Schedule: All

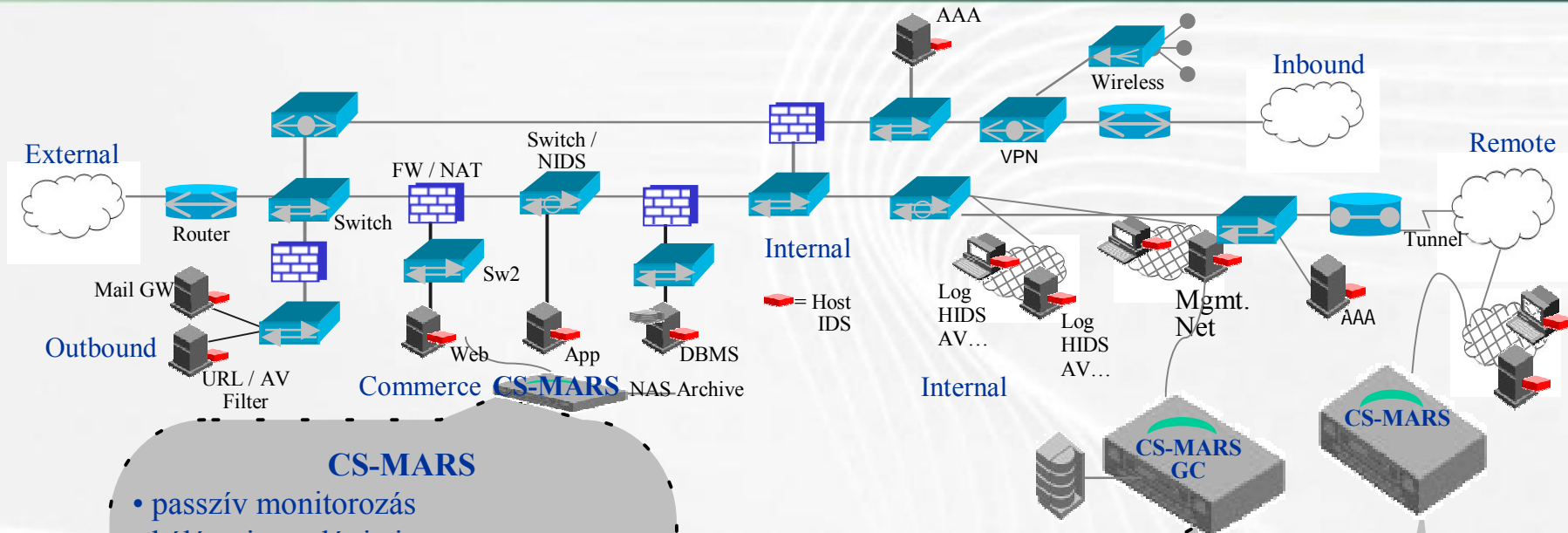
Description	Status	Submitted	Time Range
NAT connections ranked by Time	Not Run	Aug 30, 2005 9:12:20 AM PDT	Aug 29, 2005 9:12:00 AM PDT - Aug 30, 2005 9:12:00 AM PDT
Destination Ports ranked by Sessions	Finished: Sep 6, 2005 3:02:04 PM PDT	Sep 6, 2005 3:02:04 PM PDT	Sep 5, 2005 3:00:00 PM PDT - Sep 6, 2005 3:00:00 PM PDT
Destination IPs ranked by Sessions	Finished: Sep 6, 2005 3:02:03 PM PDT	Sep 6, 2005 3:02:03 PM PDT	Sep 5, 2005 3:00:00 PM PDT - Sep 6, 2005 3:00:00 PM PDT

Támogatás

- McAfee ePolicy Orchestrator
- Network Admission Control



Global Controller



CS-MARS

- passzív monitorozás
- hálózati topológia ismerete
- NAT kezelés, Netflow küszöbértékek beállítása
- Logok, riasztások, Netflow adatok korrelációja
- Valós incidensek azonosítása (téves riasztások kiszűrése)
- Valós idejű megjelenítés, visszajátszás, lekérdezés
- Részletekbe menő vizsgálat
- Konzolidálja és tárolja a helyi incidensek adatai

CS-MARS Global Controller

- központi menedzsment hálózatba csatlakozik
- globális nézet, menedzsment és riport felület
- Titkosított kommunikáció a helyi MARS-ok felé
- Frissítések, riport sablonok és hozzáférési szabályok szétosztása

CS-MARS

- távoli telephelyre kihelyezve, MARS GC felügyelet

Hogyan látszik a Sasser a MARS-ról?



Incidens megjelenítés

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	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	Mitigation
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	██████████.130.120		Total: 3						
	AAA authorization denied due to no prior authentication	██████████.131.142		Total: 2						
16544, 1390	AAA authorization denied due to no prior authentication	██████████.35.136.85	4049	██████████.55.128	445	N/A	May 3, 2004 5:40:05 AM EDT		cerberus2	Tune Mitigate
	AAA authorization denied due to no prior authentication	██████████.35.136.104		Total: 3						
	AAA authorization denied due to no prior authentication	██████████.136.205		Total: 2						
	AAA authorization denied due to no prior authentication	██████████.5.138.132		Total: 2						
	AAA authorization denied due to no prior authentication	██████████.5.138.174		Total: 3						
	AAA authorization denied due to no prior authentication	██████████.139.89		Total: 6						
	AAA authorization denied due to no prior authentication	██████████.5.140.95		Total: 3						
16538, 1390	Built/teardown/permitted IP connection	██████████.25.93.70	2503	██████████.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	██████████.136.85	4050	██████████.30.35	445	TCP	May 3, 2004 5:40:05 AM EDT		cerberus2	Tune Mitigate

Támadás útvonala, Layer 2 beavatkozás

The screenshot displays two browser windows from the Cisco Systems pnguard interface. The left window, titled "[pnguard] Topology Path Graph", shows a network diagram with a highlighted path. The path starts at a host (H-10.4.17.1) and goes through a switch (mngt), a router (wanRouter1), and another switch (switch3) to reach a destination (n-67.126.151.176/28). The path is labeled "Layer 2 Path".

The right window, titled "[pnguard] Mitigation Information", shows the "INCIDENTS" section with the user "Login: Chiu, Phil (pchiu) :: Mar 29, 2004 4:51:57 AM PST". The "Mitigation Information" section includes:

- 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
```

A "Push" button is visible at the bottom right of the mitigation information window.

Köszönöm figyelmüket!
Várom kérdéseiket!

simon.janos@synergon.hu

<http://www.cisco.com/go/mars>

<http://www.synergon.hu>