

Enterprise Security: La gestione delle informazioni

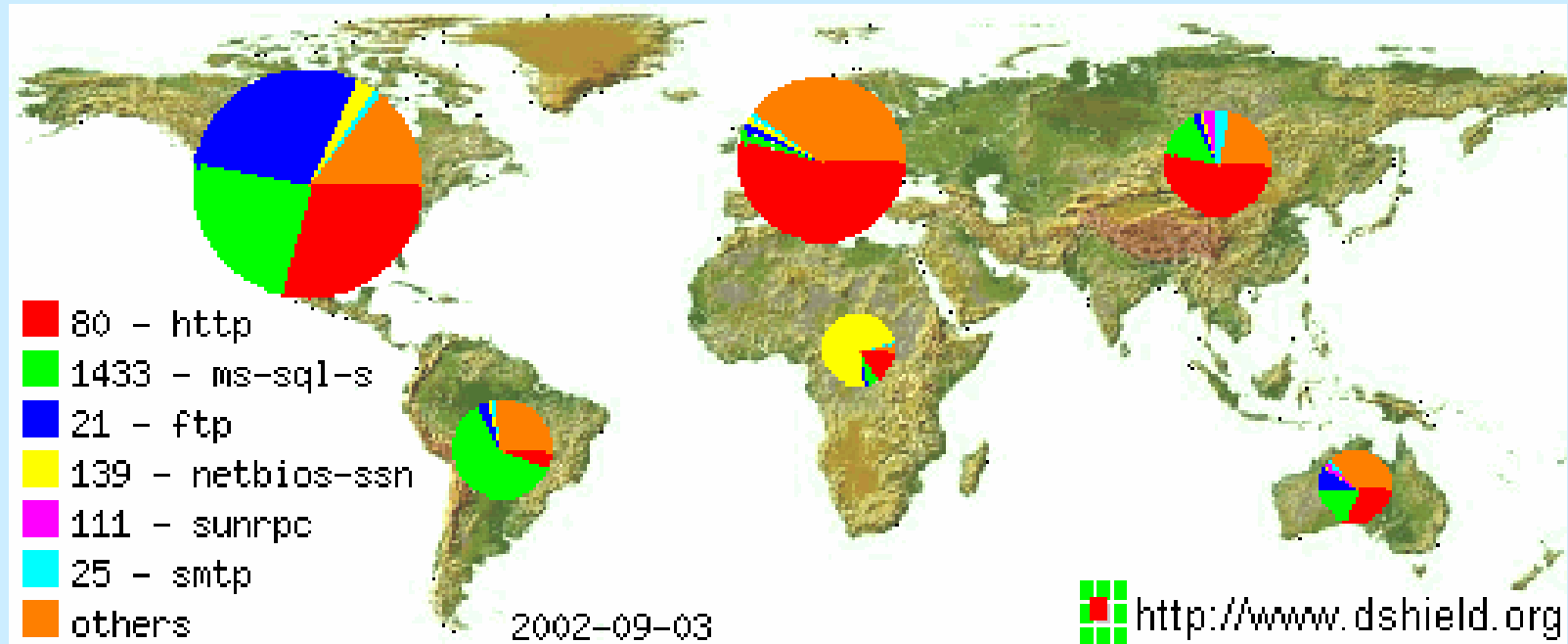


Massimo Cipriani
Consulting Manager – Technology Services
Computer Associates Italia S.p.a.
massimo.cipriani@ca.com

Internet Growth Trends

- 1977: 111 hosts on Internet
- 1981: 213 hosts
- 1983: 562 hosts
- 1984: 1,000 hosts
- 1986: 5,000 hosts
- 1987: 10,000 hosts
- 1989: 100,000 hosts
- 1992: 1,000,000 hosts
- 2001: 150 – 175 million hosts
- 2002: over 200 million hosts
- By 2010, about 80% of the planet will be on the Internet

Evoluzione dello scenario



"The Morris Worm"

(November 1988)

...security works in an era of (computer) worms that can spread across the Internet in 10 minutes"

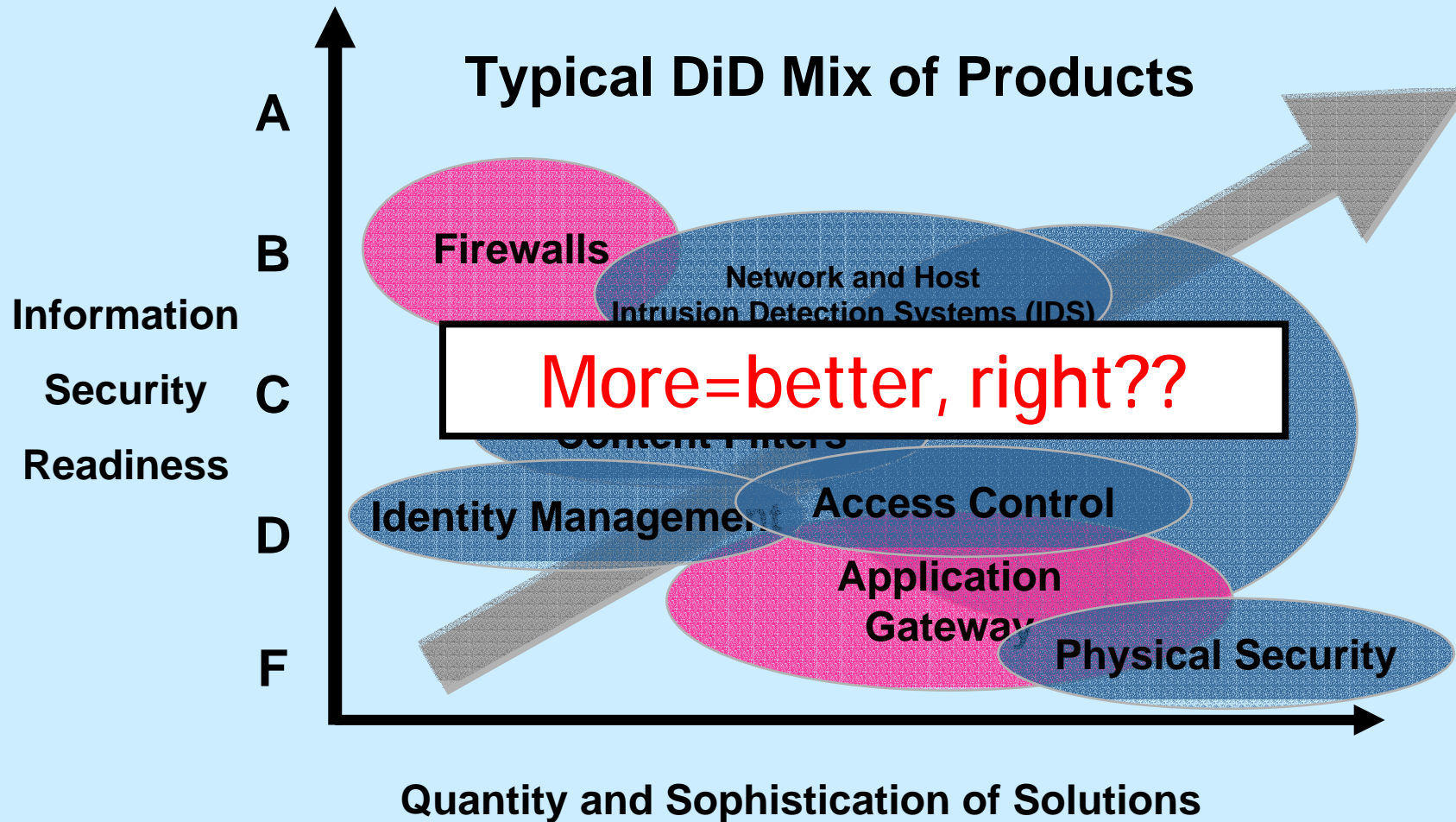
(Bruce Schneier - IEEE S&P, July/August 2003)

Le contromisure

- Router: filtraggio pacchetti (IP Spoofing)
- Firewall (Stateful Packet Inspection)
- Antivirus
- IDS (HIDS, NIDS, KIDS)
- Crittografia
- VPN
- ...

Ognuna di queste soluzioni ha il suo sistema di event e alert management, oltre a differenti sistemi di reporting.

The Theory of "Defense in Depth" (DiD)



Current State Of Information Security: Information Overload



Security information overload



Complex services and new technologies



Increasing

“I have 1.3 million events a day – I need more than a GUI that will display these. I need to see only what’s important without saturating my network.”



