L'arte e la cultura dell'impresa

ciscoexpo 2005

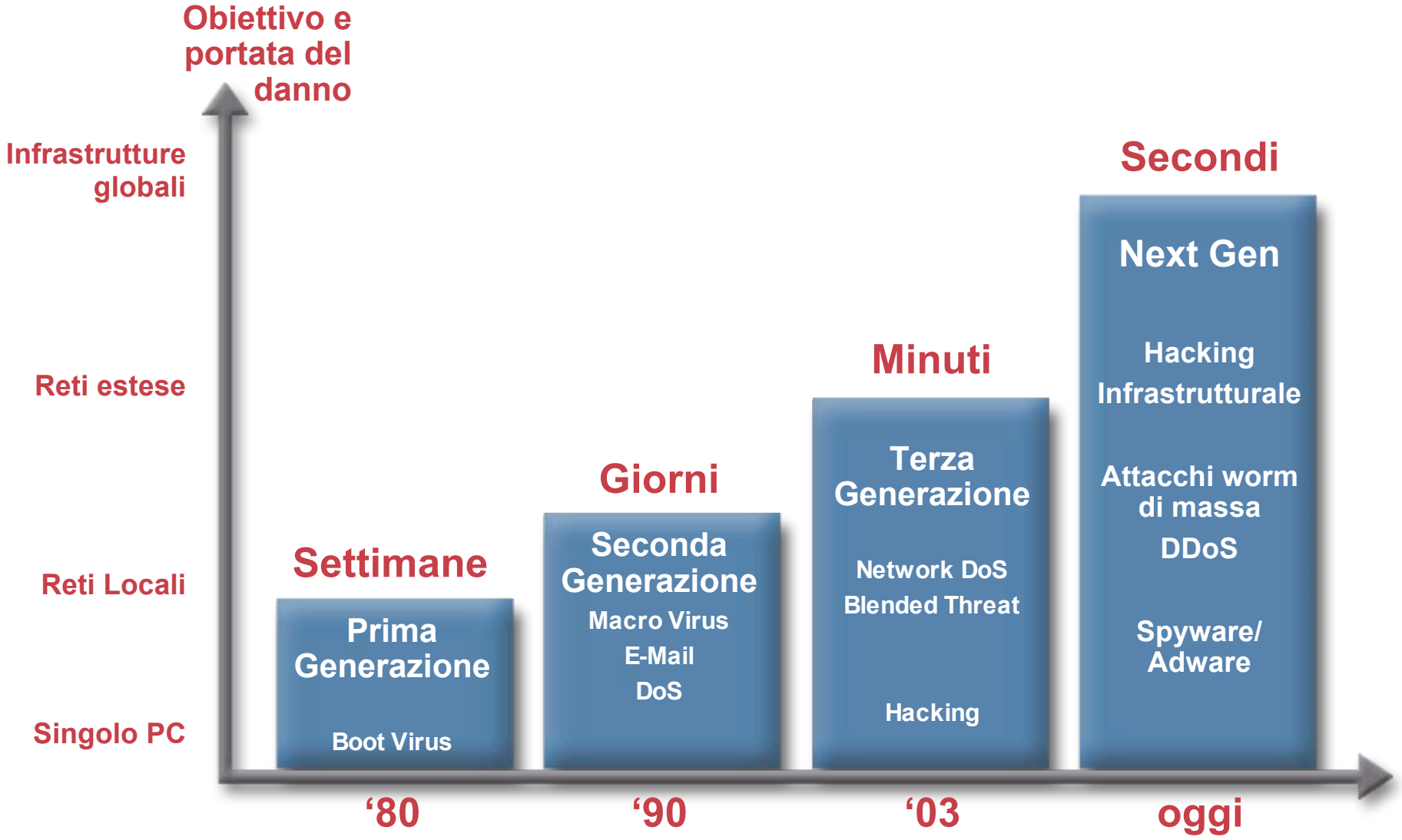
Managing the Self Defending Network

Marco Misitano, CISSP, CISM

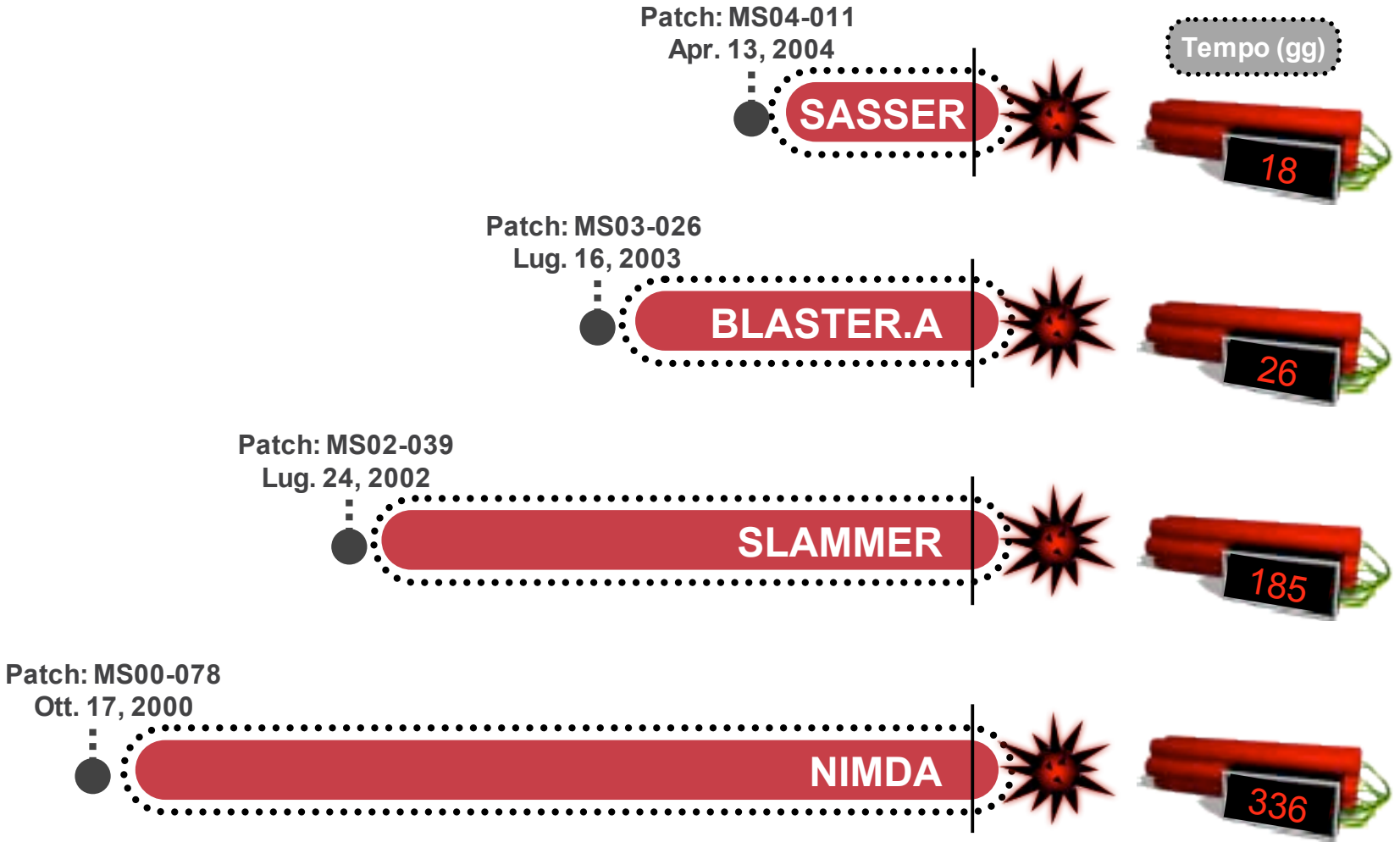
Cisco Systems Italy
misi@cisco.com

Introduzione

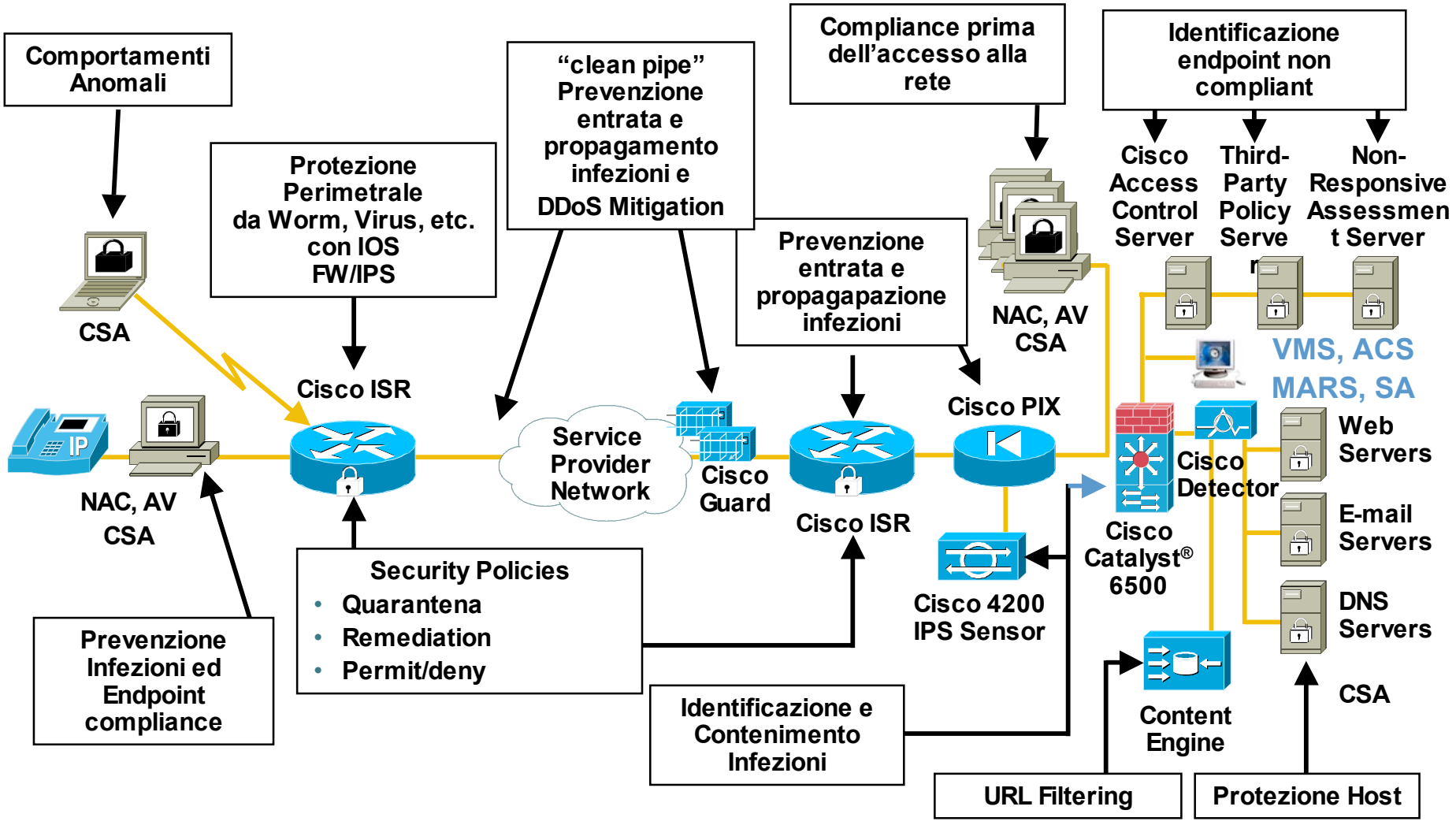
Evoluzione del problema /1



Evoluzione del problema /2



