



e-Security Lab  
2007

MILANO - 24/25 Gennaio 2007



## Security Information Management

Ruolo dei Tool, come operano nella raccolta, aggregazione e correlazione delle informazioni di sicurezza: dalla teoria alla pratica

Elio Molteni, CISM-CISSP-BS7799

Executive Security Advisor

Computer Associates

[elio.molteni@ca.com](mailto:elio.molteni@ca.com)

*Presidente Capitolo Italiano ISSA*



# Attenzione!

La numerosità dei prodotti di sicurezza...

Prontezza di  
sicurezza  
informatica

**...non significa garanzia di  
sicurezza!**

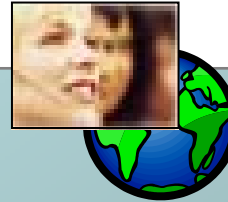
Quantità e sofisticazione delle soluzioni di sicurezza

# Ho veramente la situazione sotto controllo?

- ❑ Ho dimenticato qualche sistema importante?
- ❑ Come viene gestita la tracciabilità?
- ❑ Quand'è l'ultima volta che ho controllato i LOG?
- ❑ Riesco a correlare gli eventi in tempo reale?
- ❑ Riesco ad eliminare i falsi allarmi?
- ❑ Sono compliance? (SOX, Basilea, D.Lgs 196/03, Altro)
- ❑ Che strumenti sto usando?
- ❑ Sono integrati?
- ❑ Come sono stati implementati?
- ❑ Mi danno ciò di cui ho bisogno?

# Dalla teoria alla pratica

## Cosa fa CA per governare la “propria security?”



### Organizzazione Logistica:

- Sede principale: Islandia, NY
- 150+ sedi; 15'000+ dipendenti; (50% dipendenti mobili!)

### Infrastruttura Tecnologica

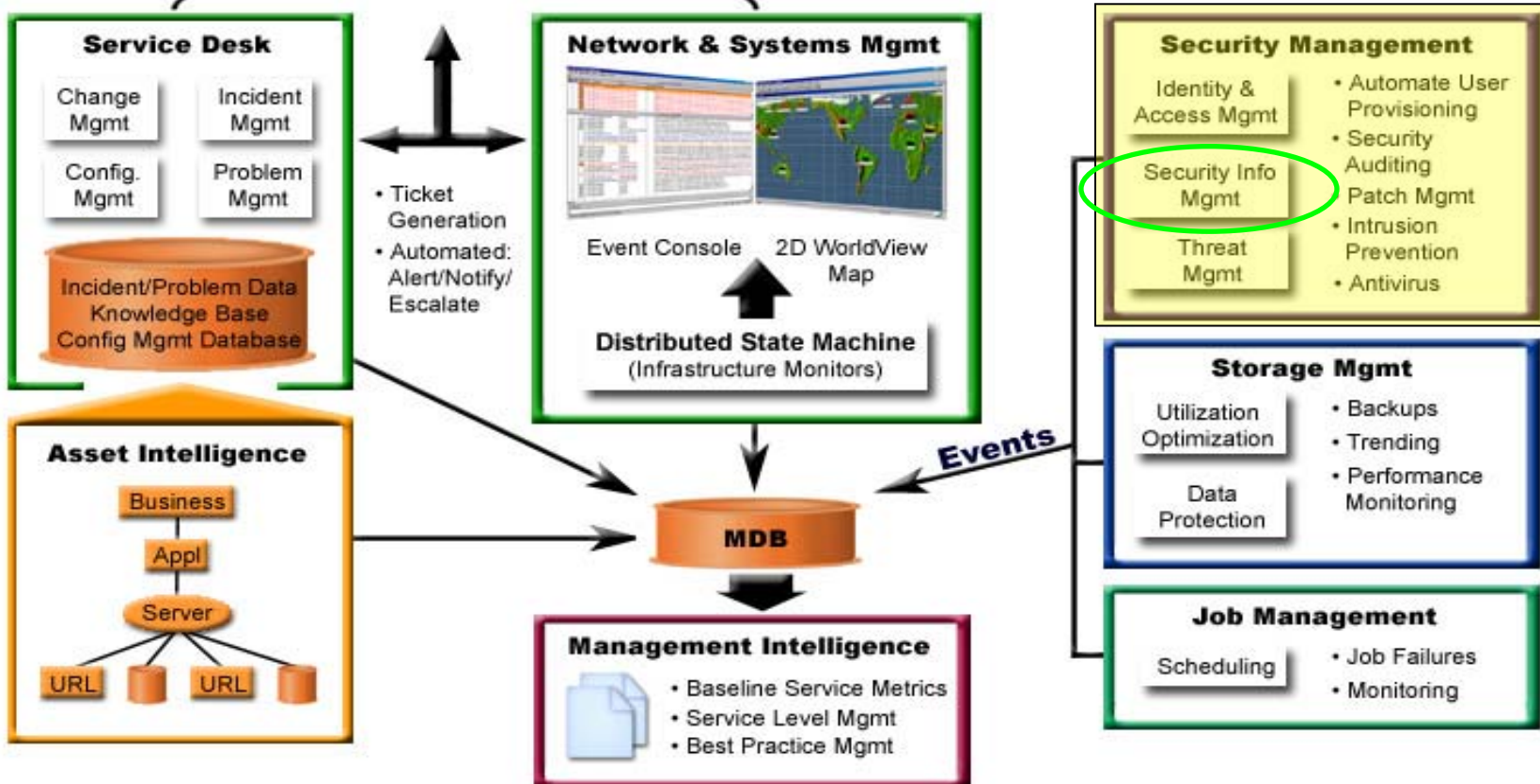
- 27'000+ PC; 40'000+ network devices
- 1'300+ Server di produzione
  - Linux, UNIX, Windows
- 4 Mainframe IBM
- 1500+ circuiti voce/data
- 150+ sistemi di telefonia
- 300+ router, 465+ switch
- 170 TB array storage

