

Sicurezza fisica e logica: due culture che si incontrano. Un approccio alla sicurezza

Infosecurity

Una definizione di protezione aziendale



Lo studio e l'attuazione delle strategie, delle politiche e dei piani operativi volti, nell'ottica di creazione di valore dell'impresa, a prevenire, a fronteggiare ed a superare eventi non competitivi che possono colpire le risorse materiali, immateriali ed umane di cui l'azienda dispone o di cui necessita per garantirsi una adeguata capacità concorrenziale nel breve, nel medio e nel lungo termine.

(A. Gilardoni- Norma UNI)

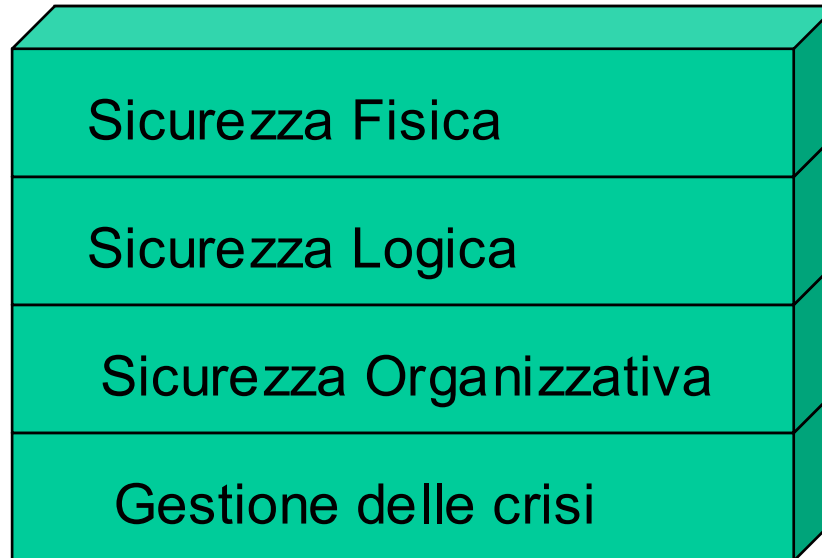


Mission della security aziendale

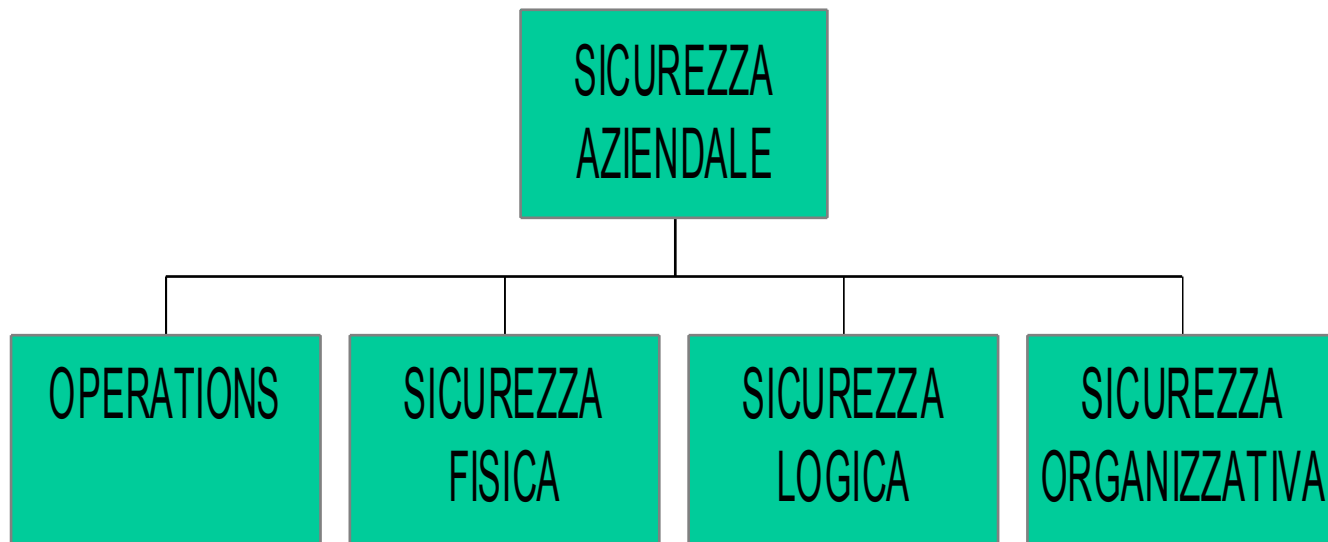
Tutelare tutte le risorse dell'azienda dagli illeciti di provenienza interna o esterna all'organizzazione con particolare attenzione agli assets:

- Critici per il perseguimento di un vantaggio competitivo
- Indispensabili per assicurare la continuità operativa oltre che reddituale dell'organizzazione
- Indispensabili per la sopravvivenza di lungo periodo