Soluzione ad problema /3



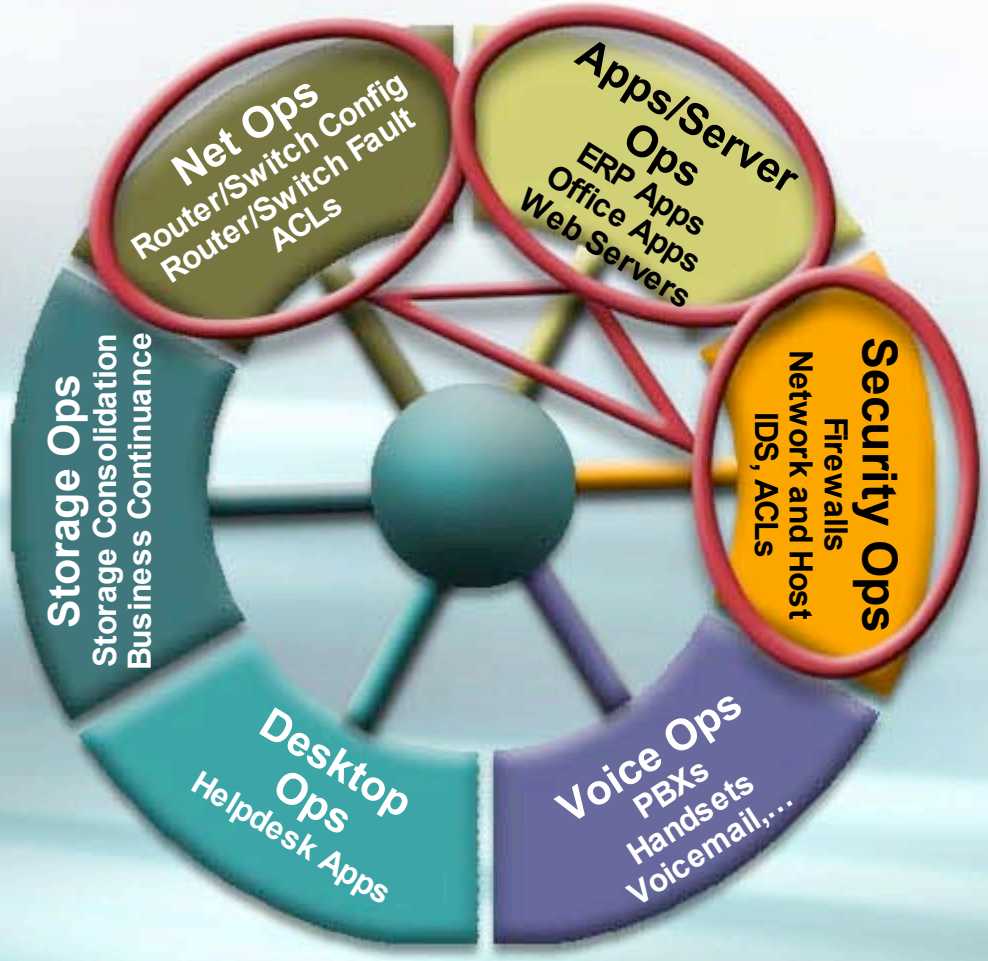
Definizione del problema

- **Information overload !**
- **Si puó 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. Necessitá di fare di piú con meno risorse**
- **Il Management é maturato, ma c'e' ancora da fare**
  - **Automatizzare di piú**
  - **Incident response**

