



A CISCO ÖNVÉDŐ HÁLÓZAT LEGÚJABB FEJLESZTÉSEI

ÁCS GYÖRGY
GACS@CISCO.COM



Networkshop 2006

Tartalom

IT biztonság - trendek

A Cisco önvédő hálózati koncepciója

Legújabb fejlesztések

Önvédő hálózatok – 2. fázis

Anti-X és SSL VPN szolgáltatások

Cisco Security Management Suite

Összefoglalás



IT BIZTONSÁG - TRENDK



Trendek

- Karantén szolgáltatások
- Hosztok védelme
- Biztonsági riportok – törvényi előírások
- Integrált biztonsági megoldások



A CISCO ÖNVÉDŐ HÁLÓZATI KONCEPCIÓJA



Cisco önvédő hálózati stratégiája

ÖNVÉDŐ HÁLÓZATI

Cisco stratégia, nagy mértékben javítja a hálózat képességét, hogy azonosítsa és megelőzze a veszélyeket, és adaptálódjon

**INTEGRÁLT
BIZTONSÁG**

**EGYÜTTMŰKÖDŐ
BIZTONSÁGI
RENDSZEREK**

**ADAPTÍV
FENYEGETÉS
ELHÁRÍTÁS**

LEGÚJABB FEJLESZTÉSEK



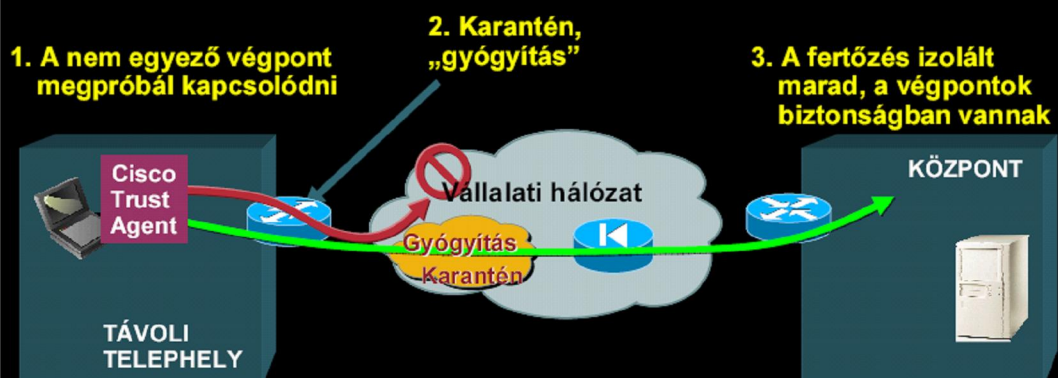
ÖNVÉDŐ HÁLÓZATOK - 2. FÁZIS



Eddigi megoldások veszélye



Ahogy a Network Admission Control működik



Cisco Network Admission Control (NAC)

- A NAC a Cisco vezette **iparági program**, melynek célja az egyre inkább elterjedő biztonsági veszélyek (férgék, vírusok) által okozott károk csökkentése
- A NAC által az üzemeltetők a hálózati hozzáférést a hiteles végpontok (PDA, PC, szerver) számára **engedélyezni** tudják, míg a nem megfelelő eszközöket **korlátozzák**
- Ez a fejlesztés nagy mértékben javítja a hálózat képességét, hogy azonosítsa, megelőzze a veszélyeket és adaptálódjon hozzájuk

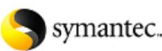


Erős NAC Partner Program

<http://www.cisco.com/en/US/partners/pr46/nac/partners.html>



SOPHOS



F-SECURE

金山在线
www.kingsoft.com



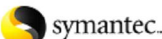
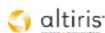
瑞星



