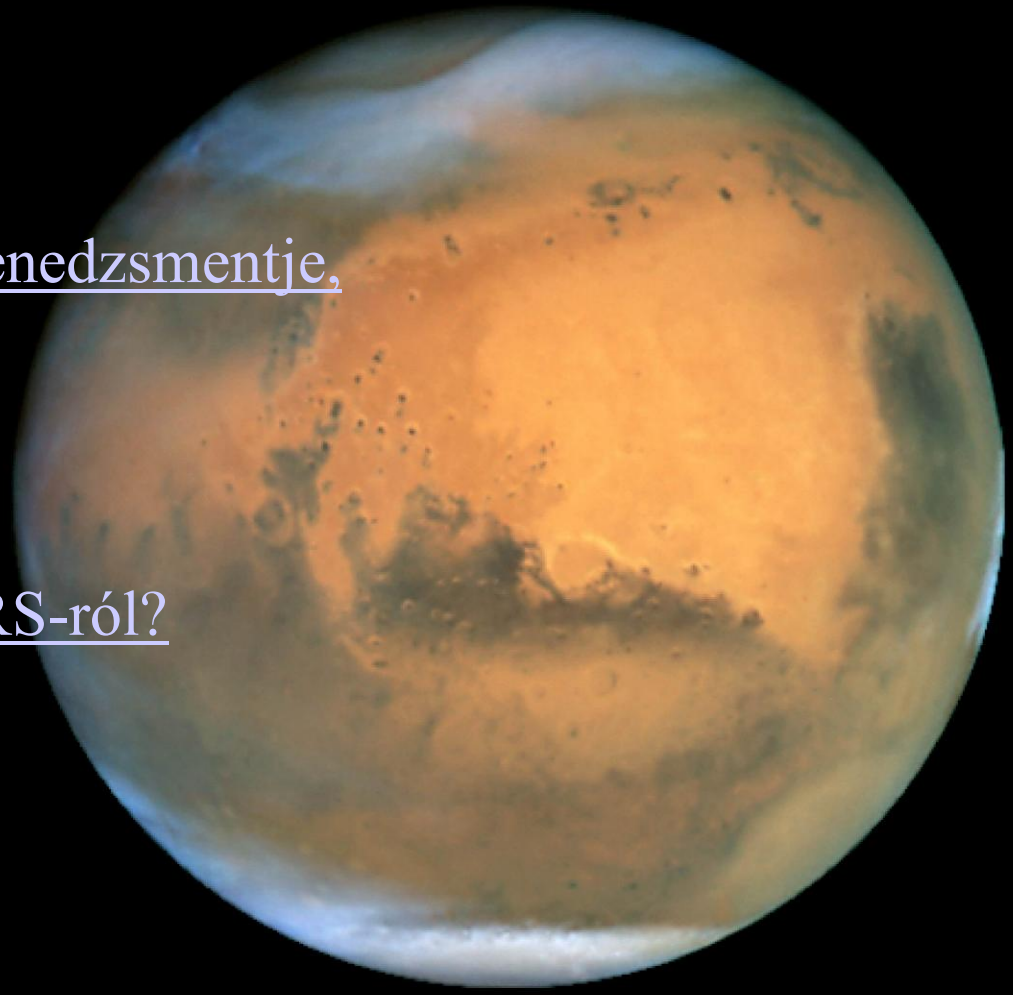
Simon János György
technikai tanácsadó, CCSP

SYNERGON
INFORMATION SYSTEMS PLC.

Biztonsági incidensek hatékony kezelése

SYNERGON GROUP
SPAN
SAO
infinity
FibeX
SYNERGON

Tartalom



SYNERGON
INFORMATION SYSTEMS PLC.

Hálózatbiztonsági eszközök menedzsmentje, avagy a nagy kihívás

SYNERGON GROUP

SPAN SAO infinity FibeX SYNERGON

Eszkalációs folyamat

SYNERGON INFORMATION SYSTEMS PLC.