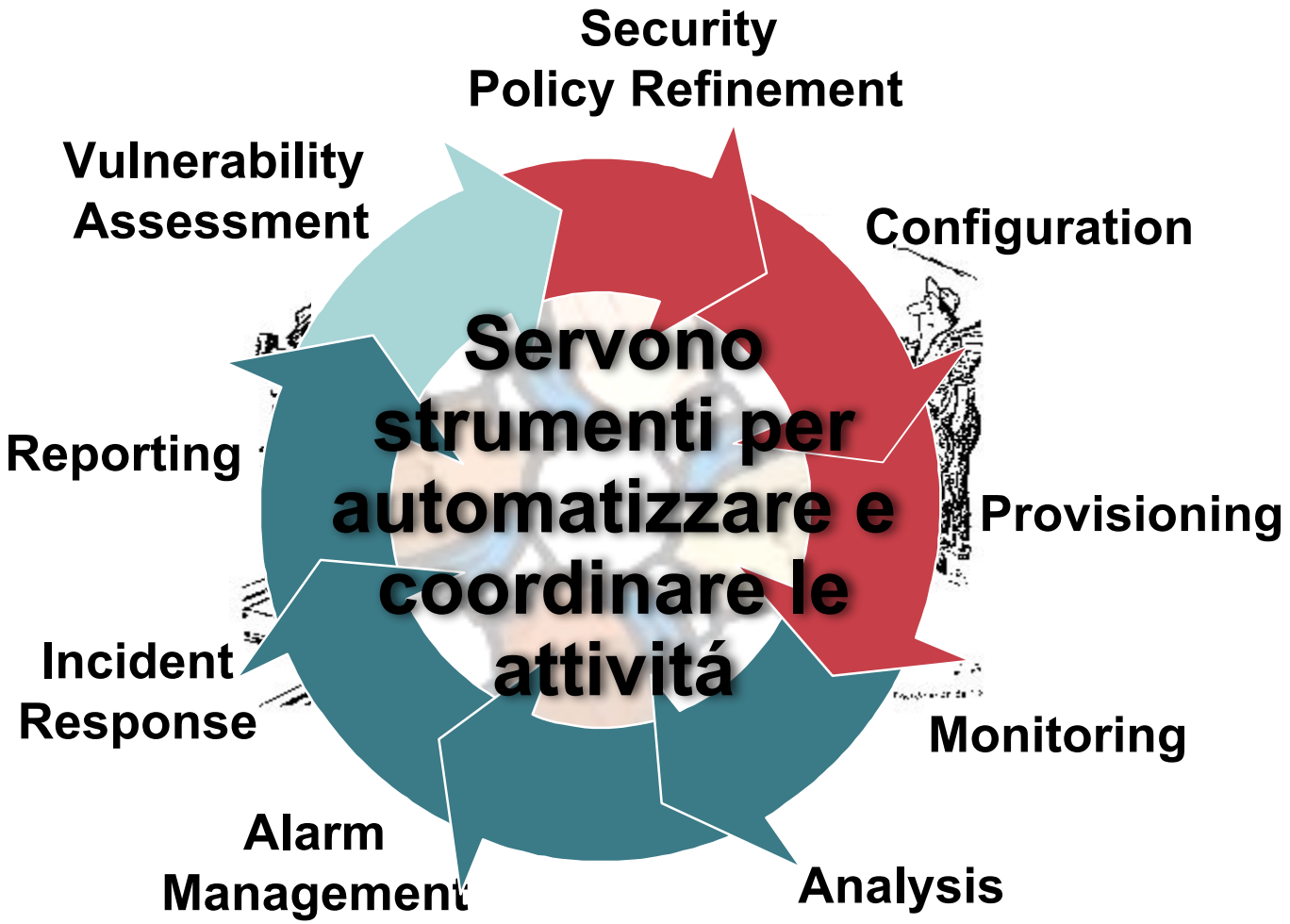
Il problema *organizzativo*

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



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

Ciclo di vita della Sicurezza

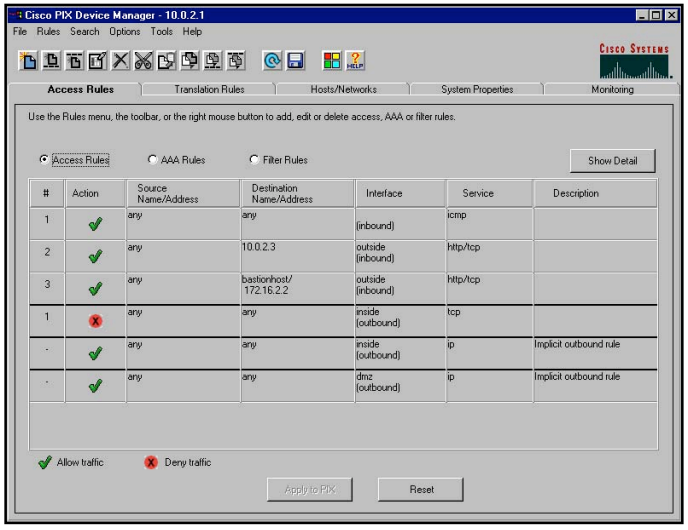


Configurazione

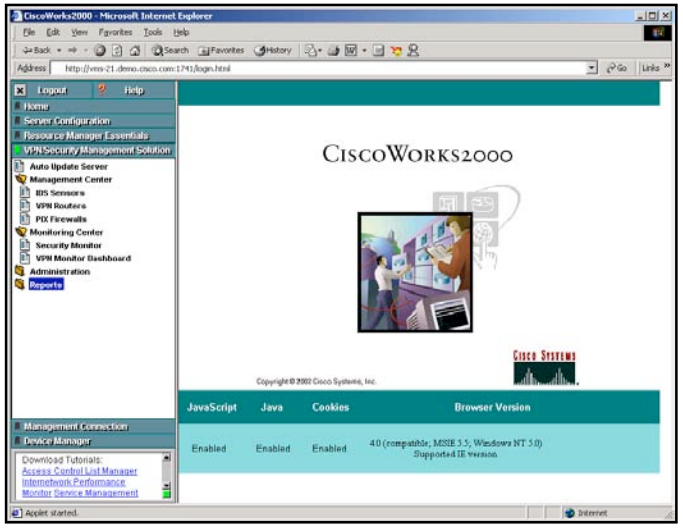
Selezionare lo strumento giusto

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'**



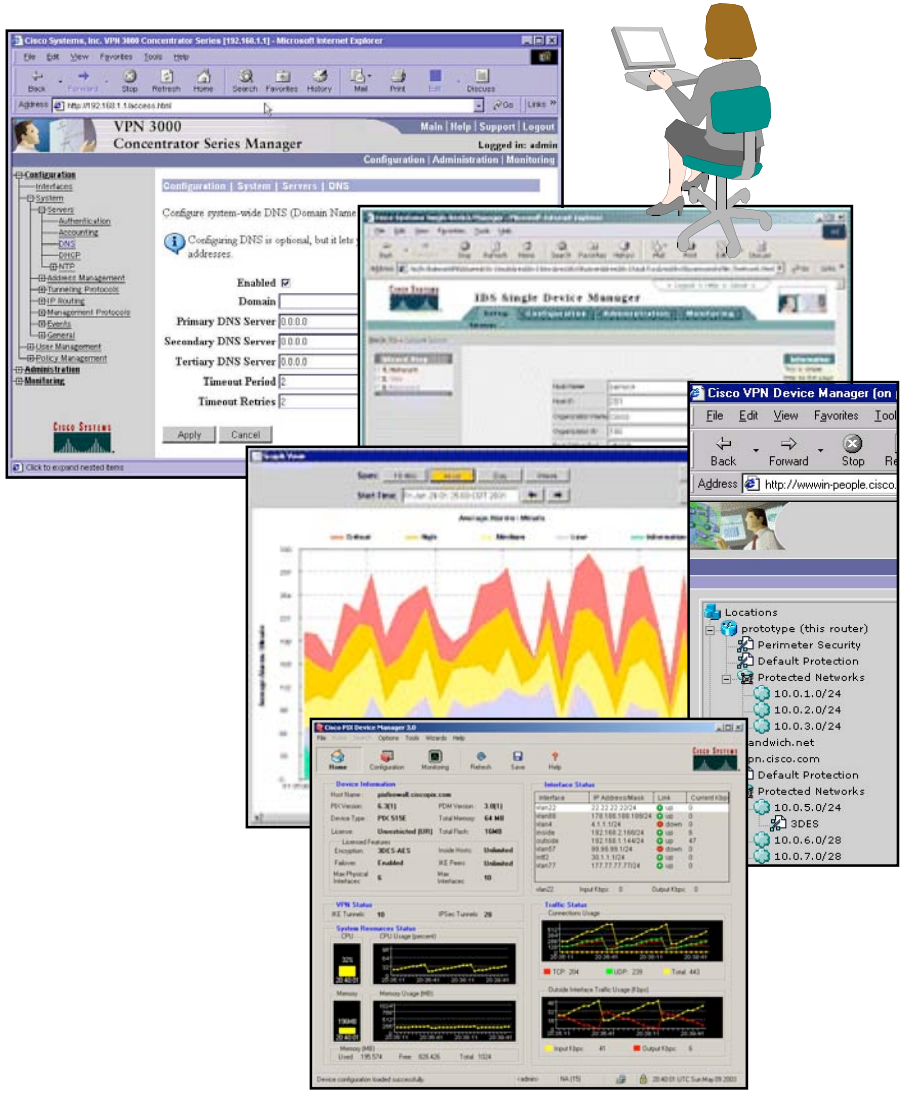
Device Manager



CiscoWorks VPN and Security Management Solutions

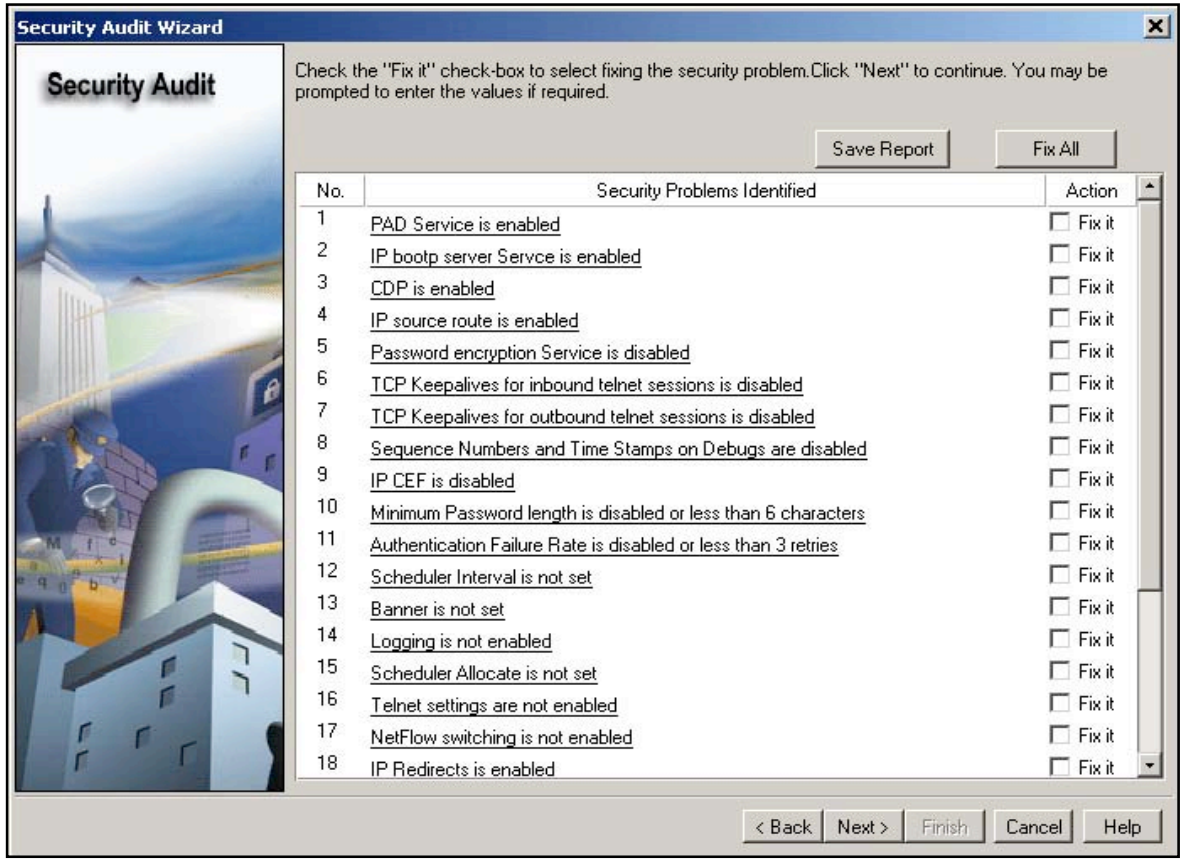
Element Management
per la gestione di piccole reti

