

# AIM

advanced infrastructure monitor

**The proactive solution**

# Chi siamo?

Fiorenzo Ottorini  
CEO – Attua s.r.l.

Paolo Marani  
CTO – Attua s.r.l.

Alessio Pennasilico  
CSO – Alba s.a.s.

# Tecres

Tecres utilizza AIM fin dalla prima versione per tenere sotto controllo ogni aspetto della sicurezza, della disponibilita' e delle performance della propria rete, al fine di prevenire i problemi e gestire rapidamente le anomalie.

# Finalita'

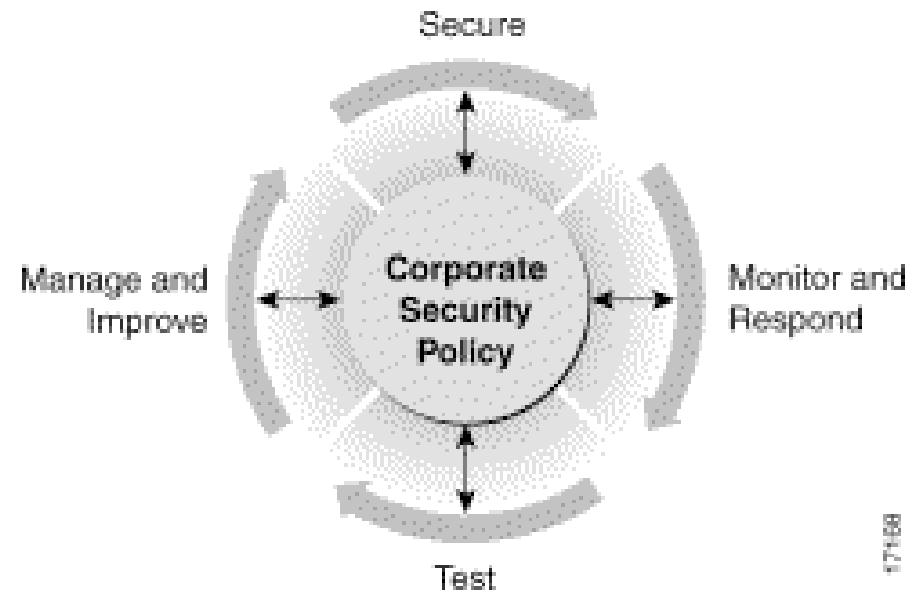
Lo scopo di questa presentazione e' mostrarvi le caratteristiche di un prodotto innovativo, frutto di anni di esperienza a diretto contatto con le esigenze e le problematiche dei nostri clienti.

# Sommario

- Security wheel
  - Secure
  - Monitor
  - Audit
  - Manage & Improve
- AIM
  - Monitoring
  - IDS
  - Logging
  - Performance
  - DPS
  - Alerting

# Security Wheel

- Secure
- Monitor
- Audit
- Manage & Improve



17168

# Secure

Sulla base della struttura esistente vengono proposte ed implementate soluzioni atte a migliorare la sicurezza globale dell'infrastruttura informatica aziendale.

# Monitor

La rete ed i suoi servizi devono essere costantemente monitorati in real-time e con storicizzazione dei dati analizzati.

E' quindi necessario implementare ed integrare strumenti di monitor passivi (es. logging centralizzato), attivi (SNMP ed IDS), proattivi.

# Disponibilita'

Non soltanto la prevenzioni delle intrusioni, ma anche evitare i fermi macchina/servizio a causa di esaurimento delle risorse o l'utilizzo non ottimale a causa di scarse performance rientra tra gli obiettivi del monitoring.

# Audit

Vulnerability Scan e Penetration Test sono gli strumenti da utilizzare per verificare che tutto ciò che è stato implementato sia davvero sicuro.

# Manage & Improve

Sulla base dei risultati di monitoring ed audit vengono elaborate le strategie con cui migliorare ulteriormente la qualita' dei servizi offerti.