# Dalla teoria alla pratica

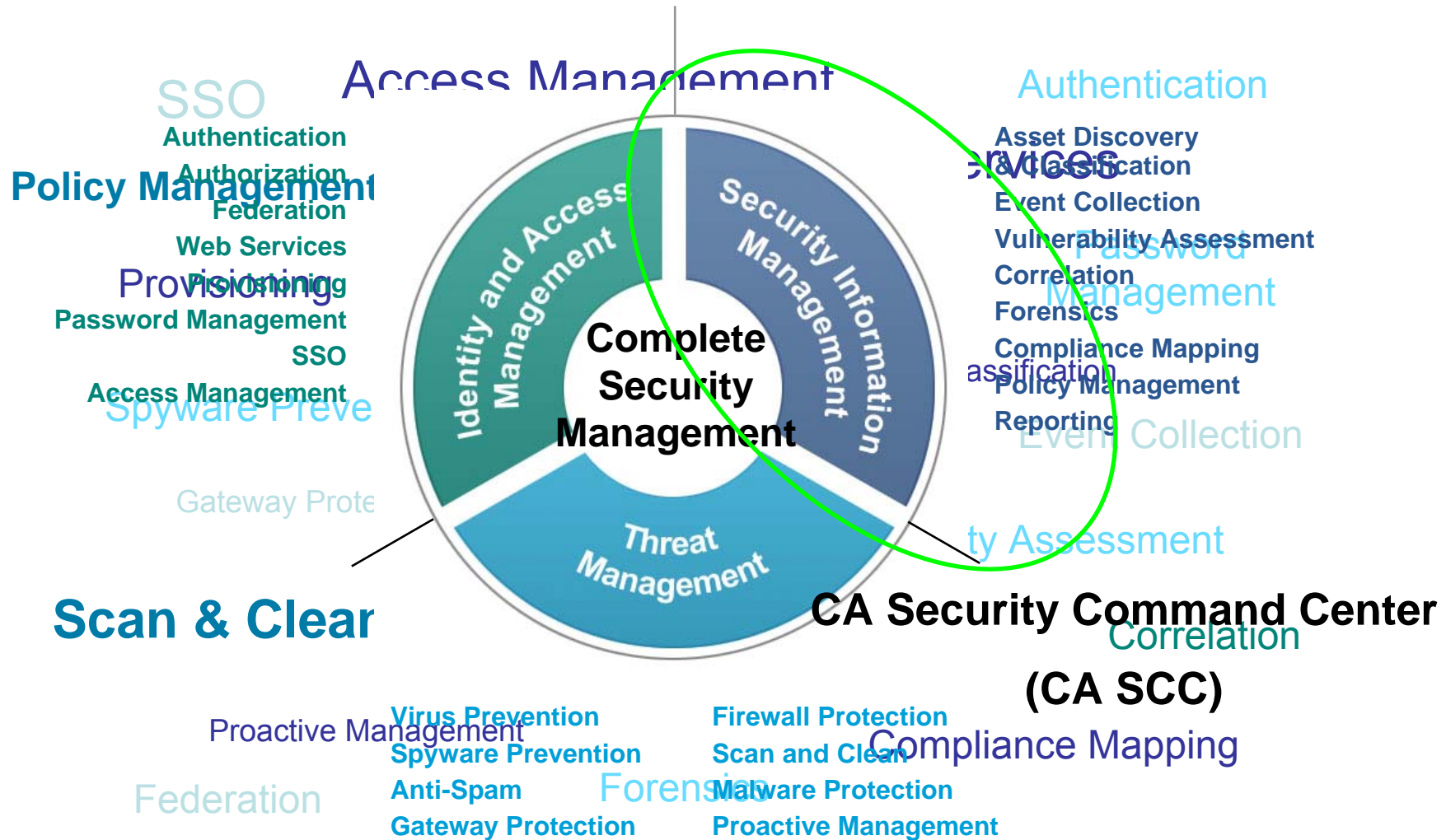
## Gestire e mantenere sicura l'infrastruttura real-time