Hálózati folyamatok

Mindig megkésve

Biztonsági folyamatok

A reakció lépései:
1. **Riasztás**
2. **Felderítés**
3. **Elhárítás**

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

Tűzfal

IDS/IPS

VPN

Sebezhetőség vizsgálók

AAA

10K Win, 100s UNIX

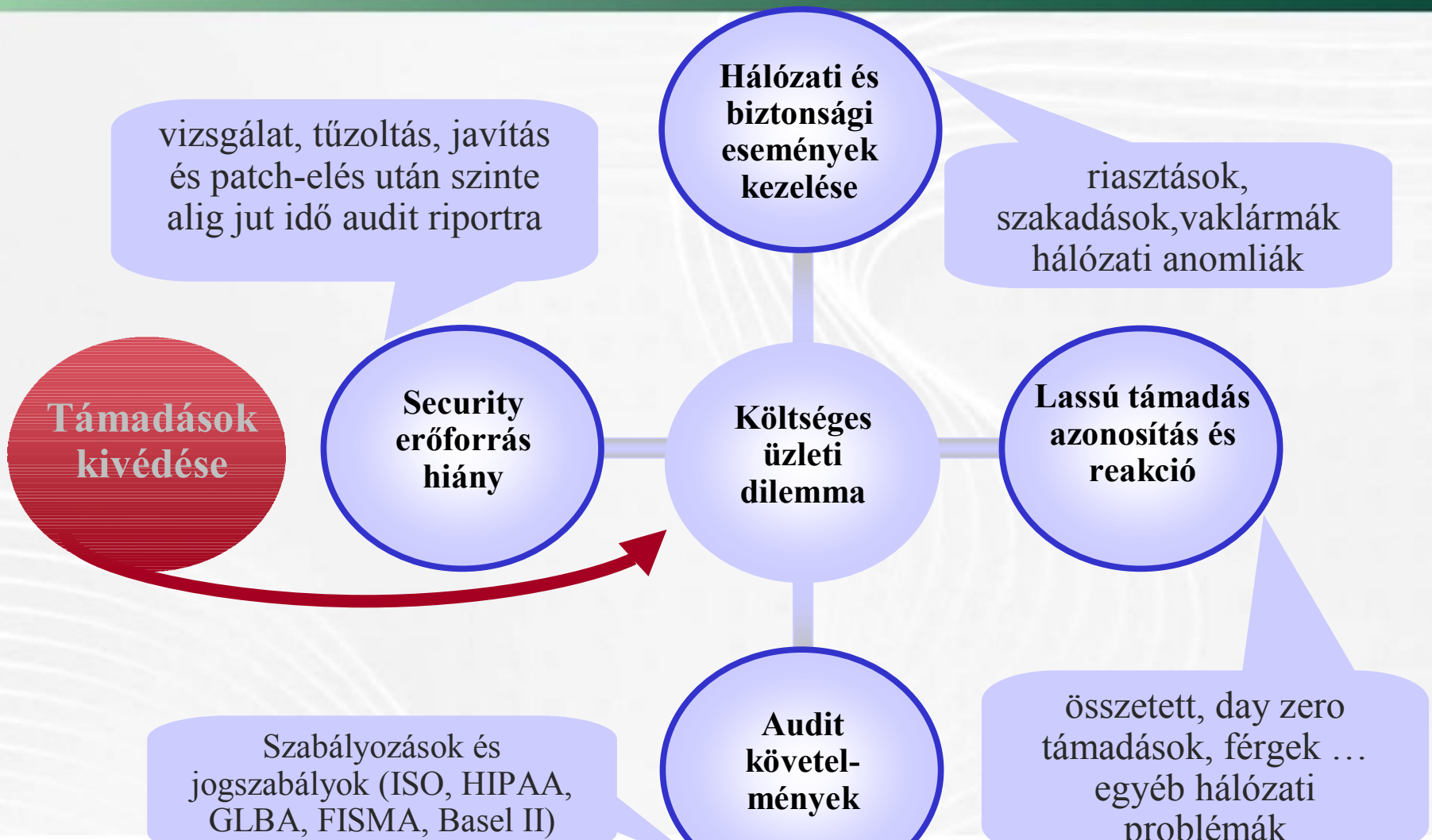
Anti-virus

Router/Switch

SYNERGON GROUP

SPAN SAO infinity FibeX SYNERGON

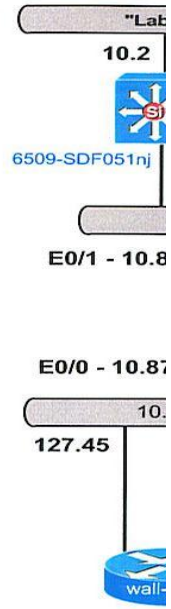
Biztonsági kihívás – üzleti dilemma

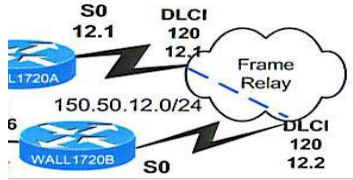


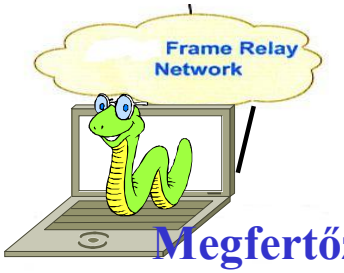
Komplex hálózat – bonyolult védelem

SYNERGON
INFORMATION SYSTEMS PLC.