Sistema integrato di sicurezza



Sicurezza Aziendale Vodafone Omnitel





Esempi di approccio integrato alla sicurezza logica-fisica

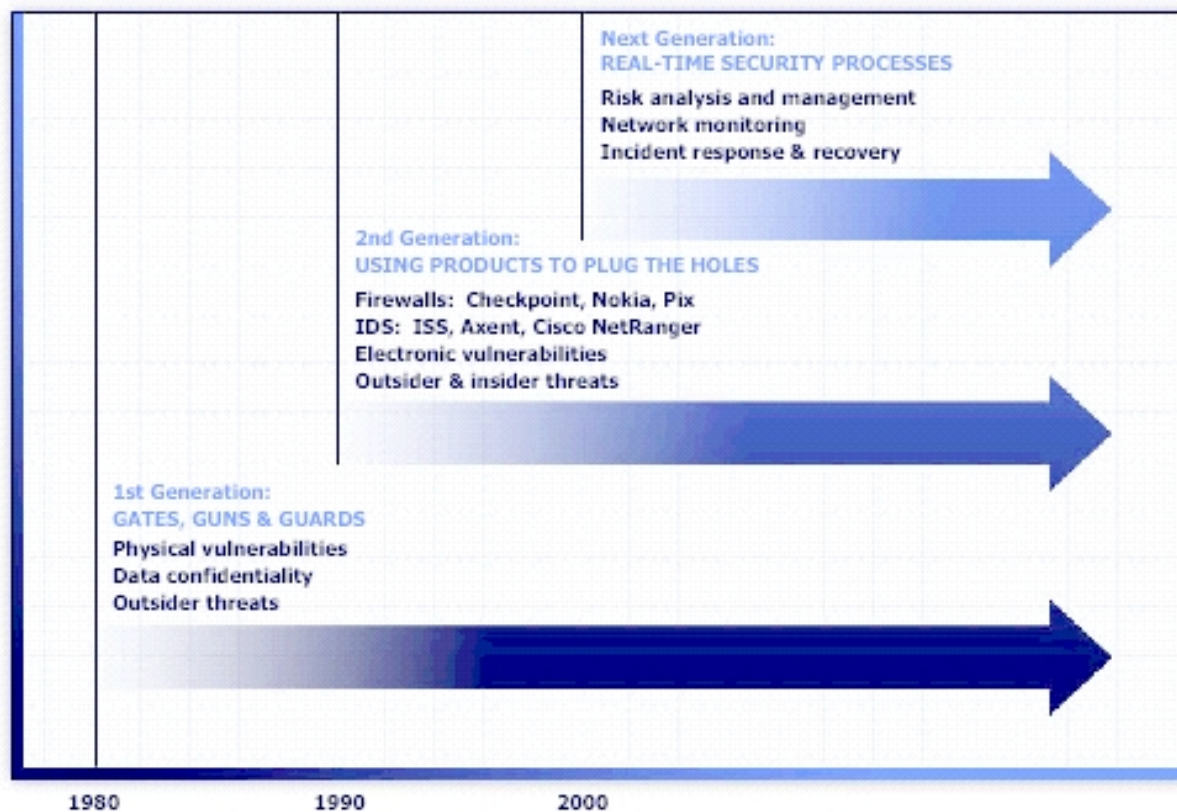
Luigi Piutti-Corradino Corradi



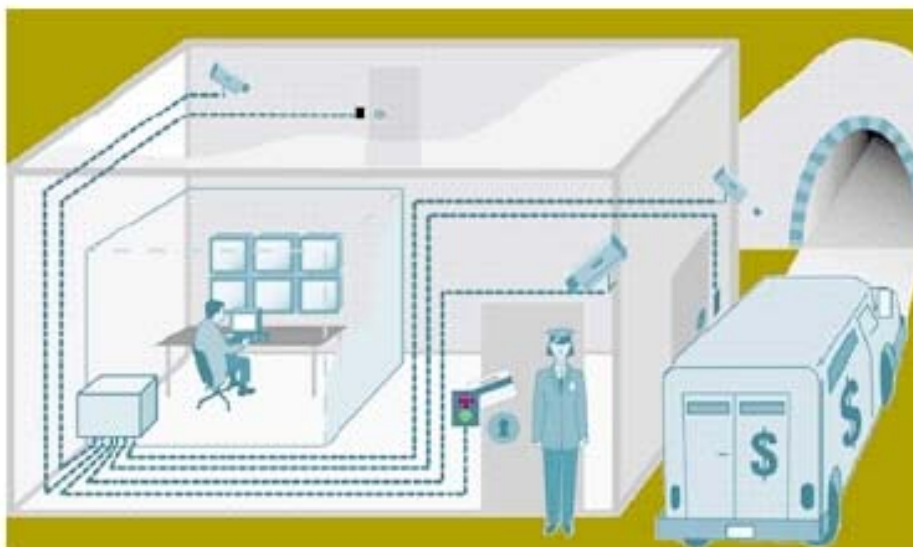
Agenda

- L'evoluzione del concetto di sicurezza
- Sicurezza perimetrale
- Sicurezza dei sistemi
- Sicurezza nello scambio sicuro di dati con terze parti
- Sicurezza delle informazioni
- Scoperta delle intrusioni
- Monitoring e sorveglianza
- L'anello piu' debole: il fattore umano

L'evoluzione del concetto di sicurezza (1)



L'evoluzione del concetto di sicurezza (2)



Like a building, a network requires multiple layers of protection to be truly secure.