ANTI VIRUS



REMEDATION



AUDIT



BELARC

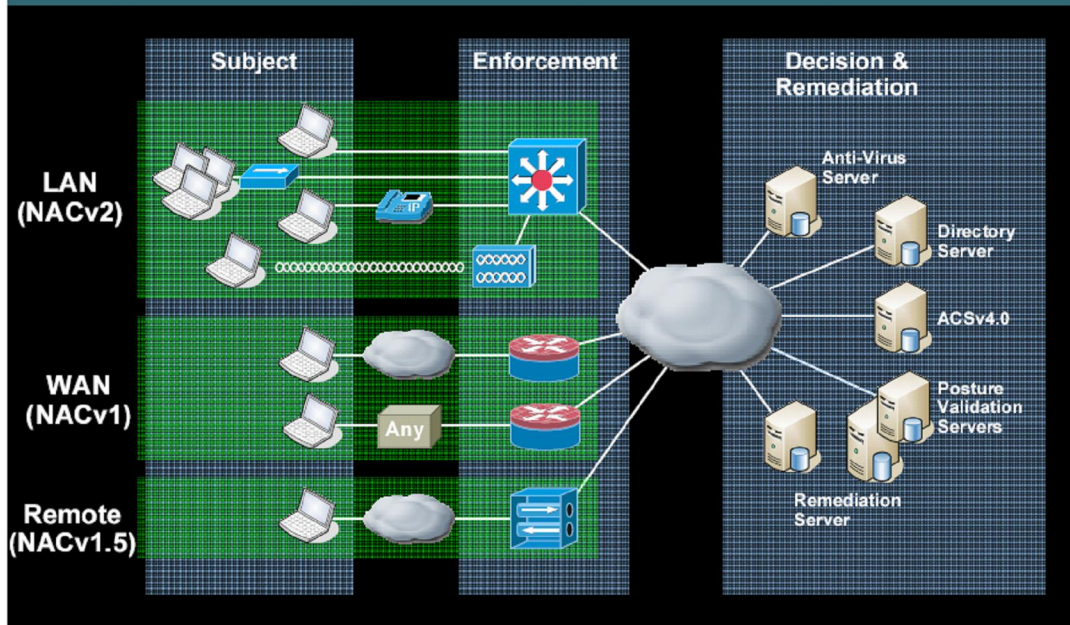


INTERNET SECURITY SYSTEMS



CLIENT SECURITY

NAC keretrendszer – megvalósítási esetek



ANTI-X ÉS SSL VPN SZOLGÁLTATÁSOK



ASA

- **Többfunkciós biztonsági megoldás:**
Tűzfal, VPN, **IPS, Antivírus, SSL VPN, ...**
- **Új hardver platform (alaplapi titkosító chip)**
- **ASA OS nagyon hasonló a PIX OS v7-hez**
Különbségek:
SSL VPN
IPS, antivírus/ SPAM / URL szűrő modulok
hardver adta különbségek (failover, USB)



Content Security and Control SSM - ASA Termék leírás

- **Funkciója: tartalom vezérlés, veszély elhárítás az internet bejáratnál, piac-vezető technológia:**
átfogó antivírus, anti-spyware,
file blocking,
anti-spam, anti-phishing,
URL blocking és filtering (munkaidő, azon túl -> kategóriánként),
tartalom szűrő szolgáltatások
- **díjnyertes anti-vírus technológia a Trend Micro's InterScan security suite alapján**
- **Teljes védelem átfogó vírus és malware adatbázis**



Modellek:

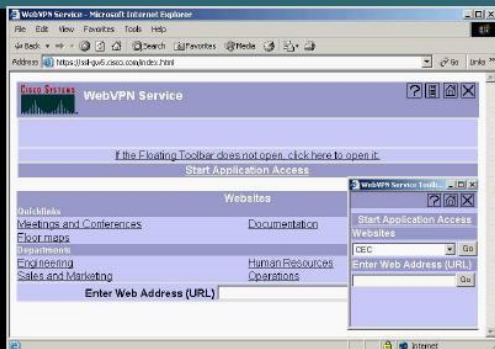
CSC-SSM-10 - 500 felhasználó

CSC-SSM-20 - 1000 felhasználó



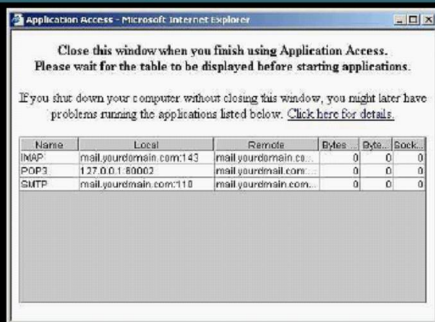
Trend Micro Certifications

Kliens nélküli hozzáférés Testreszabható távoli alkalmazás hozzáférés



- Bárhonnan hozzáférhetőek a cég felajánlott erőforrásai
- Web tartalom transzformáció > kompatibilitás a HTML és a JavaScript weblapokkal
- Egységes és hatékony alkalmazás megvalósítás – teljesen kliens nélküli Citrix támogatás
- Alkalmazások: Intranet (HTML és JavaScript), Citrix, Windows File Share (CIFS)
- Többféle browser támogatás – sokféle kapcsolat

Kliens nélküli hozzáférés Port Forwarding Application Helper



Java-based alkalmazás „helper” kiegészíti a kliens nélküli hozzáférést, kapcsolatot biztosít nem webes alkalmazásokhoz applications

- POP, SMTP vagy IMAP e-mail
- Instant messaging
- Calendar
- Kliens kezdeményezte TCP alapú alkalmazások, mint pl.: telnet

Cisco SSL VPN Client Teljes hálózati hozzáférés



Szolgáltatás	Előny
IPsec - szerű alkalmazás hozzáférés "web-pushed" kliens segítségével	Teljes hálózati hozzáférés
Csak központi konfiguráció	Alacsony működési költség
Kompatibilis a Cisco softphone-nal - VoIP támogatás	Multimédia - adat, hang
A kliens maradhat a kapcsolat végén az adott gépen, vagy törölhető	Nagyobb biztonság – kapcsolat után nincs nyoma a kliensnek
Kevesebb, mint 250KB	Gyors kliens letöltési idő
Nincs szükség újra indításra	Egyszerűbb, kényelmesebb

Nagy biztonságú VPN

Cisco Secure Desktop: átfogó végponti biztonság az SSL VPN számára

Teljes kapcsolat előtti kiértékelés:

- Hely kiértékelés – managed vagy unmanaged desktop?
- Security posture assessment – AV operational/up-to-date, personal firewall operational, malware present?

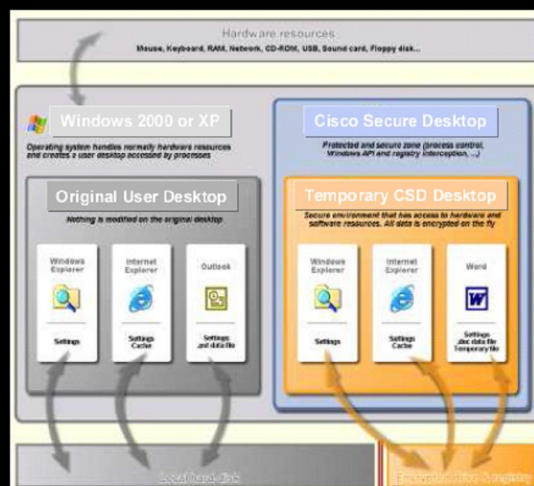
Átfogó kapcsolat alatti védelem:

- Adat „sandbox” és titkosítás véd minden kapcsolatot
- Malware detektálás a Microsoft free anti-spyware software segítségével

Kapcsolat utáni tisztítás

- Encrypted partition overwrite (not just deletion) using DoD algorithm
- Cache, history and cookie overwrite
- File download and email attachment overwrite
- Auto-complete password overwrite