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	+				







Megfertőzött

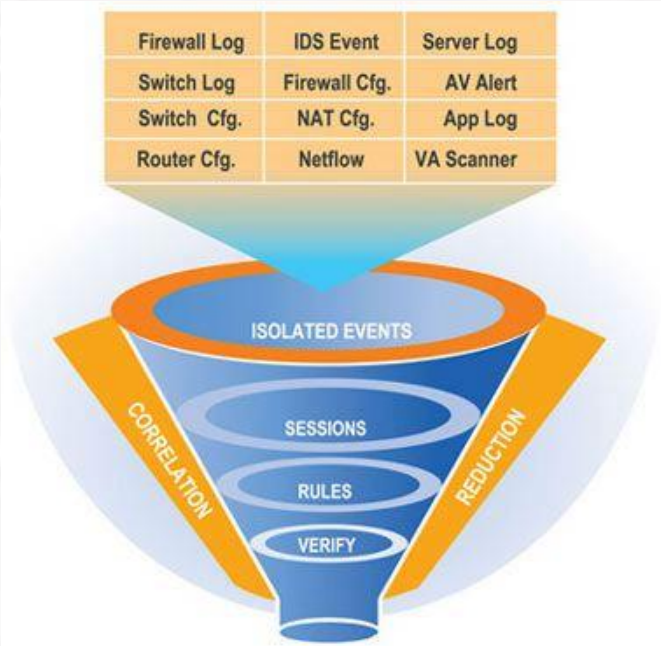
SYNERGON GROUP

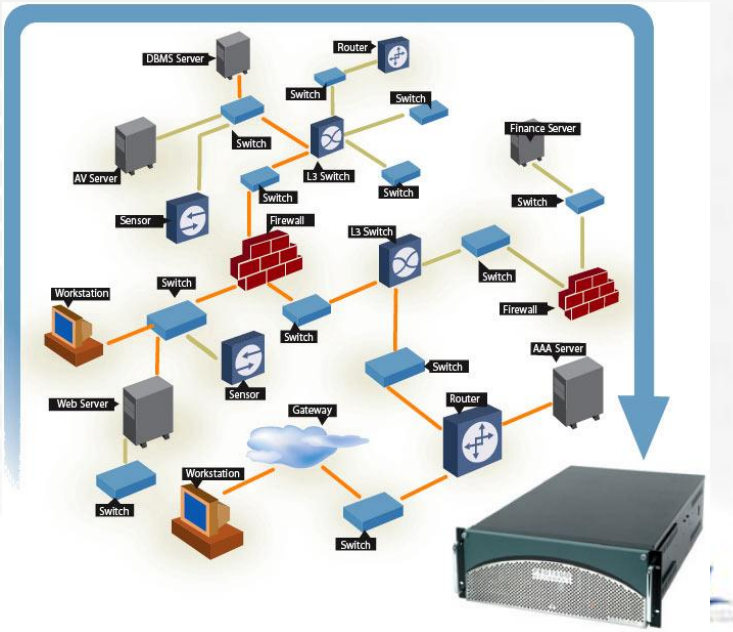
MARS termékcsalád

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

SYNERGON INFORMATION SYSTEMS PLC.

- 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



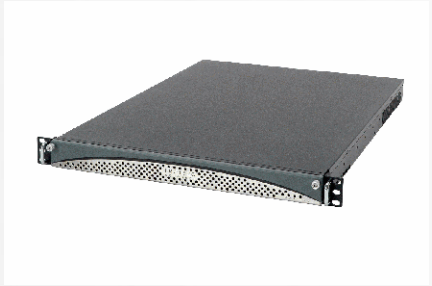


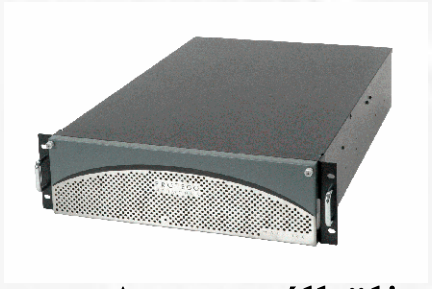
- Főbb funkciók
  - Biztonsági *incidensek* észlelése üzenetek, események és session információk alapján
  - *Incidensek* topológiai megjelenítése és visszajátszása
  - L2 és L3 védekezési mechanizmusok

SAO infinity FibeX SYNERGON

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 Entercept 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

SYNERGON
INFORMATION SYSTEMS PLC.