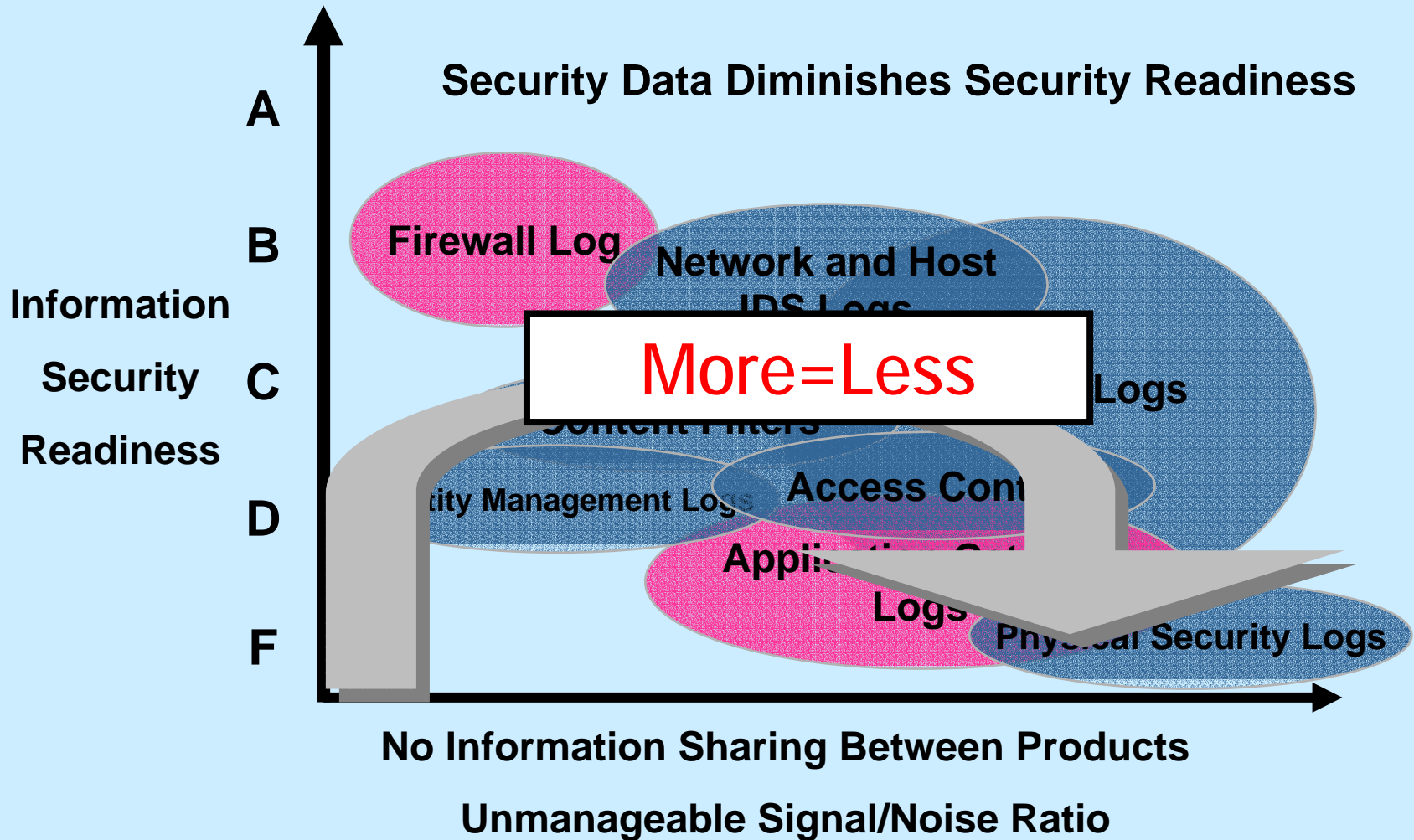
systems



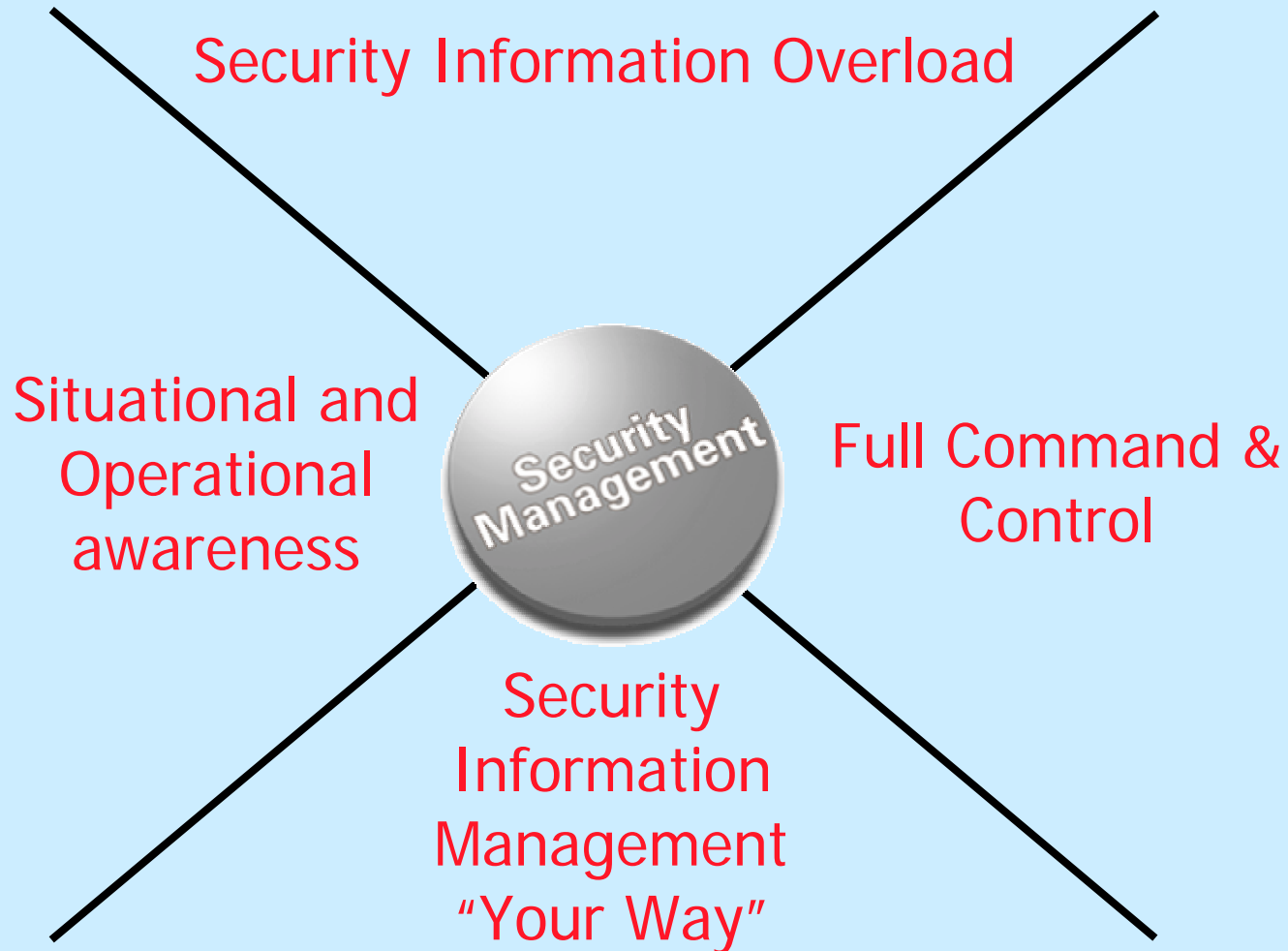
Integrating a variety of platforms and vendors



The Reality of “Defense in Depth”



I problemi dell'Enterprise Security Information Management





Le conseguenze

Per i Security Administrator:

- Necessità di analizzare moli di dati eterogenei provenienti da una molteplicità di fonti diverse, basati su protocolli differenti (Syslog, OPSEC, SNMP, Event Log, ecc.) ;
- Difficoltà di discriminare i “Falsi Positivi” dei FW e degli IDS;
- Difficoltà di riconoscimento dello stesso evento rilevato da dispositivi differenti;
- Difficoltà di mettere in relazione i dati ed estrarre informazioni rilevanti, ai fini del riconoscimento di un attacco.

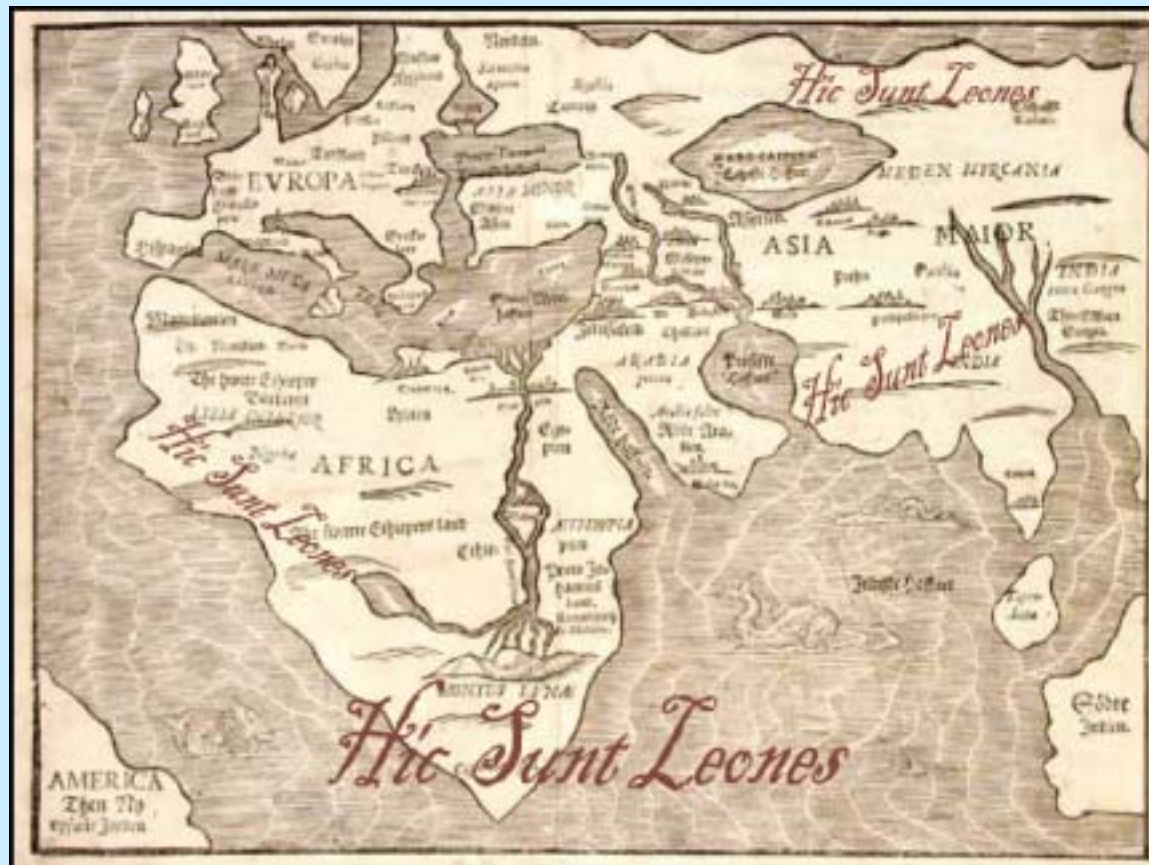
Cosa accade dei dati nativi di auditing ?

TURNED ON	TURNED OFF
<p data-bbox="220 433 742 721">So much data is created that important events can't be found.</p> <p data-bbox="220 817 789 1030">Auditors use different tools for each environment.</p>	<p data-bbox="899 433 1148 488">No data.</p>  A cartoon illustration of a man in a pink shirt and blue pants kneeling on the floor, shouting at a computer monitor. The monitor has a face with a hand covering its mouth, suggesting it is silent or ignoring him. The desk is green.
<p data-bbox="220 1078 1221 1215">Organizations don't know what's happening on their systems.</p>	 A cartoon illustration of a man in a blue suit and a woman in a pink shirt standing next to a computer monitor. The man is pointing at the screen and talking to the woman.

“Prevention is ideal but
detection is a must”

(SANS Institute)

Da chi bisogna difendersi?