Desktop Guest jogosultsággal is működik, nem kell admin jogosultság



CISCO SECURITY MANAGEMENT SUITE



Menedzsment alkalmazások

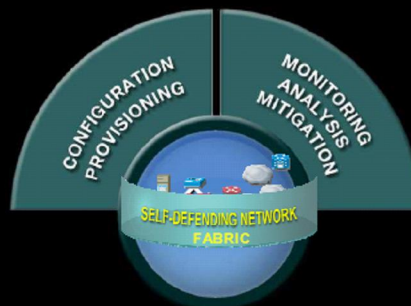
Cisco® Security Manager



Egyszerűsített **policy adminisztráció**

Végponttól végpontig terjedő konfiguráció

Hálózati széles vagy eszköz specifikus



Cisco® Security Mars



Gyors **veszély azonosítás** és enyhítés

Topológia tudása

Adat korreláció

ACS



Cisco Security Manager 3.0

✓ Feladata:

- **Kliens/szerver alkalmazás** a tűzfalak és a VPN menedzselésére - Cisco platformok támogatása
- **Könnyű, áttekinthető kezelhetőség** + skálázhatóság
- **Bővíthetőség:** CiscoWorks integráció, később IPS és más biztonsági technológiák vagy biztonsági menedzsment alkalmazások, mint például a CS-MARS

✓ Támogatott termékek

- PIX és ASA biztonsági megoldások, IOS Firewall, FWSM Service Modules, VPN Service Module és ISR VPN (8xx – 72xx),

✓ Támogatott technológiák

- **Teljes szolgáltatás lefedettség az appliance-ekre**, mint például a ASA/Pix/FWSM/VPNSM
- Biztonsági szolgáltatások az IOS eszközökön : ACL-ek, NAT, SSH/SSL, HTTPS, High Availability, Dial Backup, PKI, Certificates, **NAC**, stb....

Az alkalmazás opcionális előnyei

- **Egységes felhasználói tapasztalat és szolgáltatás halmaz** – **heterogén eszköz család** környezetben is
- **Komplex feladatok leegyszerűsített megvalósítása** grafikus felhasználói interfész segítségével
- **Non workflow és workflow modellek és RBAC (Role Based Access Control)** illetve felhasználói típusok - jogosultságok és szolgáltatások + rollback
- **Többféle nézet** – a különböző megközelítési módok közül a felhasználó választhat
 - Policy-based megközelítés
 - Device-based megközelítés
 - Map-based megközelítés

3 nézet: Device view

The screenshot shows the Cisco Security Manager interface in 'Device view'. The left sidebar contains a tree view of the device configuration, with 'Static Route' selected under the 'Routing' section. A yellow callout bubble labeled 'Eszköz választás' (Device selection) points to the 'Static Route' item. The main area displays a routing table for 'Static Route' with columns: Interface, Network, Gateway, Metric, and Tunnelled. A yellow callout bubble labeled 'Actuális beállítás' (Current settings) points to the 'Gateway' column. Another yellow callout bubble labeled 'Policy választás' (Policy selection) points to the 'Static Route' item in the left sidebar.

Interface	Network	Gateway	Metric	Tunnelled
Inside	any	193.23.35.195/32	5	
Outside	157.147.6.0/16	193.23.35.213/32	2	
Outside	157.147.6.0/21	193.23.35.213/32	2	
Outside	157.147.72.0/21	193.23.35.213/32	2	
Outside	157.147.73.0/24	193.23.35.213/32	2	
Outside	157.147.74.0/24	193.23.35.213/32	2	
Outside	157.147.75.0/24	193.23.35.213/32	2	
Outside	157.147.76.0/24	193.23.35.213/32	2	
Outside	157.147.77.0/24	193.23.35.213/32	2	
Outside	157.147.78.0/21	193.23.35.213/32	2	
Outside	157.147.79.0/24	193.23.35.213/32	2	
Outside	157.147.106.0/24	193.23.35.213/32	2	
Outside	157.148.0.0/16	193.23.35.213/32	2	
Outside	157.148.128.0/19	193.23.35.213/32	2	
Outside	167.16.0.0/16	193.23.35.213/32	2	
Outside	172.17.192.0/24	193.23.35.213/32	2	
Outside	172.17.193.0/21	193.23.35.213/32	2	
Outside	172.17.194.0/24	193.23.35.213/32	1	
Outside	172.17.195.0/26	193.23.35.213/32	2	
Outside	172.17.195.64/26	193.23.35.213/32	2	
Outside	172.17.195.128/28	193.23.35.213/32	2	
Outside	172.17.195.192/26	193.23.35.213/32	2	