CS-MARS

SYNERGON GROUP

SPAN SAO infinity FibeX SYNERGON

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
- autómatikus hálózat felderítés
- beavatkozás támogatás
- megfelelőség kezelés
- nagy teljesítmény
- hibajegy kezelés

MARS szolgáltatások

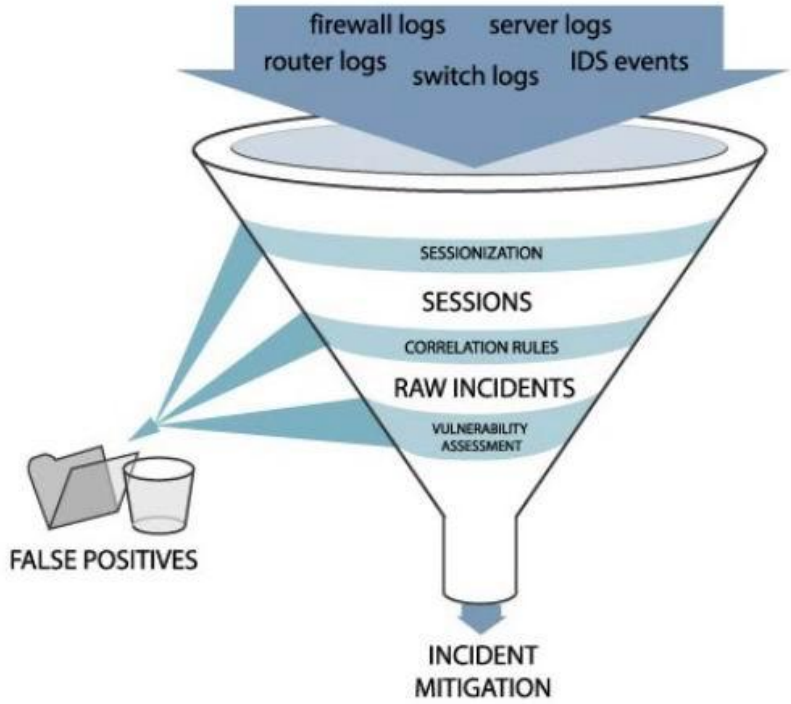
- Esemény korreláció a hálózati topológia ismeretében
  - beépített hálózat felderítés (SNMP, Telnet, SSH, CPMI)
  - konfiguráció, security policy letöltése, routing
  - session azonosítás (NAT-on keresztül is)
  - ellenlépés pontjának meghatározása (a támadóhoz legközelebb)
  - támadási útvonal megjelenítése