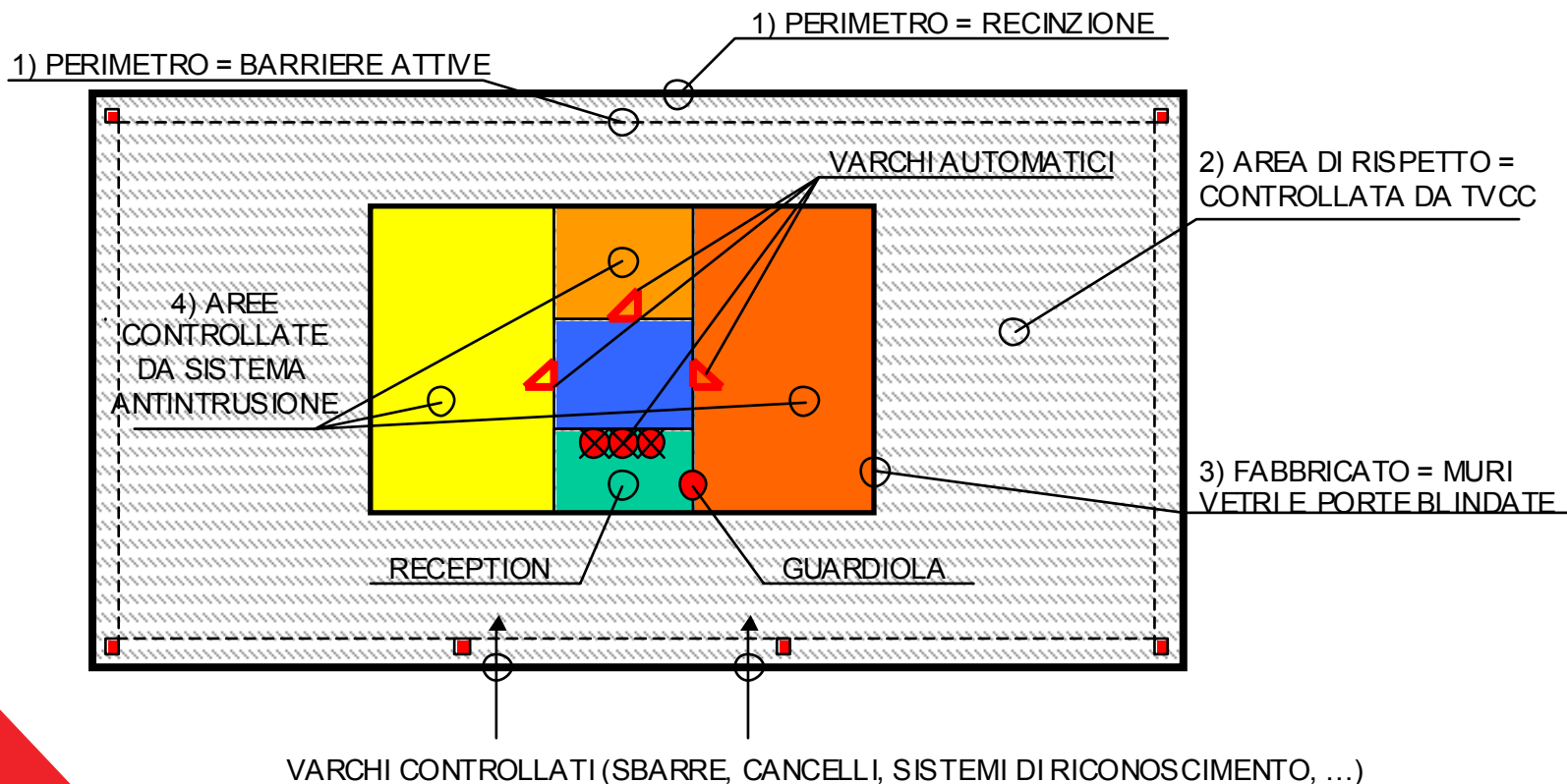
Sicurezza perimetrale: dalla mura del castello ai firewall ed IDS



Access Control Lists and Firewalls are analogous to door locks on building perimeters that allow only authorized users (those with keys or badges) access in or out.