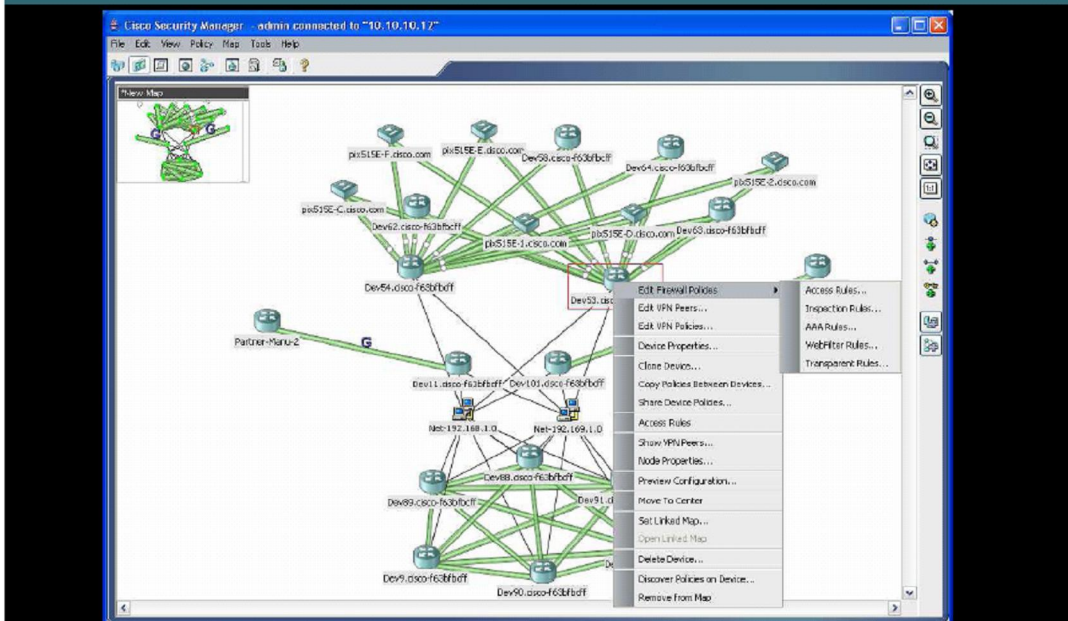
3 nézet: Policy View

The screenshot shows the Cisco Security Manager interface in 'Policy View'. The left sidebar shows a tree view of policy configurations, with 'Worm Mitigation' selected under the 'Policies' section. The main area displays a table of policies with columns: No., Permit, Source, Destination, Service, Options, and Interface. A yellow callout bubble labeled 'Ebben a nézetben konfigurálhatók a skálázhatósági szolgáltatások:' (In this view, scalability services can be configured:) points to the table. Below the table, a yellow callout bubble labeled 'Policy Inheritance (örökítés)' (Policy Inheritance (inheritance)) points to the 'Permit' column. Another yellow callout bubble labeled 'Policy Assignment (csatolás)' (Policy Assignment (assignment)) points to the 'Options' column. A third yellow callout bubble labeled 'Policy Sharing (megosztás)' (Policy Sharing (sharing)) points to the 'Interface' column.