# Perche' Security Wheel?

Le aziende, le loro esigenze ed i loro strumenti, non sono statici. Nuove vulnerabilita' vengono scoperte ogni giorno, mentre la sicurezza dell'infrastruttura non deve mai diminuire. Inoltre un crescente utilizzo dei sistemi potrebbe degradare le performance globali delle applicazioni.

- Conoscere
- Capire
- Decidere

# Ambito

- Network monitoring
- System monitoring
- Application monitoring
- Security monitoring
- Performance monitoring
- Event Reporting

# Monitoraggio e controllo

AIM permette di conoscere le informazioni, per capire qual'è l'attuale situazione e gestire preventivamente, o a fronte di anomalie, ogni esigenza che si presenti.

# Strumenti controllo preventivo

# Strumenti per il trouble shooting

# Confronto

Altri prodotti hanno parte delle  
funzionalità'

# A chi e' rivolto AIM?

AIM non e' l'ennesimo tool pieno di informazioni che richiedono competenze specialistiche per essere interpretate.

# Cos'è AIM?

AIM è un cruscotto pensato per l'operatore che voglia avere velocemente un'immagine precisa della situazione, per decidere quali risorse utilizzare per prevenire o risolvere le anomalie.

# AIM

Advanced Infrastructure Monitor (AIM)  
e' una suite da noi sviluppata,  
integrando diversi strumenti  
OpenSource al fine di monitorare i  
parametri vitali dell'intera  
infrastruttura aziendale.