### Global IT Organization

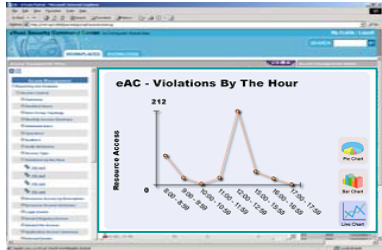


# La necessità di gestire la complessità

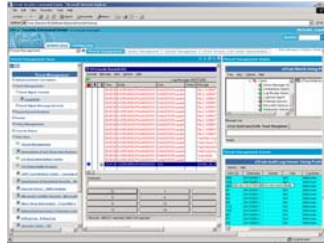


# L'architettura di CA Security Command Center

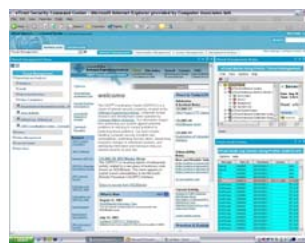
Security Director



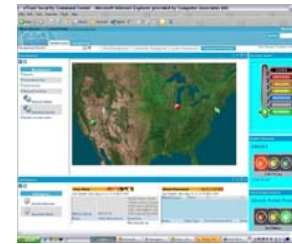
Security Administrator



Antivirus Administrator



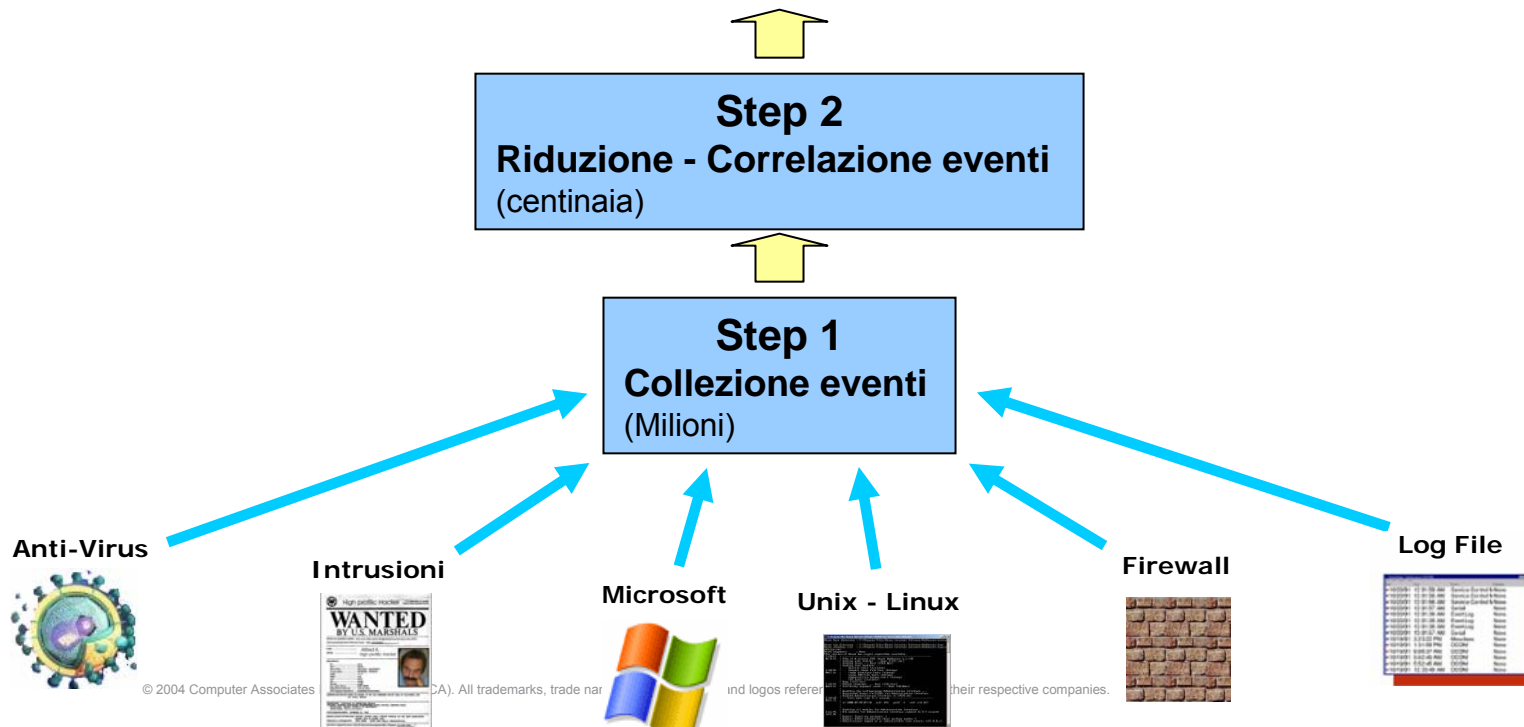
CSO



Help Desk



**CA Security Command Center**  
Presentazione eventi, Reporting, Azioni e Rimedi



# Dalla teoria alla pratica

## Il SOC in CA!

### CA Security Command Center

è la soluzione CA per il SIM: converte enormi quantitativi di dati di sicurezza in informazioni di qualità, utili per dare azioni immediate

### Risposta proattiva

- La Correlazione di eventi permette di concentrarsi solo sui reali problemi, piuttosto che su migliaia di informazioni ridondanti
- Riduce il TCO attraverso una gestione delle informazioni di sicurezza efficiente
- Una soluzione integrata — Unicenter NSM, ServicePlus SD, e Automation Point — permette agli operatori di identificare più velocemente eventi di sicurezza ad alto rischio