Alapfogalmak

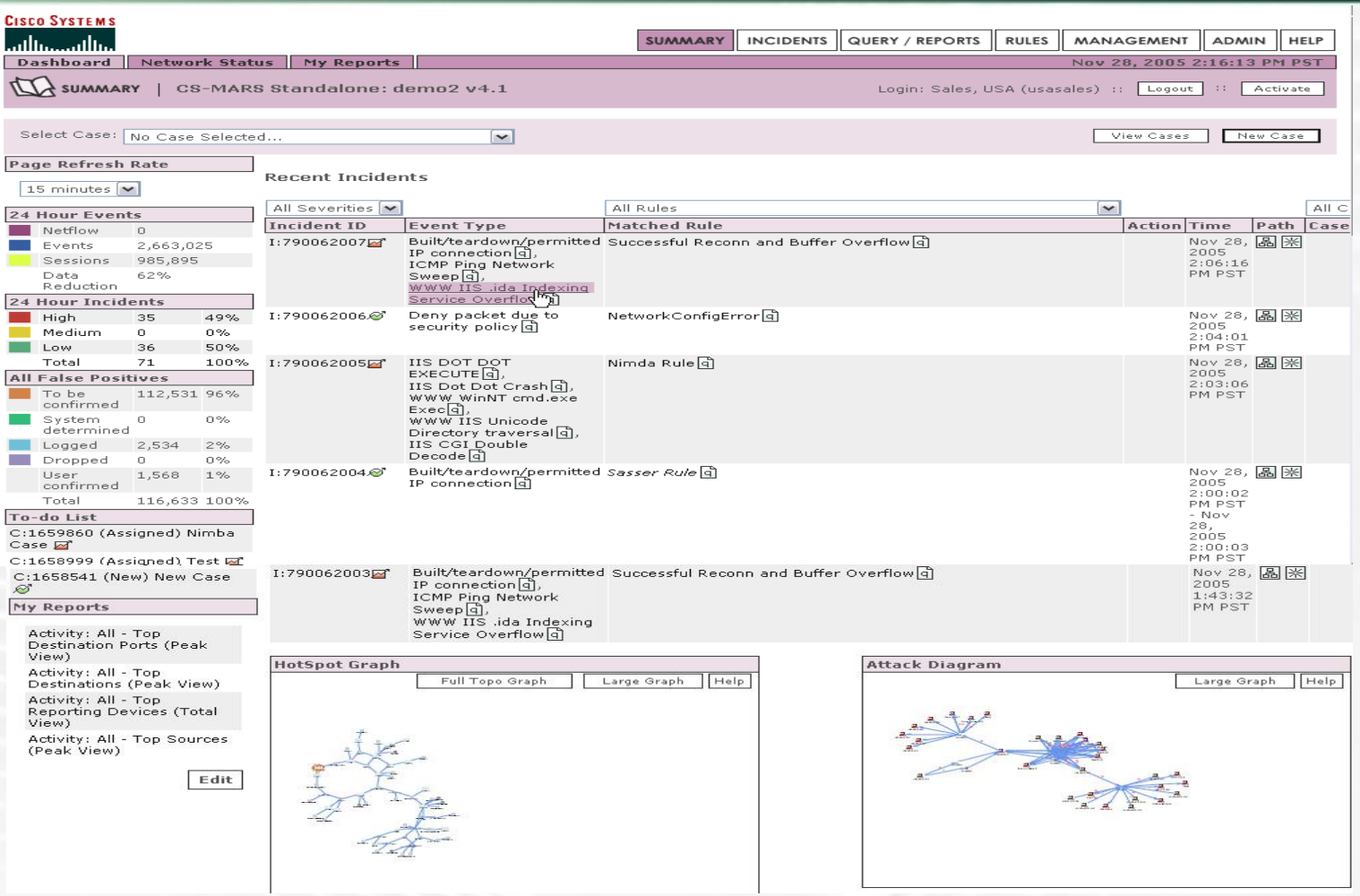
- Esemény (Event)
  - Riportoló eszközöktől (tűzfal, IPS, router) kapott nyers formátumú üzenet
- Kapcsolat (Session)
  - Korrelált esemény halmaz (NAT figyelembevételével)
- Incidens (Incident)
  - Kapcsolatok korrelációs szabályok alapján azonosított sorozata