- Esempio di topologia di un sito tecnico
- Esempio di topologia di rete

Sicurezza perimetrale: topologia di sito tecnico



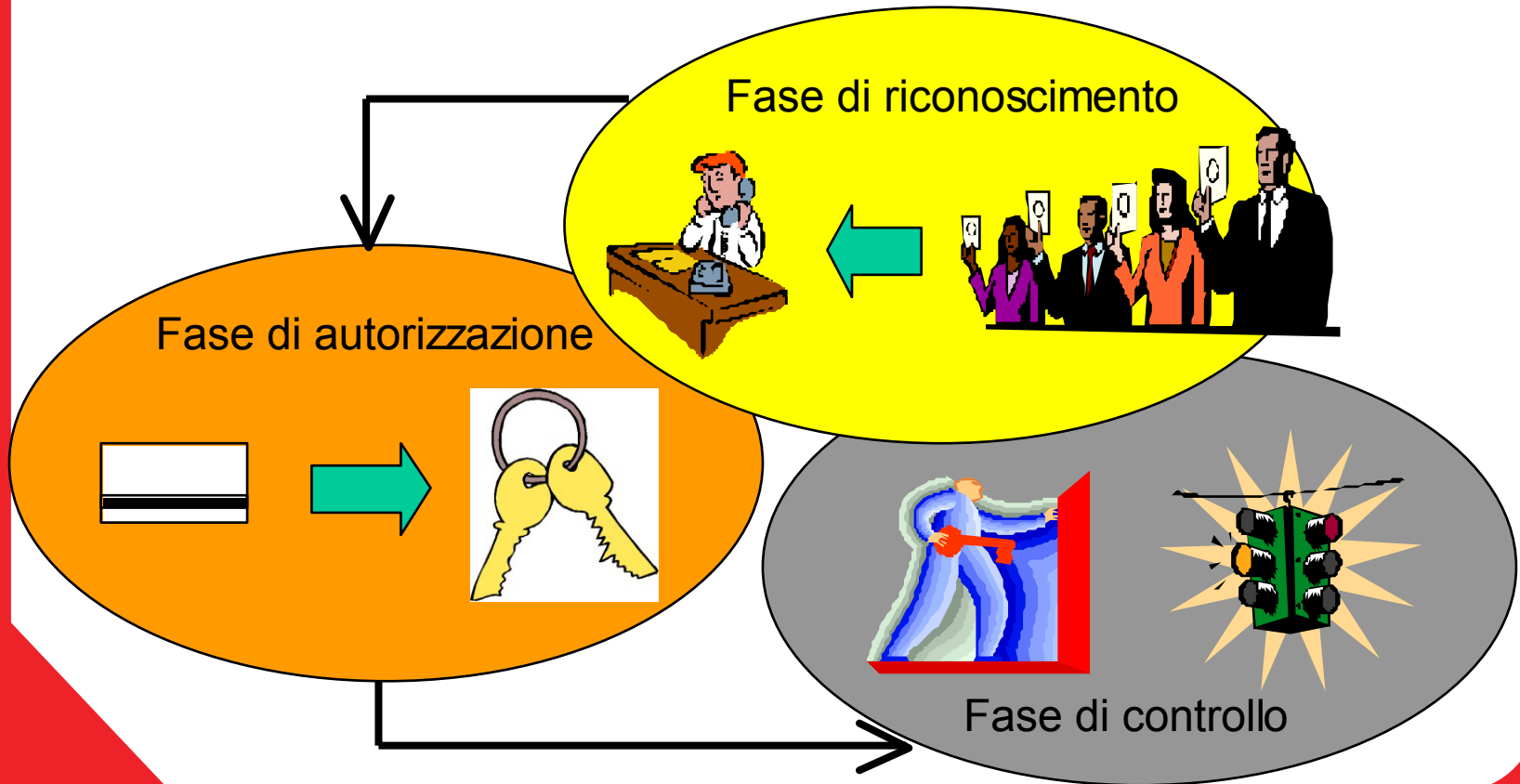
Sicurezza dei sistemi: dalla parola d'ordine ai sistemi informatici di controllo accessi



Access Control Servers function like door access cards and the gatekeeper that oversees site security, providing centralized authorization, authentication and accounting (AAA) for traffic and users

- Esempio di identificazione degli utenti su reception, uffici e locali tecnici
- Controlli logici sui sistemi di Call Center (progetto di identity management)

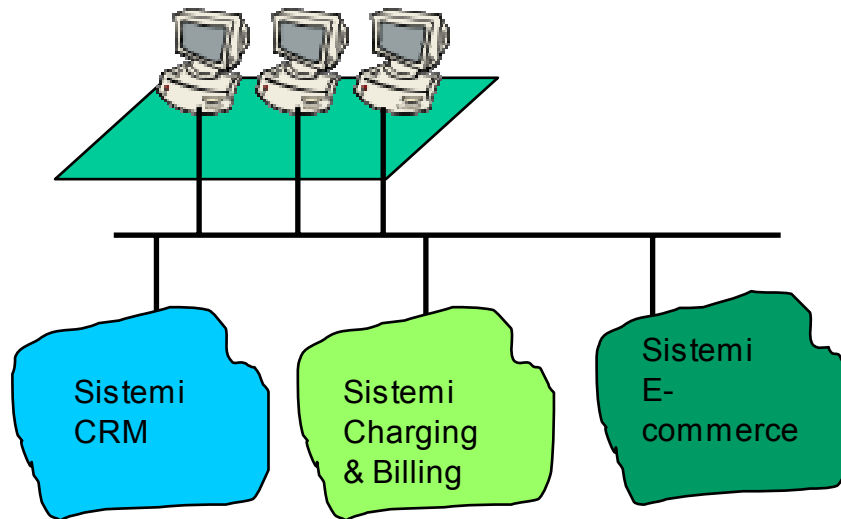
Sicurezza dei sistemi: identificazione degli utenti su reception, uffici e locali tecnici



Sicurezza dei sistemi: controlli logici sui sistemi di Call Center

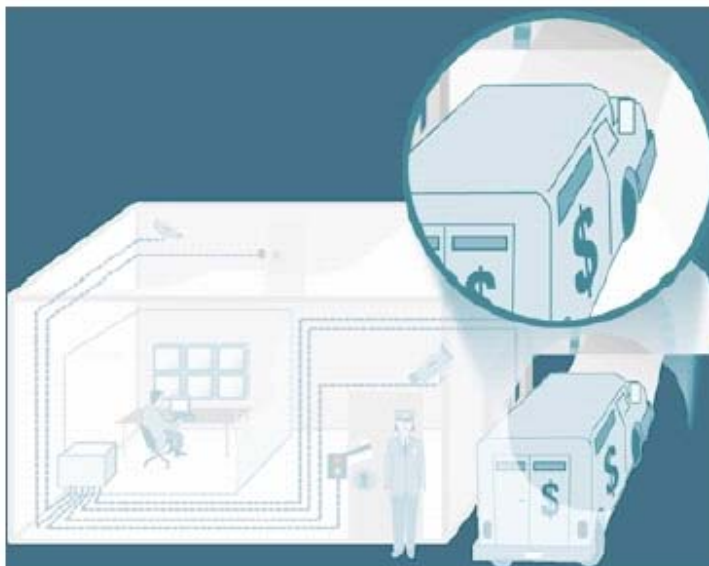


Postazioni del call center



- Sviluppo dei sei agenti Control-SA per la gestione centralizzata dei sei applicativi del Call Center
- Gestione dei Profili Utente
- Operazioni di massa
- Tracciabilità delle operazioni amministrative

