

■ L'arte e la cultura dell'impresa

ciscoexpo

2005



Managing the Self Defending Network

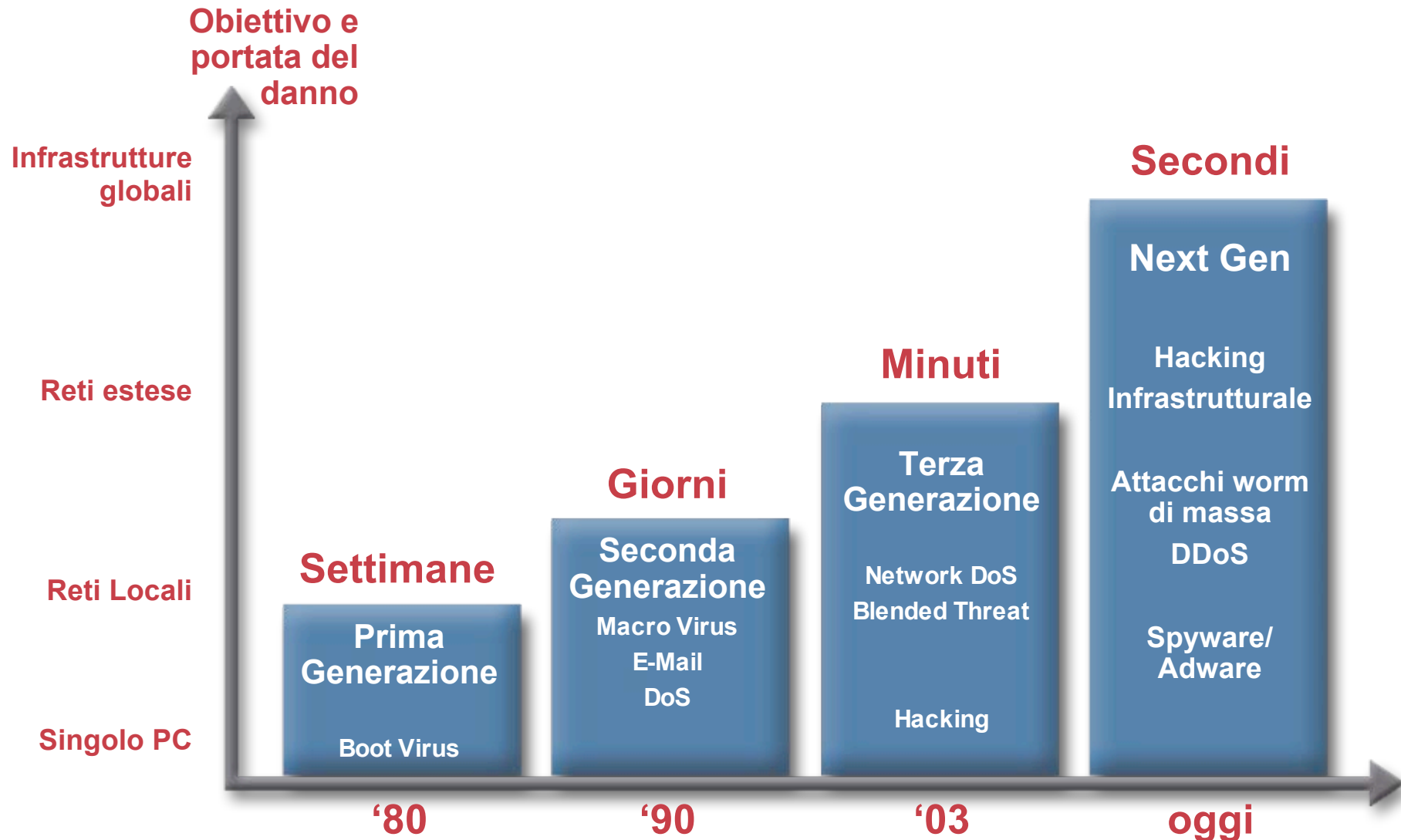
Marco Misitano, CISSP, CISM

Cisco Systems Italy
misi@cisco.com

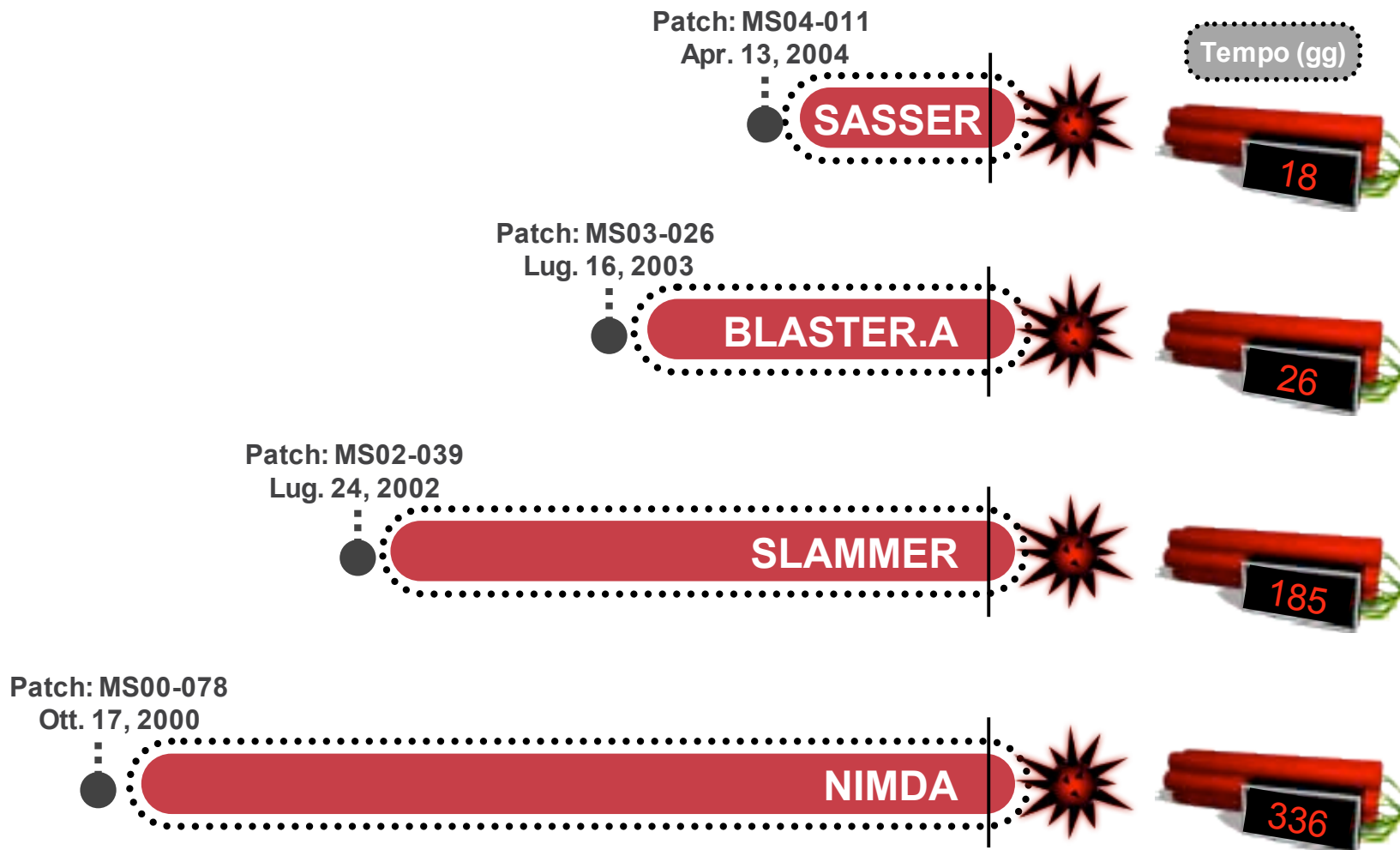
L'arte e la cultura dell'impresa
ciscoexpo
2005