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



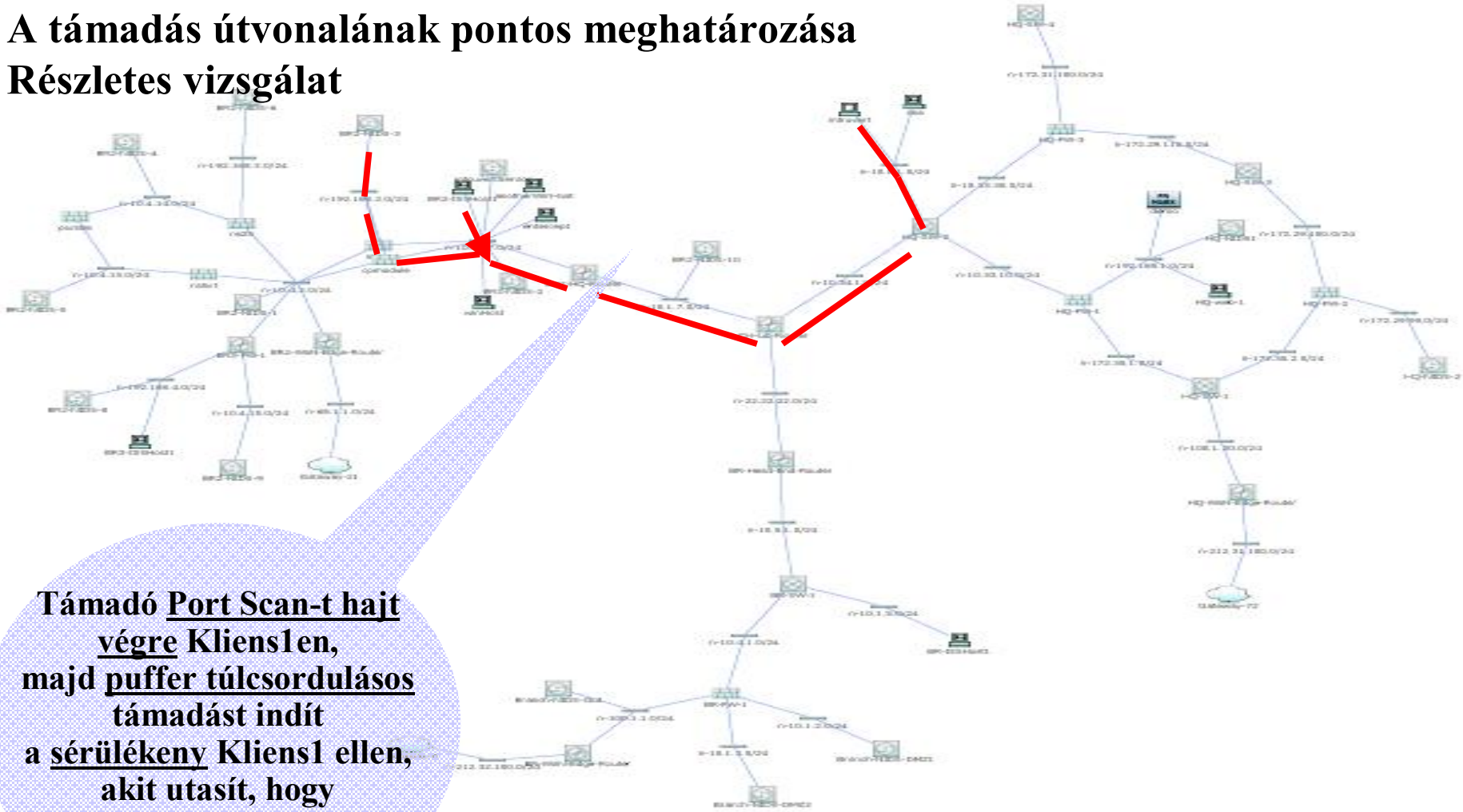
A MARS felszíne



Támadási útvonal meghatározás

SYNERGON
INFORMATION SYSTEMS PLC.

A támadás útvonalának pontos meghatározása
Részletes vizsgálat



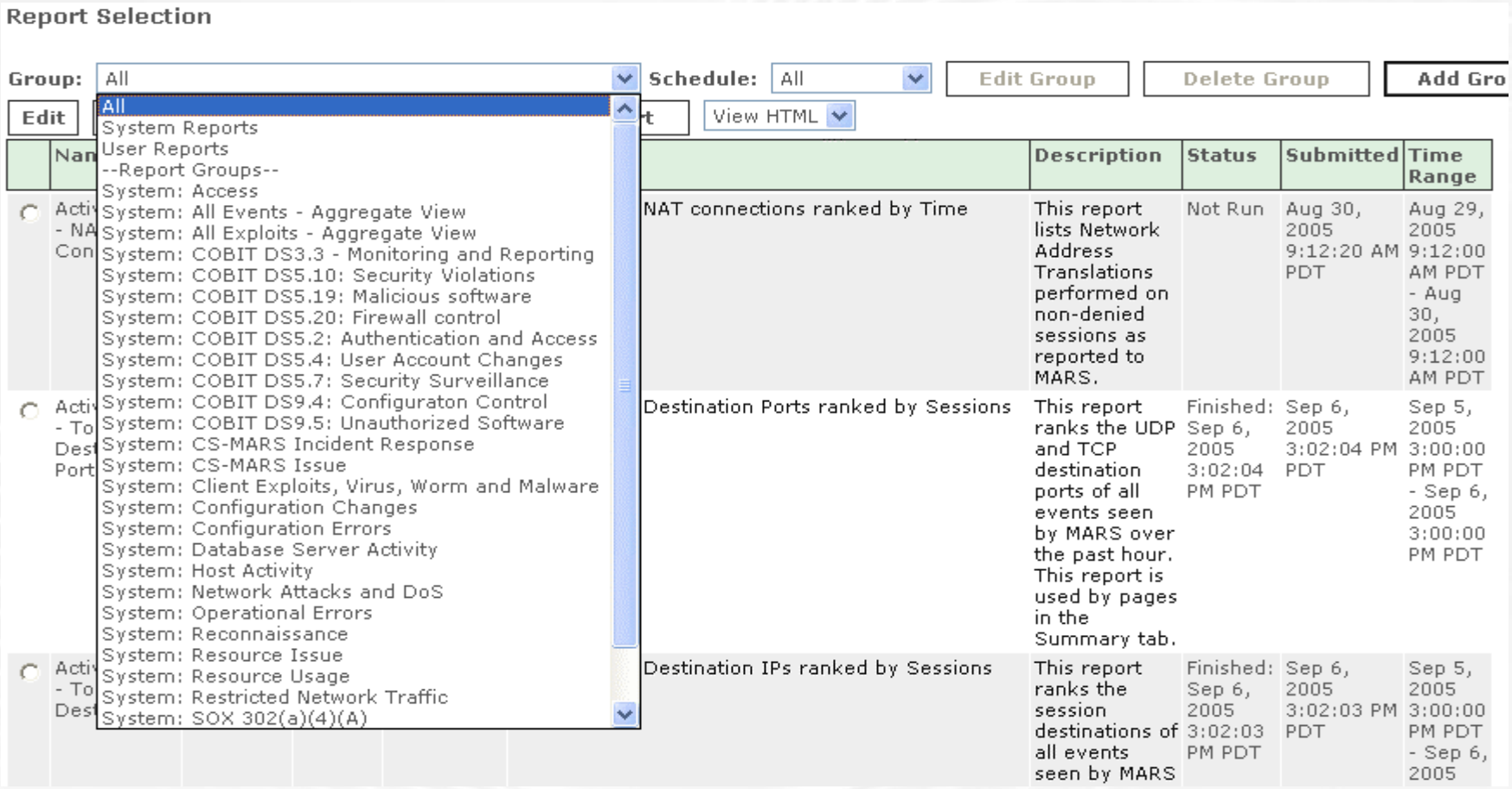
Támadó Port Scan-t hajt végre Kliens1en,
majd puffer túlcsordulásos támadást indít
a sérülékeny Kliens1 ellen,
akit utasít, hogy
jelszó támadást végezzen
Célpont ellen