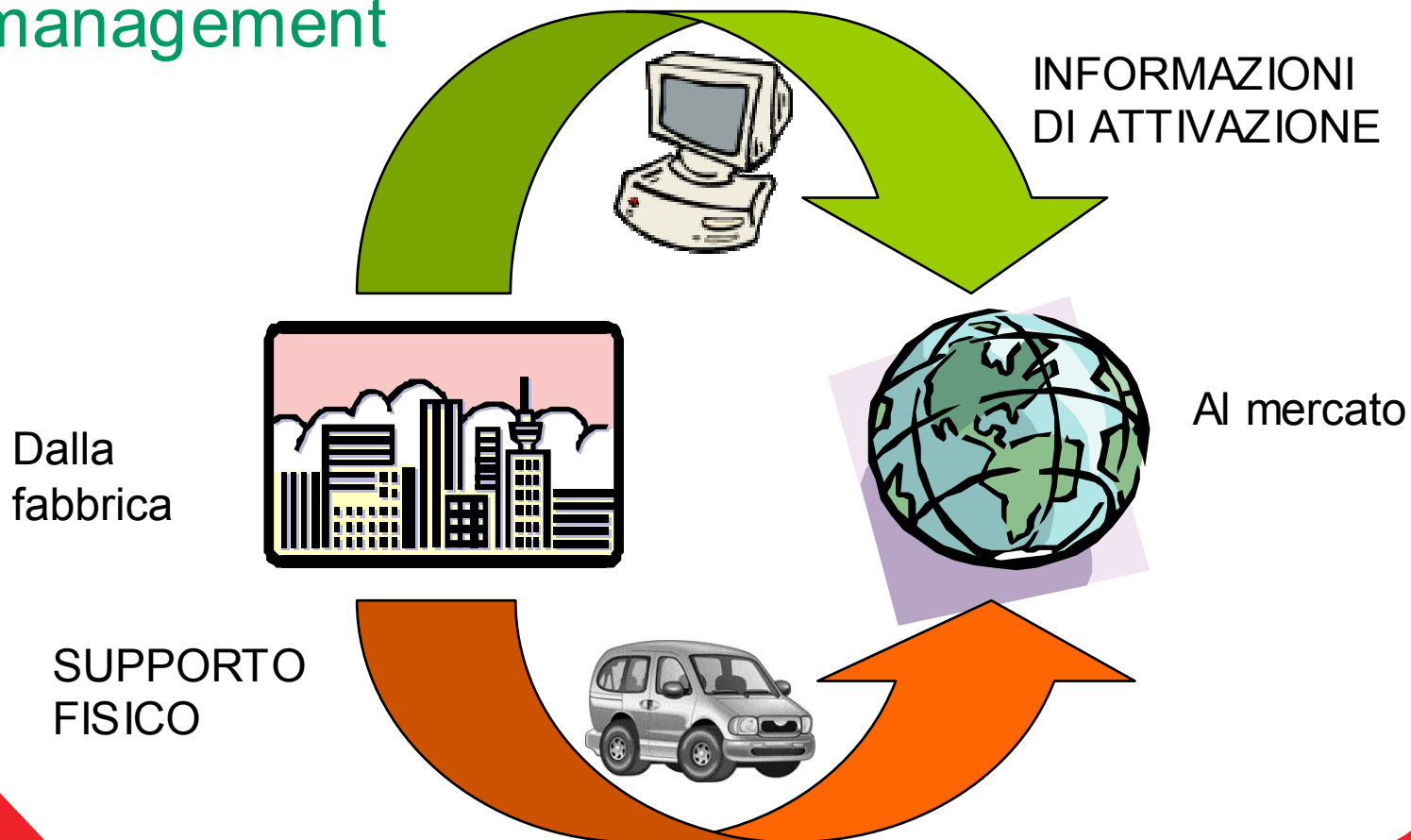
Sicurezza nello scambio sicuro di dati con terze parti : dal portavalori alle VPN