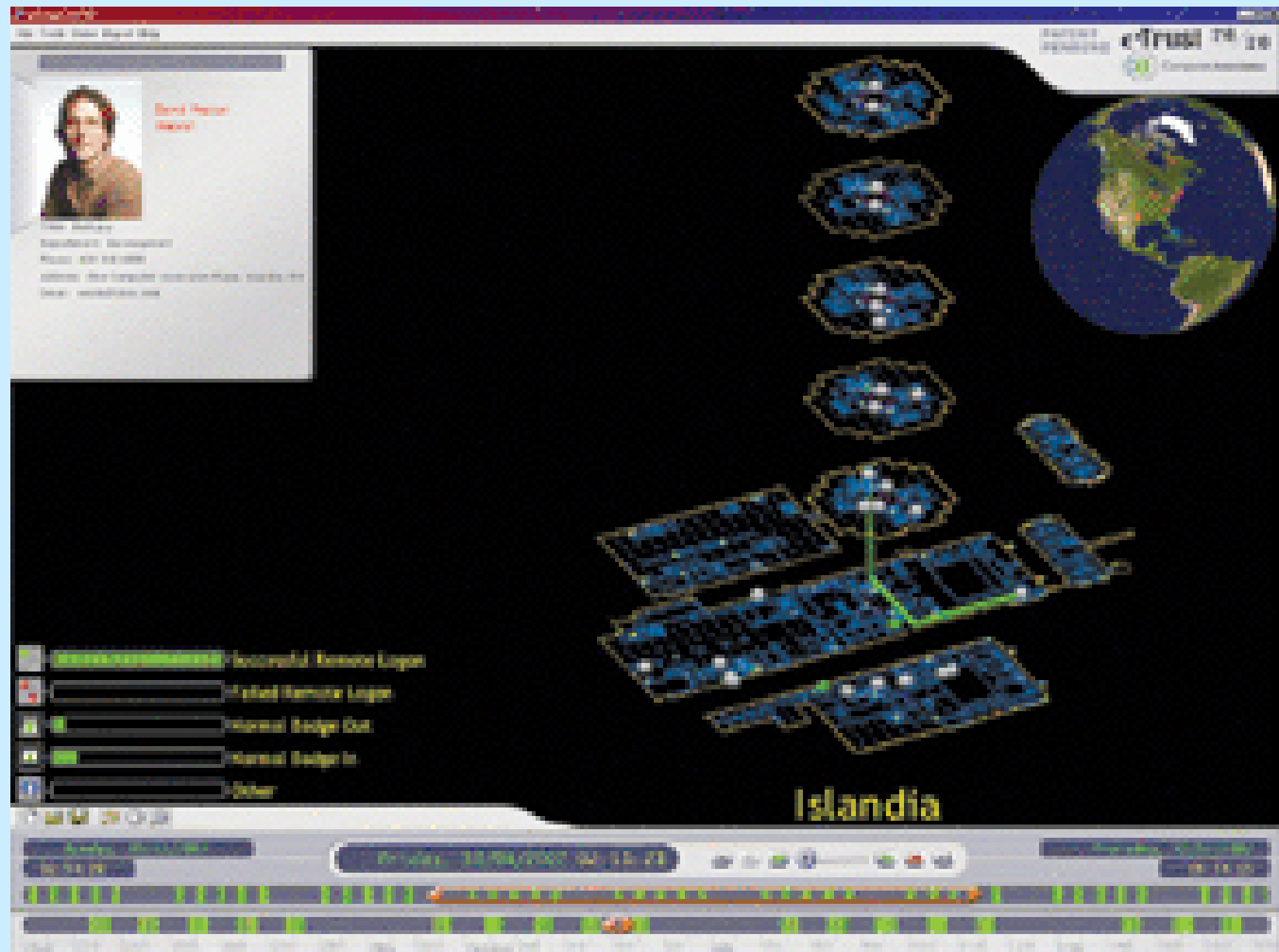
Le questioni aperte

- Probabili fonti di Attacchi – Utenti interni “scontenti”?
- Perdite Finanziarie - Utilizzo improprio (abuso) degli accessi alla Rete ?
- Incidenti per accessi interni non autorizzati?
- Conformità alle normative?
- Capacità di riconoscimento di un attacco?

I numeri

- 90% - Probabili fonti di Attacchi – Utenti interni “scontenti”
- 70% - Perdite Finanziarie - Utilizzo improprio (abuso) degli accessi alla Rete
- 55% - Incidenti per accessi interni non autorizzati
- 48% - Mancanza di conformità alle normative
- 33% - Incapacità di riconoscimento di un attacco

Convergenza tra Sicurezza Fisica e Logica



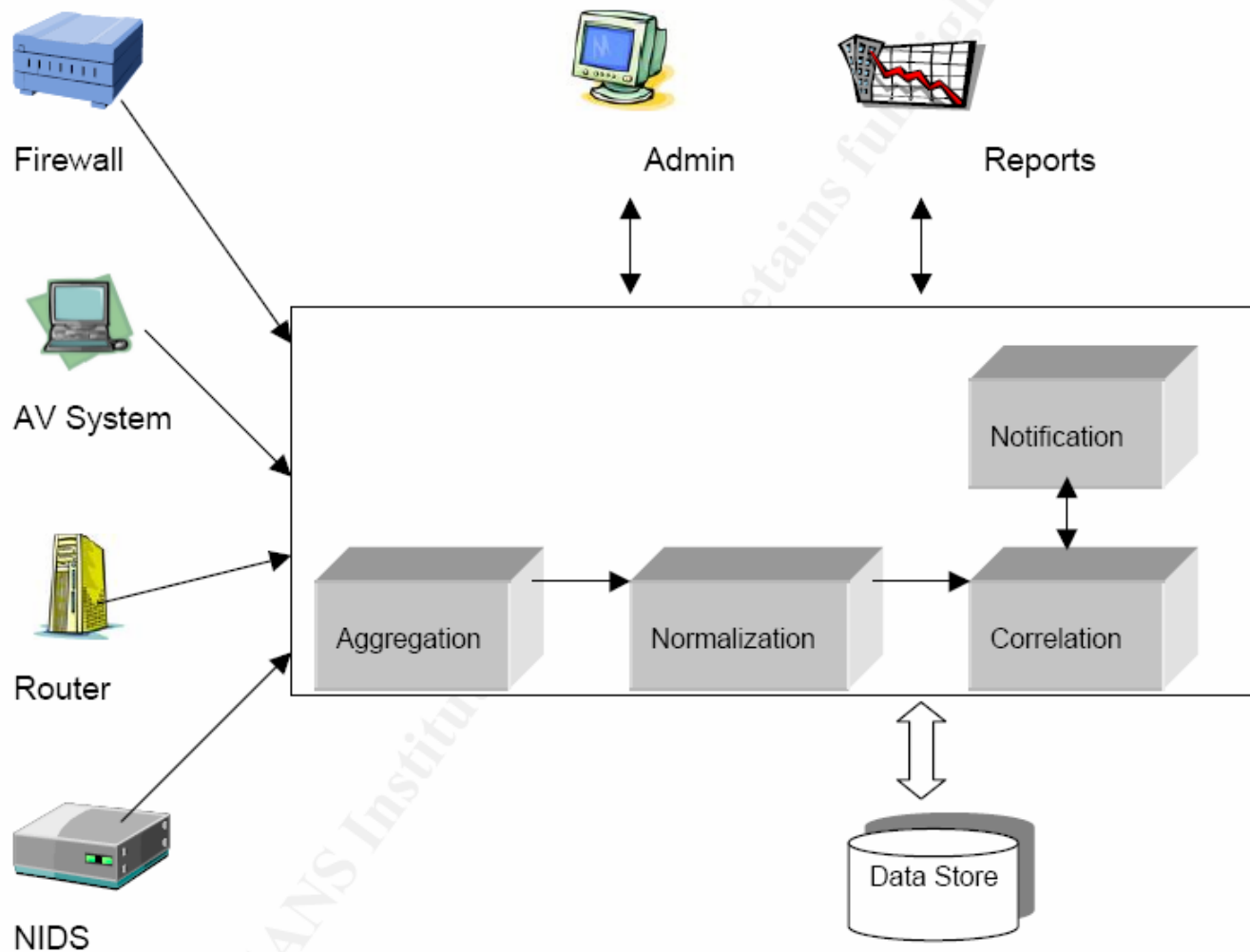


Figure 1: Enterprise Security Information Management (ESIM) Architecture

Sistema di Enterprise Security Information Management

Componenti architetturali

- Agenti
- Motore di analisi
- Data Store
- Management Console
- Report

Sistema di Enterprise Security Information Management

Agenti

Raccolgono informazioni sulle attività in rete o sui sistemi.

Possono interfacciare i Log file o ricevere gli eventi direttamente dai dispositivi.

Ruotano gli eventi al server centrale di Management.

Sistema di Enterprise Security Information Management

Motore di analisi

E' il componente critico e centrale del sistema che realizza le funzioni di:

- Aggregazione
- Normalizzazione
- Correlazione
- Notifica

Sistema di Enterprise Security Information Management

Data Store

Rappresenta il Repository centrale delle informazioni.

Consente analisi Real-time e produzione di report

Sistema di Enterprise Security Information Management

Management Console

- Permette la definizione delle policy.
- Consente la vista centralizzata dell'intero sistema.
- Rappresenta il punto di raccolta degli allarmi.
- Permette l'aggiornamento automatico dei pattern/signature.

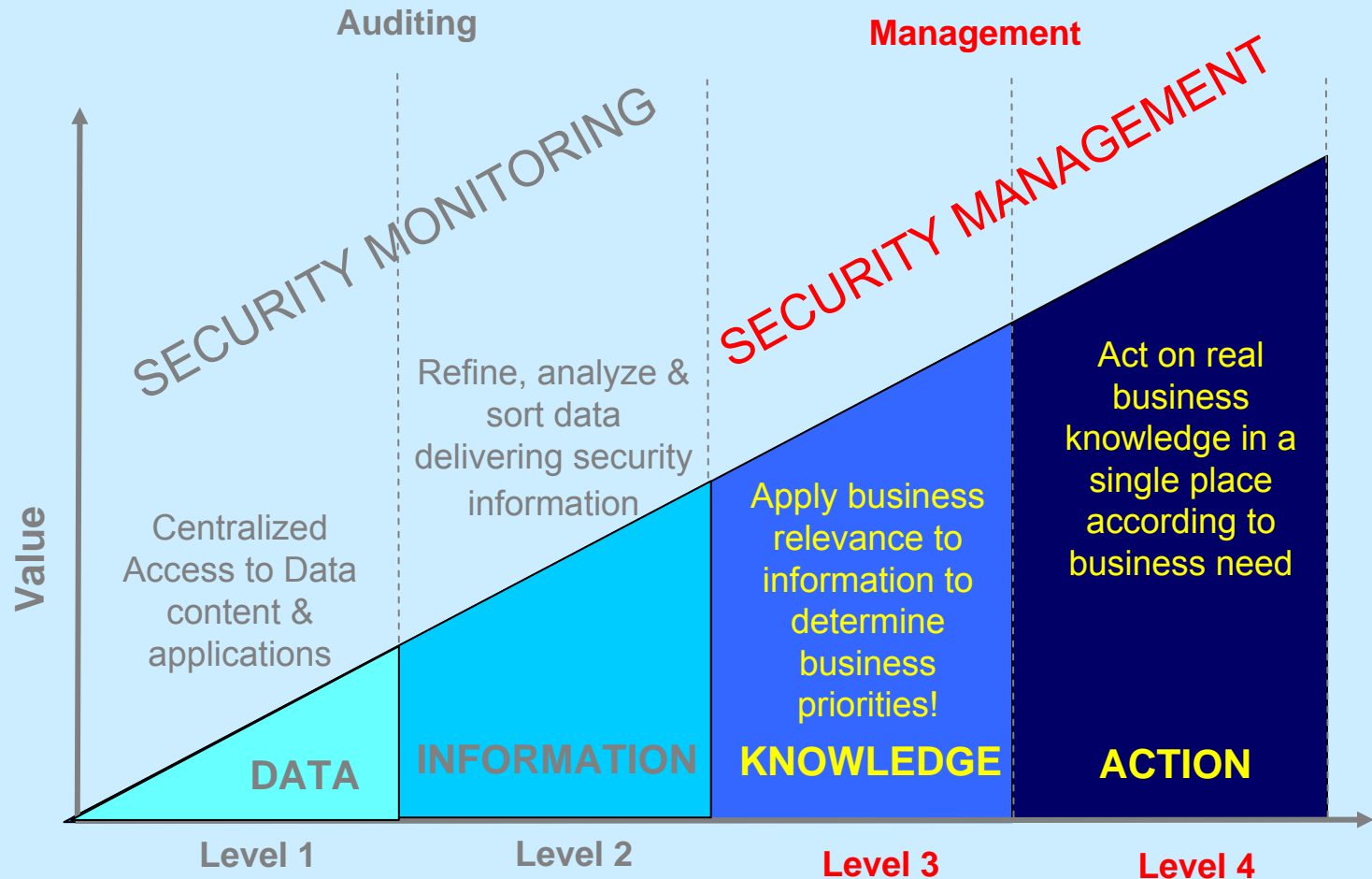
Sistema di Enterprise Security Information Management