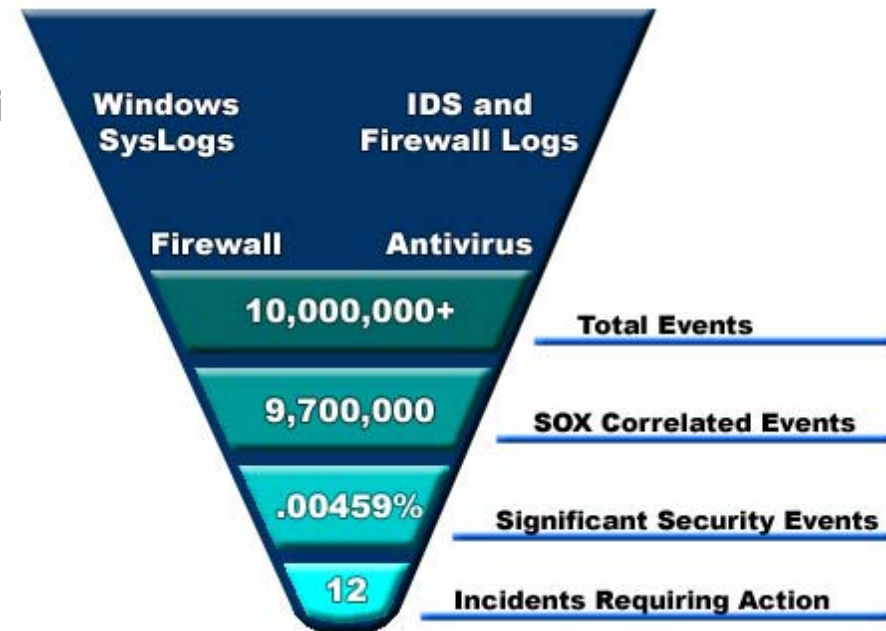


# Dalla teoria alla pratica

## Il SOC in CA grazie a CA Security Command Center!

- 3 Operatori di Security, 4 Sviluppatori, 1 VP
- Patch di aggiornamento distribuite al 90% dei 24'000 global windows hosts entro 48 ore dall'avvio del processo
- **Impatto ZERO** derivante dalle minacce più temute, es. Blaster, Sasser etc.