Introduzione

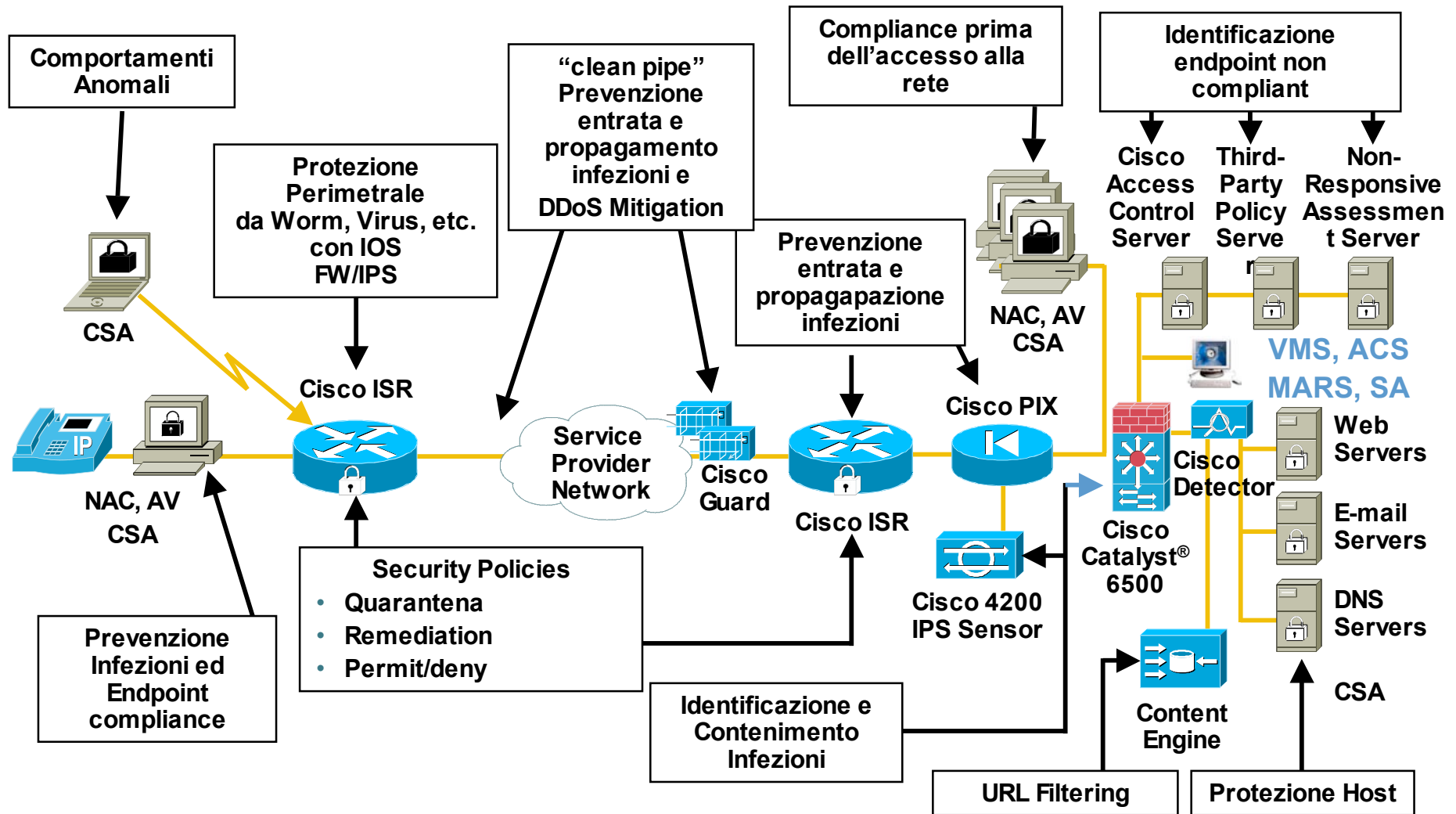
Evoluzione del problema /1



Evoluzione del problema /2



Soluzioni ad problema /3

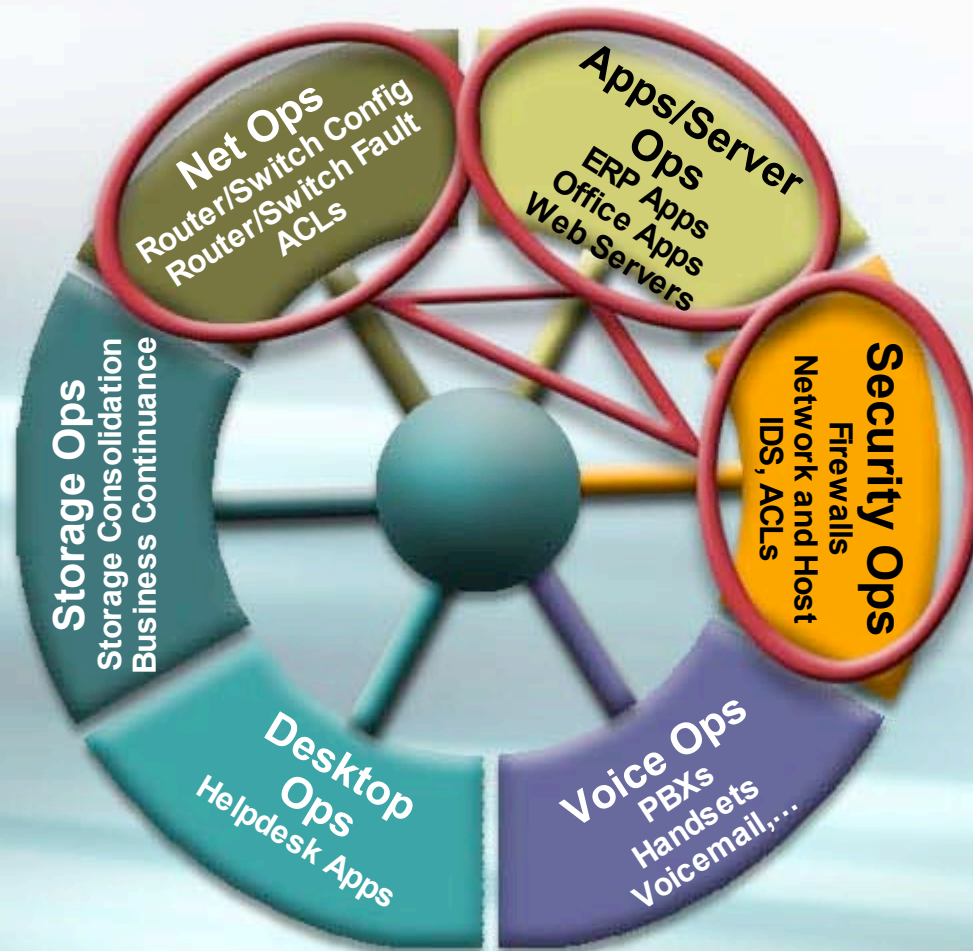


Definizione del problema

- **Information overload !**
- **Si può non guardare le informazioni....ma ?**
- **Succedono svariate cose nella rete....**
 - Audit in ogni momento**
 - Verificare l'efficacia delle configurazioni**
 - Semplificare la gestione di ambienti complessi**
 - Team non si ampliano. Necessità di fare di più con meno risorse**
- **Il Management é maturato, ma c'e' ancora da fare**
 - Automatizzare di più**
 - Incident response**

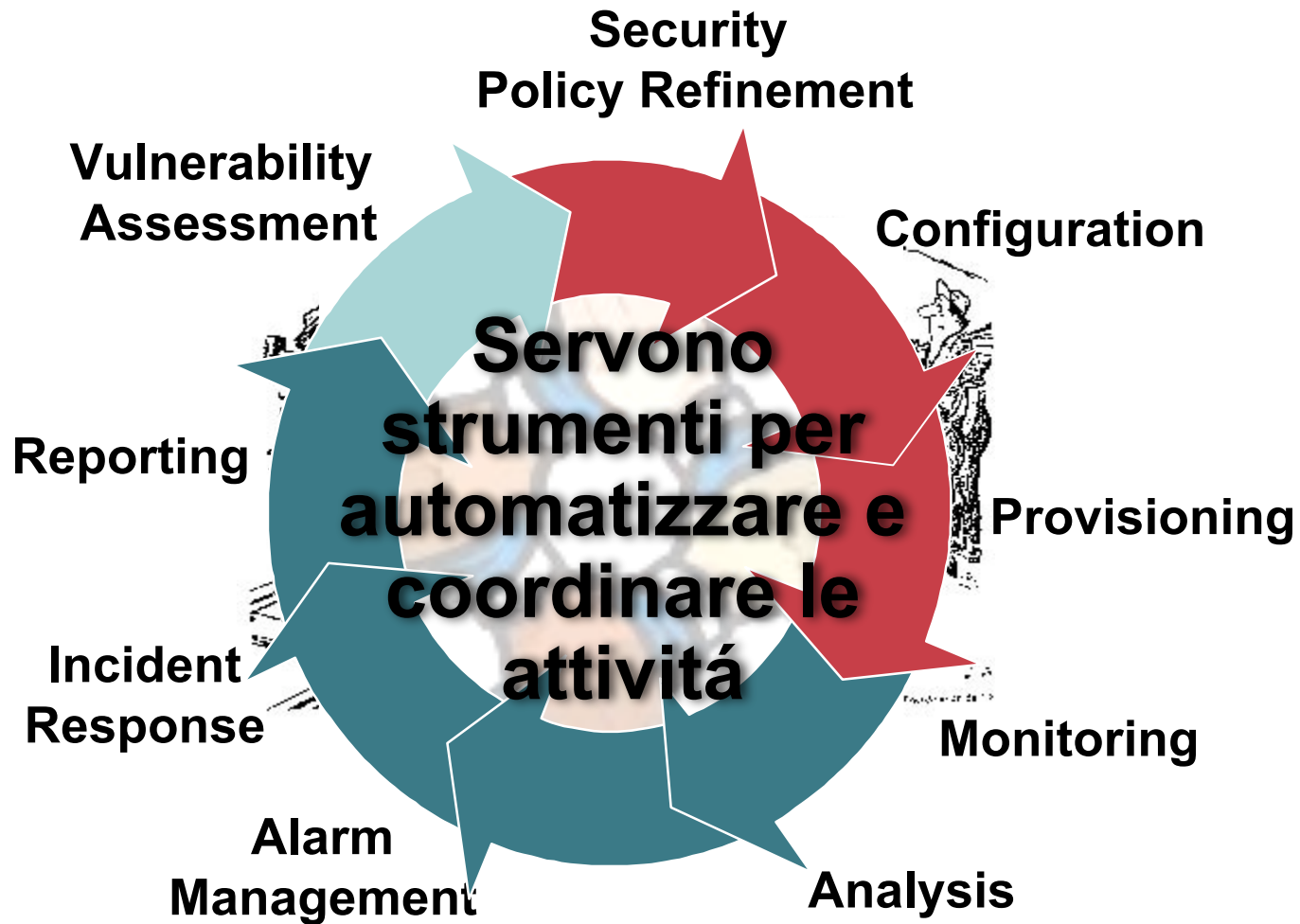
Il problema organizzativo

- **Gruppi Security, network, application/server**
- **La sicurezza non può essere gestita indipendentemente dalla infrastruttura**