Report

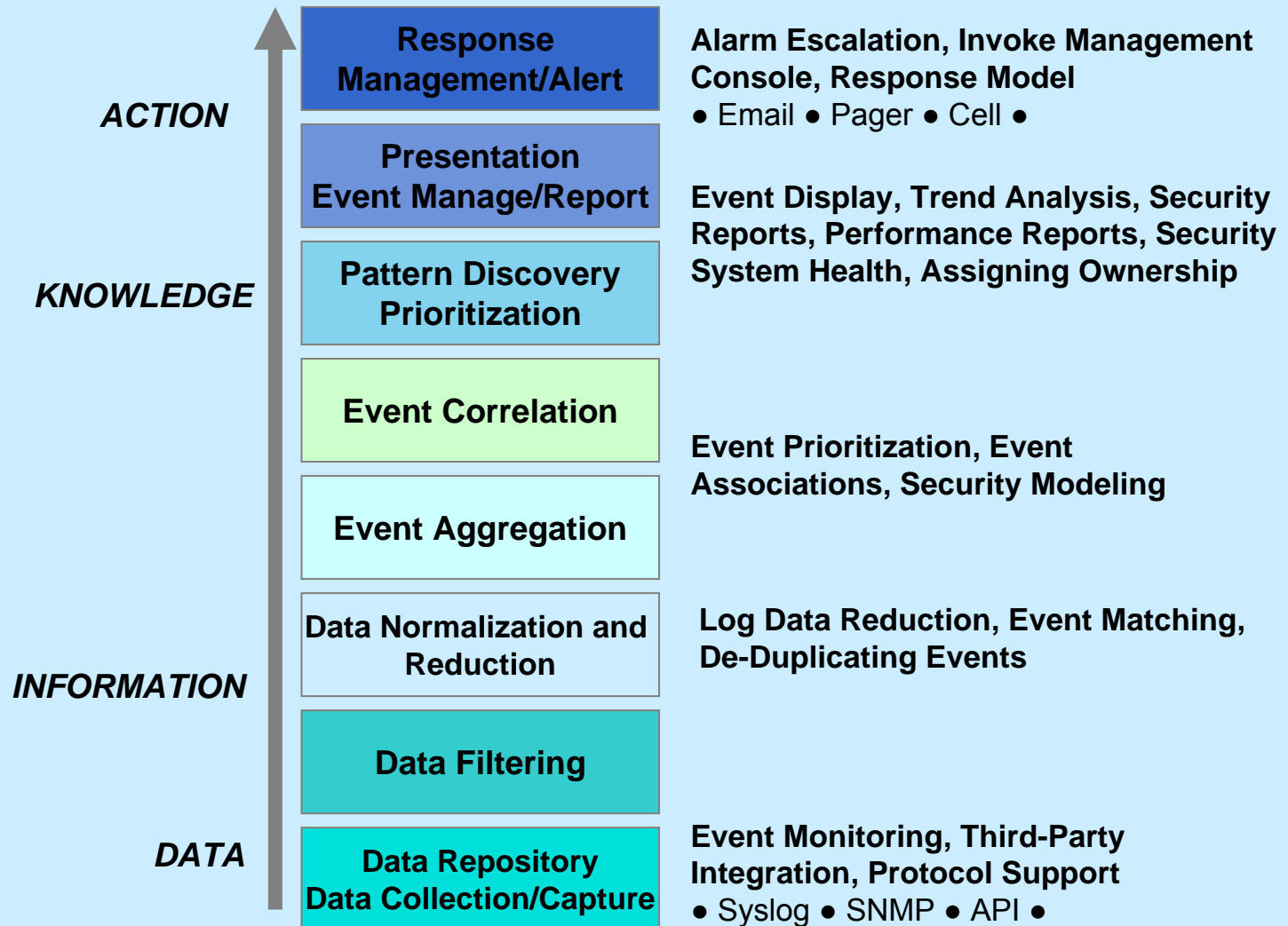
La sicurezza è un processo continuo non una soluzione definitiva.

I Report vengono generati per comprendere i trend degli eventi e per rappresentare il livello di Security al management dell'organizzazione

Information Delivery Maturity Level



Enterprise Security Information Management: Data Hierarchy

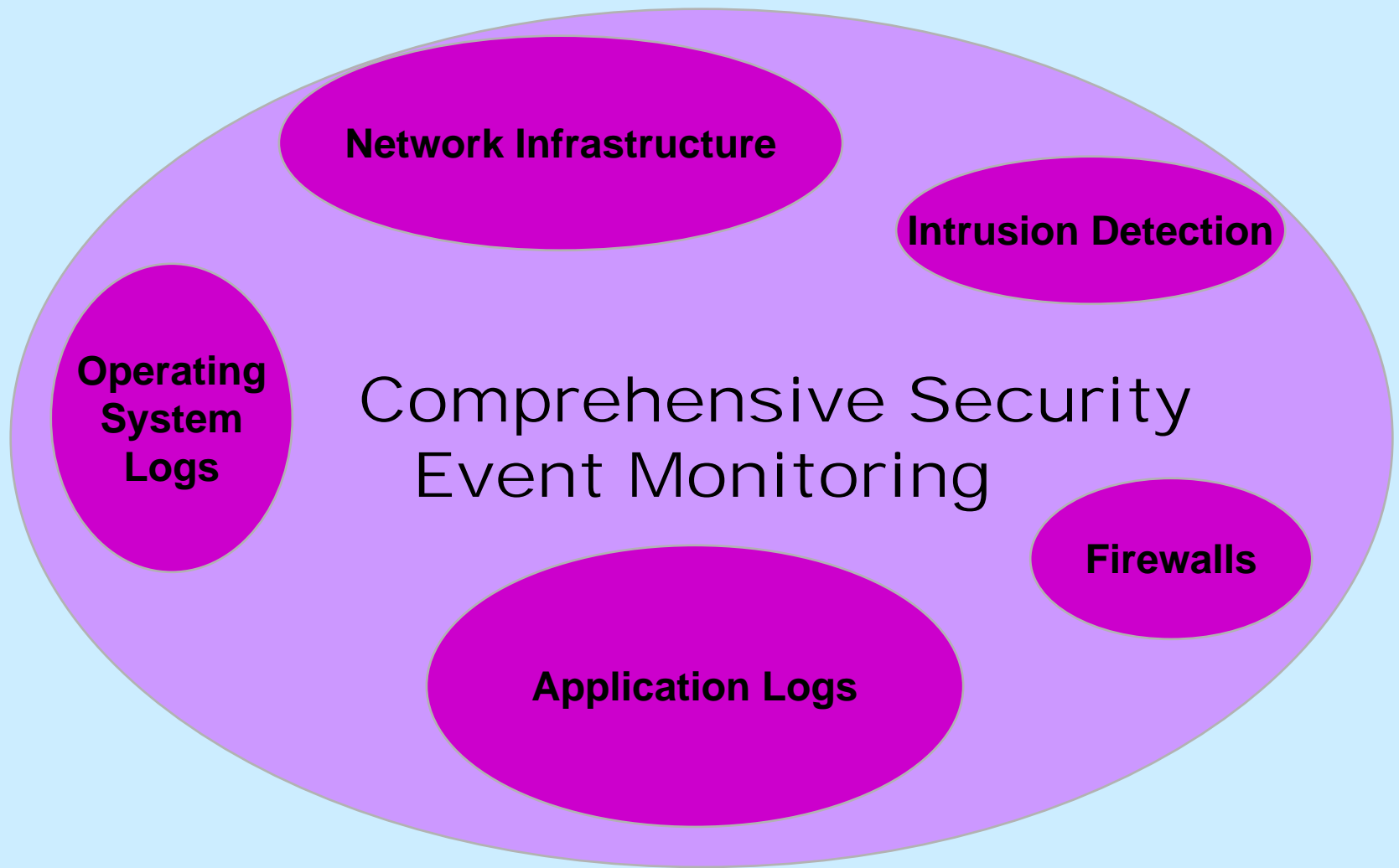


Sicurezza tra processo e tecnologie

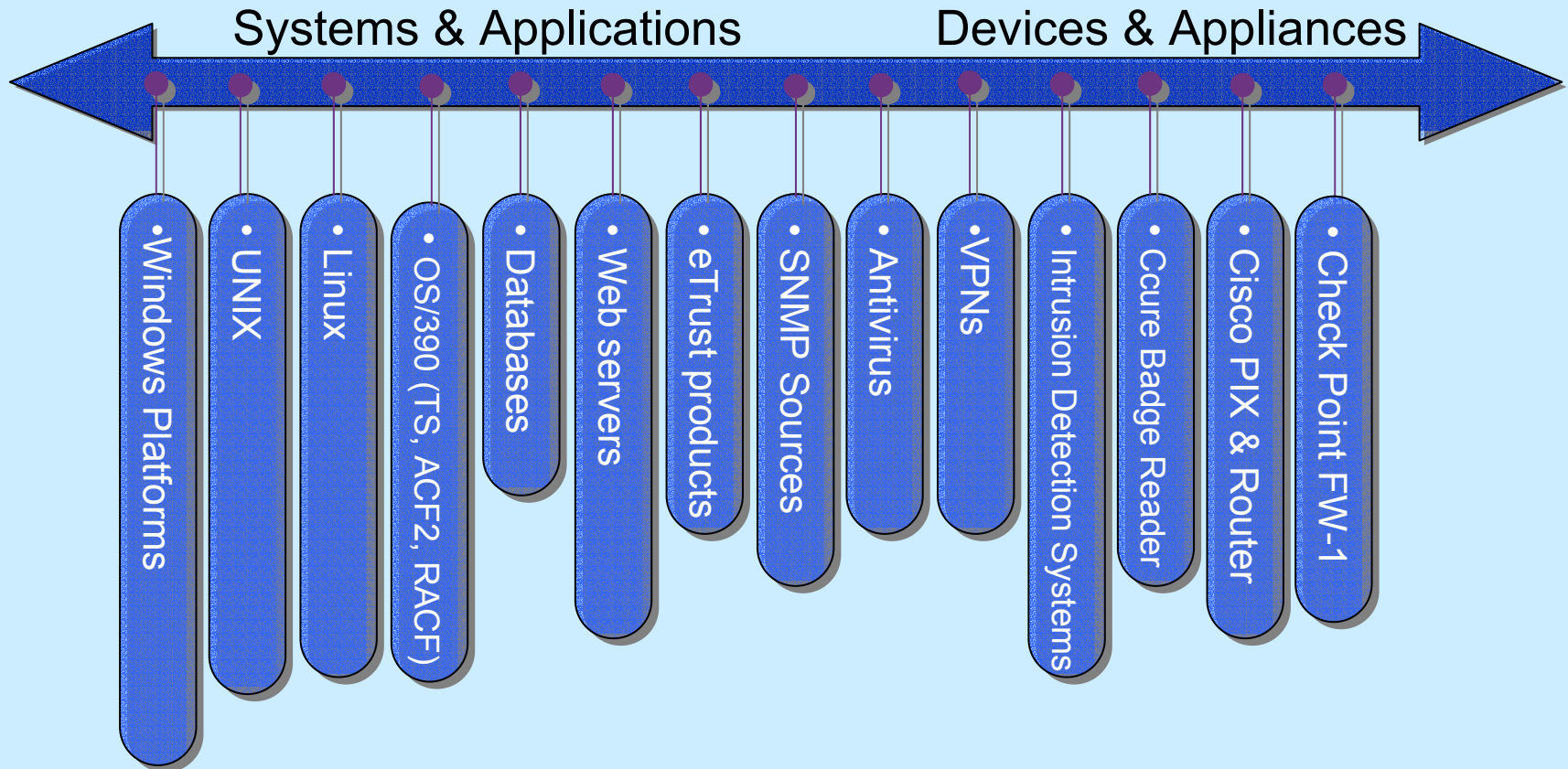
■ “La sicurezza è un processo, non un prodotto”
Bruce Schneier