- **Soluzione di Automazione per soddisfare i requisiti SOX**

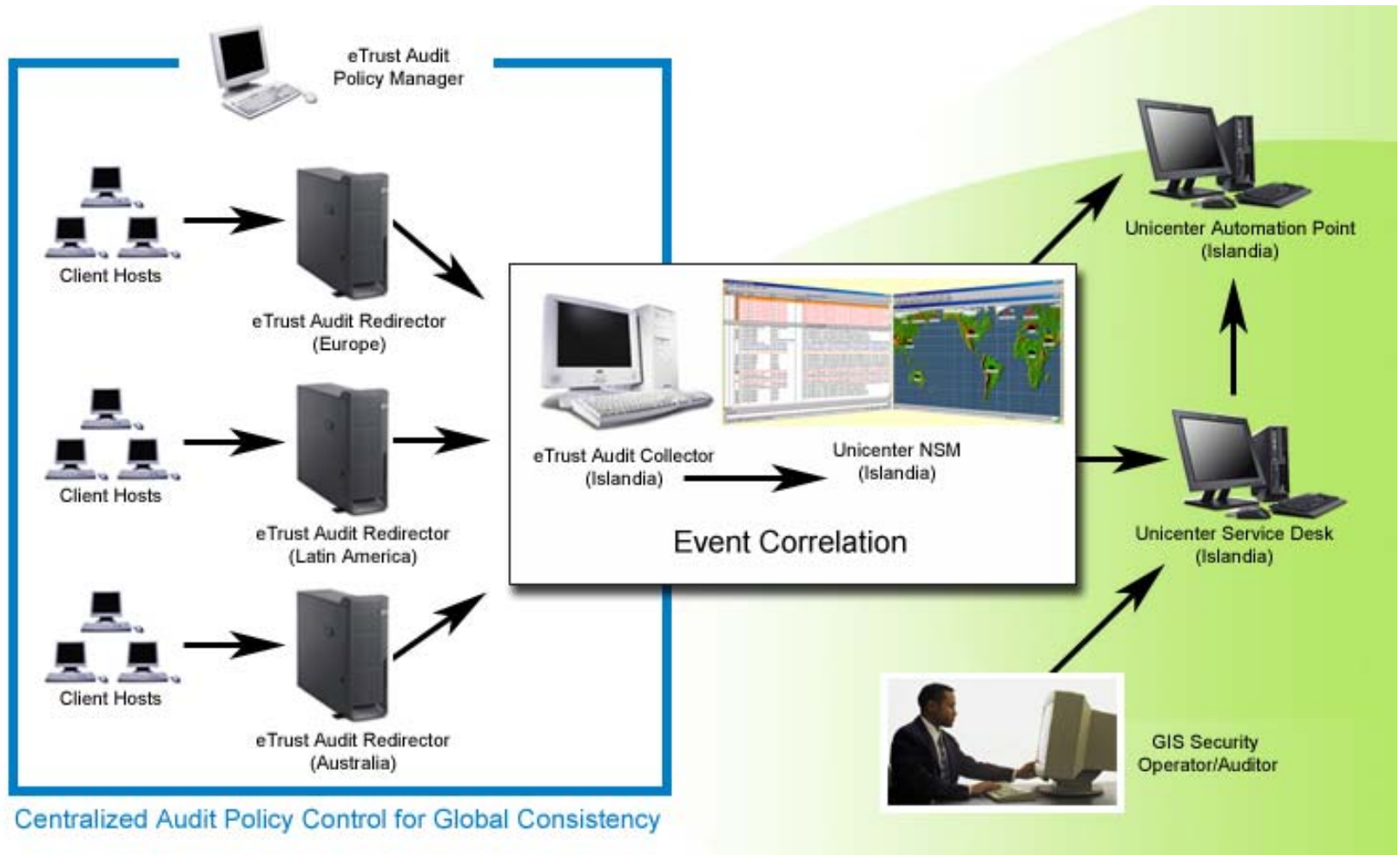
Attività rilevate in oltre 30 giorni vengono automaticamente tracciate, generando 9.7m di eventi SOX, quali cambi di privilegi di accesso, logon / logoff su applicazioni SOX – Financial, HR