- **La sicurezza é integrata nella rete**
- **L'adozione di endpoint security**
- **Identità e controllo degli accessi**
- **VPN, Firewall, IDS/IPS**

Ciclo di vita della Sicurezza

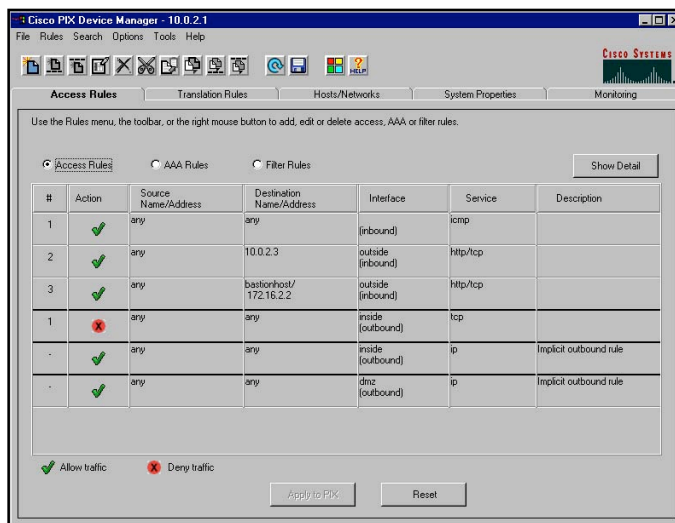


Configurazione

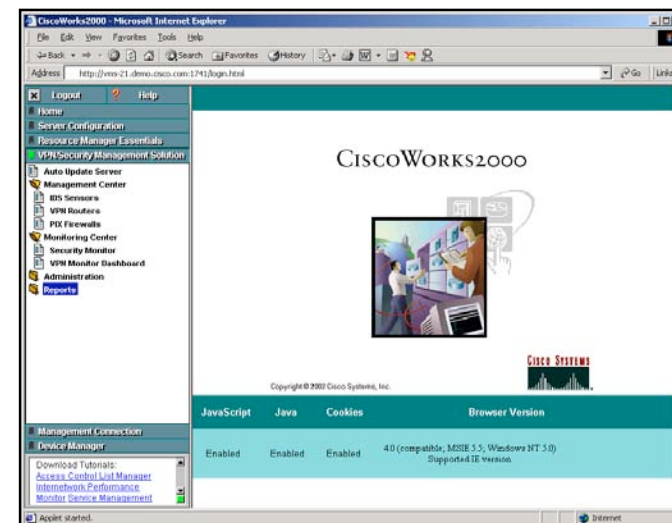
Selezionare lo strumento giusto

Il Management deve far risparmiare

- Singolo Device Manager per pochi devices, per numeri crescenti ed esigenze piu sofisticate, multi device manager come CiscoWorks
- Value proposition: 'configure once, deploy many'



Device Manager



CiscoWorks VPN and Security Management Solutions

Element Management per la gestione di piccole reti

L'arte e la cultura dell'impresa
ciscoexpo
2005

- **PIX® firewalls**
PIX Device Manager (ASDM)
- **ASA**
ASA Device Manager (ASDM)
- **IDS sensors**
Intrusion Device Manager (IDM)
- **Cisco IOS routers** 
Security Device Manager (SDM)
- **VPN 3000**
VPN 3000 Device Manager (VDM)
- **Catalyst 6000**
Cisco View Device Manager (CVDM)



Cisco Security Device Manager

L'arte e la cultura dell'impresa
ciscoexpo
2005

SDM é uno strumento Web-Based per la gestione di Cisco Router IOS individuali



Security Audit Wizard

Check the "Fix it" check-box to select fixing the security problem. Click "Next" to continue. You may be prompted to enter the values if required.

Save Report Fix All

No.	Security Problems Identified	Action
1	PAD Service is enabled	<input type="checkbox"/> Fix it
2	IP bootp server Service is enabled	<input type="checkbox"/> Fix it
3	CDP is enabled	<input type="checkbox"/> Fix it
4	IP source route is enabled	<input type="checkbox"/> Fix it
5	Password encryption Service is disabled	<input type="checkbox"/> Fix it
6	TCP Keepalives for inbound telnet sessions is disabled	<input type="checkbox"/> Fix it
7	TCP Keepalives for outbound telnet sessions is disabled	<input type="checkbox"/> Fix it
8	Sequence Numbers and Time Stamps on Debugs are disabled	<input type="checkbox"/> Fix it
9	IP CEF is disabled	<input type="checkbox"/> Fix it
10	Minimum Password length is disabled or less than 6 characters	<input type="checkbox"/> Fix it
11	Authentication Failure Rate is disabled or less than 3 retries	<input type="checkbox"/> Fix it
12	Scheduler Interval is not set	<input type="checkbox"/> Fix it
13	Banner is not set	<input type="checkbox"/> Fix it
14	Logging is not enabled	<input type="checkbox"/> Fix it
15	Scheduler Allocate is not set	<input type="checkbox"/> Fix it
16	Telnet settings are not enabled	<input type="checkbox"/> Fix it
17	NetFlow switching is not enabled	<input type="checkbox"/> Fix it
18	IP Redirects is enabled	<input type="checkbox"/> Fix it

< Back Next > Finish Cancel Help

Adaptive Security Device Manager (ASDM)

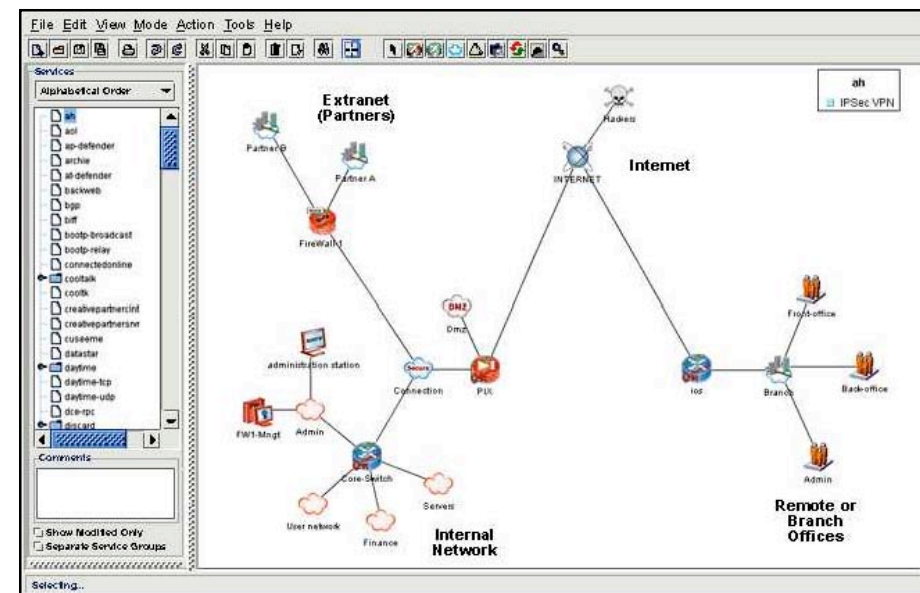
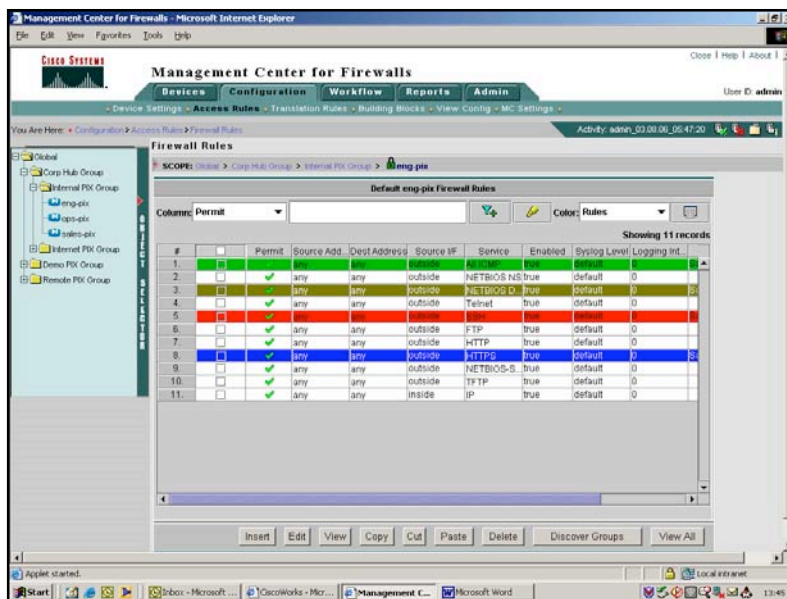
L'arte e la cultura dell'impresa
ciscoexpo
2005

