



PIERO FIOZZO

Servizi di Sicurezza Gestita

Affrontare le nuove sfide riducendo
contemporaneamente i costi
operativi

Security Day 2010



PLEASE ROB ME



Listing all those empty homes out there

Check out the same results on [Twitter search](#).

Recent Empty Homes

47 new opportunities



@Hmtigert left home and checked in 2 minutes ago.
I'm at Tigert Communications (2015 Dogwood Pl, Nashville) <http://4sq.com/9sAgff>



@WilliamRyanRE left home and checked in 2 minutes ago
I'm at William Ryan Homes (175 N Patrick Blvd, Brookfield) <http://4sq.com/a6q19f>



@ankitg left home and checked in 3 minutes ago:
[@blue_quartz](#) that's not exactly invasion of privacy ... those people chose to sign up for 4sq and enable the twitter option. Nice idea thou.



@mnauj left home and checked in 3 minutes ago
I'm at Ultra Mannos (260 3rd St., Hoboken) <http://4sq.com/dcLbJ5>



@bvargas left home and checked in 3 minutes ago
Quick pit stop (@ The Coffee Scene) <http://4sq.com/9GB1PO>



@bro_appleby left home and checked in 3 minutes ago
I'm at Minnie Pearl Building (2806 Opryland Dr, Nashville) <http://4sq.com/9L23C5>



@Iskandar_ahmat left home and checked in 3 minutes ago:
quick drink @ Cosmo Lounge (@ Kuala Lumpur Hilton) <http://4sq.com/6uETTx>



Spesso la necessità delle Aziende è quella di realizzare riduzioni di costo a breve termine gestendo contemporaneamente i cambi strutturali

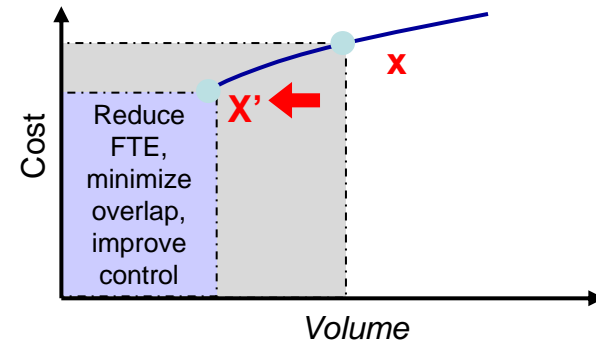
- **Riduzione dei costi a breve termine**

- Blocco delle assunzioni
- Blocco del budget su nuovi progetti
- Cessazione di accordi con subcontractor
- Piani di incentivazione al outplacement
- Prepensionamenti

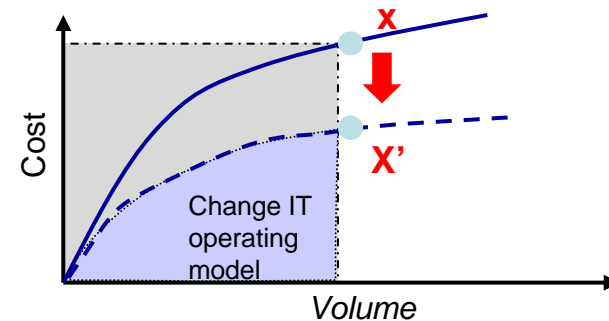
- **Riduzione dei costi di struttura**

- Trasferimento di risorse/applicazioni
- Centralizzazione della governance IT
- Ridefinizione di strategie e priorità
- Sourcing transformation
- Ottimizzazione dei processi