*L'abilità di identificare 12 incidenti reali su + di 10 milioni di eventi è una dimostrazione di efficienza*

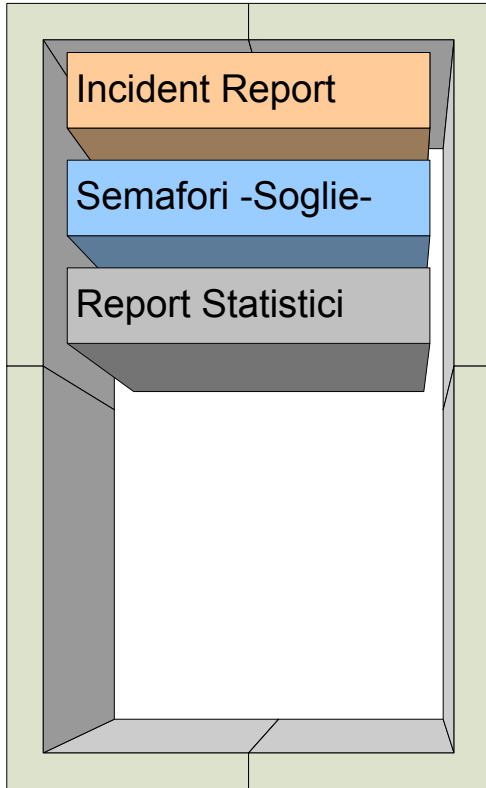
# Dalla teoria alla pratica

## Gestione globale degli eventi



# Dalla teoria alla pratica

## Un esempio di CA SCC



Incidents

Incident Viewer Using Profile: Default Incidents (Node: \*)