The screenshot displays the Cisco ASDM 5.0 for PIX web interface. The main window shows the 'Configuration > Features > Security Policy' path. A 'Live Log' window is open, displaying a list of messages. The 'Filter Incoming Messages' section is set to filter by the IP address '10.48.82.67'. The 'Find Messages' section is empty. The log table shows the following data:

Severity	Time	Message
7	Apr 26 2005 09:20:07	710005: UDP request discarded from 10.48.82.67/1985 to inside:224.0.0.2/1985
7	Apr 26 2005 09:20:04	710005: UDP request discarded from 10.48.82.67/1985 to inside:224.0.0.2/1985
7	Apr 26 2005 09:20:01	710005: UDP request discarded from 10.48.82.67/1985 to inside:224.0.0.2/1985
7	Apr 26 2005 09:19:58	710005: UDP request discarded from 10.48.82.67/1985 to inside:224.0.0.2/1985
7	Apr 26 2005 09:19:55	710005: UDP request discarded from 10.48.82.67/1985 to inside:224.0.0.2/1985
7	Apr 26 2005 09:19:52	710005: UDP request discarded from 10.48.82.67/1985 to inside:224.0.0.2/1985
7	Apr 26 2005 09:19:49	710005: UDP request discarded from 10.48.82.67/1985 to inside:224.0.0.2/1985
7	Apr 26 2005 09:19:46	710005: UDP request discarded from 10.48.82.67/1985 to inside:224.0.0.2/1985
7	Apr 26 2005 09:19:43	710005: UDP request discarded from 10.48.82.67/1985 to inside:224.0.0.2/1985
7	Apr 26 2005 09:19:40	710005: UDP request discarded from 10.48.82.67/1985 to inside:224.0.0.2/1985
7	Apr 26 2005 09:19:37	710005: UDP request discarded from 10.48.82.67/1985 to inside:224.0.0.2/1985
7	Apr 26 2005 09:19:34	710005: UDP request discarded from 10.48.82.67/1985 to inside:224.0.0.2/1985
7	Apr 26 2005 09:19:31	710005: UDP request discarded from 10.48.82.67/1985 to inside:224.0.0.2/1985

The interface also shows a sidebar with navigation options: Features, Interfaces, Security Policy, NAT, VPN, IPS, Routing, Building Blocks, Device Administration, Properties, and Wizards. The status bar at the bottom indicates the user is 'admin' and the time is 9/8/04 8:58:29 PM PDT.