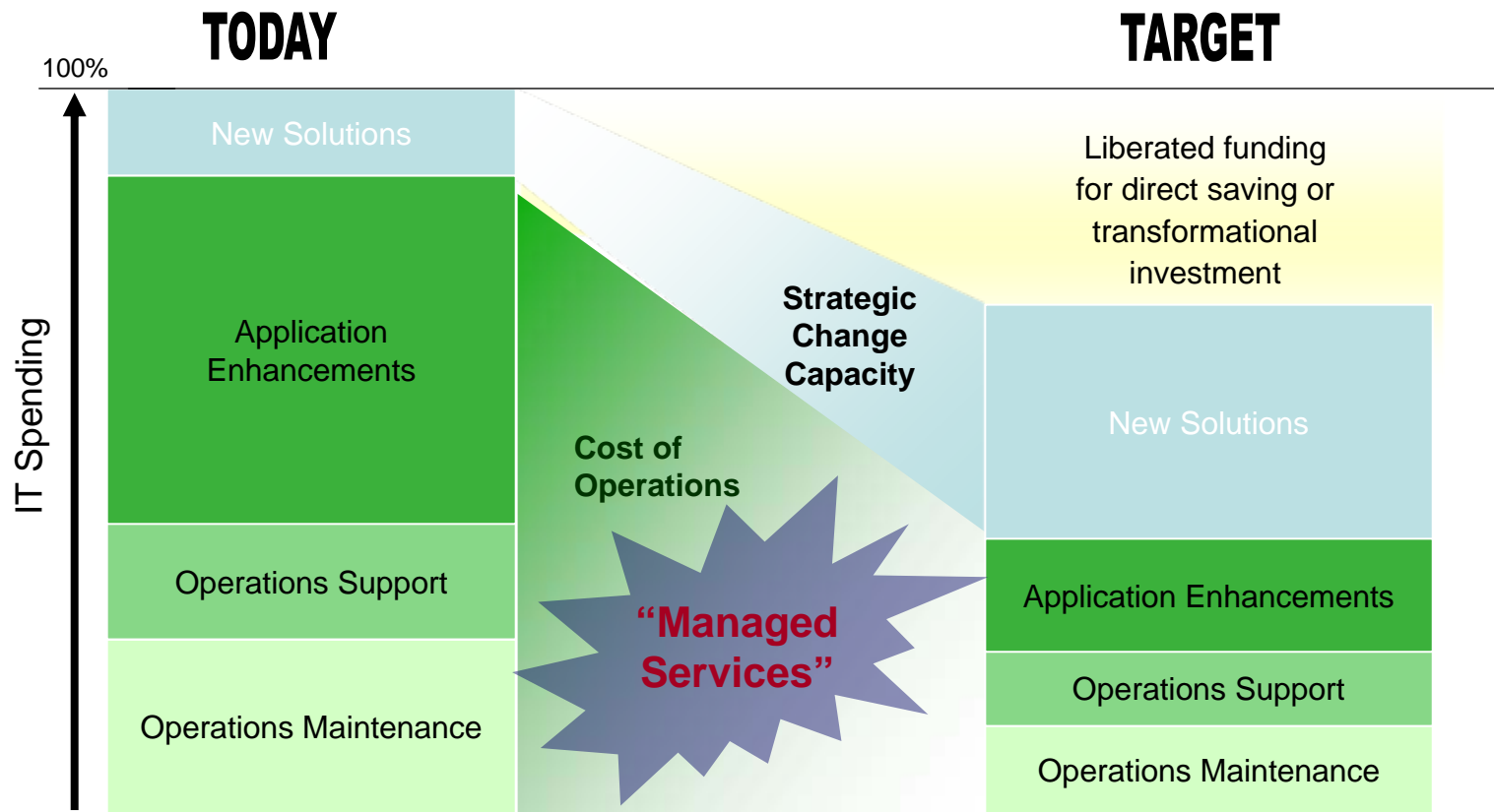
Type 1 Rationalization "Reduce Capacity"



Type 2 Structural Change "Transform Fixed into Variable Costs"



IBM può aiutare i propri Clienti ad aumentare l'efficienza operativa e la capacità di gestione IT che si traduce in risparmio e possibile aumento degli investimenti in nuove tecnologie



Per fornire servizi ai propri Clienti IBM investe in:

- competenze
- tecnologie
- talenti
- infrastrutture
- ricerca

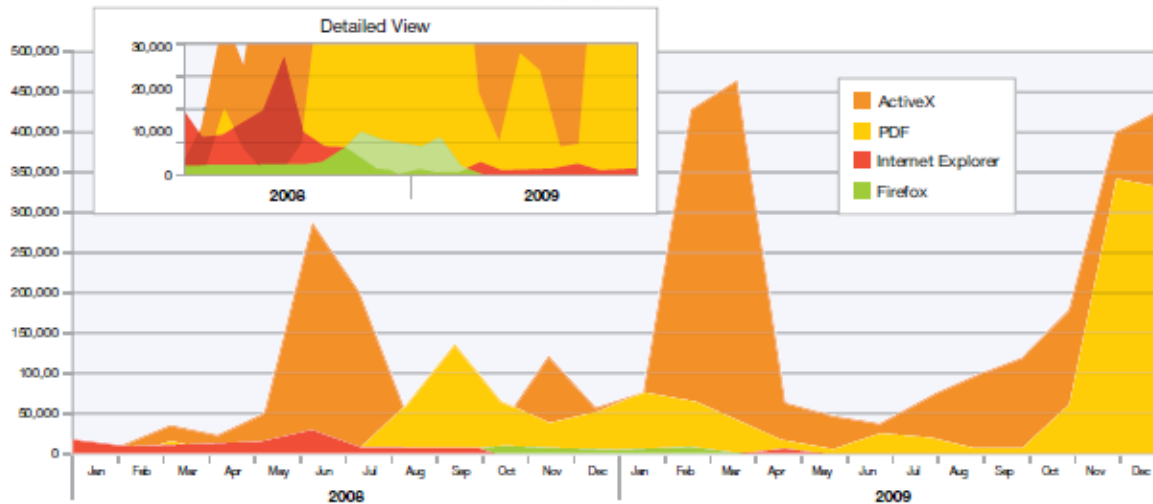


9 Security Operation Center
costituiscono l'infrastruttura del singolo
Global Security Operation Center

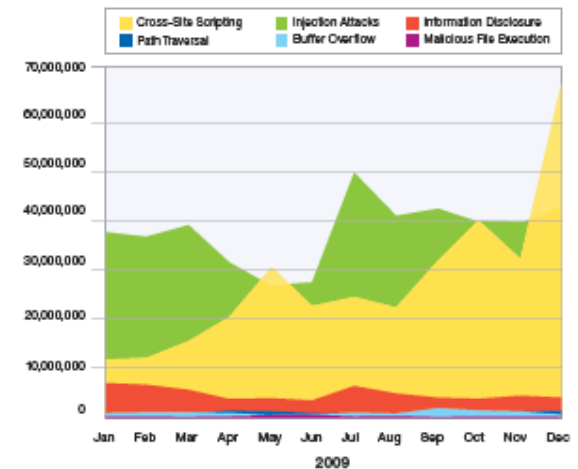
L'esperienza maturata dai nostri specialisti MSS si traduce in valore per:

- la nostra ricerca
- per i nostri Clienti

Browser and PDF Exploitation
Source: IBM Managed Security Services
2008-2009

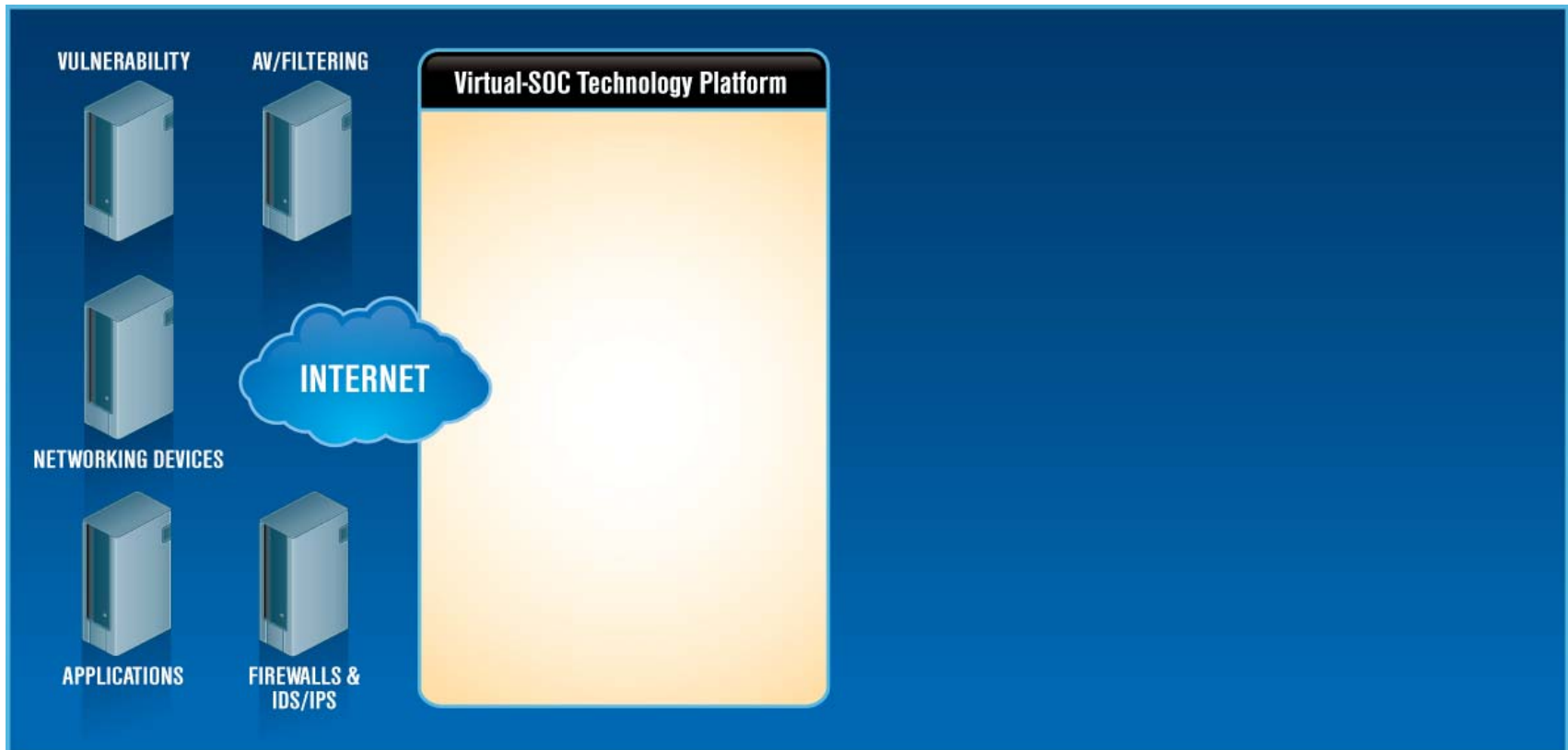


Web Application Attacks by Category
IBM Managed Security Service
2009



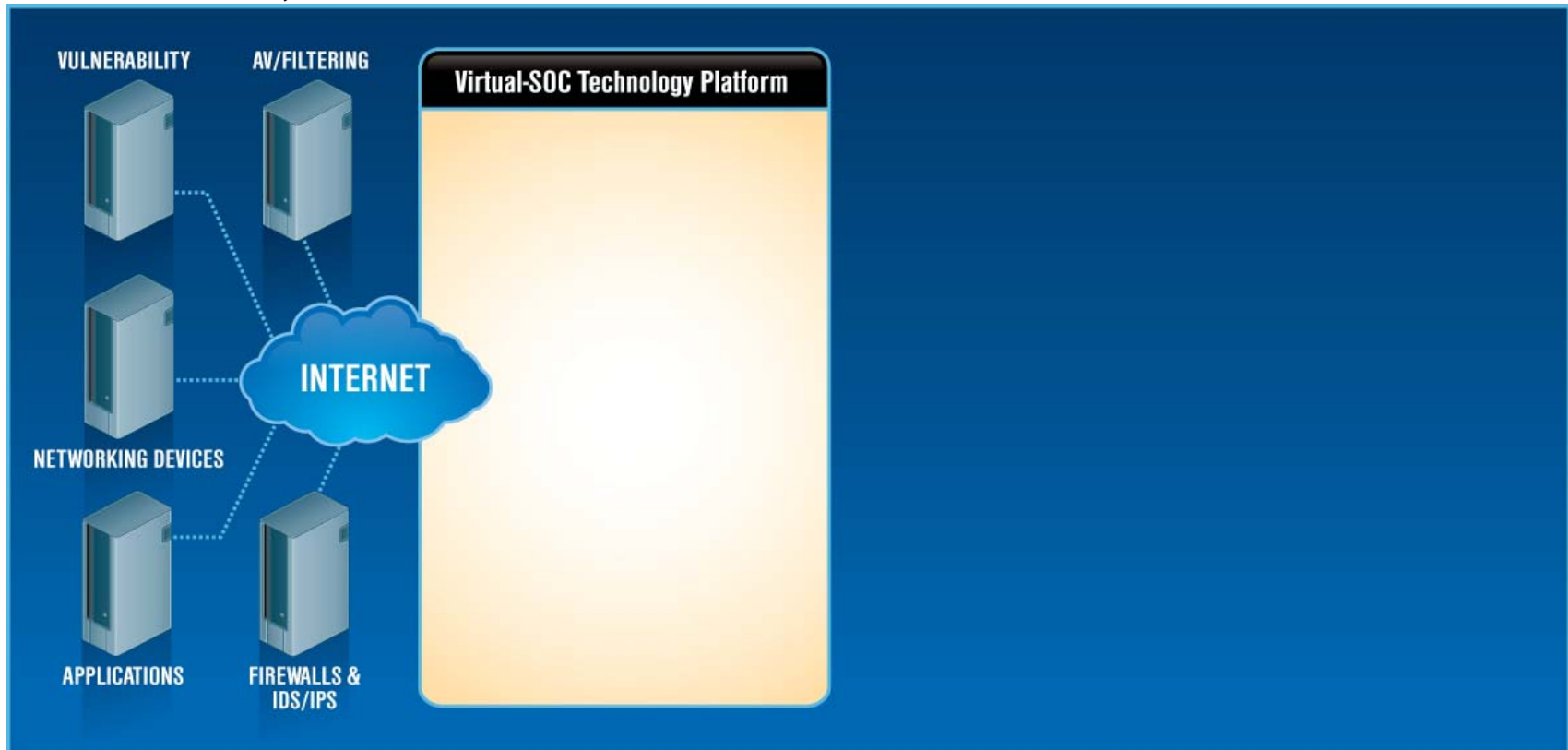
Virtual-SOC: un'architettura per l'integrazione di servizi