No.	Permit	Source	Destination	Service	Options	Interface
1	any	any	any	Sasser		AllInterf
1	any	any	any	IP		AllInterf

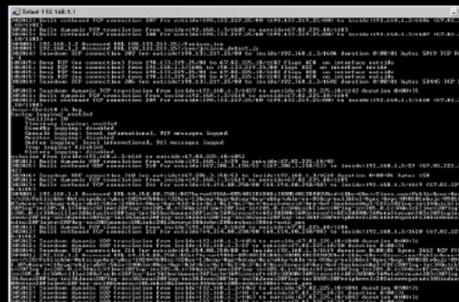
- **Policy Inheritance (örökítés)**
- **Policy Assignment (csatolás)**
- **Policy Sharing (megosztás)**

3 nézet: Map centric view



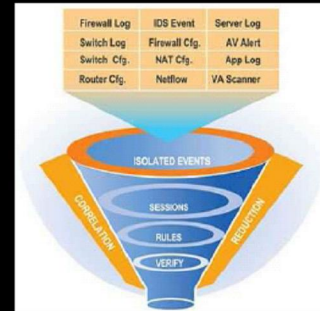
Biztonsági incidensek kezelése

- Támadások mindig lesznek -> elő kellene készülni
- Sokféle hálózati és biztonsági eszköz -> gigantikus mennyiségű napló -> valódi esemény?
- Válaszreakció?
- Törvényi előírások: Sarbanes-Oxley, Mo.: PSZÁF



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 **lokálizálja és enyhíti** a támadásokat



- Főbb jellemzők



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

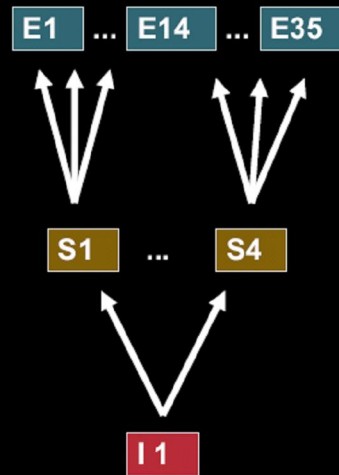
Az incidens **topológiájának birtokában** lehetőség van ábrázolásra és visszajátzásra

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



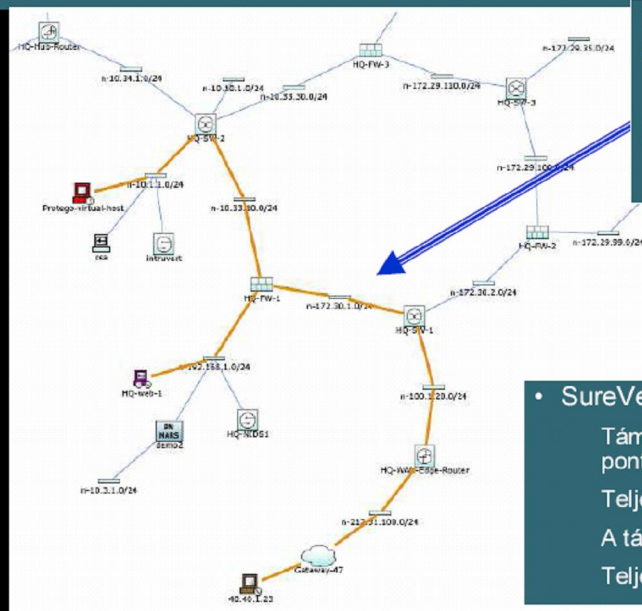
CS-MARS – analízis egy lapon

The screenshot shows the CS-MARS web interface. At the top, there are navigation tabs: SUMMARY, INCIDENTS, QUERY / REPORTS, RULES, MANAGEMENT, ADMIN, HELP. Below this is a dashboard with several sections:

- Page Refresh Rate:** Set to 15 minutes.
- Recent Incidents:** A table listing incidents with columns for Incident ID, Event Type, Matched Rule, Action, Time, and Path.