- **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)**

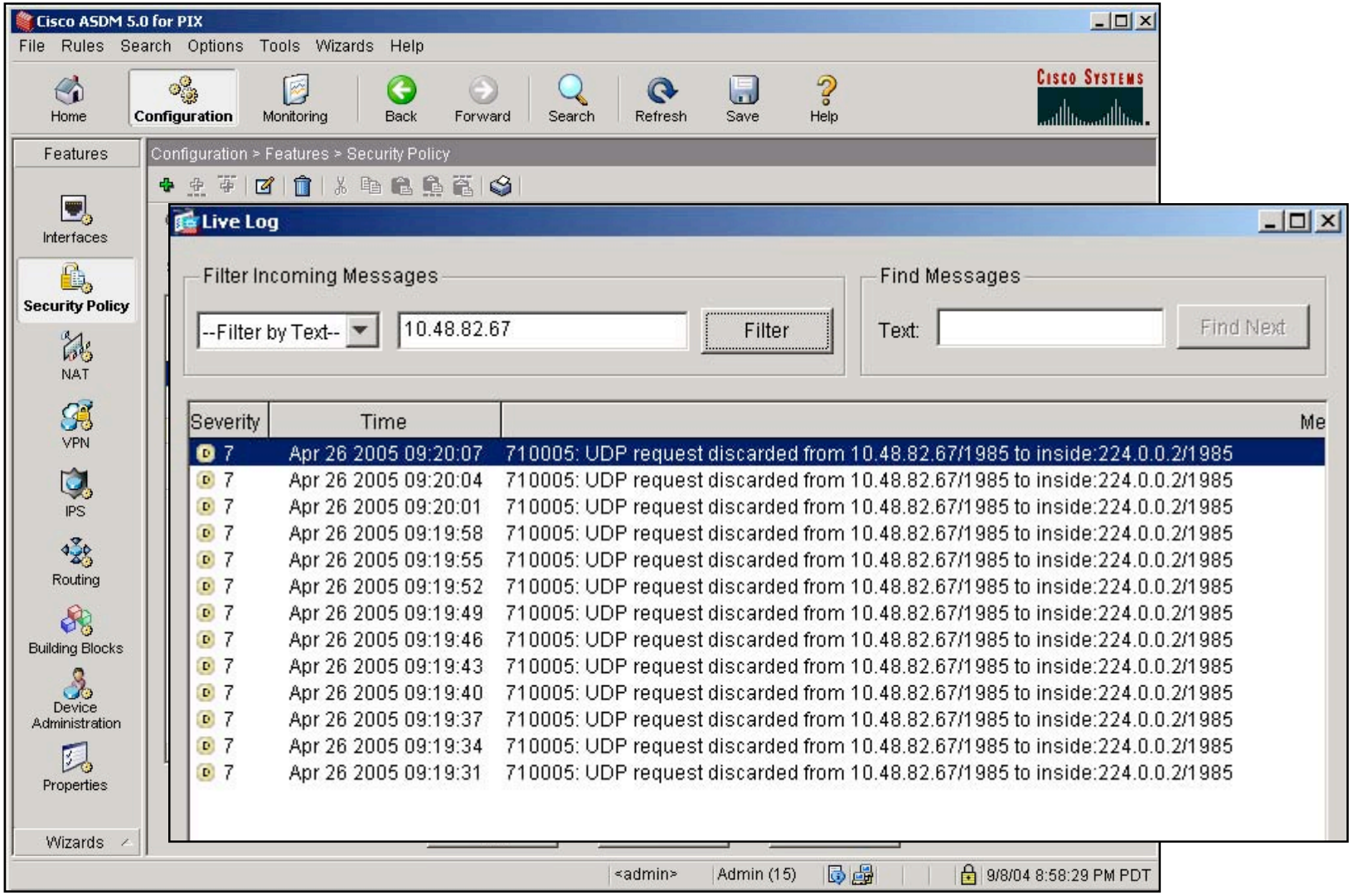


Cisco Security Device Manager

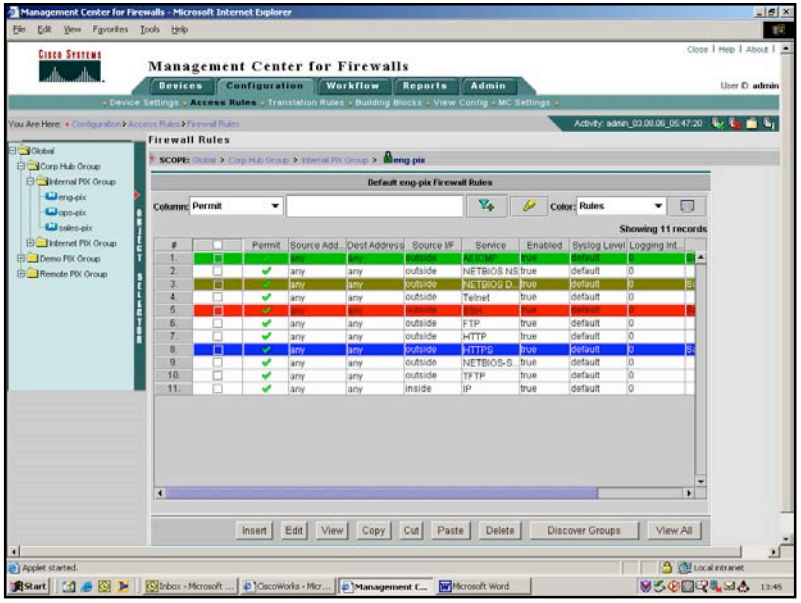
SDM é uno strumento Web-Based per la gestione di Cisco Router IOS individuali

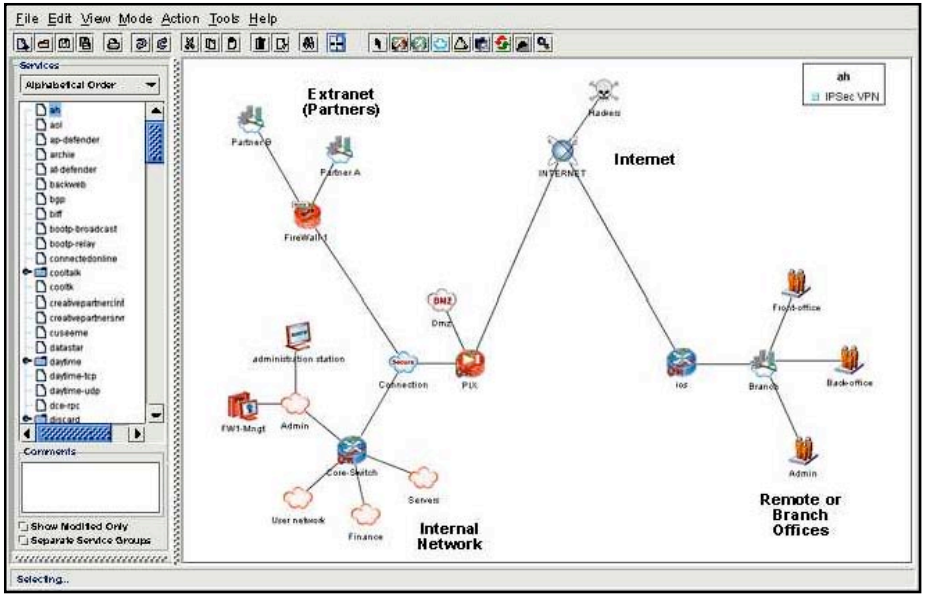


Adaptive Security Device Manager (ASDM)



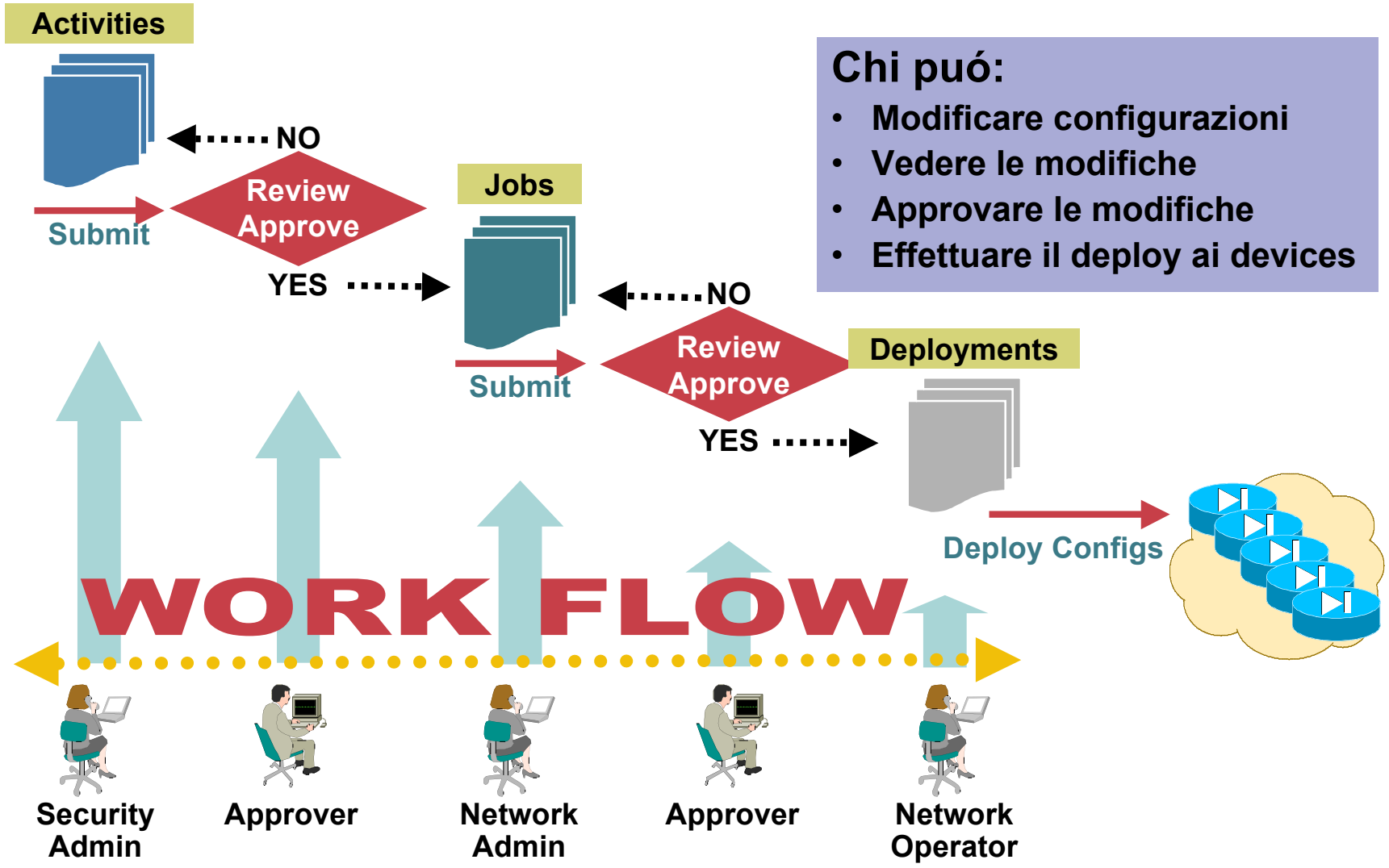
Multidevice o Policy-Based





- **VMS: cosa é comune ai dispositivi e possibiitá di configurazione a gruppi**
- **Solsoft (Cisco Partner): gestione multivendor grafica**

Ruoli e Responsabilitá



Chi puó:

- Modificare configurazioni
- Vedere le modifiche
- Approvare le modifiche
- Effettuare il deploy ai devices