- A. **Sistemi di sicurezza multi-vendor generano una enorme quantità di log ed eventi**



Virtual-SOC: un'architettura per l'integrazione di servizi

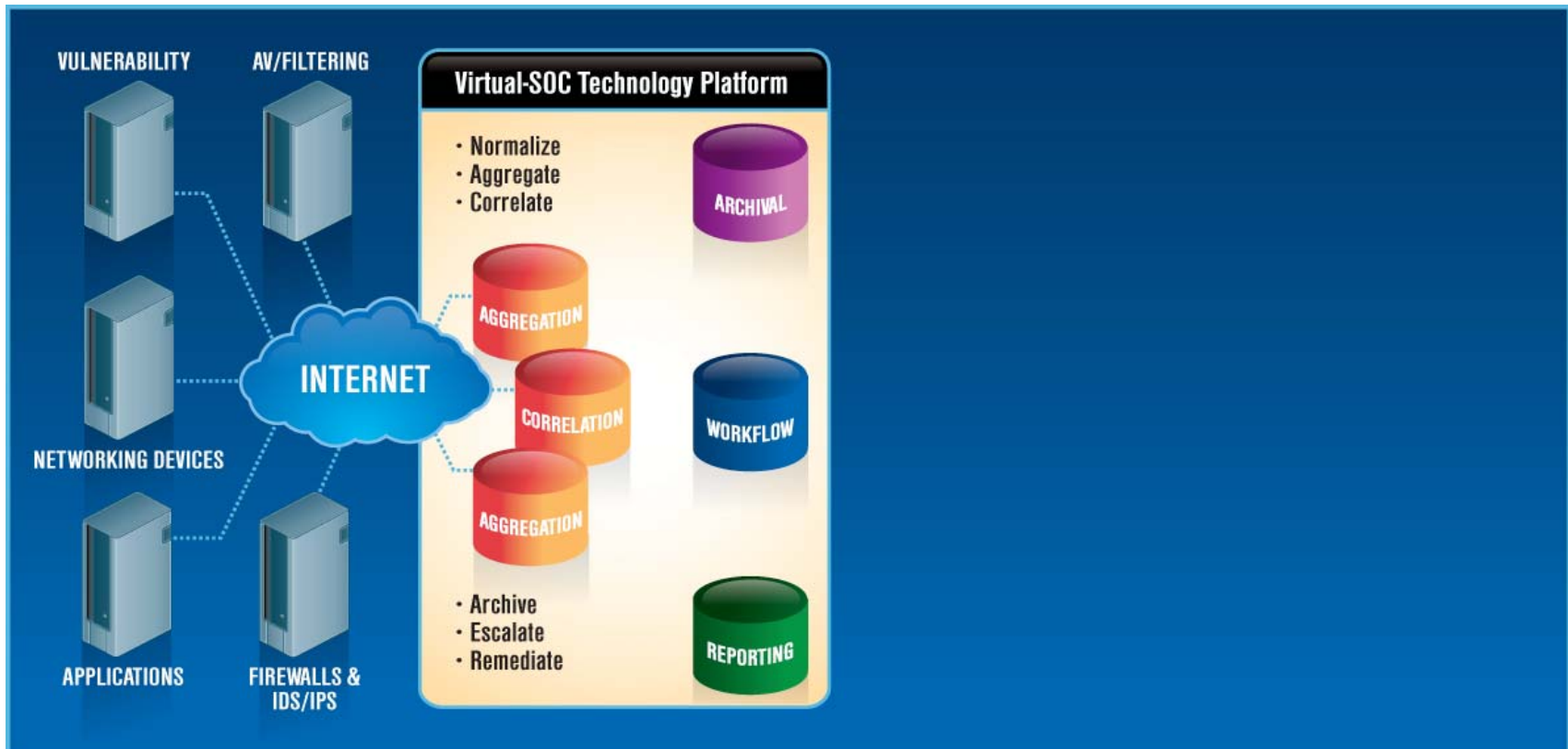
- B.** In tempo reale, tutti gli eventi vengono importati nella piattaforma tecnologica dei Security Operation Center (SOC), dove vengono: autenticati, cifrati verificati e normalizzati.