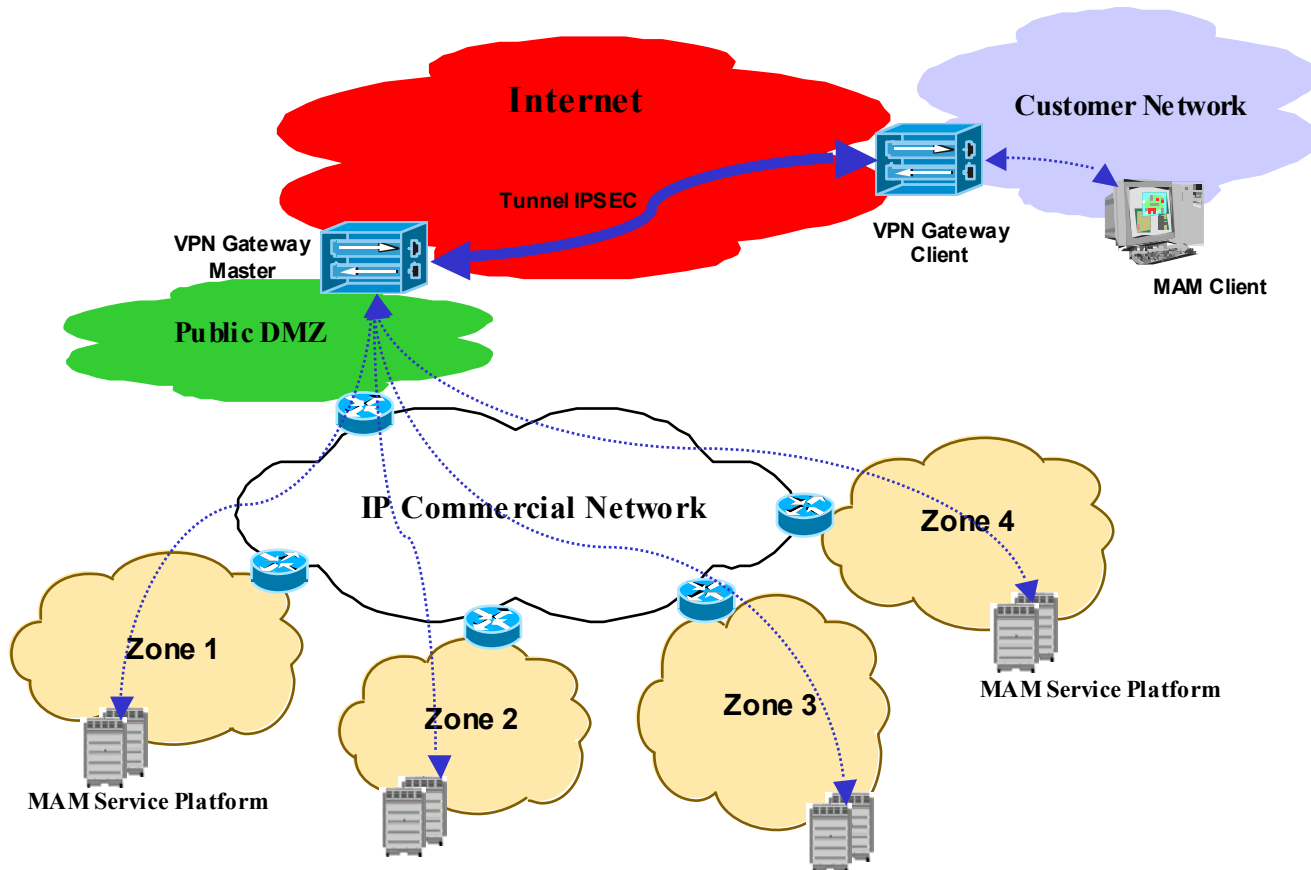
Virtual Private Networks (VPNs) are analogous to armored cars that carry precious cargo to an assigned drop-off point to ensure secure and confidential passage.

- Esempio di processo di SIM management (dal fornitore al negozio Omnion)
- Esempio di VPN con altre Vodafone OpCo

Sicurezza nello scambio sicuro di dati con terze parti : processo di SIM management



Sicurezza nello scambio sicuro di dati con terze parti : VPN MAM



Scoperta delle intrusioni: dalle telecamere agli IDS



Intrusion Detection is analogous to a surveillance camera and motion sensor detecting activity, triggering alerts, and generating an armed response. Scanning is like a security guard that checks and closes open doors or windows before they can be breached.

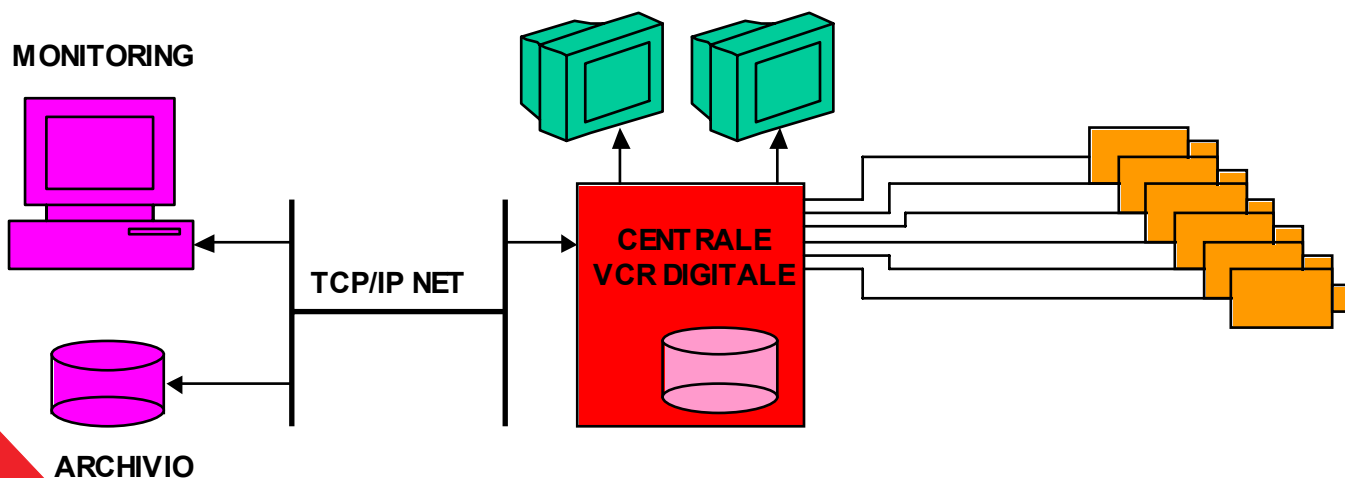
- Esempio di gestione delle telecamere nei locali tecnici
- Esempio di topologia di rete con NIDS