Options Help

| Time stamp          | Collector N... | Collector Table         | Owner   | Pending                             | Pending ID | Priority | Annotated                |
|---------------------|----------------|-------------------------|---------|-------------------------------------|------------|----------|--------------------------|
| 07/13/2004 09:48:02 | bruar01-audr80 | Default Audit Collector |         | <input checked="" type="checkbox"/> | 2          | 1        | <input type="checkbox"/> |
| 07/13/2004 09:47:04 | bruar01-audr80 | Default Audit Collector |         | <input checked="" type="checkbox"/> | 2          | 1        | <input type="checkbox"/> |
| 07/13/2004 09:45:18 | bruar01-audr80 | Default Audit Collector |         | <input checked="" type="checkbox"/> | 3          | 1        | <input type="checkbox"/> |
| 07/13/2004 09:42:20 | bruar01-audr80 | Default Audit Collector |         | <input checked="" type="checkbox"/> | 3          | 1        | <input type="checkbox"/> |
| 07/13/2004 09:31:21 | bruar01-audr80 | Default Audit Collector |         | <input checked="" type="checkbox"/> | 2          | 1        | <input type="checkbox"/> |
| 07/13/2004 09:30:18 | bruar01-audr80 | Default Audit Collector |         | <input checked="" type="checkbox"/> | 4          | 1        | <input type="checkbox"/> |
| 07/13/2004 09:28:41 | bruar01-audr80 | Default Audit Collector |         | <input checked="" type="checkbox"/> | 3          | 1        | <input type="checkbox"/> |
| 07/13/2004 09:28:41 | bruar01-audr80 | Default Audit Collector |         | <input checked="" type="checkbox"/> | 5          | 1        | <input type="checkbox"/> |
| 07/13/2004 09:28:41 | bruar01-audr80 | Default Audit Collector |         | <input checked="" type="checkbox"/> | 1          | 1        | <input type="checkbox"/> |
| 07/13/2004 09:28:41 | bruar01-audr80 | Default Audit Collector |         | <input checked="" type="checkbox"/> | 1          | 1        | <input type="checkbox"/> |
| 07/13/2004 09:28:41 | bruar01-audr80 | Default Audit Collector |         | <input checked="" type="checkbox"/> | 2          | 1        | <input type="checkbox"/> |
| 07/13/2004 09:28:41 | bruar01-audr80 | Default Audit Collector |         | <input checked="" type="checkbox"/> | 4          | 1        | <input type="checkbox"/> |
| 07/13/2004 09:28:41 | bruar01-audr80 | Default Audit Collector |         | <input checked="" type="checkbox"/> | 1          | 1        | <input type="checkbox"/> |
| 07/13/2004 09:28:41 | bruar01-audr80 | Default Audit Collector |         | <input checked="" type="checkbox"/> | 1          | 1        | <input type="checkbox"/> |
| 07/12/2004 20:28:04 | bruar01-audr80 | Default Audit Collector | bruar01 | <input checked="" type="checkbox"/> | 2          | 1        | <input type="checkbox"/> |

Ready

Computer Associates CIO Command Center Friday, May 14th, 2004 Search

Welcome **Walt Thomas** to the CIO Dashboard

CIO Dashboard USPSD Dashboard Security Command Center CA Dashboard Technology

Performance of Top 5 Enterprise Applications (SLMO SQL)

Select application url: <http://supportconnect> Response or throughput: Response

Max & Avg Response Time (msec) for <http://supportconnect.ca.com>. Goal < 2000 msec

Open Issues Past SLA at Week End (USPSD Excel Report)

% Closed Issues Past SLA at Week End (USPSD Excel)

Project Tracker (Proprietary)

Milestones Met vs. System Type

| System Type                | Total Milestones | Total Met |
|----------------------------|------------------|-----------|
| Core, Support, & Reporting | 145              | 120       |
| Sales, Mktg. & Svcs        | 282              | 235       |
| Finance, HR, & Emp/Svcs    | 286              | 233       |

WAN Performance Between Key CA Sites (from NPO)

Select WAN Link: [Islandia to Herndon](#)

© 2004 Computer Associates International, Inc. (CA). All trademarks, trade

HelpDesk Announcements (USPSD Inures): Item with 5 digit dialing in or out with the Mississauga and Montreal office. AllStre :: 2/2/2004 4:37 PM We are currently experiencing

Conf EXPO  
RSI



e-Security Lab  
2007

MILANO - 24/25 Gennaio 2007



# Domande?

Elio Molteni, CISM-CISSP-BS7799  
Executive Security Advisor  
Computer Associates  
elio.molteni@ca.com

*Presidente Capitolo Italiano ISSA*



Computer Associates International, Inc. (CA). All trademarks, trade names, services marks and logos referenced herein belong to