Virtual-SOC: un'architettura per l'integrazione di servizi

C.

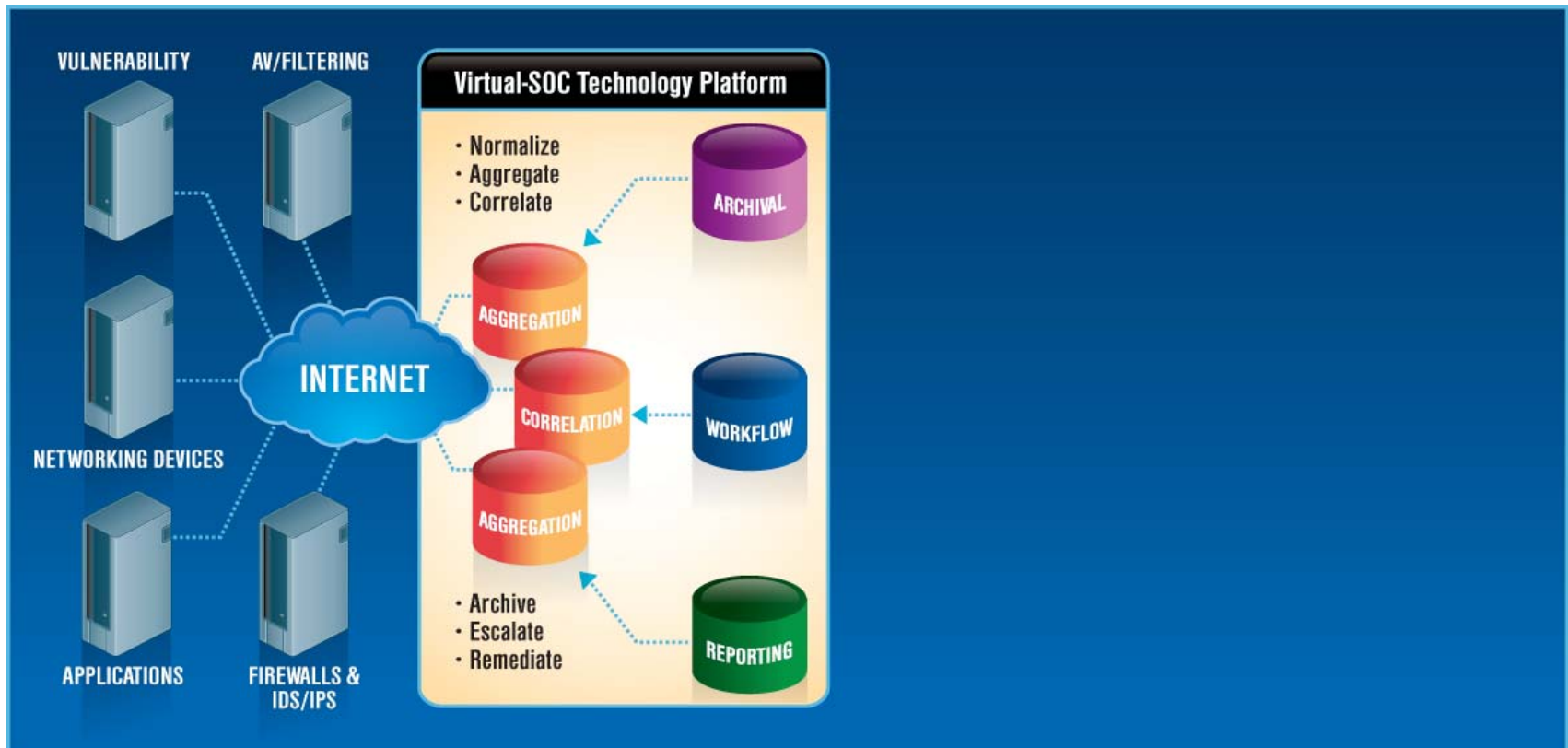
- **Gli eventi di sicurezza vengono conservati nel data warehouse MSS**
- **Un sistema proprietario di Data Mining ricerca, analizza, correla e assegna una priorità agli eventi.**