■ La sicurezza è un processo che coinvolge le tecnologie, le persone, le organizzazioni, ma non c'è sicurezza senza tecnologie

I requisiti di un sistema di gestione delle informazioni di Enterprise Security



End-to-end Security Monitoring



Broad Coverage of Security Technologies

Il numero di eventi è dato da:

SOLUZIONI SICUREZZA

Multiple AV Vendors

Firewall

VPN

Access Control

Web Access Control

Intrusion Detection

User Administration

PKI

Vulnerability Tools

Alarms / Alerts

PIATTAFORME

MS Windows 98

MS Windows 2000

MS Windows XP

Linux

Unix

ZOS

Embedded Systems

NUMERO

DI

Servers

Gateway

DesktopS

PDA's

Phones

Mobile Handhelds

APP

SAP

Oracle

Peoplesoft

External

Internal

Shared

Numero
Utenti



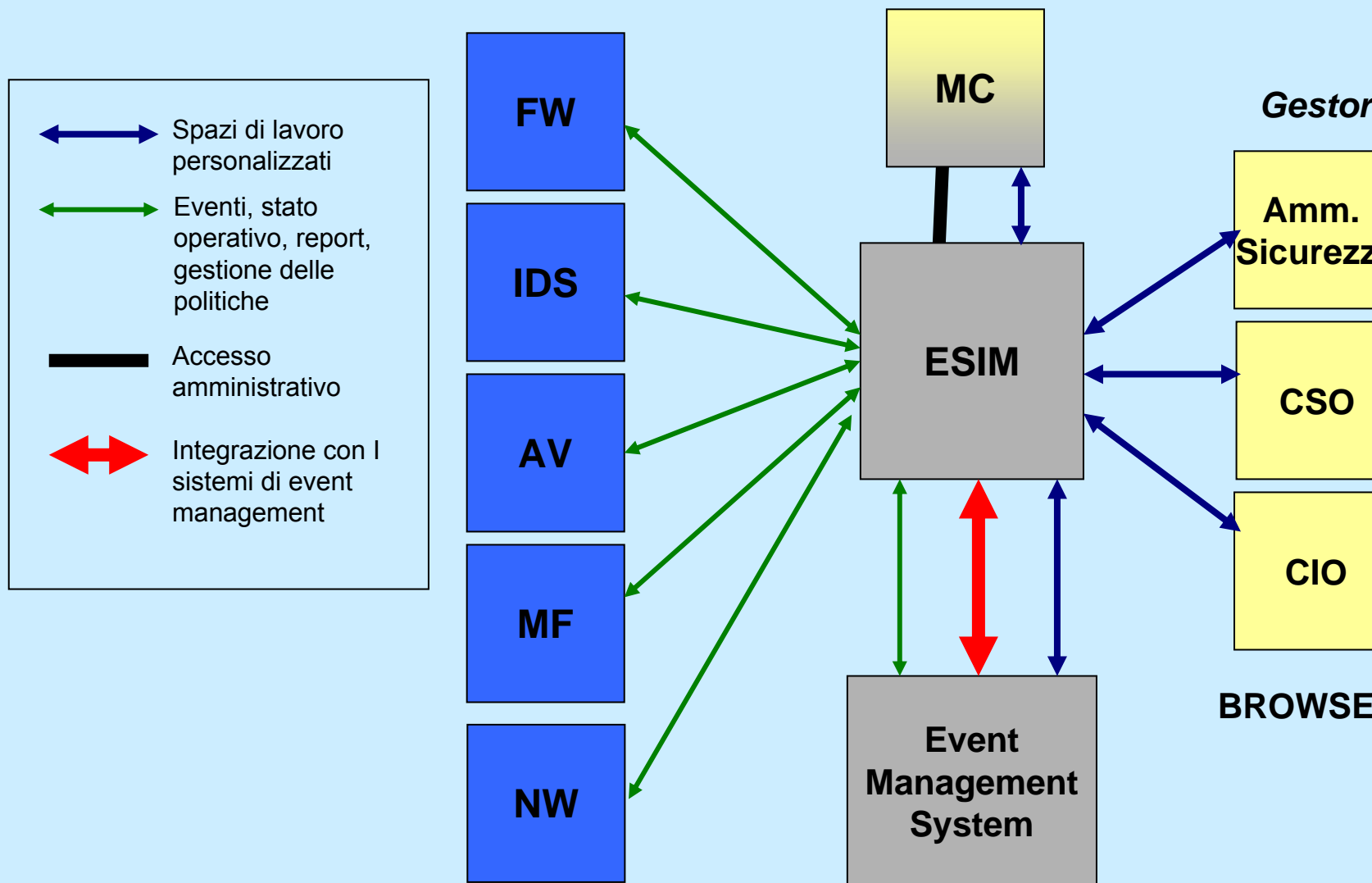
Enterprise Security Information Management :

Caratteristiche Funzionali

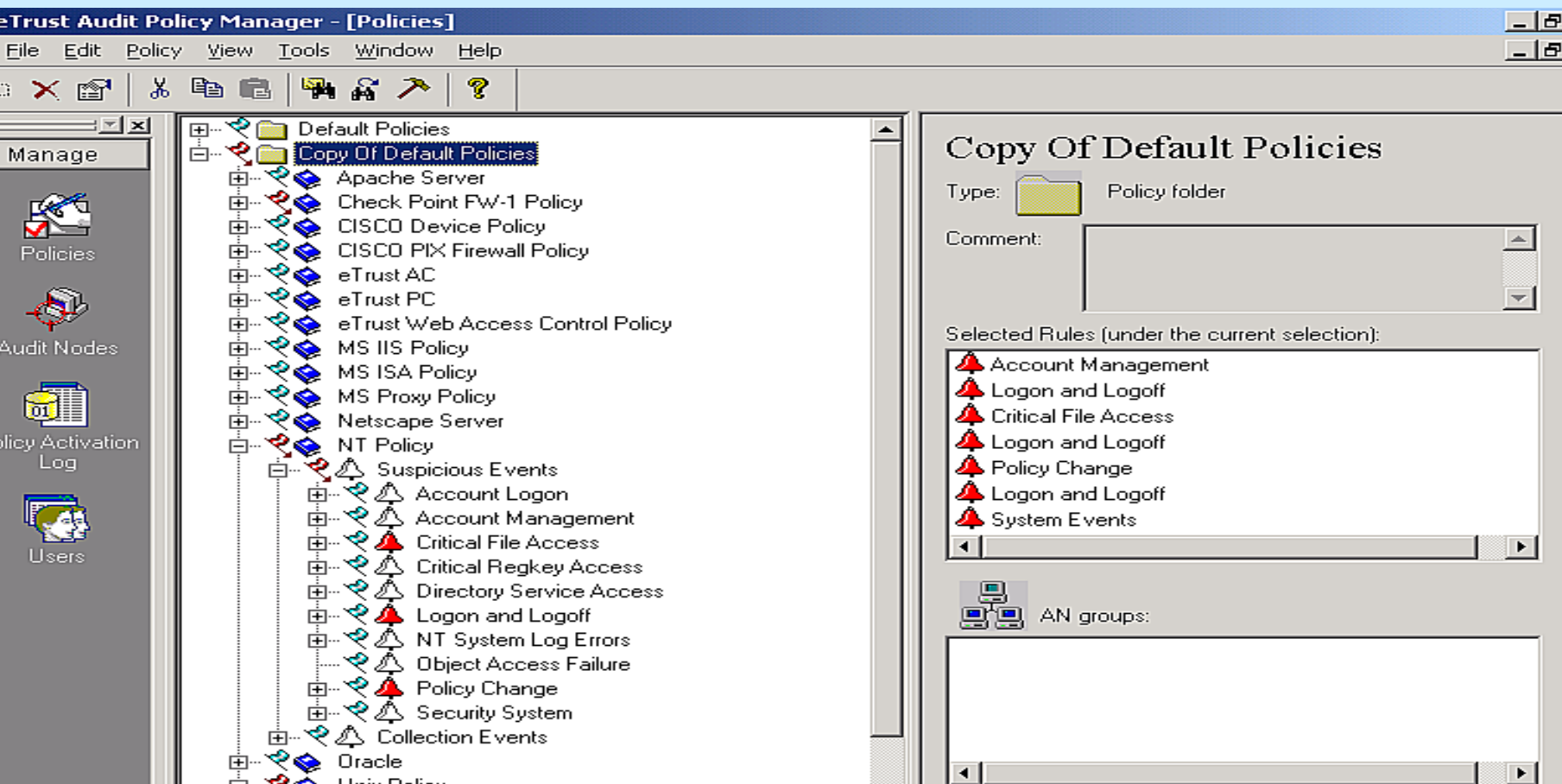
- ❑ controllo centralizzato dei dati di auditing
- ❑ gestione centralizzata delle policy di auditing
- ❑ gestione degli eventi di sicurezza granulare, selettiva e su log separato
- ❑ sistema di sort, filtering e analisi sui dati di auditing
- ❑ sistema di correlazione degli eventi
- ❑ monitor centralizzato dello stato operativo dei sistemi di sicurezza
- ❑ profilazione degli utenti di amministrazione
- ❑ sistema di reporting centralizzato
- ❑ supporto nativo cross-platform, cross-protocol
- ❑ monitor degli incidenti integrabile con un sistema di gestione (help desk, system/network management)

Architettura di un Enterprise Security Information Management

Dispositivi / Applicativi di Sicurezza



Centralized Security Event Policy Management



Predefined, customizable rules and policies

Audit Viewer - [eTrust Audit Data Tools Event Database 1]