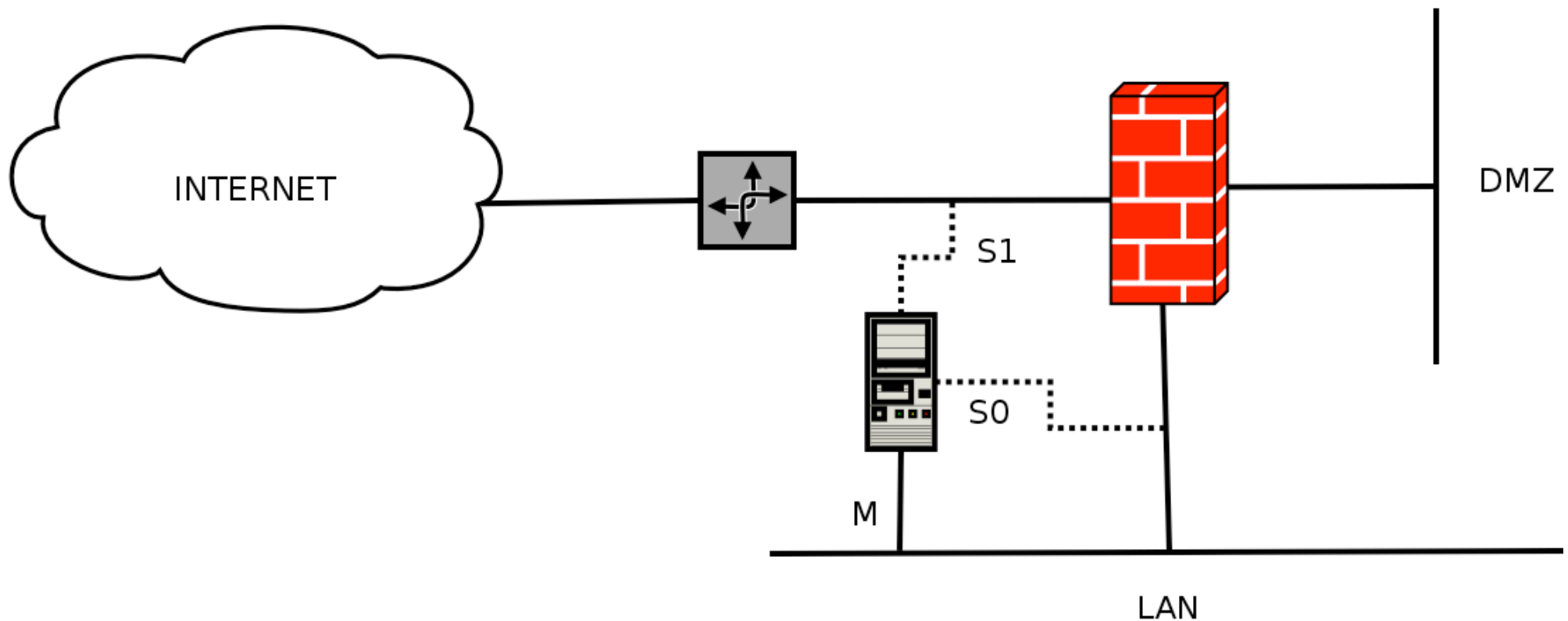
# Performance

AIM e' interamente consultabile via WEB e puo' monitorare, ad esempio, l'utilizzo CPU, l'occupazione dischi ed il traffico di rete di diversi dispositivi (server Windows, Linux, IBM iSeries, router, firewall, etc etc).

# IDS

AIM comprende anche un potente IDS, integrato con un database relazionale, i cui log e statistiche possono essere consultati via WEB. Ad ogni evento puo' essere associata una azione.

# Diagramma di rete



# Logging Centralizzato

La macchina su cui gira AIM e' configurata come repository dei log di tutti gli apparati della rete aziendale.

Un altro modulo e' in grado di analizzare i log ricevuti e scatenare delle azioni (es. spedire mail o sms).

# Help Desk

E' possibile creare delle pagine personalizzate dedicate agli operatori di help desk per il trouble-shooting dei problemi piu' comuni.

# Esempio

Vediamo una dimostrazione pratica

# Referenze

Rossetto – wan/wifi (slide)  
melegatti – gestione rete  
tecres -  
arag – sicurezza (slide)  
fro - wan

(v1-v3)

# Offerta Commerciale Standard

- AIM Standard Version
  - Server IBM Tower (dischi scsi mirroring, garanzia IBM 3 anni on site)
  - Servizi di installazione HW e software di base, database, webserver
  - Configurazione ed attivazione della soluzione AIM
  - Configurazione servizi sugli host da monitorare
  - Misure minime DPS
  - Gestione LOG e Monitor performance di: 2 server, 1 router, 1 firewall
  - Monitor disponibilita'servizi base (posta, telnet, web)
  - IDS e statistiche traffico
- 5900 euro

# Funzionalità incluse

- Situazione
  - Sistemi (2 server, 1 firewall, 1 router)
  - Reti (1 sede remota)
  - Servizi (4 servizi relativi ai sistemi monitorati)
  - Sicurezza – Misure minime DPS
    - Manutenzione firewall
    - Patch Software
    - Aggiornamento Password
    - Aggiornamento Antivirus (agg. prodotto)

# Funzionalità Incluse

- Dettaglio stato sistemi
  - Dettaglio stato servizi
  - Dettaglio servizi down
- Performance e statistiche
  - Sessioni TCP attive
  - Utilizzo banda per sistemi
  - Volume traffico per protocollo
- Intrusion Detection System
  - Anomalie rilevate- Categorie
  - Anomalie rilevate - Tipo

# Moduli Avanzati

- Gestione log IBM iSeries
- Alerting via SMS
- Monitor servizi Domino
- Monitor aggiornamento definizioni virus
- Monitor servizi Avanzati
- Ulteriori sistemi
- Ulteriori reti geografiche

# Personalizzazioni

## Gestione Help Desk

Possibilita' di monitor di tutti i parametri di tutti gli apparati pubblicati via SNMP tramite le librerie del produttore

# Conclusioni

Sicurezza non e' un prodotto  
che si compra.

E' il risultato di un continuo e  
costante processo.

Oggi e' impensabile,  
visti i rischi e le vigenti leggi,  
non occuparsene.

**Grazie della partecipazione.**

**Siamo a vostra  
disposizione per  
qualsiasi chiarimento o  
precisazione.**