Virtual-SOC: un'architettura per l'integrazione di servizi

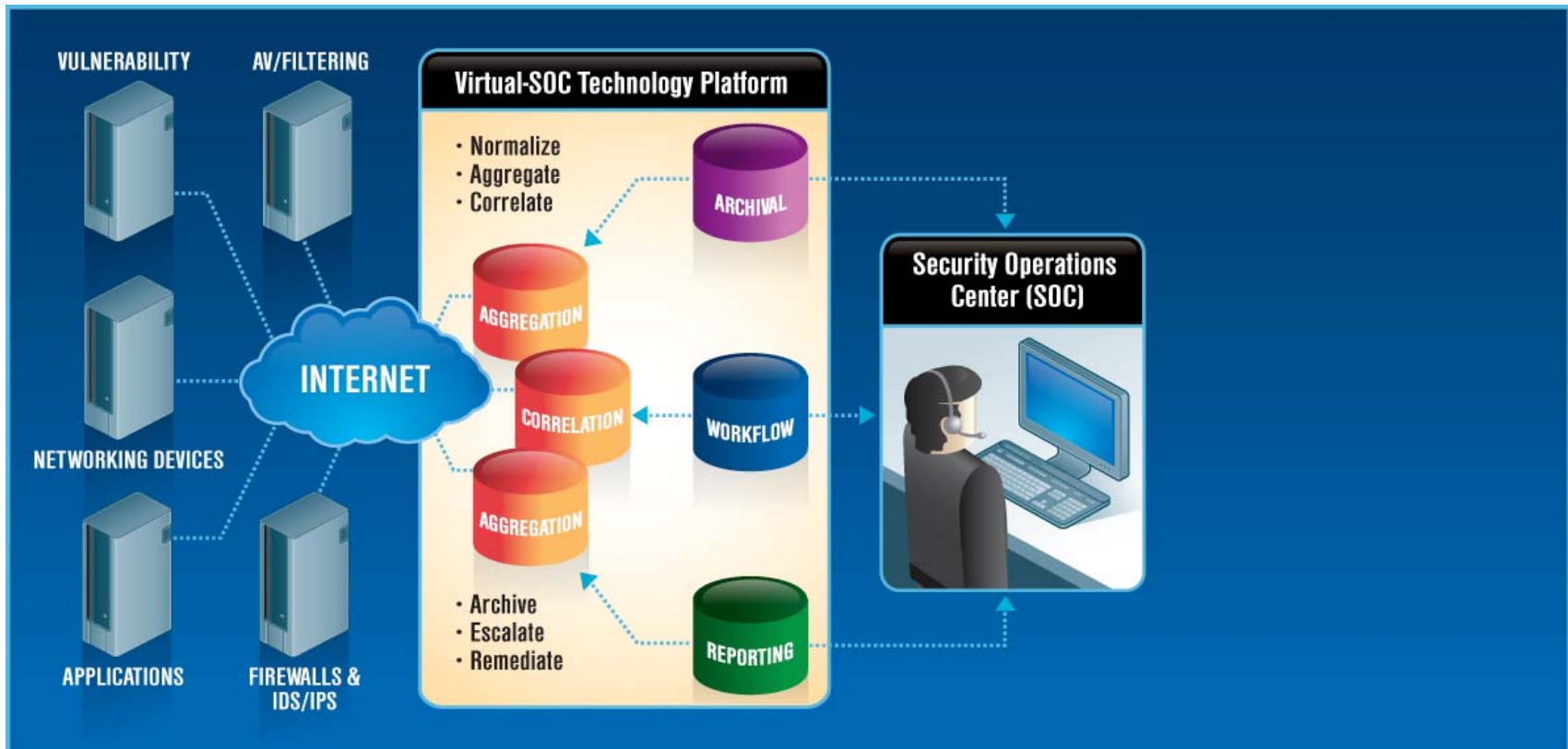
D.

- I pattern delle minacce sono identificati e riportati come eventi di sicurezza



Virtual-SOC: un'architettura per l'integrazione di servizi

- E. **Gli analisti di sicurezza IBM analizzano gli eventi e quando necessario si mettono in contatto con il Cliente che gestiscono per suggerire azioni di contenimento dell'incidente rilevato.**