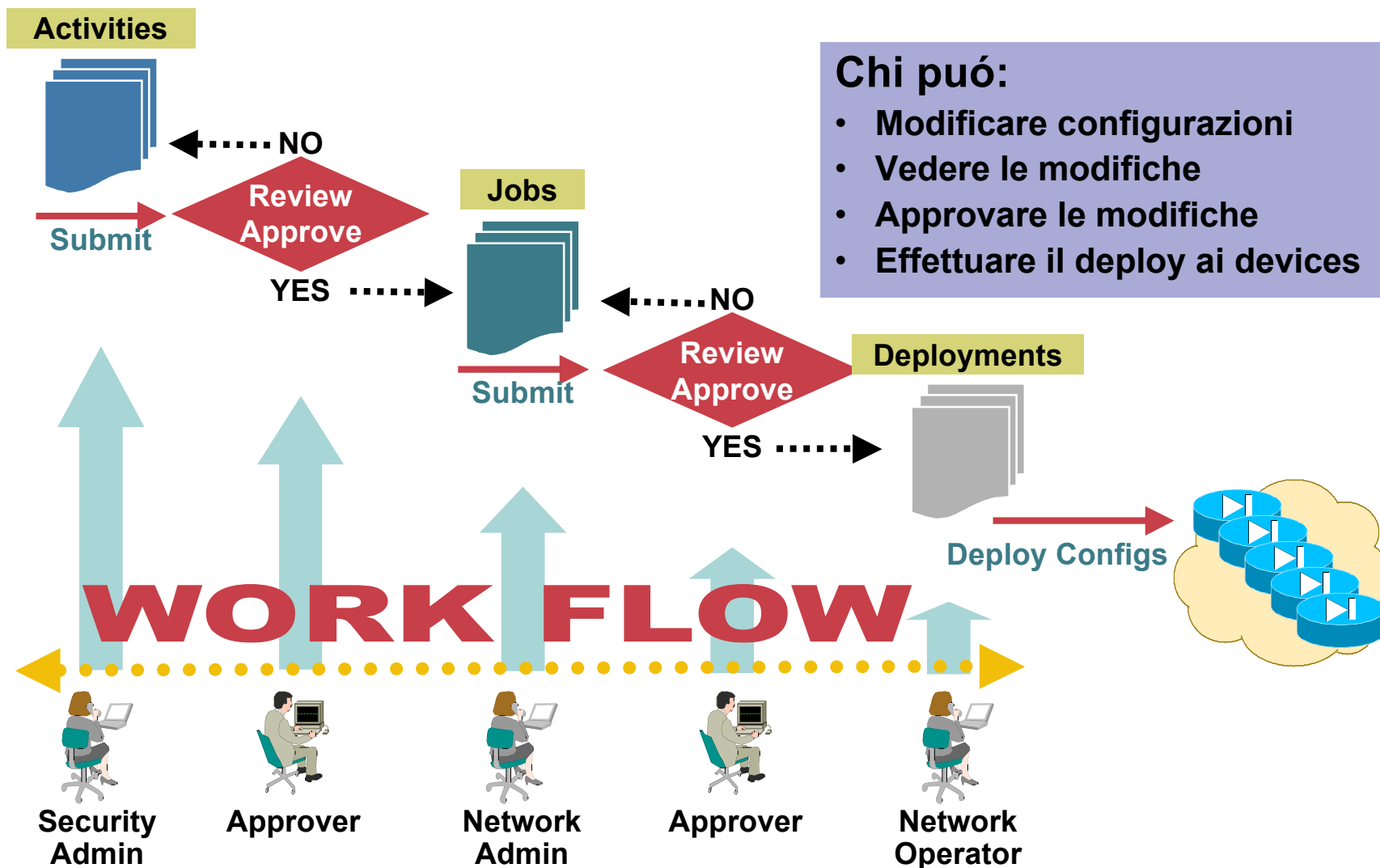
Multidevice o Policy-Based



- **VMS:**
cosa é comune ai dispositivi e possibilità di configurazione a gruppi

- **Solsoft (Cisco Partner):**
gestione multivendor grafica

Ruoli e Responsabilità



CiscoWorks VMS

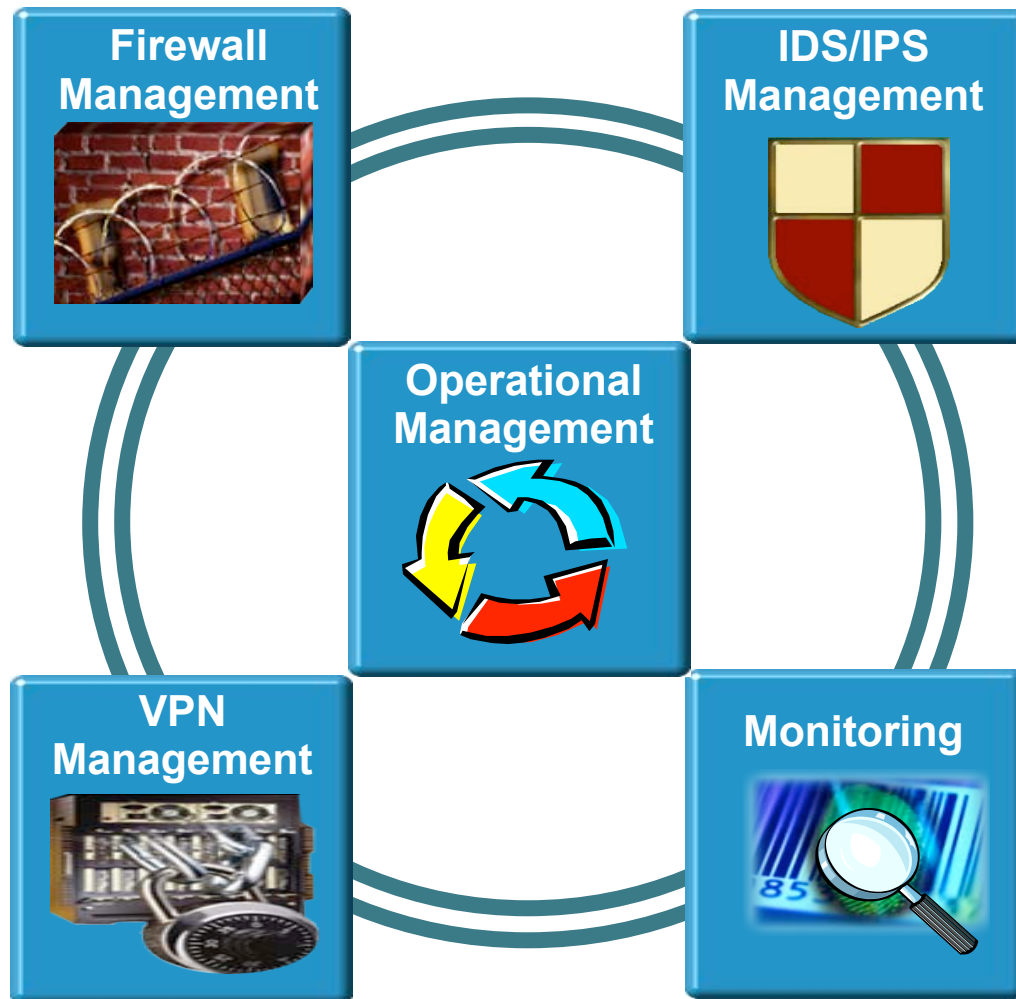
Supporto per l'intero lifecycle

Security Management
Multitecnologia Integrato

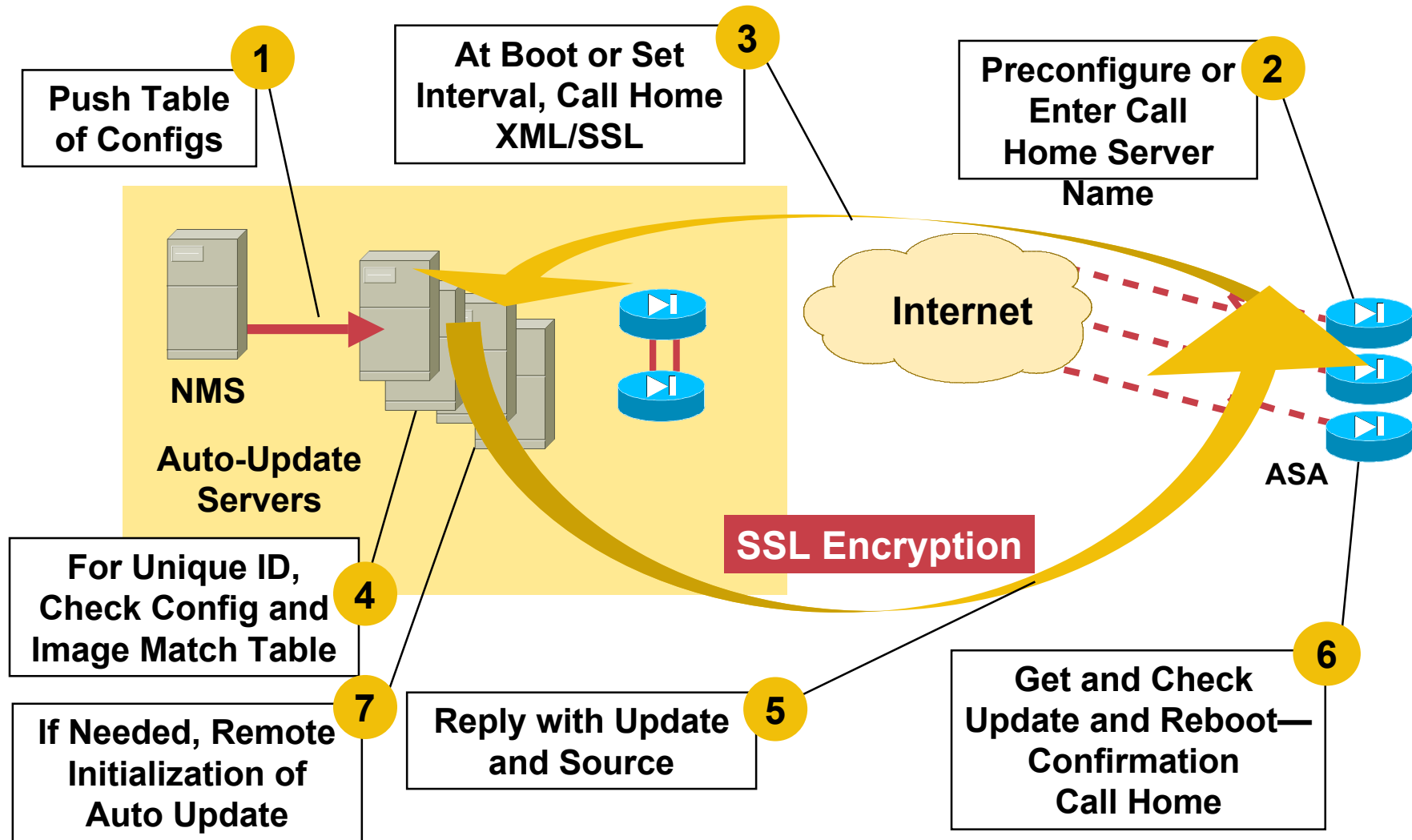
Integrazione della
gestione operativa

Miglioramento della
efficienza operativa

Monitoring delle
performances e dei processi



Tecnologia Call-Home (PIX, ASA)



Monitoring

Security Logging



	Events/Sec	MB/Hr
Small VPN Gateway	50	27.4
Entry Firewall	100	54.8
High Router	200	109.6
Mid IPS	400	219.2

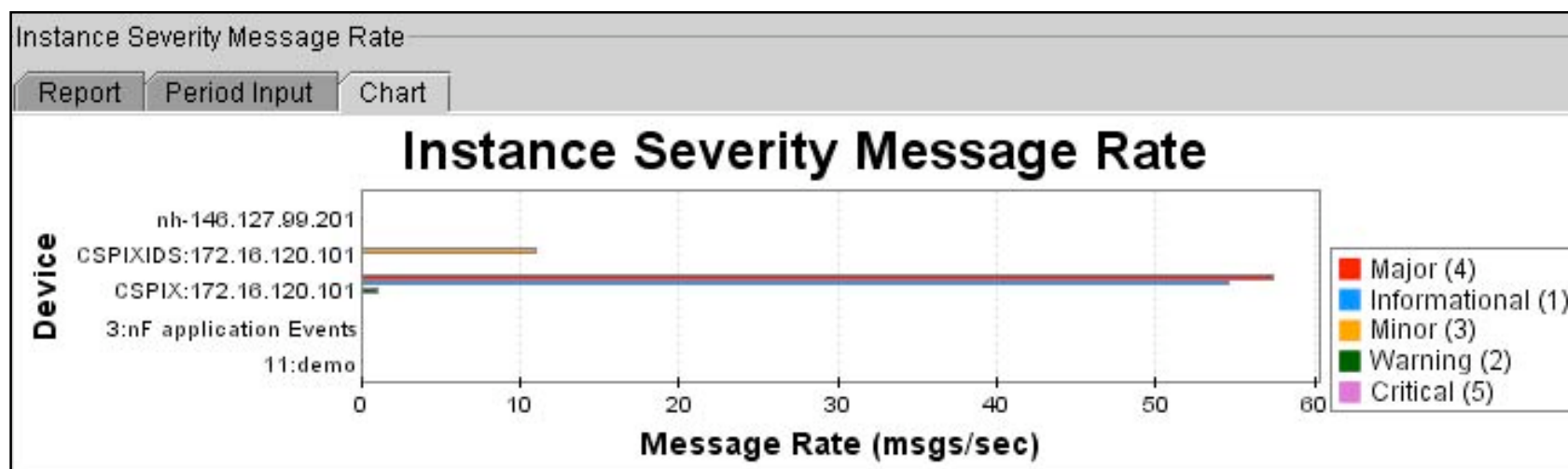
Strategie:

- Non ne ho bisogno, non loggo.
- Non lo guardo, ma lo loggo.
- Loggo solo ciò che mi interessa
- Devo loggare per ragioni legali



EPS: Best Practices

- **Abilitare tutti gli eventi; dopo qualche giorno i report mi daranno delle figure**
- **Disabilitare eventi che non mi interessano..**



Host IPS Management

Management Center for Cisco Security Agents

Close | Help | About

Monitor Systems Configuration Maintenance Reports Profiler Search Help

Systems > Groups > IIS Web Servers - Dedicated

OTHER GROUPS

Quick links

- [Modify host membership](#)
- [Modify policy associations](#)
- [View related events](#)
- [Explain rules](#)

Name: IIS Web Servers - De

Description: **Microsoft IIS** web se

Target operating sy: Windows

View All rules

Items : 85 (click the header links to sort)

ID	Type	Status	Action	Log	Description	Policy
59	Application control	Enabled	+	✗	Application builder rule, add to Virus scanner services applications	Virus Scanner Module
30	Agent service control	Enabled	✗	✗	All applications, modify agent configuration (exclude Virus Scanners from logging)	Required Windows System Module V4.0.0.119
118	Data access control	Enabled	✗	✗	IIS and Apache Web Servers, Common Windows file exploits	Common Web Server Security Module
290	Application control	Enabled	✓	✗	Installers, invoke Command shell, regedit, net, ...	Common Security Module
297	Application control	Disabled	✓	✗	Mass software deployment applications, invoke Installation applications	Common Security Module
31	Application control	Enabled	✓	✗	Desktop interface applications, invoke Command Shells (DOS command line)	Required Windows System Module V4.0.0.119
33	Application control	Enabled	✓	✗	MS User Init application, invoke MS Logon Setup application	Required Windows System Module V4.0.0.119

Legend:

- ✗ High Priority Deny
- ✓ Allow
- ? Query User (Default Allow)
- ? Query User (Default Deny)
- ✗ Deny

Sofisticazione della Prevenzione

Risk Rating: raggiungere il massimo dell'affidabilità!