SYNERGON GROUP

SPAN SAO infinity FibeX SYNERGON

Riport csoportok

- beépített és testreszabható riportok

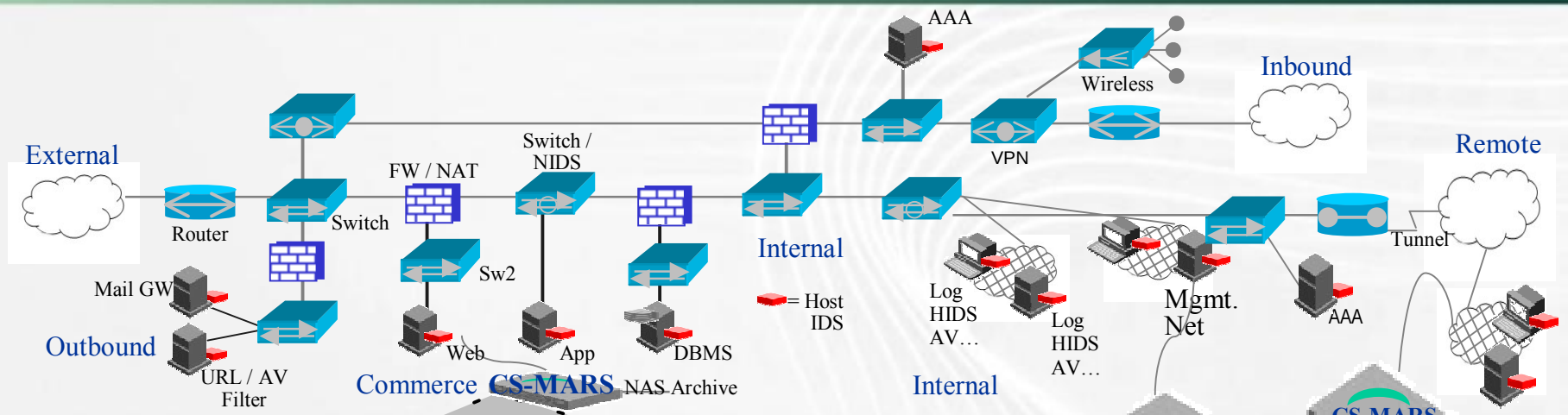


Alkalmazás

Támogatás

- McAfee ePolicy Orchestrator
- Network Admission Controll

Global Controller



CS-MARS
- passzív monitorozás
- hálózati topológia ismerete
- NAT kezelés, Netflow küszöbértékek beállítása
- Logok, riasztások, Netflow adatok korrelációja
- Valós indcidensek azonosítása (téves riasztások kiszűrése)
- Valós idejű megjelenítés, visszajátszás, lekérdezé
- Részletekbe menő vizsgálat
- Konszolidálja 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 sablokon és hozzáférési szabályok szétosztása

CS-MARS
távoli telephelyre kihelyezve, MARS GC felügyelet

SYNERGON
INFORMATION SYSTEMS PLC.

Hogyan látszik a Sasser a MARS-ról?

SYNERGON GROUP

SPAN SAO infinity FibeX SYNERGON

Incidens megjelenítés

SYNERGON INFORMATION SYSTEMS PLC.