File Edit View Filter Report Window Help

Pre-defined filters

Administration records

All records

Last 2 days' records

Last 7 days' records

Login records

Today's records

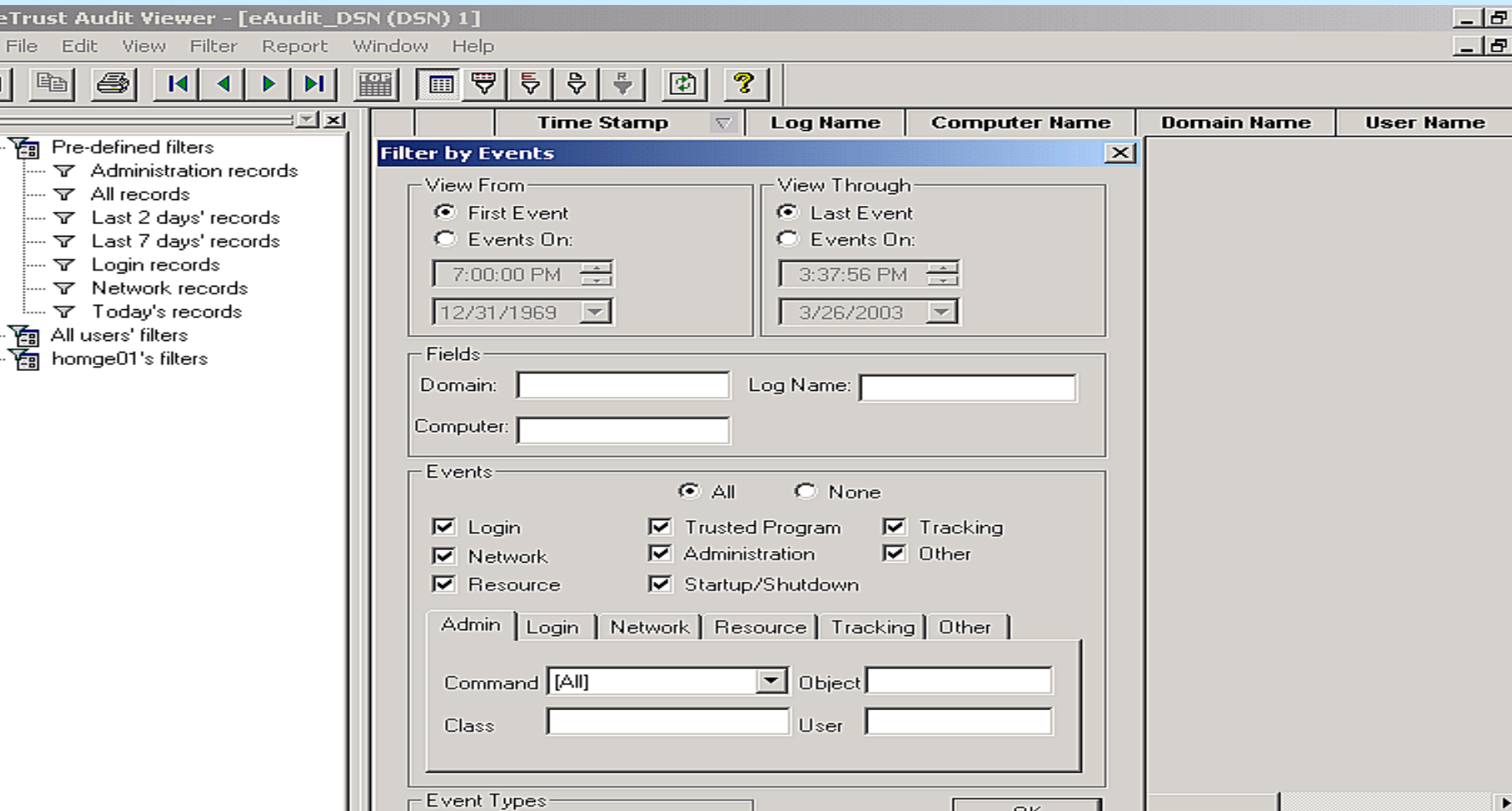
All users' filters

homge01's filters

		Time Stamp	Log Name	Computer Name	Domain Name	User Name	Source	Event Category	Event
		09/13/2002 03:38:15 PM	NT-Security	HOMGE01_NB1		homge01	Security	Privilege Use	577
		09/13/2002 03:38:15 PM	NT-Security	HOMGE01_NB1		homge01	Security	Detailed Tracking	592
		09/13/2002 03:38:15 PM	NT-Security	HOMGE01_NB1		homge01	Security	Privilege Use	577
		09/13/2002 03:37:57 PM	NT-Application	HOMGE01_NB1		SYSTEM	eAudit Actio	Quota Limit	256
		09/13/2002 03:37:53 PM	NT-Security	HOMGE01_NB1		homge01	Security	Detailed Tracking	593
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	562
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	560
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	562
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	560
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	562
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	560
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	562
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	560
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	562
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	560
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	562
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	560
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	562
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	560
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	562
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	560
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	562
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	560
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	562
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	560
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	562
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	560
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	562
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	560
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	562
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	560
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	562
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	560
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	562
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	560
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	562
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	560
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	562
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	560
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	562
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	560
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	562
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	560
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	562
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	560
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	562
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	560
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	562
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	560
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	562
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	560
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	562
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	560
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	562
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	560
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	562
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	560
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	562
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	560
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	562
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	560
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	562
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	560
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	562
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	560
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	562
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	560
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	562
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	560
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	562
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	560
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	562
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	560
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	562
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	560
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	562
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	560
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	562
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	560
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	562
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	560
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	562
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	560
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	562
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	560
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	562
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	560
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	562
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	560
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	562
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	560
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	562
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	560
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	562
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	560
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	562
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	560
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	562
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	560
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	562
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	560
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	562
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	560
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	562
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	560
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	562
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	560
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	562
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	560
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	562
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	560
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	562
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	560
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	562
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	560
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	562
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	560
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	562
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	560
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	562
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	560
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	562
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	560
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	562
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	560
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	562
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	560
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	562
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	560
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	562
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	560
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	562
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	560
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	562
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	560
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	562
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	560
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	562
		09/13/2002 03:37:51 PM	NT-Security	HOMGE01_NB1		SYSTEM	Security	Object Access	560

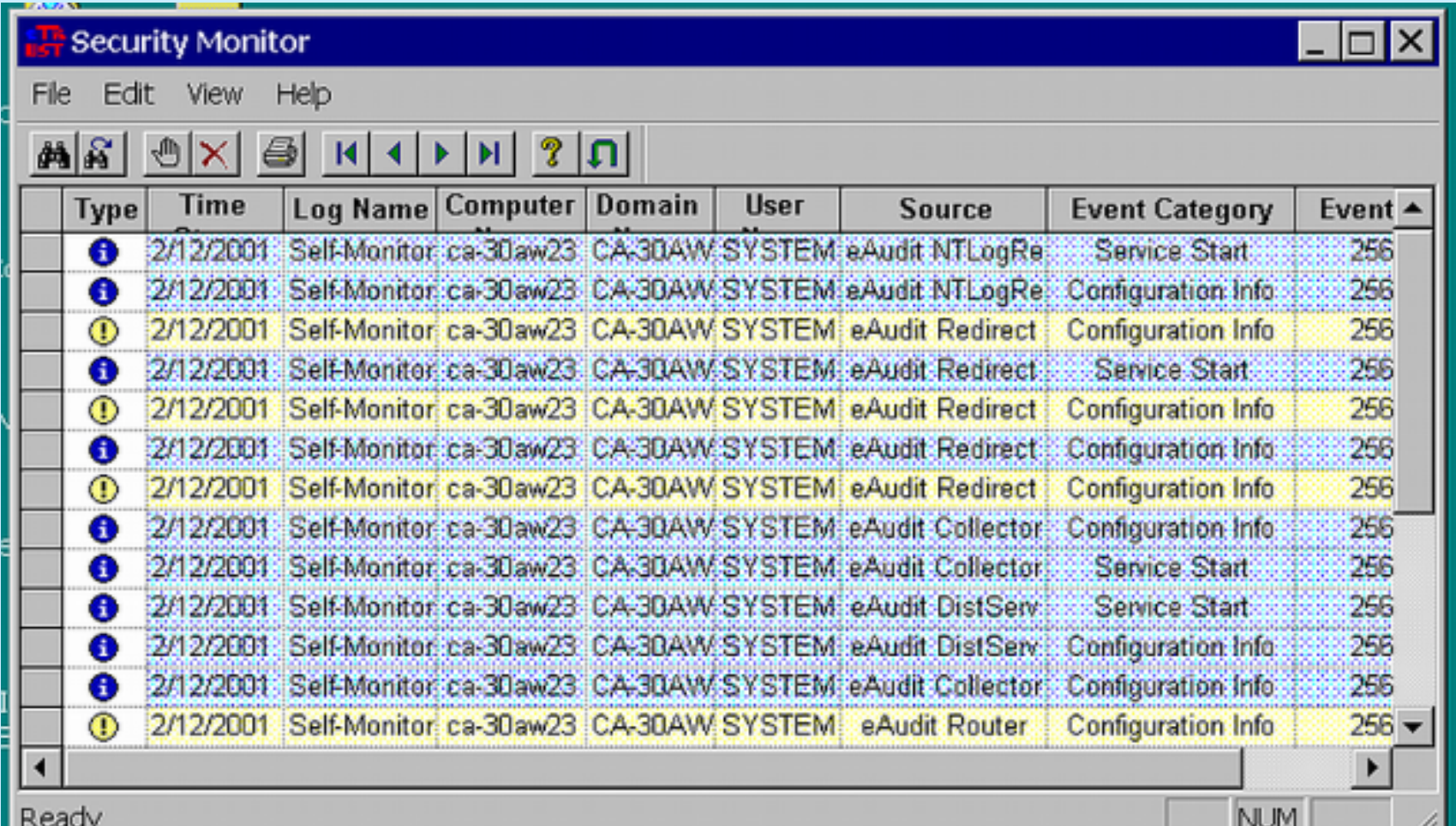
Database-driven querying

Versatile Filtering



**Multi-layered Filtering and data reduction
of Security Events**

Continuous Security Monitoring



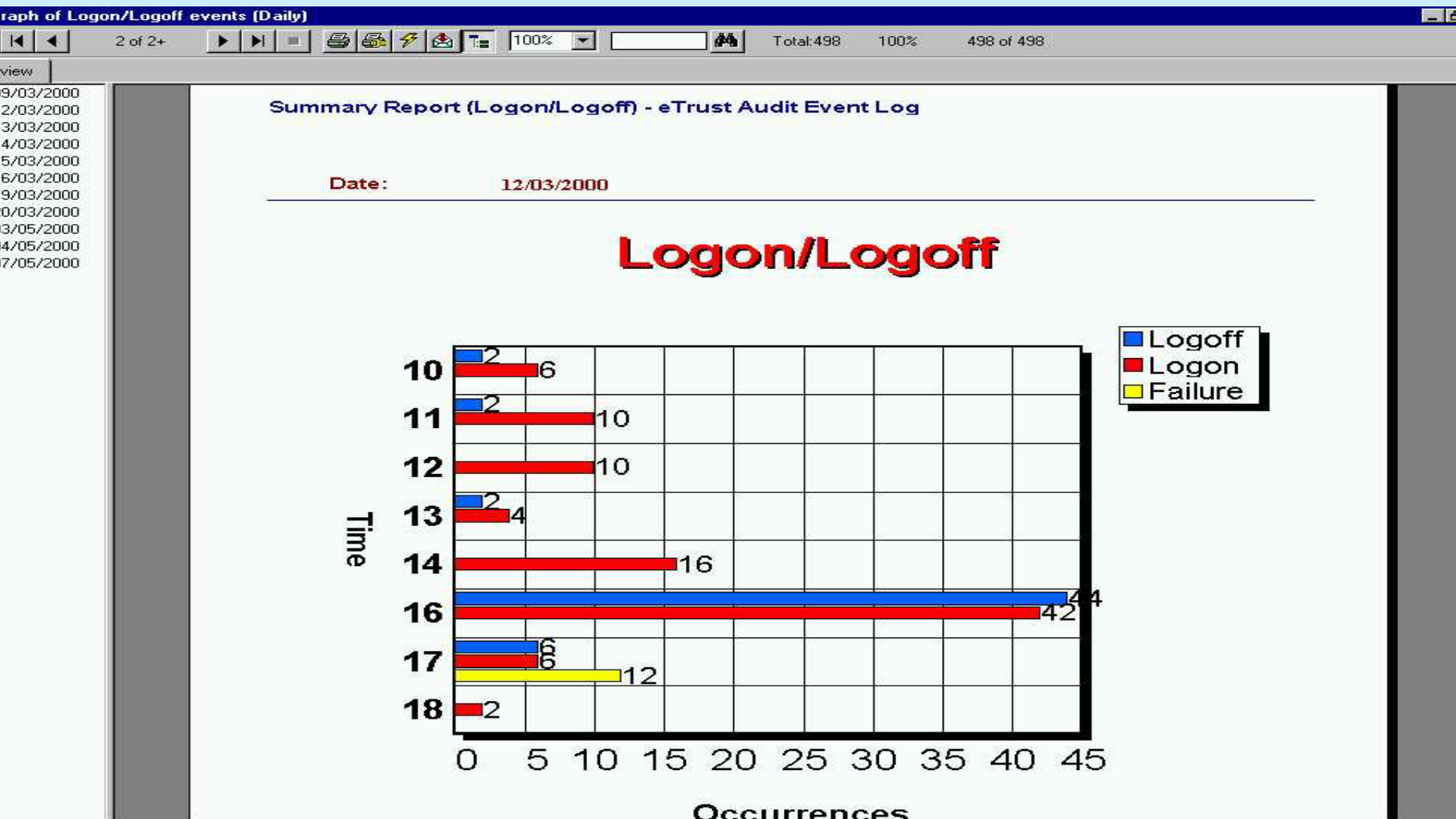
The screenshot shows the 'Security Monitor' application window. It has a menu bar with 'File', 'Edit', 'View', and 'Help'. Below the menu is a toolbar with icons for home, back, forward, and other navigation functions. The main area is a table of security events. The table has columns for Type, Time, Log Name, Computer, Domain, User, Source, Event Category, and Event. The events listed are all from 2/12/2001 and involve 'Self-Monitor' logs on 'ca-30aw23' within the 'CA-30AW' domain, performed by the 'SYSTEM' user. The sources include 'eAudit NTLogRe', 'eAudit Redirect', 'eAudit Collector', 'eAudit DistServ', and 'eAudit Router'. The event categories are 'Service Start' and 'Configuration Info'. The event numbers are all 256.