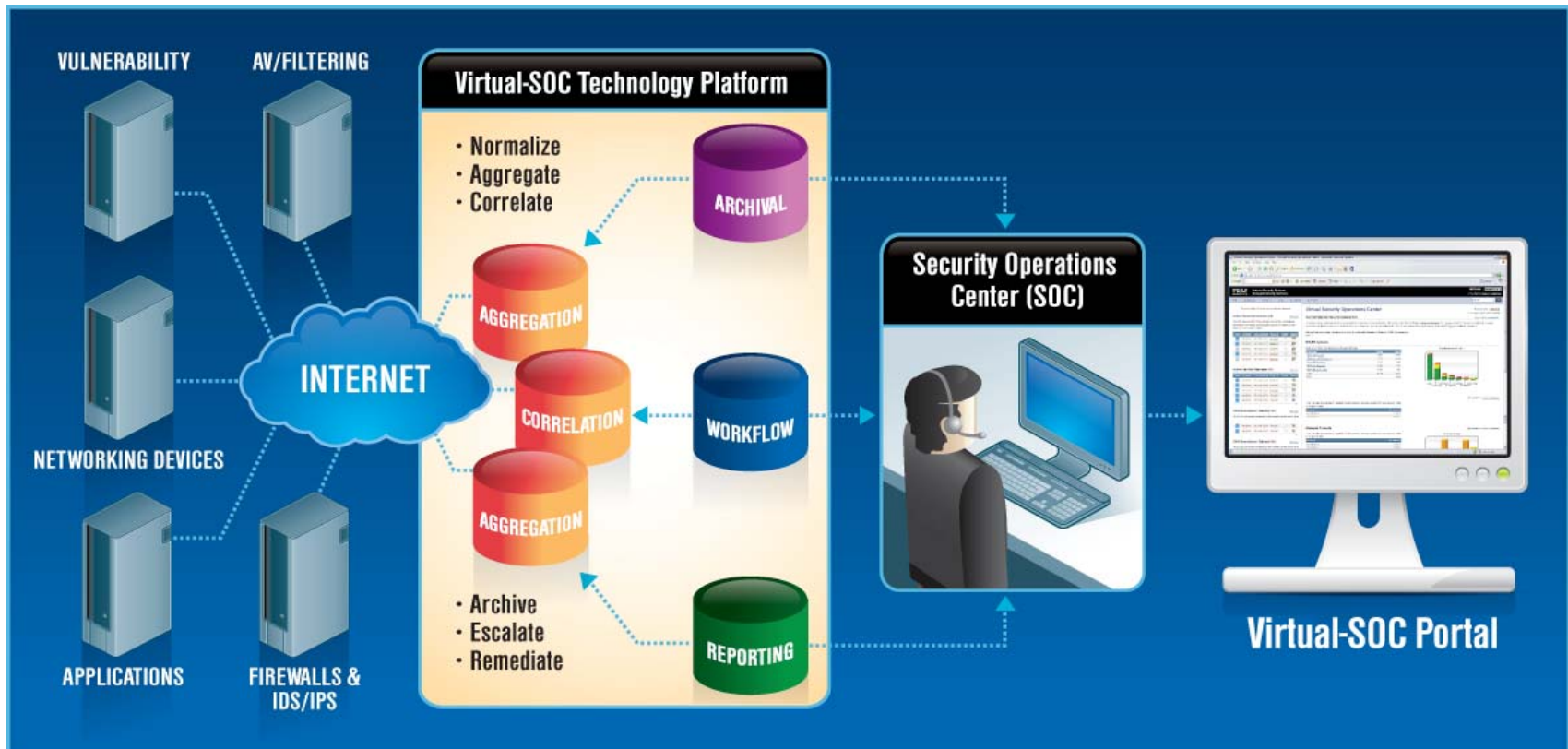


Virtual-SOC: un'architettura per l'integrazione di servizi

F.

Tramite il portale MSS il Cliente è in grado di:

- Avere evidenza del livello di sicurezza della propria organizzazione
- Tenere costantemente sotto controllo il profilo delle minacce e lo stato degli attacchi



MSS Portfolio

ENABLEMENT SERVICES



MSS Portfolio

MANAGED SERVICES

IBM Managed Security Services

**Managed and Monitored
Firewall Services**

Managed Identity Services

**Managed IPS and IDS
Services**

**Managed Protection Services for
Networks, Servers and Desktops**

MSS for UTM

MSS for UTM

Networks, Servers and Desktops



IBM Internet Security Systems Virtual SOC Portal

Virtual Security Operations Center
Bulletins • Impostazioni • Logout

Dashboards
Tickets
LOGS
VMS
Intelligence
Rapporti
Supporto

ALERTCON 1
Search

HOME
Gestione Device
X-Force Threat Analysis
Gestore vulnerabilità
Responsabile Sicurezza Eventi
Welcome [Portal User] of Demo Customer

Incidenti di sicurezza attivi (89)

Visualizza tutti >

Il SOC ha analizzato 11,371,444 eventi concernenti la sicurezza, investigato 1 eventi anomali, e proposto alla vostra attenzione mediante escalation 4 incidenti concernenti la sicurezza negli ultimi 7 giorni.

Tipo	Creato	Ultimo Aggiornamento	ID Ticket	Notifica	Stato
	13/05/09	14/05/09 10:44	71042029		
	13/05/09	14/05/09 10:44	71041819		
	13/05/09	14/05/09 10:44	71041824		
	08/05/09	14/05/09 10:44	71038865		
	29/04/09	14/05/09 10:44	71035795		

Valutazione corrente sicurezza internet

Visualizza lo Storico delle Analisi >

Updated Tue May 12 18:30 2009 GMT
 Microsoft's May 2009 Security release this afternoon consists of one security bulletin. We strongly recommend that all clients apply the applicable Microsoft patches. Please review the Microsoft Security Bulletin breakout displayed below, which is based on the vendor's severity rating and contains key information pertaining to each update.

Microsoft May 2009 Security Release

Microsoft Maximum Severity Rating: Critical

Microsoft Security Bulletin...

[continua >](#)

Richieste di servizio attive (38)

Visualizza tutti >

Tipo	Creato	Ultimo Aggiornamento	ID Ticket	Notifica	Stato
	21/03/09	14/05/09 11:03	01095153		
	12/05/09	14/05/09 10:28	71041253		
	04/05/09	14/05/09 09:47	01144195		
	13/05/09	14/05/09 09:04	01152334		
	29/04/09	14/05/09 08:57	01138385		

Sensori IDS/IPS

Most active high-risk signatures in the last 24 hours.