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

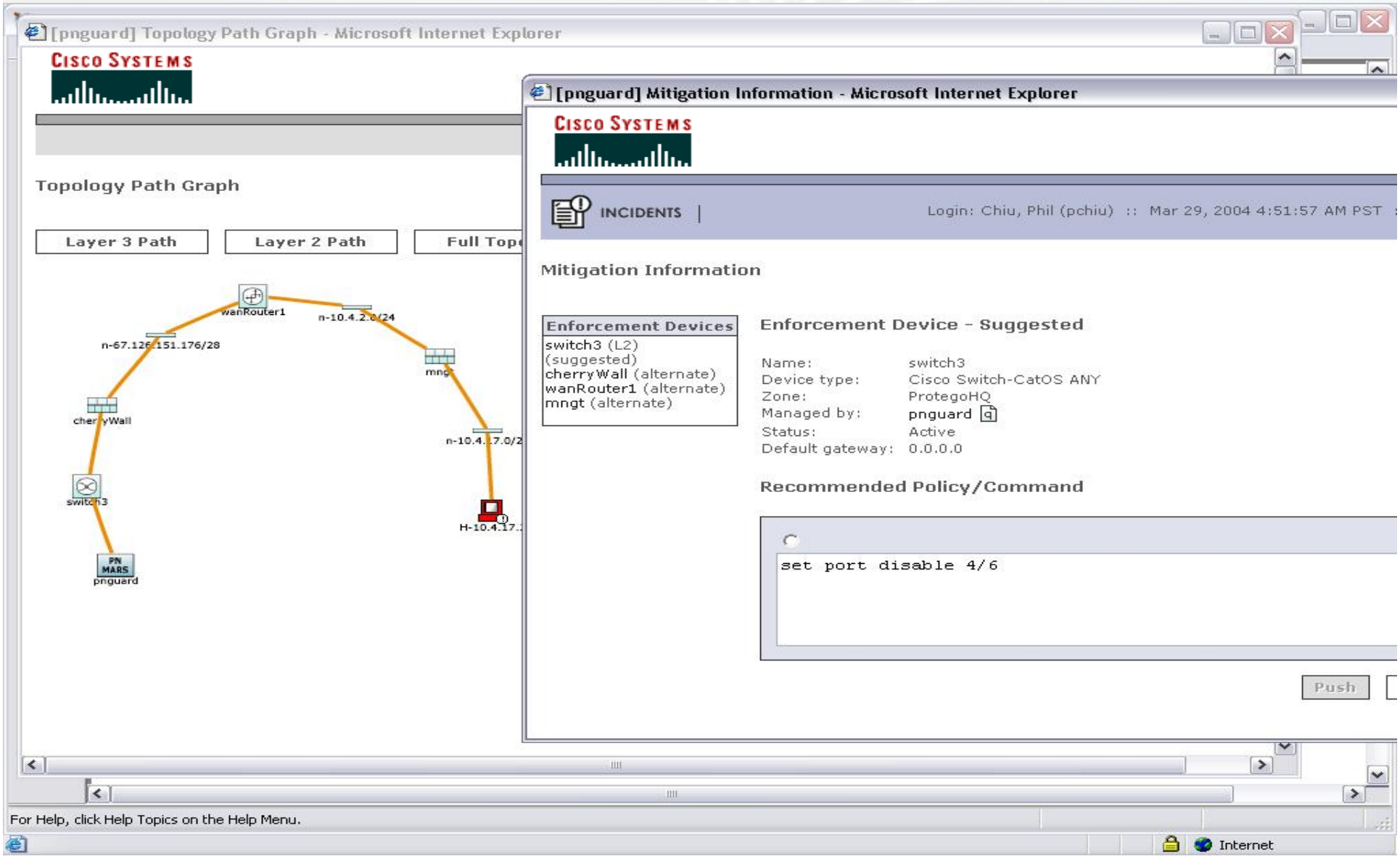
pen (	Source IP	Destination IP	Service Name	Event	Device	Severity	Counts	Zone	) Close	Action/Operation	Time-range
	ANY	ANY	ANY	System Rule: Sudden Traffic Increase To Port	ANY	ANY	1	NJIT			0hh:10mm:0ss

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

Támadás útvonala, Layer 2 beavatkozás

SYNERGON
INFORMATION SYSTEMS PLC.



Simon János
technikai tanácsadó, CCSP

SYNERGON
INFORMATION SYSTEMS PLC.

Köszönöm figyelmüket!
Várom kérdéseiket!

simon.janos@synergon.hu

http://www.cisco.com/go/mars
http://www.synergon.hu

SYNERGON GROUP SPAN SAO infinity FibeX SYNERGON