Event Severity

Quanto è pericoloso o urgente?

Signature Fidelity

Quanto è possibile che sia un falso?

Attack Relevancy

E' rilevante per il bersaglio?

Asset Value of Target

Quanto è critico il bersaglio?

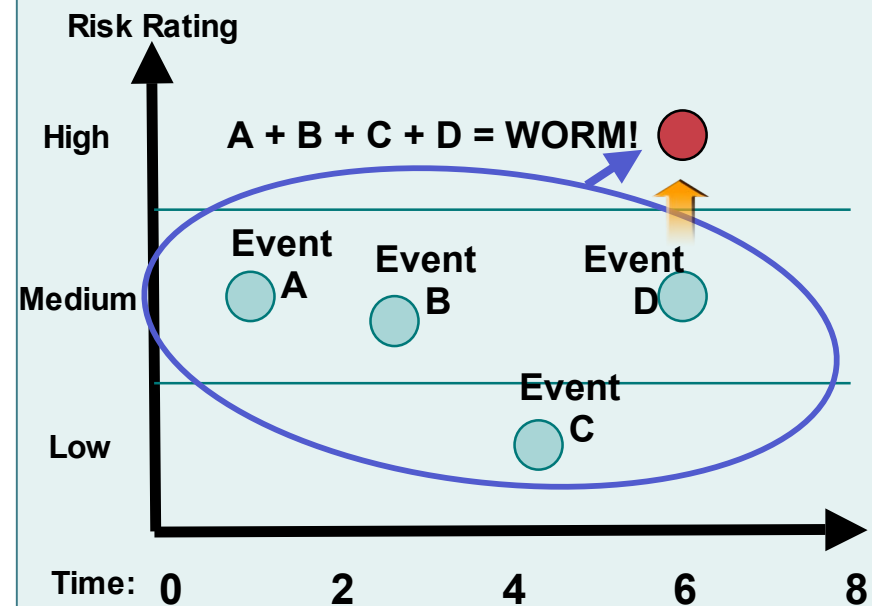
RISK RATING

Decisione sulle azioni

Meta Event Generator: Correlazione On-box che lega diversi eventi a piubasso rischio in un meta-evento.

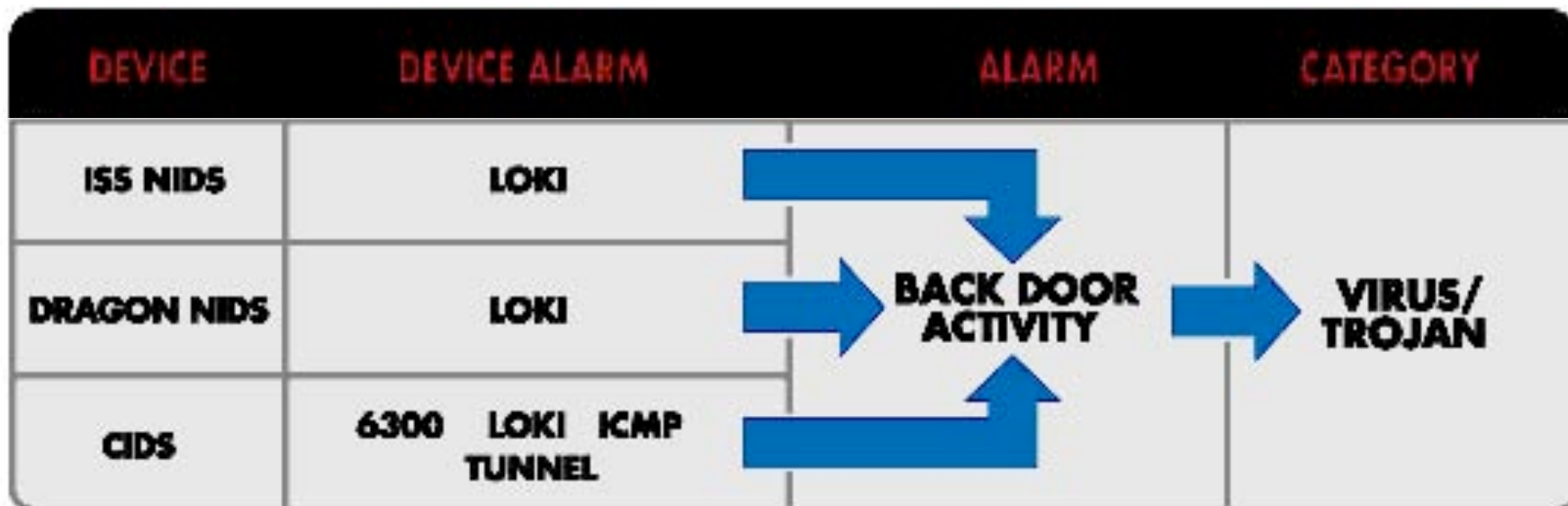
Modella il comportamento dell'attacco in base a:

- Tipo di evento
- Spazio Temporale



Normalizzazione

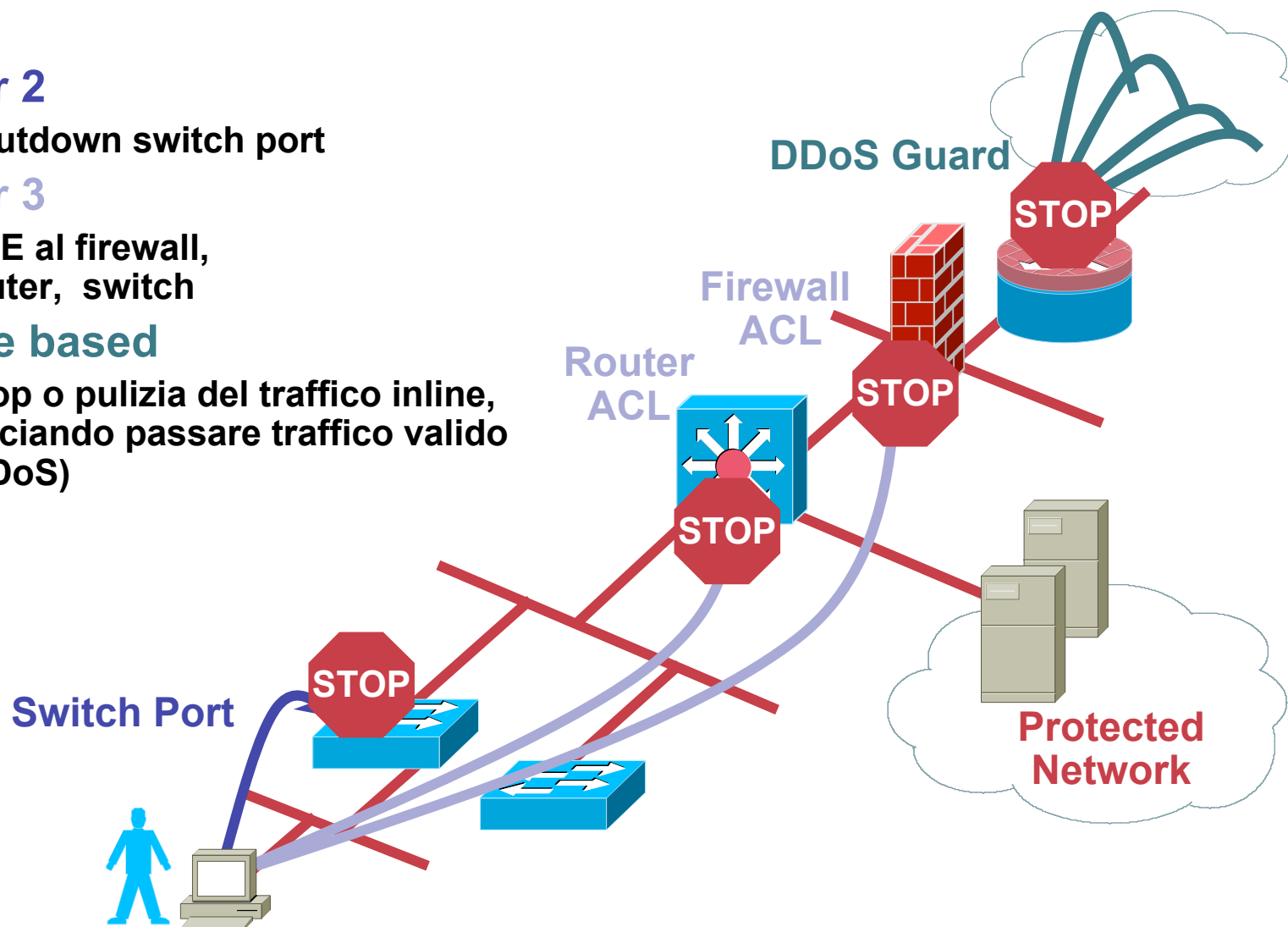
- L'ambiente di Security monitoring può essere multivendor
- Eventi da dispositivi diversi hanno formati differenti
- Necessità di processare eventi
- Necessità di comparare eventi simili (normalizzati) da tecnologie differenti