Type	Time	Log Name	Computer	Domain	User	Source	Event Category	Event
i	2/12/2001	Self-Monitor	ca-30aw23	CA-30AW	SYSTEM	eAudit NTLogRe	Service Start	256
i	2/12/2001	Self-Monitor	ca-30aw23	CA-30AW	SYSTEM	eAudit NTLogRe	Configuration Info	256
!	2/12/2001	Self-Monitor	ca-30aw23	CA-30AW	SYSTEM	eAudit Redirect	Configuration Info	256
i	2/12/2001	Self-Monitor	ca-30aw23	CA-30AW	SYSTEM	eAudit Redirect	Service Start	256
!	2/12/2001	Self-Monitor	ca-30aw23	CA-30AW	SYSTEM	eAudit Redirect	Configuration Info	256
i	2/12/2001	Self-Monitor	ca-30aw23	CA-30AW	SYSTEM	eAudit Redirect	Configuration Info	256
!	2/12/2001	Self-Monitor	ca-30aw23	CA-30AW	SYSTEM	eAudit Redirect	Configuration Info	256
i	2/12/2001	Self-Monitor	ca-30aw23	CA-30AW	SYSTEM	eAudit Collector	Configuration Info	256
i	2/12/2001	Self-Monitor	ca-30aw23	CA-30AW	SYSTEM	eAudit Collector	Service Start	256
i	2/12/2001	Self-Monitor	ca-30aw23	CA-30AW	SYSTEM	eAudit DistServ	Service Start	256
i	2/12/2001	Self-Monitor	ca-30aw23	CA-30AW	SYSTEM	eAudit DistServ	Configuration Info	256
i	2/12/2001	Self-Monitor	ca-30aw23	CA-30AW	SYSTEM	eAudit Collector	Configuration Info	256
!	2/12/2001	Self-Monitor	ca-30aw23	CA-30AW	SYSTEM	eAudit Router	Configuration Info	256

Ready NUM

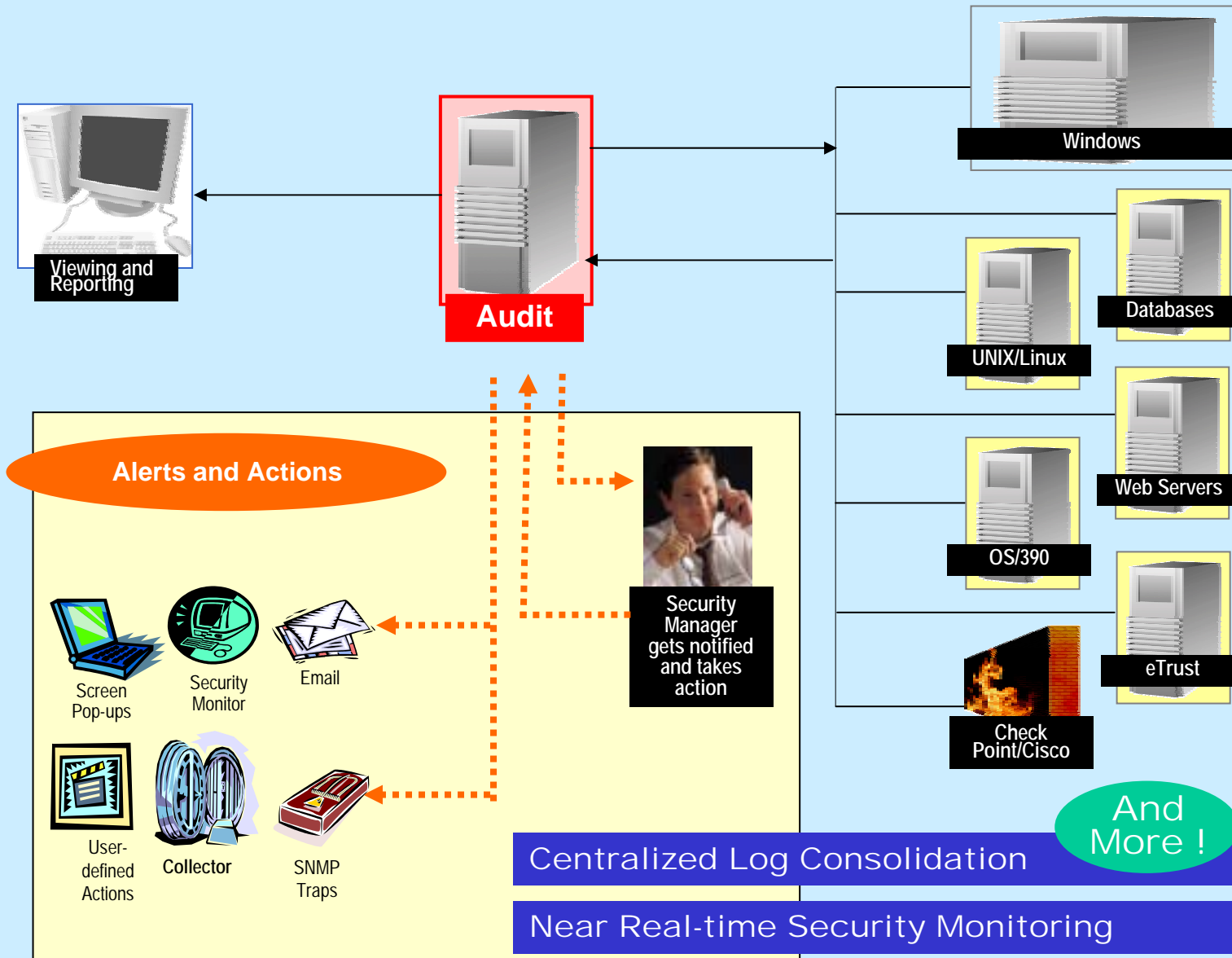
Near real-time monitoring, attack detection and alerting

Robust Reporting

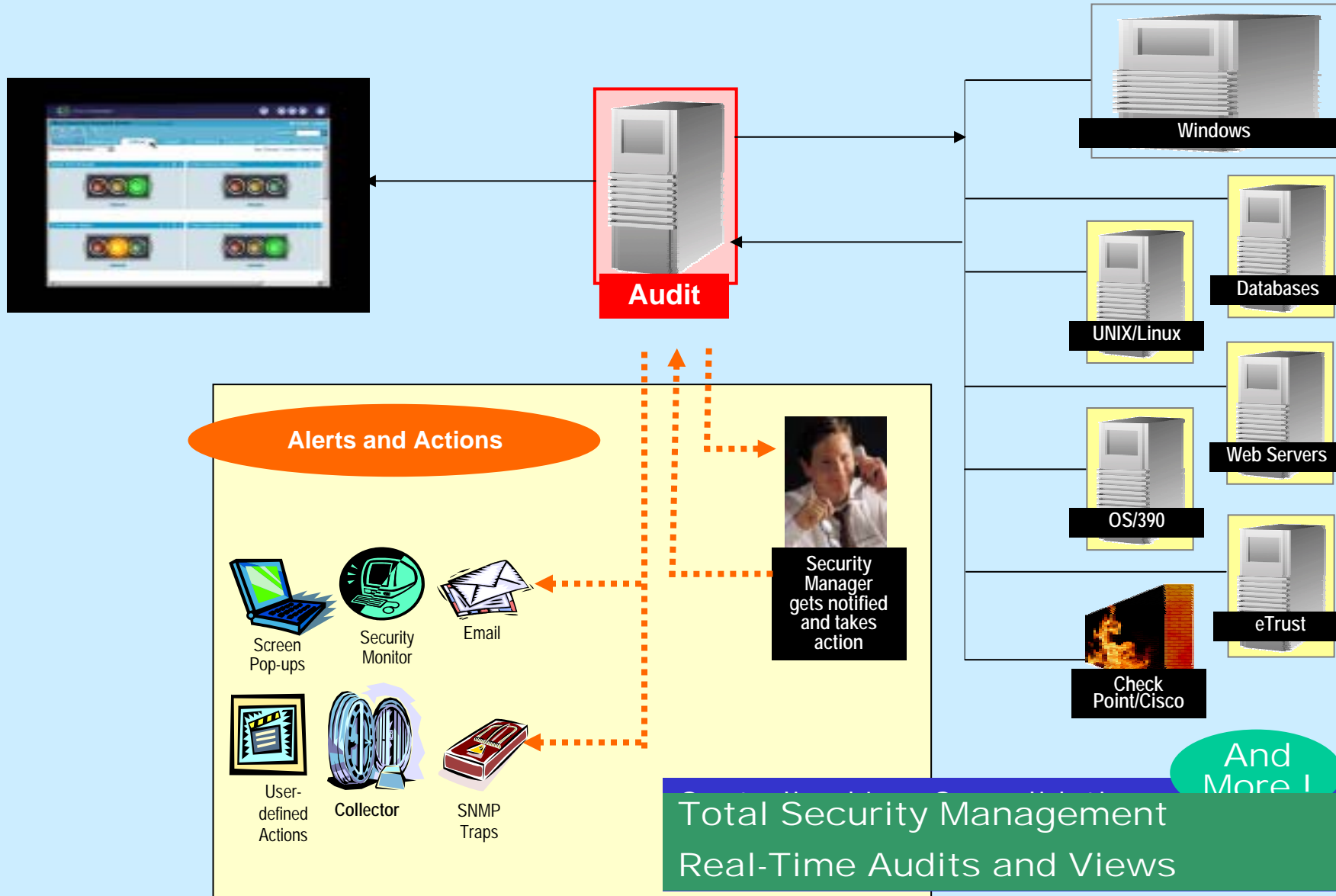


Predefined, Customizable, Detailed, Graphical

Esempio di gestione degli eventi



Esempio di gestione degli eventi



eTrust Security Command Center

eTrust Security Command Center by Computer Associates My Profile | Logoff

SEARCH go

WORKPLACES STATUS EVENTS REPORTING POLICY MGMT KNOWLEDGE

Access Management New | Manage | Configure | Reset | Help

Access Management Events

eTrust Audit Log Viewer Using Profile: Access Management (Node: 142-e...)