CiscoWorks VMS

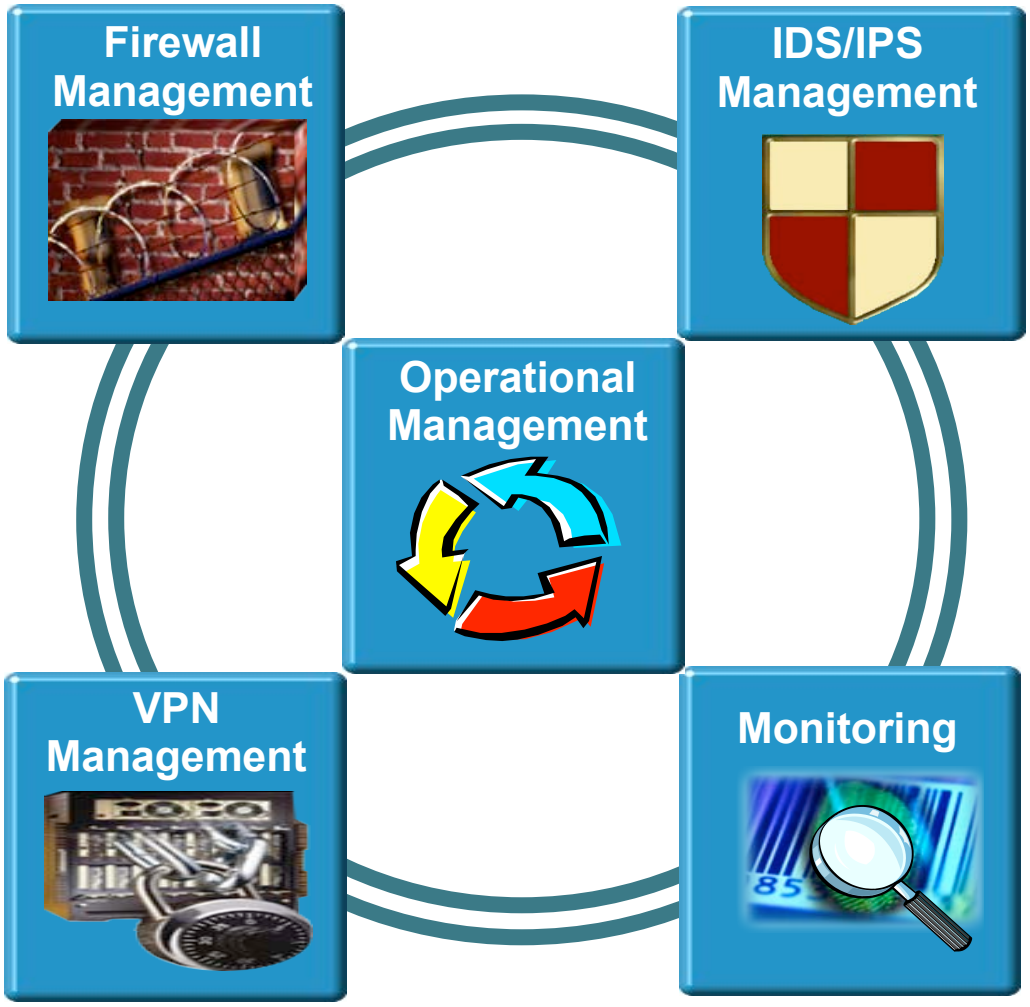
Supporto per l'intero lifecycle

Security Management Multitecnologia Integrato

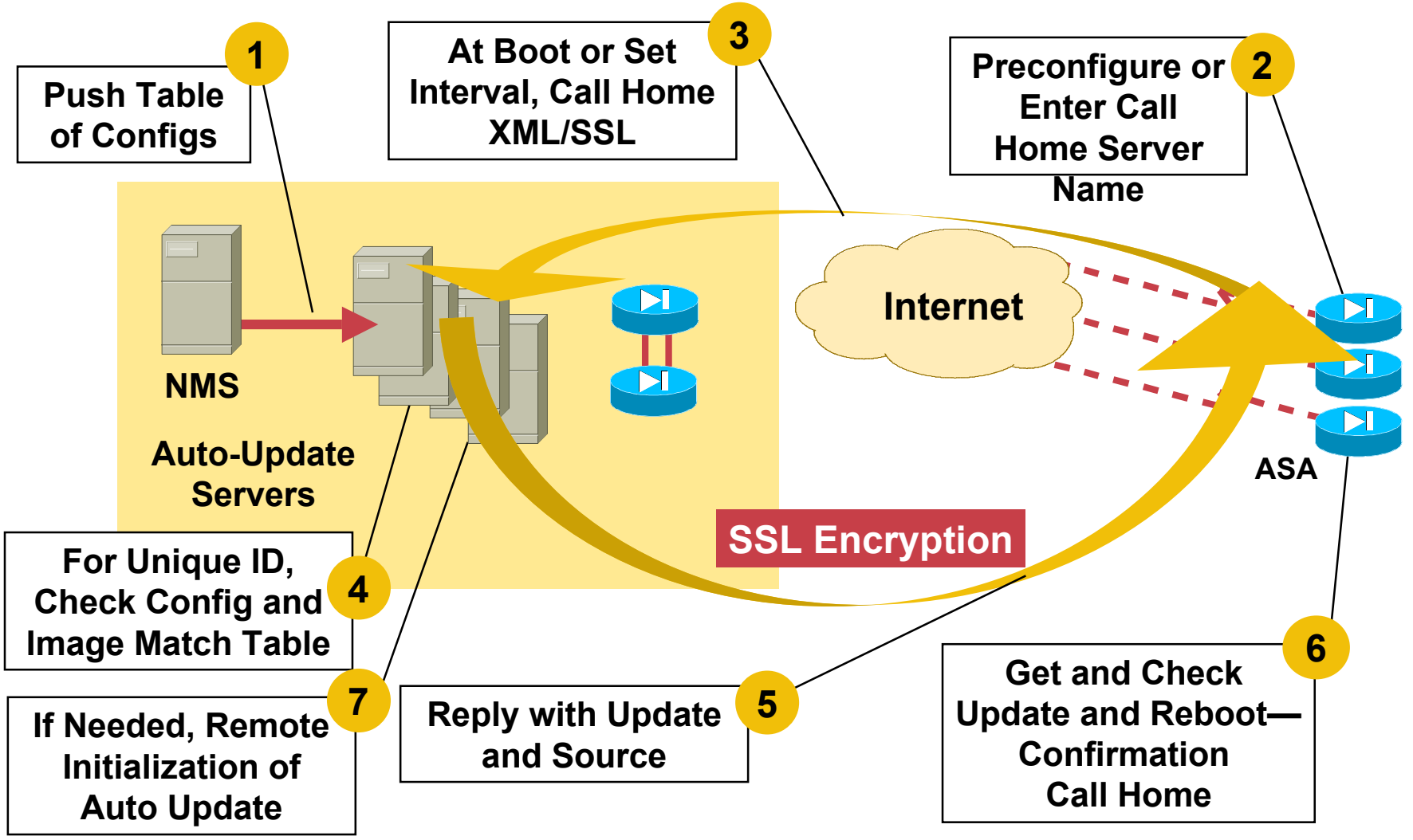
Integrazione della gestione operativa

Miglioramento della efficienza operativa

Monitoring delle performances e dei processi



Tecnologia Call-Home (PIX, ASA)



Monitoring

Security Logging

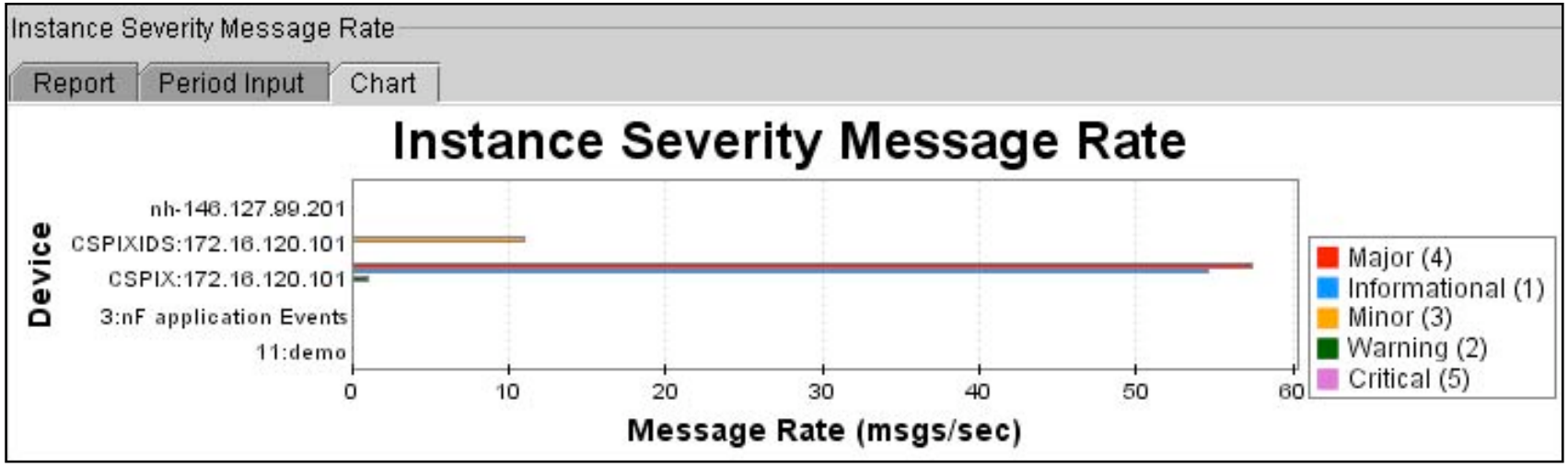
	Events/Sec	MB/Hr
Small VPN Gateway	50	27.4
Entry Firewall	100	54.8
High Router	200	109.6
Mid IPS	400	219.2

Strategie:

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

EPS: Best Practices

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



Host IPS Management

Sofisticazione della Prevenzione

Risk Rating: raggiungere il massimo dell'affidabilitá!

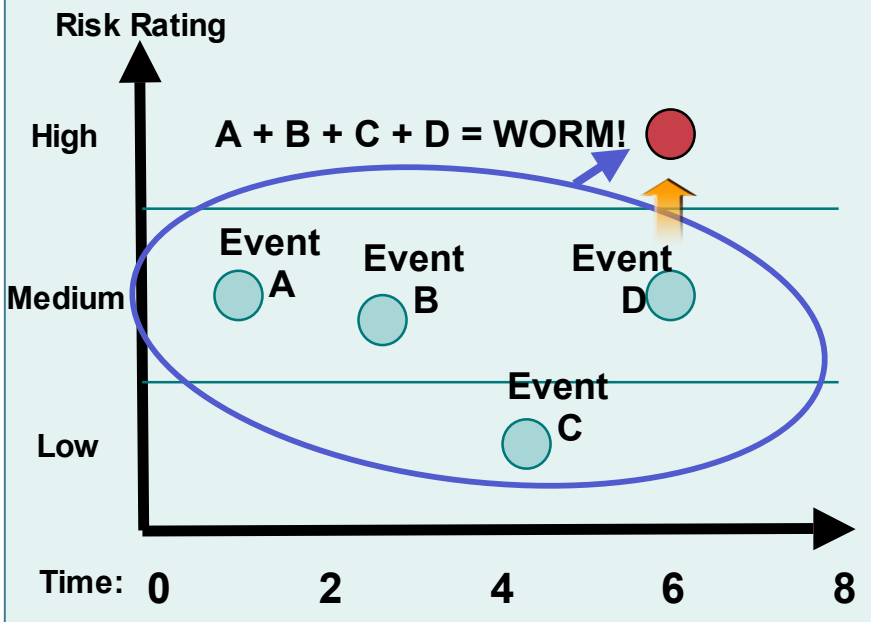
- **Event Severity** — Quanto è pericoloso o urgente?
- \+ **Signature Fidelity** — Quanto è possibile che sia un falso ?
- \+ **Attack Relevancy** — E' rilevante per il bersaglio ?
- \+ **Asset Value of Target** — Quanto è critico il bersaglio ?