Monitoring Avanzato

Mitigation

- **Layer 2**
Shutdown switch port
- **Layer 3**
ACE al firewall,
router, switch
- **Route based**
Drop o pulizia del traffico inline,
lasciando passare traffico valido
(DDoS)



Investigazione degli Incidenti

- Conoscenza di un attacco
- Ricerca ed Investigazione
- Collezione degli eventi di rete
- Determinazione di misure di mitigazione

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) Close	Action/Operation	Time-range
1		\$TARGET02	\$TARGET01	ANY	Probe/HostSweep/Non-stealth	ANY	ANY	1		OR	
2		\$TARGET02	\$TARGET01	ANY	Probe/PortSweep/Stealth, ApplPolicyViolation/Misc	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

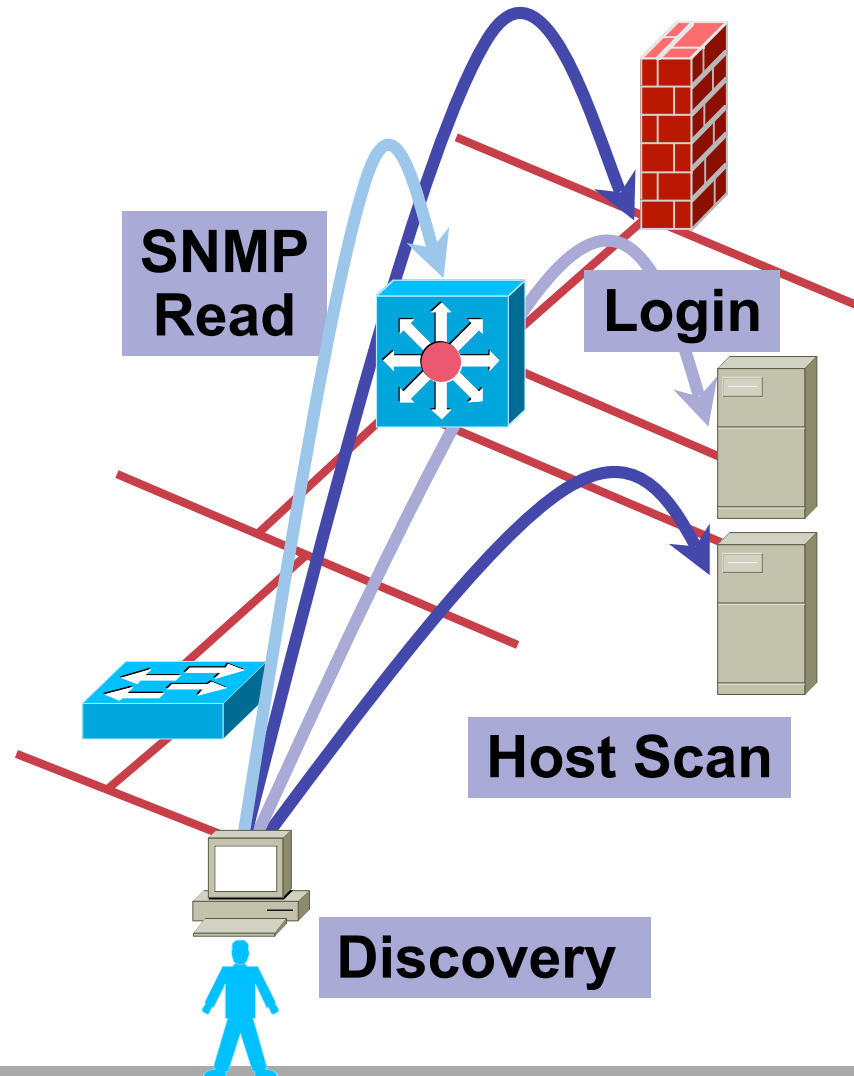
Incident ID: 38572801

Escalate Expand All Collapse All

Offset	Session / Incident ID	Event Type	Source IP/Port	Destination IP/Port	Protocol	Time	Reporting Device	Reported User	Path / Mitigate	False Positive
1		ICMP Ping Network Sweep	40.40.1.23	+ Total: 2						
1	S:105756188, I:38572801	ICMP Ping Network Sweep	40.40.1.23	100.1.4.10	ICMP	May 2, 2005 10:41:50 PM CDT	HQ-SW-1-idsm			False Positive
1	S:105756189, I:38572801	ICMP Ping Network Sweep	40.40.1.23	192.168.1.10	ICMP	May 2, 2005 10:41:50 PM CDT	HQ-NIDS1			False Positive
3	S:105756238, I:38572800, I:38572801	WWW IIS_uda Indexing Service Overflow	40.40.1.23	100.1.4.10	TCP	May 2, 2005 10:41:50 PM CDT	HQ-SW-1-idsm			False Positive
4		Built/teardown/permitted IP connection	192.168.1.10	+ Total: 3						
4	S:105756209, I:38572801	Built/teardown/permitted IP connection	192.168.1.10	10.1.1.10	TCP	May 2, 2005 10:41:50 PM CDT	HQ-FW-1			False Positive
4	S:105756210, I:38572801	Built/teardown/permitted IP connection	192.168.1.10	10.1.1.10	TCP	May 2, 2005 10:41:50 PM CDT	HQ-FW-1			False Positive
4	S:105756211, I:38572801	Built/teardown/permitted IP connection	192.168.1.10	10.1.1.10	TCP	May 2, 2005 10:41:50 PM CDT	HQ-FW-1			False Positive

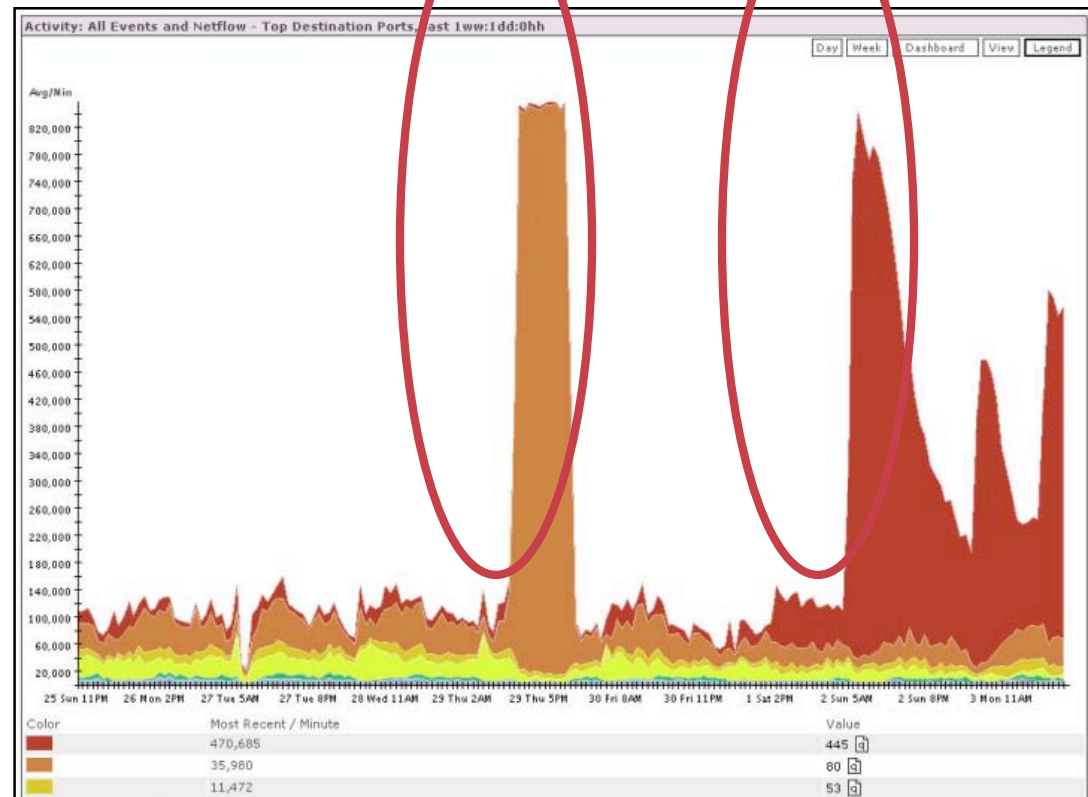
Integrazione con Vulnerability Assessment

- Foundstone, eEye, Nessus, Qualys, ...
- Tipo di OS
- Patch level
- Open Ports
- Applicazioni e servizi
- Personal firewall
- Host IPS



Rilevamento traffico e dispositivi anomali

- **Misura contro il profilo tipico**
- **Utilizzo CPU, memoria, utilizzazione del link**
- **Anomalie del traffico - NetFlow**
- **Rilevamento attacchi zero day**



Auditing & Compliance

Criticità dei Security Audit

Policy Settings - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Cisco S

You Are Here: Policy S

View All

Expand

Security Auditor Graphical Report - Microsoft Internet Explorer

CISCO SYSTEMS **Security Auditor**
 Audit Graphical Report as of 08/11/2004 13:45:00 PDT for Audit Name: demo