Options Help

Message	Entry ID	Timestamp	Domain	User	Log Name	Source
The descripti...	32021	02/14/2003 0...	CALI-ETRUS...	SYSTEM	NT-Security	Security
The descripti...	32342	02/14/2003 1...	CALI-ETRUS...	eAdmin	NT-Security	Security
The descripti...	32339	02/14/2003 1...	CALI-ETRUS...	eAdmin	NT-Security	Security
The descripti...	32338	02/14/2003 1...	CALI-ETRUS...	eAdmin	NT-Security	Security
The descripti...	32337	02/14/2003 1...	CALI-ETRUS...	eAdmin	NT-Security	Security

Ready

Access Management Status

eTrust World Using Profile

Tree View Options Help

- + eTrust World

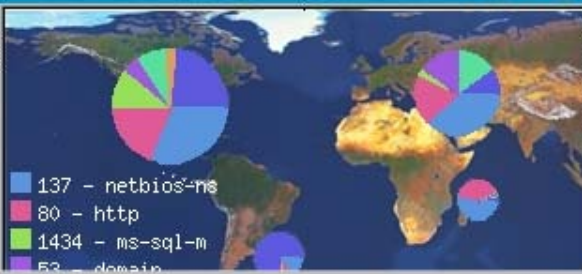
Ready

Alert

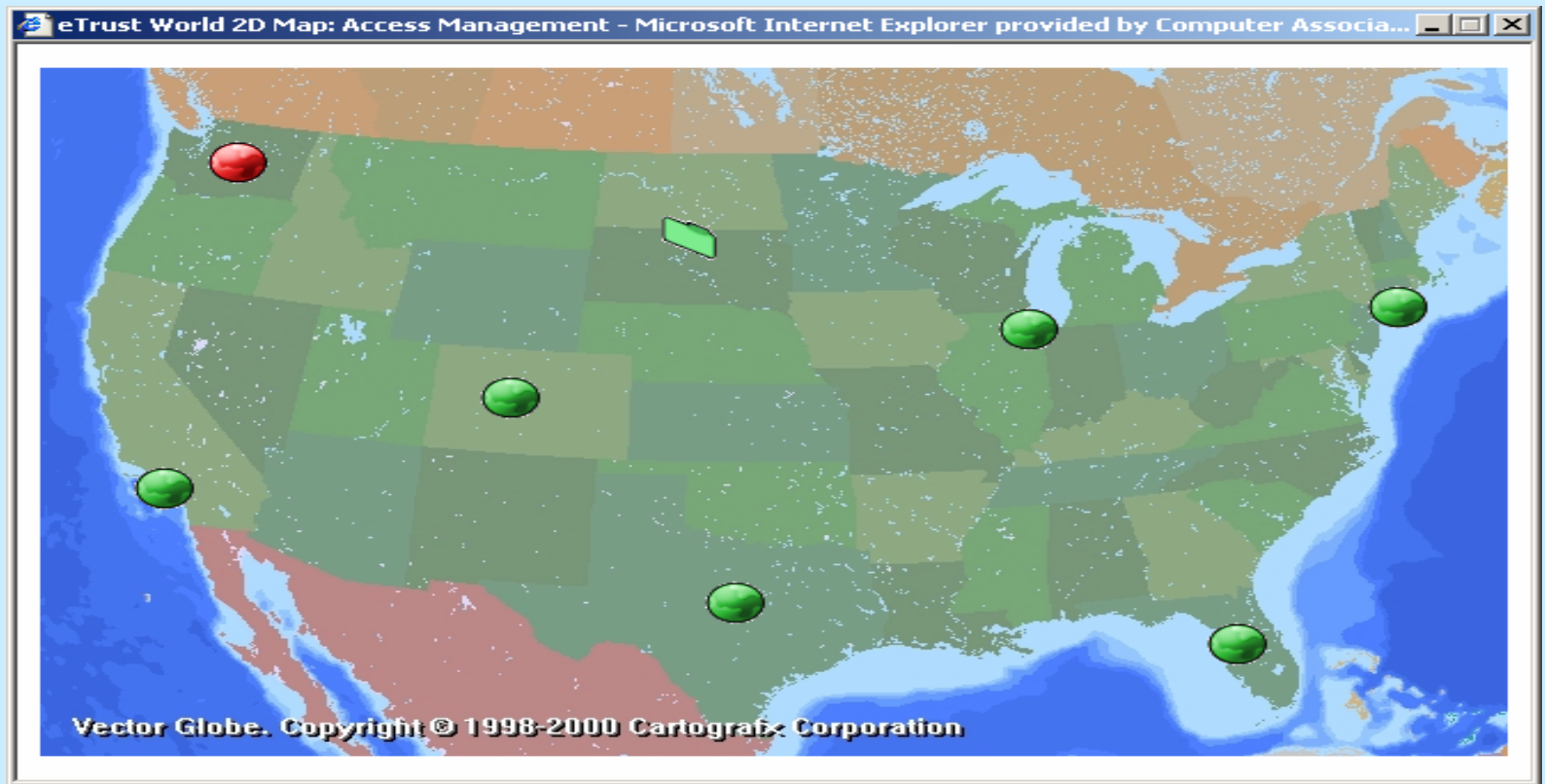
Security Condition 0:
Normal Status

Access Management Menu

- + Reporting and Analysis
- + Cisco Easy VPN Solution
- + Checkpoint Firewall
- + eTrust Audit
- + eTrust Antivirus



137 - netbios-ne
80 - http
1434 - ms-sql-m
53 - domain



Security Condition- Normal

Microsoft Internet Explorer
http://secvm003:8080/servlet/portal?resend=startup

eTrust Security Command Center by Computer Associates

My Profile | Log Out | Search

WORKPLACES KNOWLEDGE

Security Condition Process Management Intrusion Discovery **Security Condition** Databases

How | Manage | Configure | Reset | Help

Security Ticker

Security Condition 0 - Normal Status

Security Status

Security Status

A vertical gauge with a green needle pointing to the 'NORMAL' level. The levels from top to bottom are: DOWN (red), CRITICAL (red), MAJOR (orange), MINOR (yellow), WARNING (blue), UNKNOWN (blue), and NORMAL (green).

Advanced Correlation

Advanced Correlation

Correlated Events

A map showing a geographical area with green and brown patches, likely representing land and water.

eTrust Audit Log Viewer Using Profile: AEC (Node: secvm003)

Options Help

Message	Entry ID	Timestamp	Domain	User	Log Name	Source
OS	15002	05/29/2003 21:28:4	N/A	AEC	AEC	secvm003
OS	15042	05/29/2003 21:28:0	N/A	AEC	AEC	141.132.26.4
OS	15041	05/29/2003 21:28:0	N/A	AEC	AEC	141.132.26.4
OS	15040	05/29/2003 21:28:0	N/A	AEC	AEC	192.168.1.156
OS	15039	05/29/2003 21:28:0	N/A	AEC	AEC	192.168.1.231
OS	15038	05/29/2003 21:28:0	N/A	AEC	AEC	141.132.26.4
OS	15037	05/29/2003 21:28:0	N/A	AEC	AEC	141.132.26.4
OS	15036	05/29/2003 21:28:0	N/A	AEC	AEC	192.168.1.156
OS	15035	05/29/2003 21:28:0	N/A	AEC	AEC	192.168.1.231
OS	15034	05/29/2003 21:28:0	N/A	AEC	AEC	141.132.26.4
OS	15033	05/29/2003 21:28:0	N/A	AEC	AEC	141.132.26.4
OS	15032	05/29/2003 21:28:0	N/A	AEC	AEC	192.168.1.156
OS	15031	05/29/2003 21:28:0	N/A	AEC	AEC	192.168.1.231

Ready

Security Condition- Critical

Microsoft Internet Explorer - eTrust Security Command Center - Microsoft Internet Explorer

http://secvm003.6060/servlet/portal/?rescmd=startup

eTrust Security Command Center by Computer Associates

My Profile | Log Out

SEARCH

WORKPLACES KNOWLEDGE

Security Condition

Process Management | Intrusion Discovery | **Security Condition** | Databases

New | Manage | Configure | Reset | Help

Security Ticker

Advanced Correlation discovered simultaneous attacks from multiple systems


Security Ticker

Security

Security Status

Security Status

Security Status



A vertical gauge with a red needle pointing to the 'CRITICAL' level. The levels from top to bottom are: DOWN (red), CRITICAL (red), MAJOR (orange), MINOR (yellow), WARNING (blue), UNKNOWN (grey), and NORMAL (green).

Advanced Correlation

Advanced Correlation

Correlated Events

secvm003

eTrust Audit Log Viewer Using Profile: AEC (Node: secvm003)

Options: Help

Message	Entry ID	Timestamp	Domain	User	Log Name	Source
OS	15644	06/06/2003 12:23:3	N/A	AEC	541.132.26.4	
OS	15643	06/06/2003 12:23:3	N/A	AEC	541.132.26.4	
OS	15642	06/06/2003 12:23:3	N/A	AEC	192.168.1.156	
OS	15641	06/06/2003 12:23:3	N/A	AEC	192.168.1.231	
OS	15640	06/06/2003 12:23:3	N/A	AEC	541.132.26.4	
OS	15639	06/06/2003 12:23:3	N/A	AEC	541.132.26.4	
OS	15613	06/06/2003 12:23:3	N/A	AEC	192.168.1.156	
OS	15612	06/06/2003 12:23:3	N/A	AEC	192.168.1.231	
OS	15611	06/06/2003 12:23:2	N/A	AEC	541.132.26.4	
OS	15610	06/06/2003 12:23:2	N/A	AEC	541.132.26.4	
OS	15609	06/06/2003 12:23:2	N/A	AEC	192.168.1.156	
OS	15608	06/06/2003 12:23:2	N/A	AEC	192.168.1.231	
OS	15607	06/06/2003 12:23:2	N/A	AEC	541.132.26.4	

Ready



MORE SECURITY DOESN'T MAKE YOU MORE SECURE. BETTER MANAGEMENT DOES.

The secret to a secure enterprise lies in not just monitoring the parts, but managing it as a whole. That's exactly what eTrust™ lets you do. In fact, our eTrust™ Security Command Center is the perfect solution to security information overload. It gives you the big picture from a single vantage point, with all your event information prioritized. So you can identify actual internal and external threats before they can wreak havoc. Anything less would be, well, alarming. For more information on security management, go to ca.com/etrust/management.

eTrust™

ACCESS • THREAT • IDENTITY
SECURITY MANAGEMENT SOFTWARE



Computer Associates®

Bibliografia

1. Sridhar, Juvvadi. "Requirements For Managing Security Information Overload". 20 June 2003.

<http://www.sans.org/rr/papers/index.php?id=1147>

2. Boettger, Larry. "The Morris Worm: how it Affected Computer Security and Lessons Learned by it". 24 December 2000.

http://www.giac.org/practical/gsec/Larry_Boettger_GSEC.pdf