RISK RATING → Decisione sulle azioni

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

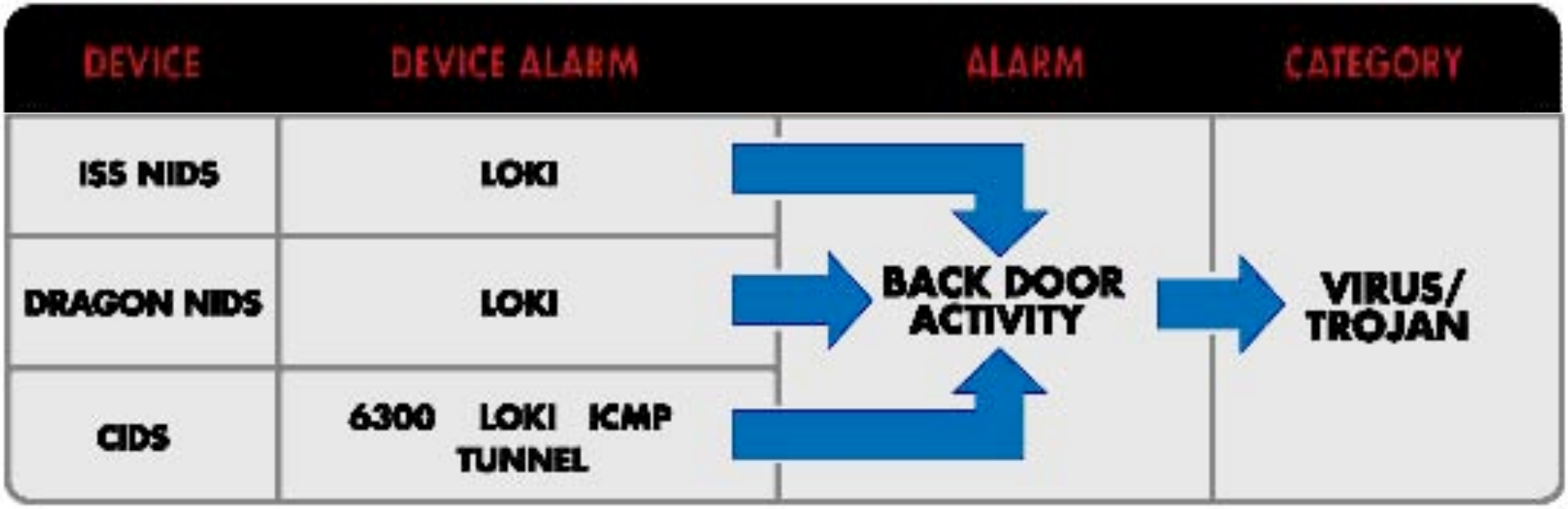
Modella il comportamento dell'attacco in base a:

- Tipo di evento
- Spazio Temporale



Normalizzazione

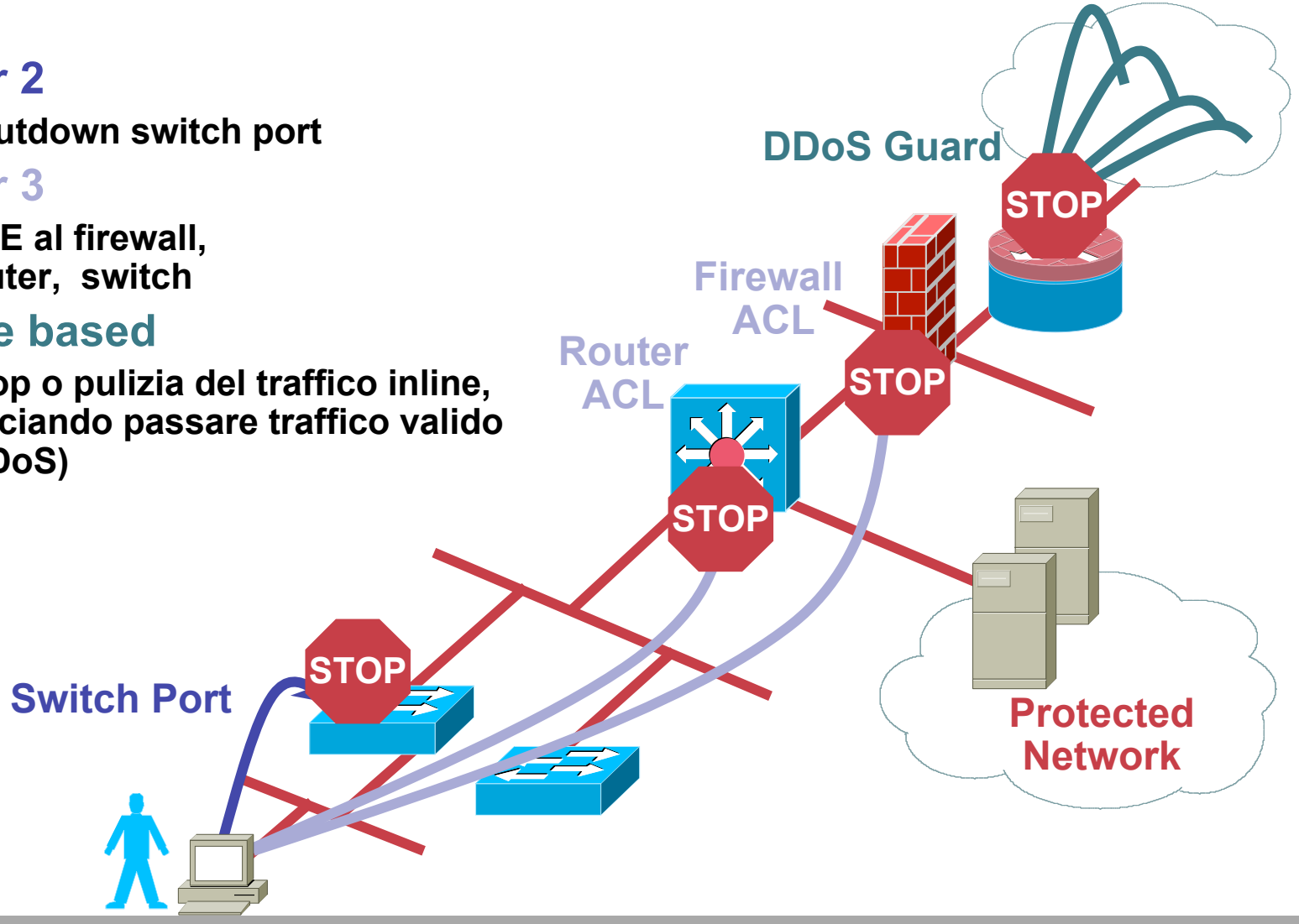
- L'ambiente di Security monitoring puó essere multivendor
- Eventi da dispositivi diversi hanno formati differenti
- Necessitá di processare eventi
- Necessitá di comparare eventi simili (normalizzati) da tecnologie differenti



Monitoring Avanzato

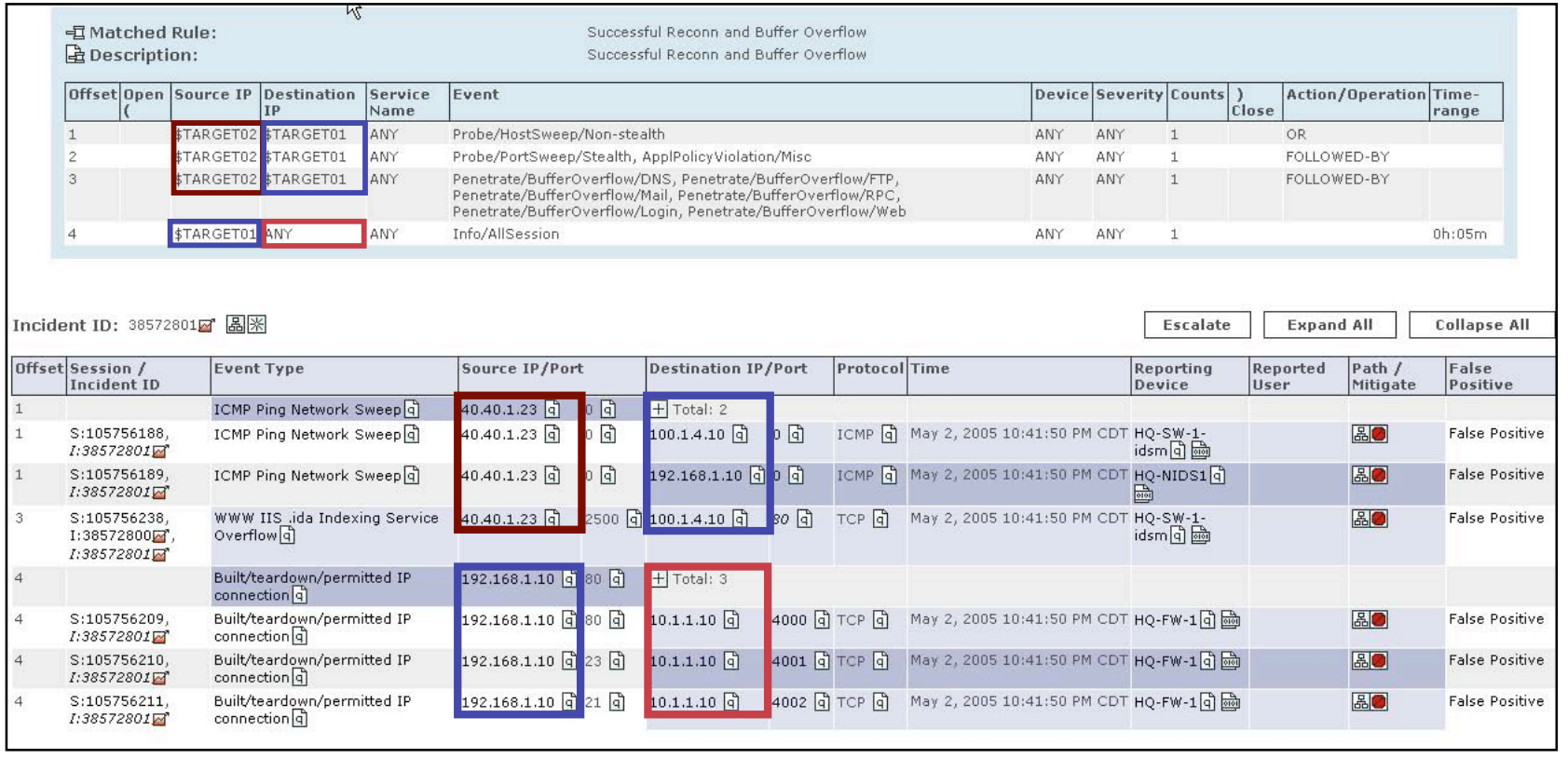
Mitigation

- **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 Reconn and Buffer Overflow