Incident ID	Event Type	Matched Rule	Action	Time	Path
145713706	IS DOT DOT EXECUTE	Mimda Rule		Nov 3, 2004 1:22:09 PM PST	
145713704	IS Dot Dot Crash				
145713703	WWW WinNT cmd.exe Exec				
145713702	WWW IIS Unicode Directory traversal				
145713701	IS CGI Double Decode				
145713700	Built/teardown/permited IP connection	Sasser Rule		Nov 3, 2004 1:21:50 PM PST	
145713699	Deny packet due to security policy	Network.ConfigError		Nov 3, 2004 12:02:19 PM PST	
145713698	Deny packet due to security policy	Network.ConfigError		Nov 3, 2004 12:05:19 PM PST	
145713697	IS DOT DOT EXECUTE	Mimda Rule		Nov 3, 2004 12:02:41 PM PST	
145713696	IS Dot Dot Crash				
145713695	WWW WinNT cmd.exe Exec				
145713694	WWW IIS Unicode Directory traversal				
145713693	IS CGI Double Decode				
- 24 Hour Events:** Summary of network events, sessions, and data reduction.
- 24 Hour Incidents:** Summary of incidents by severity (High, Medium, Low).
- All False Positives:** Summary of false positives.
- HotSpot Graph:** A network diagram showing connections between various nodes.
- Attack Diagram:** A diagram showing the flow of an attack through the network.
- ToDo List:** No escalated incidents.
- My Reports:** No reports selected.

CS-MARS - a végpontok összekötése

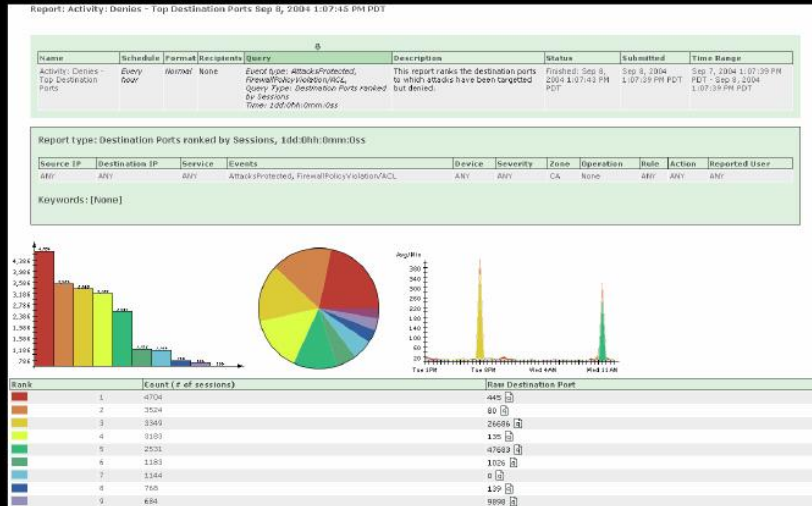


1. Host A port szkeneli X célt
2. Host A Buffer Overflow támadja X-et, ahol X NAT eszköz mögött van és X sérülékeny az adott támadásra
3. X cél jelszó támadást hajt végre Y cél ellen, ami egy NAT mögött lévő eszköz

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

CS-MARS megfelelıségi riportok

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



KÉRDÉSEK
ÉS
VÁLASZOK



ÖSSZEFOGLALÁS



Összefoglalás

Témák:

- IT biztonsági trendek
- Legújabb megoldások:
 - Önvédő hálózatok – 2. fázis
 - Anti-x és SSL VPN szolgáltatások
 - Cisco Security Management Suite

További információ

NAC

www.cisco.com/go/nac

ASA

www.cisco.com/go/asa

CS Manager

www.cisco.com/go/csmanager

MARS

www.cisco.com/go/mars

Cisco SAFE Blueprints

www.cisco.com/go/safe

CISCO SYSTEMS