Nome Evento	% sul Totale	Conteggio
HTTP_Misc_Password	25.47%	7,093
HTTP_GET.aspprint	23.17%	6,997
IPMI_Received_TCP_Connection	12.90%	3,886
HTTP_GET_DeDot_Data	12.07%	3,646
SQL_Injection	5.19%	1,569
Other	21.20%	6,402
TOTAL		28,203

Ticket di riparazione VMS (188)

Visualizza tutti >

Of your 19 active scan schedules, 9 are currently running.

Creato	ID Ticket	Stato	# Vulns	# Assets
12/05/09	710221		1	1
29/04/09	710207		1	1
20/04/09	710206		2	1
20/04/09	710205		1	1
17/04/09	710204		1	1

Firewall gestiti

I firewall hanno bloccato o respinto dal traffico sulla vostra rete 172,861 eventi potenzialmente dannosi negli ultimi 7 giorni.

IP origine	Sessioni totali
12.173.210.17	1150004
12.173.210.9	1030825
12.173.210.82	844975
209.134.186.8	737960
207.231.129.9	704497

Destinazioni Principali - 24hr

Tendenza eventi FW

Copyright © 2009 IBM Corporation
Privacy
Terms of use
14/05/09 11:11 BRT
14/05/09 14:11 GMT
Last Login: 05/14/09 10:32 BRT
#02.3.34225



Virtual Security Operations Center
Bulletins • Settings • Logout

Dashboards Tickets Alerts (88) Logs VMS Intelligence Reports Support
ALERTCON 1 Search

Home Device Manager X-Force Threat Analysis **Vulnerability Manager** Security Event Manager
Welcome [Demo User] of Demo Customer

Vulnerabilities Breakdown

[View all vulns](#)

- Low Severity, Assigned
- Low Severity, Unassigned
- Medium Severity, Assigned
- Medium Severity, Unassigned
- High Severity, Assigned
- High Severity, Unassigned

Vulnerability Trend by Severity

[View all vulns](#)

Legend: Open High (red), Open Medium (yellow), Open Low (green)

Active Vulnerabilities

[View all vulns](#)

Severity	Count
High	28
Medium	20
Low	215
Total	272

Results for Recently Completed Scans

Of your 20 active scan schedules, 0 are currently running.

[Create a new scan schedule](#) (36,082 external IPs left)

Start Time	Schedule Name	Scan Type	Interval	Assets	Vulnerabilities
05/11/09 21:04	Monday Scan	External	Weekly	58	24
05/11/09 19:01	Discover2	External	Weekly	2	0
05/11/09 13:01	test-00	External	Monthly	2	0
05/11/09 03:01	Todd and Marc	External	Weekly	2	0
05/10/09 13:01	Sunday-L3	Internal	Weekly	9	1
05/10/09 07:01	Saturday Scan	External	Weekly	64	24
05/10/09 01:01	Weekly SFLD SOC Lab Scan	External	Weekly	15	0
05/09/09 23:01	Dale's Saturday Scan	External	Weekly	0	0
05/09/09 10:01	L3 Server	Internal	Weekly	26	3
05/08/09 21:01	Friday Scan	External	Weekly	68	25

Remediation Status

[View tickets](#)

[Create a new subordinate user](#)

Subordinate	Assets	Tickets
Al Hutchinson	0	58
Alden Hutchison	0	48
Alexia	4	41
Tom Wallace	0	20
VMS Subordinate User	1	24

10 Most Severe Vulns

[View all vulns](#)

Name	Status	Severity	Risk	Ticket
SNMPv2Discovery			10.0	200033
Smsc_Sec_Public_C...			10.0	200031
TelnetCotnTel...			10.0	210081
SNMPv1Discovery			10.0	202903
TelnetCotnTel...			10.0	208444
SNMPv2Discovery			10.0	202922
SNMPv1Discovery			10.0	202919
Smsc_Sec_Overabl...			10.0	208445
SNMPv2Discovery			10.0	202918
TelnetCotnTel...			10.0	202917

Copyright © 2009 IBM Corporation [Privacy](#) [Terms of use](#)

05/12/09 07:38 EDT - 05/12/09 11:38 GMT

Last Login: 05/12/09 03:44 EDT #01.3.34225



IBM MSS Total Cost of Ownership Calculator



United States [change]

Search

Home Solutions Services Products Support & downloads My IBM Welcome Gail Gullotti [Not you?] [IBM Sign in]

The IBM ISS Virtual EXECUTIVE BRIEFING CENTER

Security Solutions for a smarter planet.

Managed Security Services

Global Security Operations Centers

Our Managed Security Services help you regain control over your entire security infrastructure, including managed and unmanaged devices at any location, regardless of device type or vendor. We offer a broad portfolio of services and service levels to meet your business needs. But the best part... it could cost you significantly less than trying to do it internally.

[View video \(14:05\)](#)
[Download transcript \(PDF, 614KB\)](#)

Professional Security Services

IBM offers industry leading, end-to-end security solutions that protect critical data and keep system components ahead of emerging threats. We can even implement digital controls to secure events—on people or things—in physical space. IBM understands that your job is to run a business that can compete and grow—even in times of tightening budgets.

[View video \(14:33\)](#)
[Download transcript \(PDF, 474KB\)](#)

We're here to help

Easy ways to get the answers you need.

[Chat now](#)

[E-mail us](#)

or call us at
1-800-IBM-7080
Mention 108AE08W

How much can you save?