Description: Successful Reconn and Buffer Overflow

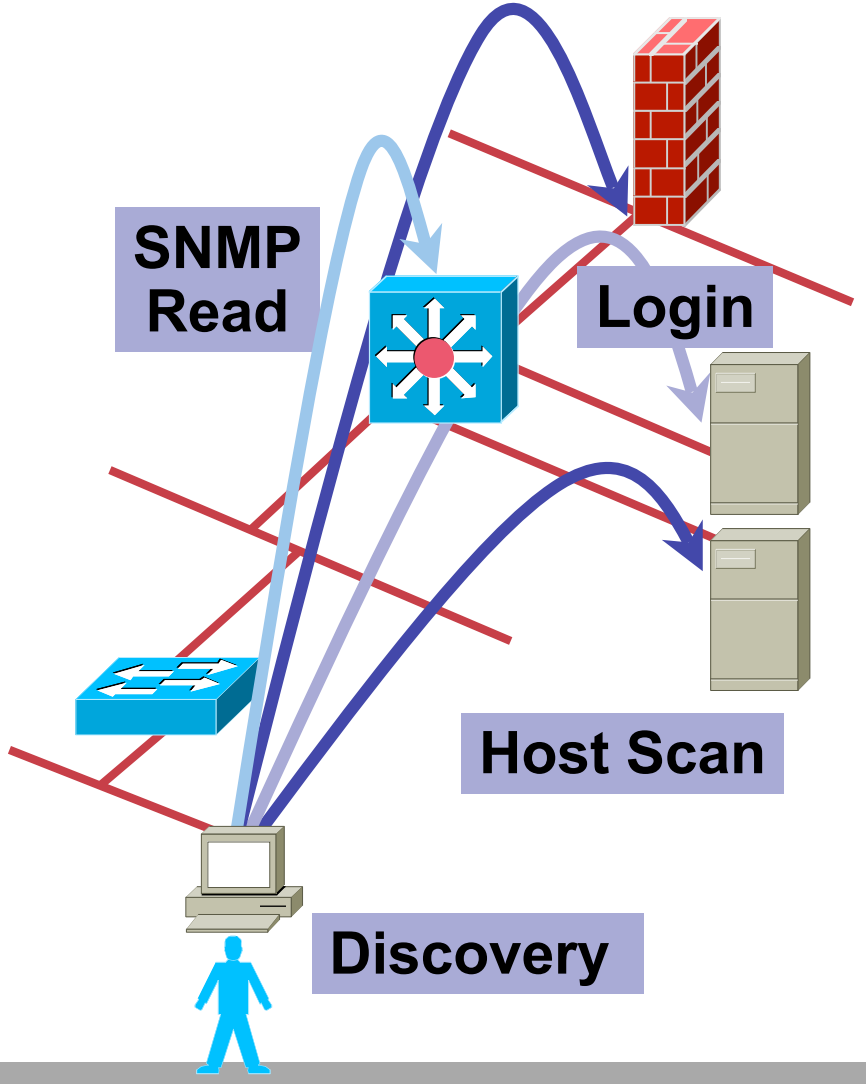
Offset	Open (	Source IP	Destination IP	Service Name	Event	Device	Severity	Counts	) Close	Action/Operation	Time-range
1		$TARGET02	$TARGET01	ANY	Probe/HostSweep/Non-stealth	ANY	ANY	1		OR	
2		$TARGET02	$TARGET01	ANY	Probe/PortSweep/Stealth, ApplPolicyViolation/Misc	ANY	ANY	1		FOLLOWED-BY	
3		$TARGET02	$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 0	Total: 2						
1	S:105756188, I:38572801	ICMP Ping Network Sweep	40.40.1.23 0	100.1.4.10 0	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 0	192.168.1.10 0	ICMP	May 2, 2005 10:41:50 PM CDT	HQ-NIDS1			False Positive
3	S:105756238, I:38572800, I:38572801	WWW IIS .ida Indexing Service Overflow	40.40.1.23 2500	100.1.4.10 80	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 80	Total: 3						
4	S:105756209, I:38572801	Built/teardown/permitted IP connection	192.168.1.10 80	10.1.1.10 4000	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 23	10.1.1.10 4001	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 21	10.1.1.10 4002	TCP	May 2, 2005 10:41:50 PM CDT	HQ-FW-1			False Positive

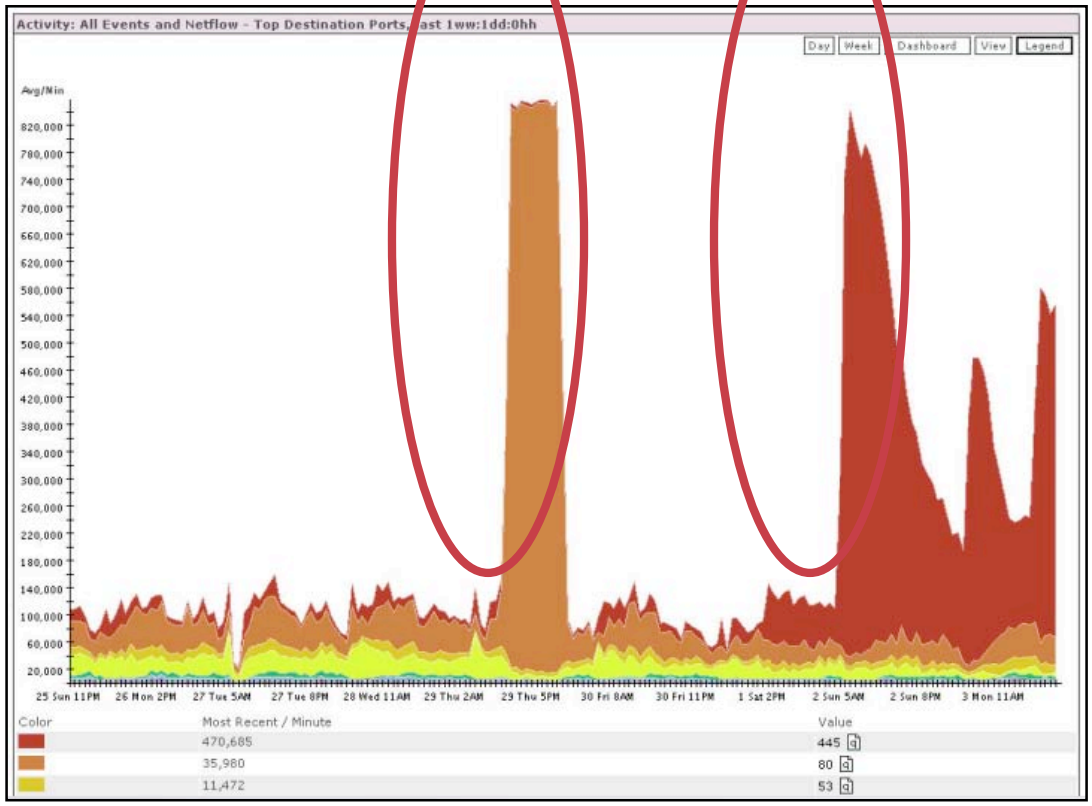
Integrazione con Vulnerability Assessment

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



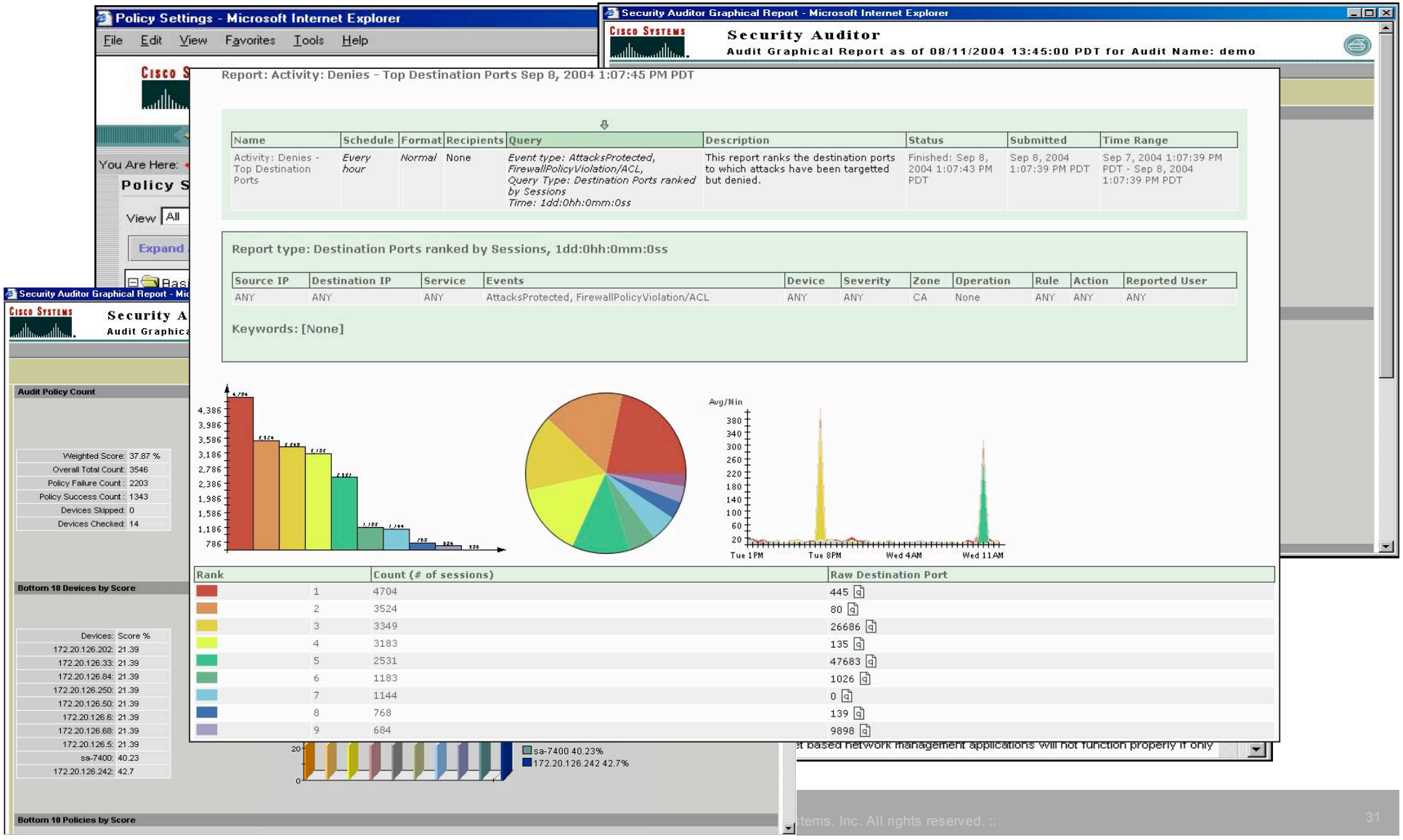
Rilevamento traffico e dispositivi anomali