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

Audit Policy Count

Weighted Score: 37.87 %
 Overall Total Count: 3546
 Policy Failure Count: 2203
 Policy Success Count: 1343
 Devices Skipped: 0
 Devices Checked: 14

Bottom 10 Devices by Score

Devices	Score %
172.20.126.202	21.39
172.20.126.33	21.39
172.20.126.84	21.39
172.20.126.250	21.39
172.20.126.50	21.39
172.20.126.6	21.39
172.20.126.68	21.39
172.20.126.5	21.39
sa-7400	40.23
172.20.126.242	42.7

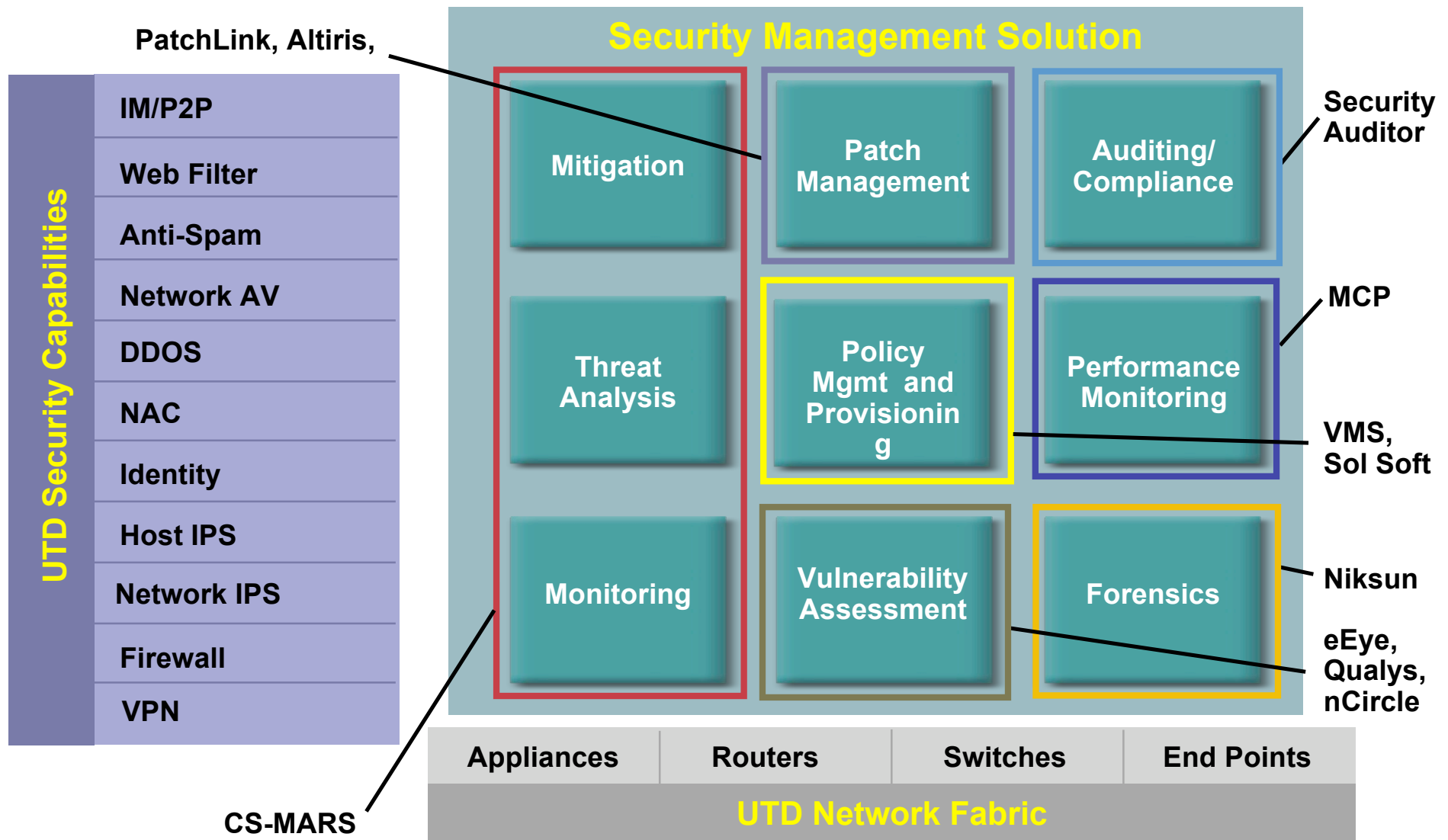
sa-7400 40.23%
 172.20.126.242 42.7%

at based network management applications will not function properly if only

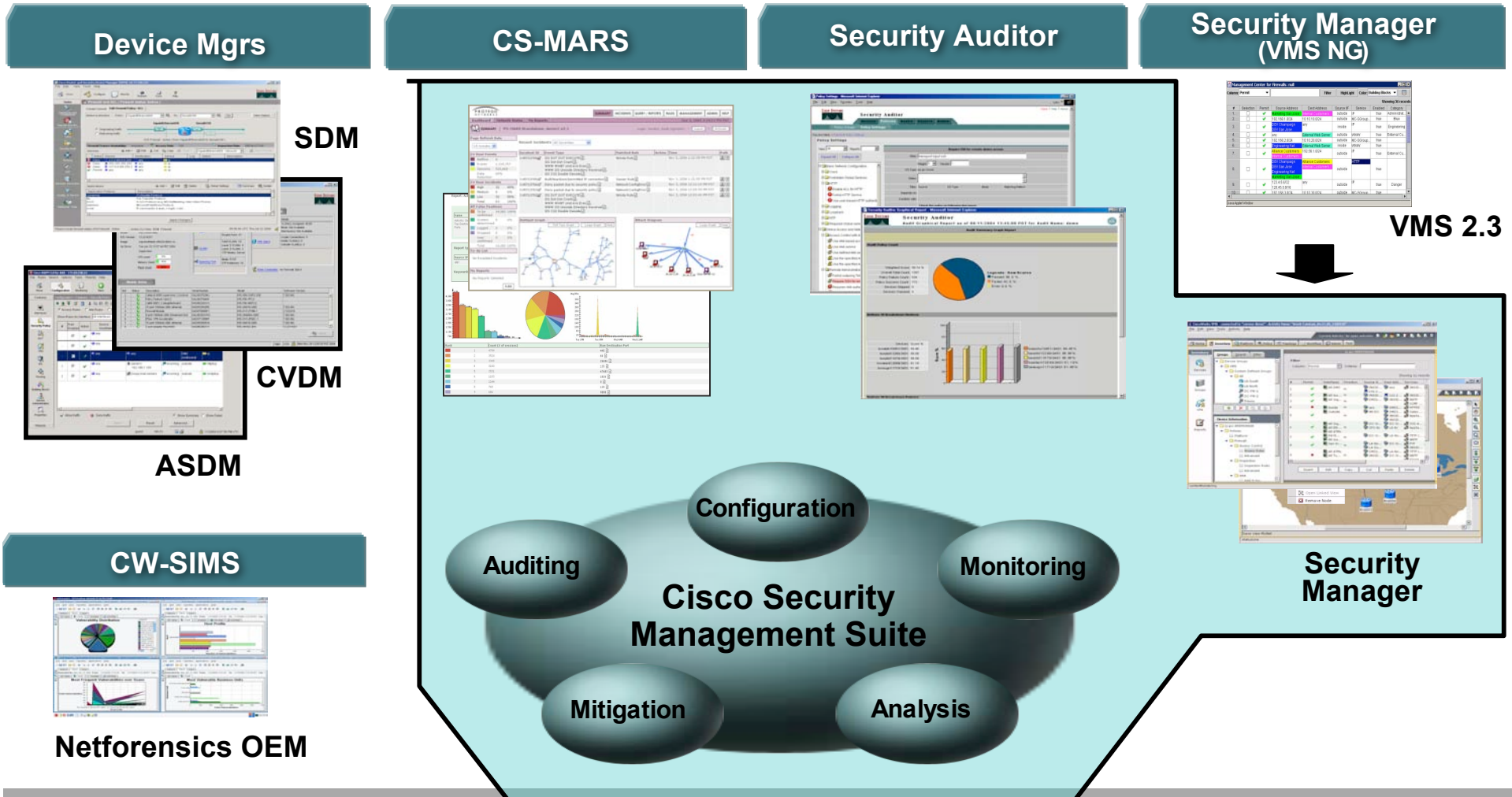
Conclusioni

Gestione della infrastruttura

Unified Threat Defense



Cisco Security Management Framework



La visione tecnologica Cisco a 3-5 anni Intelligent Information Network: un approccio globale di sistema

L'arte e la cultura dell'impresa
ciscoexpo
2005

Adozione delle Reti IP



Tempo



Marco Misitano, CISSP, CISM

Cisco Systems Italy
misi@cisco.com

L'arte e la cultura dell'impresa
ciscoexpo
2005



poweredbycisco.
networkers
2005

**Ci vediamo a Cannes
12-15 Dicembre 2005**

**building the intelligent
information network**