Scoperta delle intrusioni: gestione delle telecamere nei locali tecnici

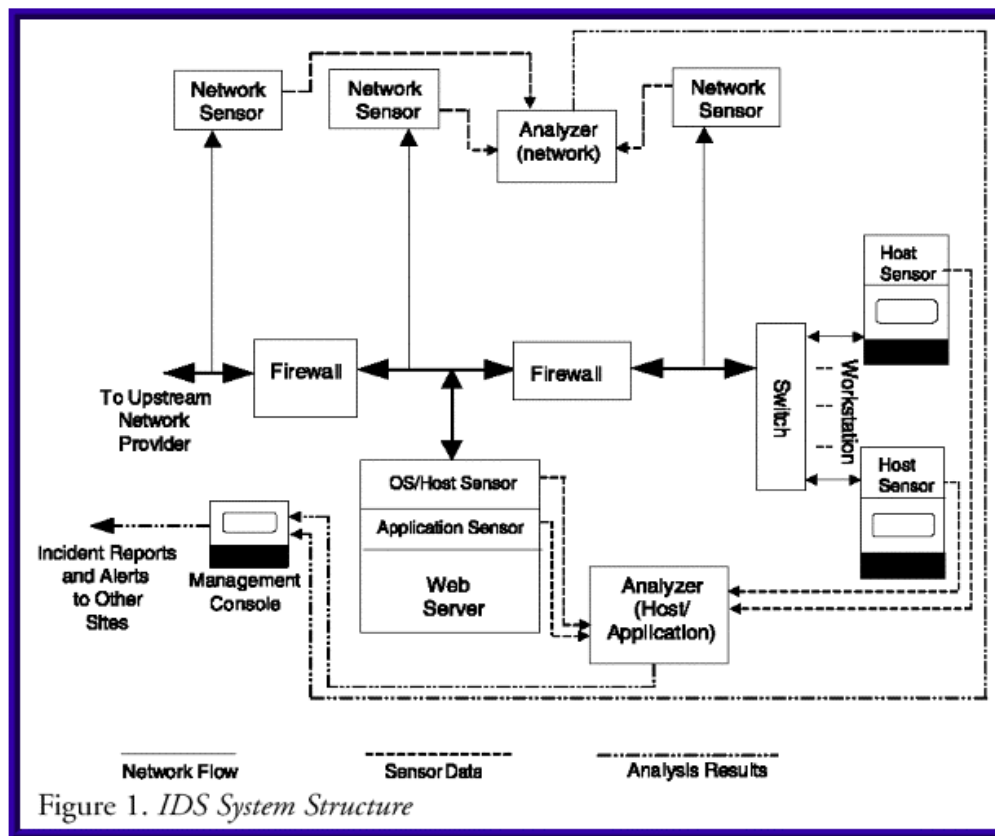


- DETERRENZA
- SUPPORTO VIGILANZA
- CONTROLLO SPECIFICO
- AIUTO ALL'INDAGINE

- SISTEMI MATRICIALI
- CENTRALE-VCR DIGITALE
- CONNESSIONE IN RETE
- CENTRALIZZAZIONE



Monitoring e sorveglianza: topologia di rete con NIDS



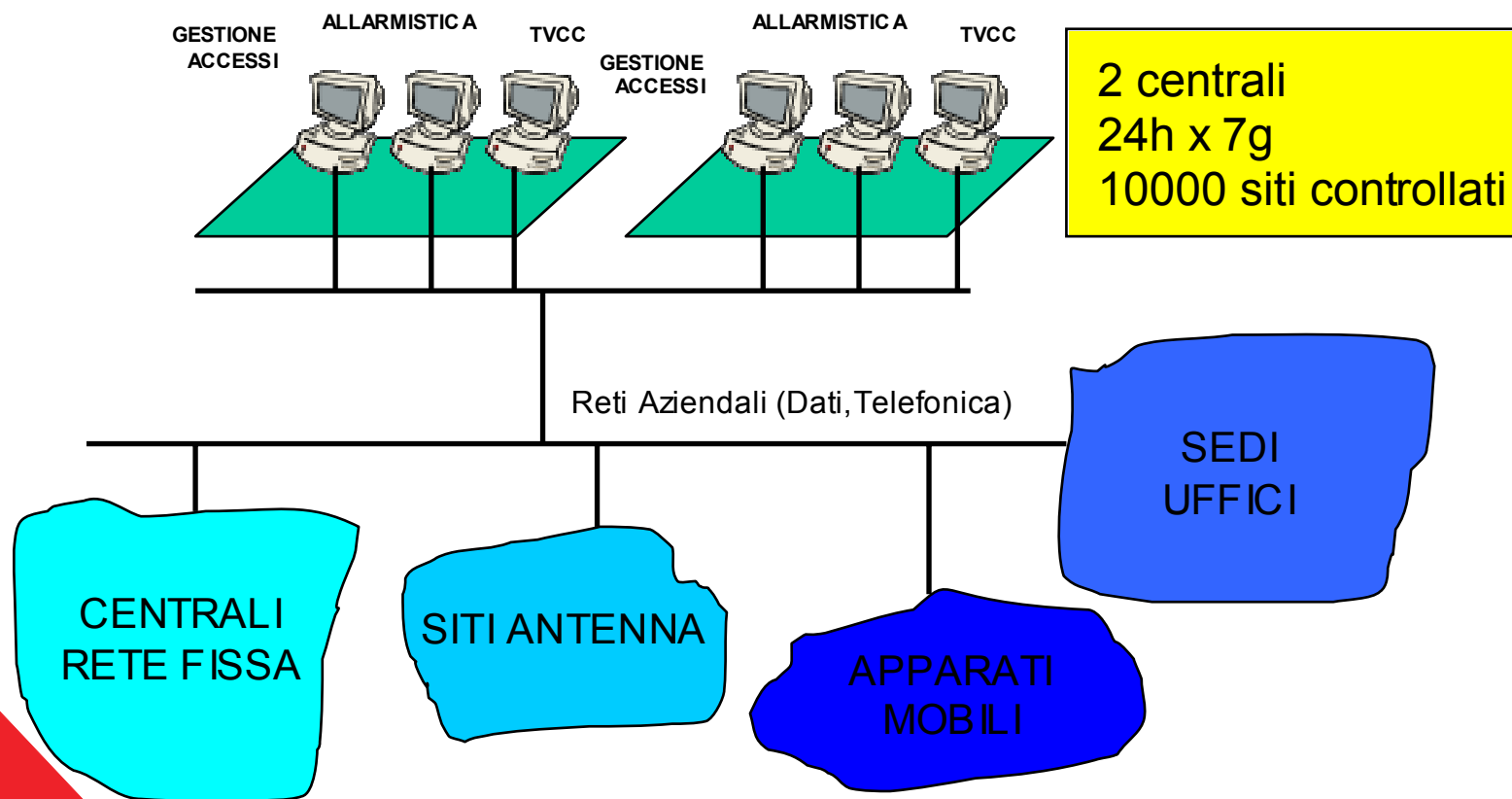
Monitoring e sorveglianza: l'evoluzione dei sistemi di gestione degli allarmi



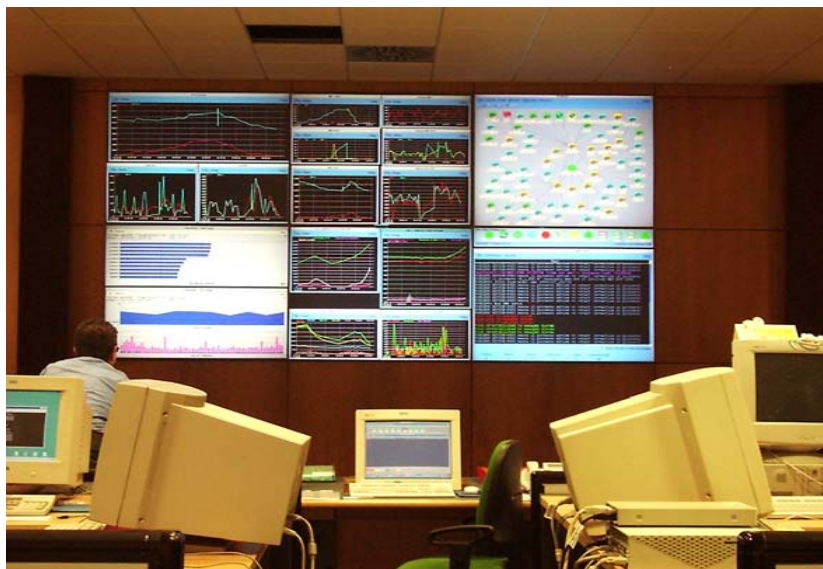
Security Policy, Device, and Multidevice Management functions as a central security control room where security personnel monitor building or campus security, initiate patrols, and activate alarms.

- Esempio di gestione degli eventi di sicurezza fisica
- Esempio di gestione degli eventi di sicurezza logica

Monitoring e sorveglianza: gestione degli eventi di sicurezza fisica



Monitoring e sorveglianza: gestione degli eventi di sicurezza logica



Monitoring Team:

12 operators, 4 supervisors

24 h x 365 days preside on site

Monitoring Area:

150 square meters

23 working positions

6 Electrohome wall screens

10 Unix & NT servers

50 Services controlled

- 137 Unix nodes
- 109 NT Nodes
- 800 network nodes
- 297 monitoring agents
 - 10.000 Fault check points
 - 30.000 Event messages received per day

•Management Systems

- HP Open view
- BMC Patrol
- Business Object
- Web Trends

The weakest link: il fattore umano



- Altri elementi fondamentali per la riuscita dei progetti di sicurezza logica-fisica sono:
 - la formazione sulla sicurezza per gli utenti finali
 - la formazione tecnica di sistemisti e personale tecnico
 - la gestione accorta dei contratti per il maintenance di hardware e software
 - L'inserimento di requisiti di sicurezza sugli user requirement di tutti i nuovi prodotti e servizi
 - La formalizzazione di un processo di incident handling
 - La gestione controllata dei processi di outsourcing