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



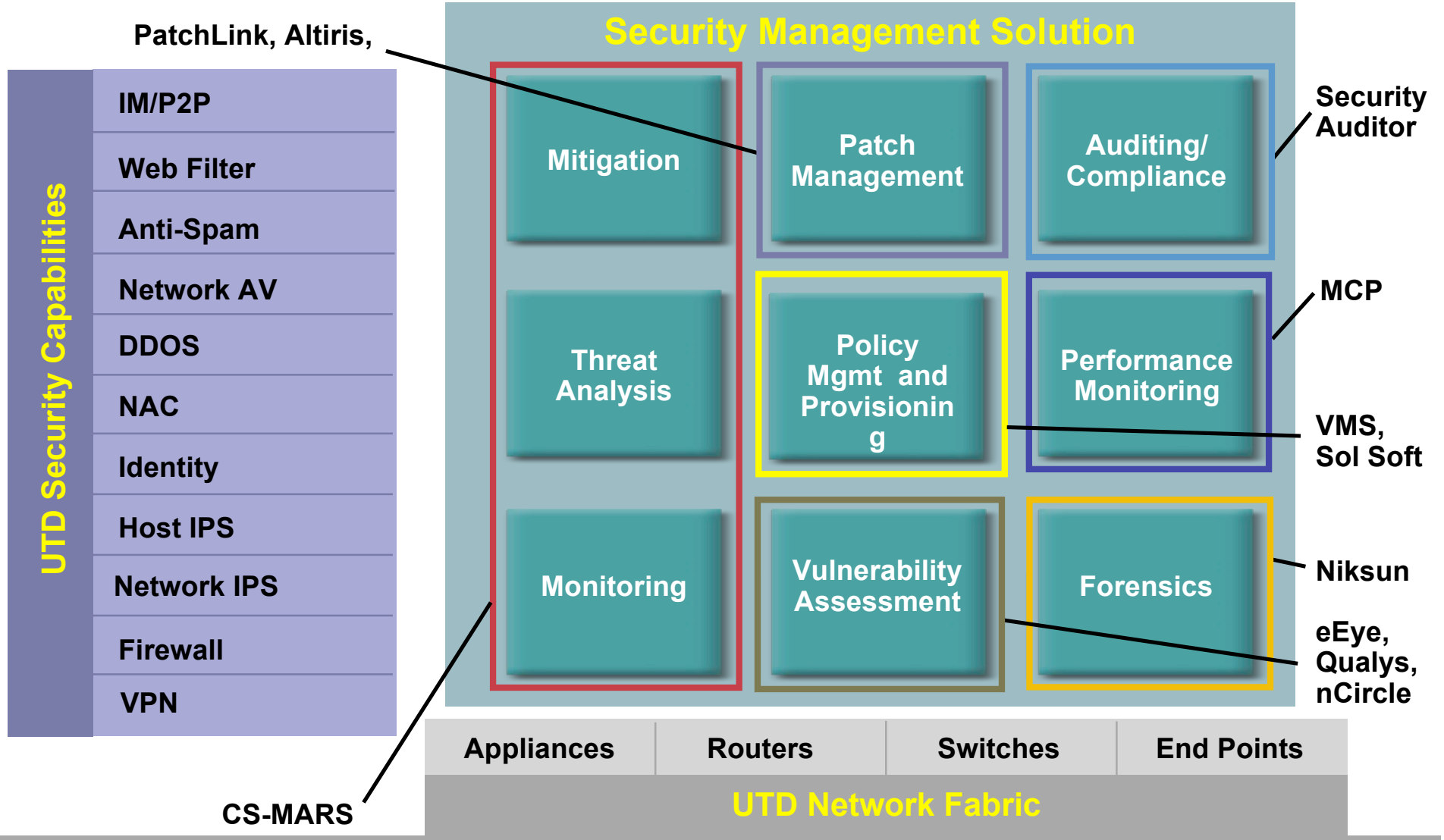
Auditing & Compliance

Criticitá dei Security Audit



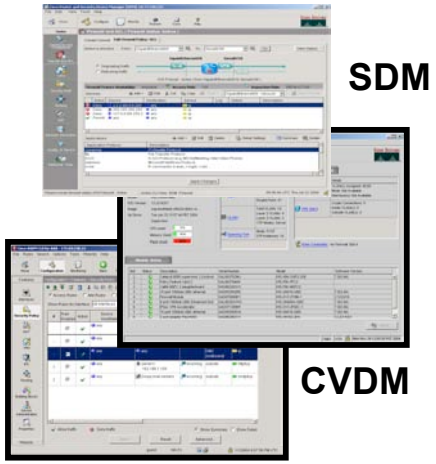
Conclusioni

Gestione della infrastruttura
Unified Threat Defense

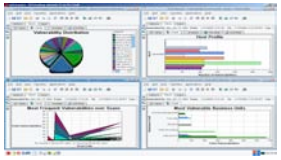


Cisco Security Management Framework

Device Mgrs

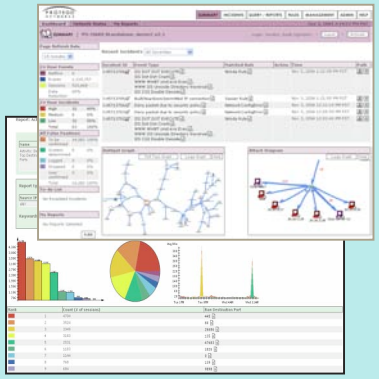


CW-SIMS

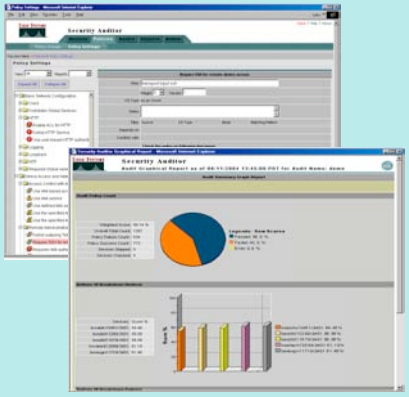


Netforensics OEM

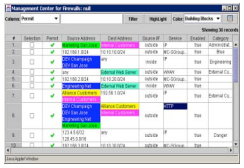
CS-MARS



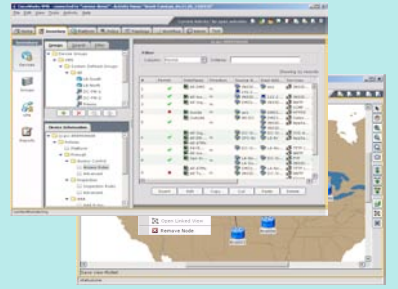
Security Auditor



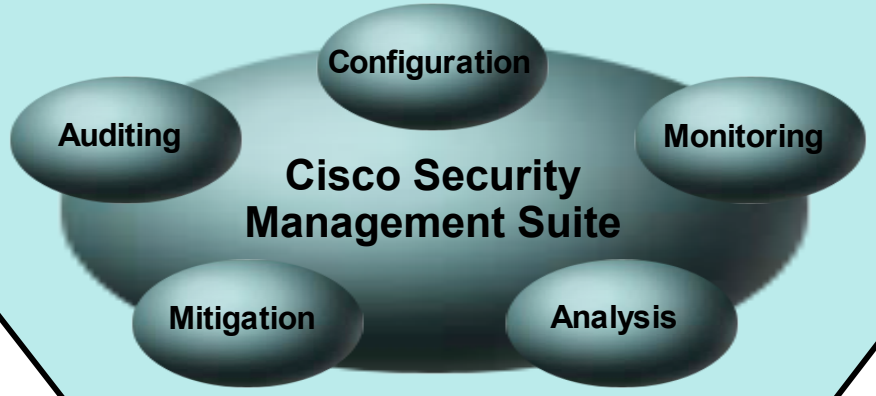
Security Manager (VMS NG)



VMS 2.3



Security Manager



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

Infrastruttura di Rete

Sistemi Globali

Risorse e Applicazioni

INTEGRAZIONE APPLICAZIONI

Rete e Servizi *Application-Aware*

FASE 3

INTEGRAZIONE SERVIZI

Virtualizzazione delle risorse in rete

FASE 2

INTEGRAZIONE TRASPORTO

Gestione intelligente di Dati / Voice / Video attraverso un insieme di reti

FASE 1

Adozione delle Reti IP

Tempo

Marco Misitano, CISSP, CISM

Cisco Systems Italy
misi@cisco.com

poweredbycisco.
networkers
2005

Ci vediamo a Cannes
12-15 Dicembre 2005

building the intelligent
information network

Cisco Systems