SERVICE & RISK MANAGEMENT FORUM 2011

Security Operations Center

¿construir o contratar?

Fernando Guimarães

MSS Global Architect

feguima@br.ibm.com

© 2010 IBM Corporation

Agenda

- ***SOC** – ¿construir o contratar? ¿Qué **aspectos** considerar?*

- *El **Portafolio** de Servicios MSS de IBM*

- *Visión integrada: Portal **Virtual-SOC***

SOC - ¿construir o contratar?

- Necesito **estructurar** un proceso formal para gestionar y supervisar mi infraestructura de seguridad.

- **¿Qué hacer?**
  - ¿Construir la estructura **internamente**? o
  - ¿Adquirir el servicio a través de **MSSPs**?

¿Que Aspectos Considerar?

- *build x buy...*
  - Cobertura **24x7**
  - Designación del **Equipo de Seguridad**
  - **Ámbito**
  - **Reducción de costos** de la Infraestructura tecnológica
  - **Procesos Internos** estructurados
  - *Experiencia en **Outsourcing***

Cobertura 24x7

- Al establecer el requisito de supervisión 24x7, pretendo:
  - Contratar,
    - capacitar constantemente, mantener políticas de retención, estructura organizativa propia, 6 analistas por puesto

O

  - Dejarlo todo a cargo del MSS Provider

Designación del Equipo de Seguridad

- **Su organización:**
  - ¿**No cuenta con personas** capacitadas en seguridad de la información?
  - ¿Quiere que los **recursos existentes se concentren en** actividades **estratégicas**?

La contratación de un MSSP:

- **Elimina la carga operacional** de gestionar y supervisar los componentes de seguridad de los hombros de su equipo
- **Reducirá los costos** de contratación y capacitación
- **Liberará al equipo de seguridad** para actividades de mayor valor agregado

Servicios Administrados de Seguridad

- **Un MSSP típico es capaz de ofrecer la gestión de los siguientes procesos de seguridad:**
  - Monitoreo y Gestión **remotas**
- Un MSSP típico **NO** ofrece:
  - Implantar **correcciones de vulnerabilidades** de equipos **no gestionados**
  - **Recuperación de desastres** generados por incidentes
- **El cliente autoriza los cambios** de configuración en los dispositivos gestionados

Reducción de costos de la Infraestructura tecnológica

- Poca diferencia con los costos relacionados a los **componentes de seguridad**.

- **Gran reducción de costos** en herramientas de back-office:
  - *trouble-tickets*, correlación de eventos, generadores de informes, portal web, storage, backup-offline, etc.
  - El MSSP reduce el costo de estas herramientas para el cliente al **compartirlas** y utilizarlas en mayor **escala**.

Procesos Internos estructurados

¿Tiene su organización un proceso **de respuestas a incidentes estructurado?**

- **En caso positivo**, tendrá capacidad de aprovechar todos los beneficios de conocer más rápida y profundamente los potenciales incidentes de seguridad.
- **Sin este proceso** internamente estructurado, **se reducen los beneficios de la empresa** al contratar un MSSP.

SERVICE & RISK MANAGEMENT FORUM 2011

Experiencia en Outsourcing

IBM.

- Outsourcing = **desistir** de determinados controles en pro de la **eficacia / efectividad** y del ***expertise*** ofrecido por el proveedor de servicios.

- El Outsourcing de la seguridad, a veces, trae la **impresión de desistimiento** de controles importantes de la organización.

- ¿Tiene usted **experiencia en outsourcing** de otras tareas operacionales?, por ejemplo, gestión de redes, servidores:

  ↳ entonces, su experiencia va a simplificar la tarea de gestionar un outsourcing de infraestructura de seguridad.

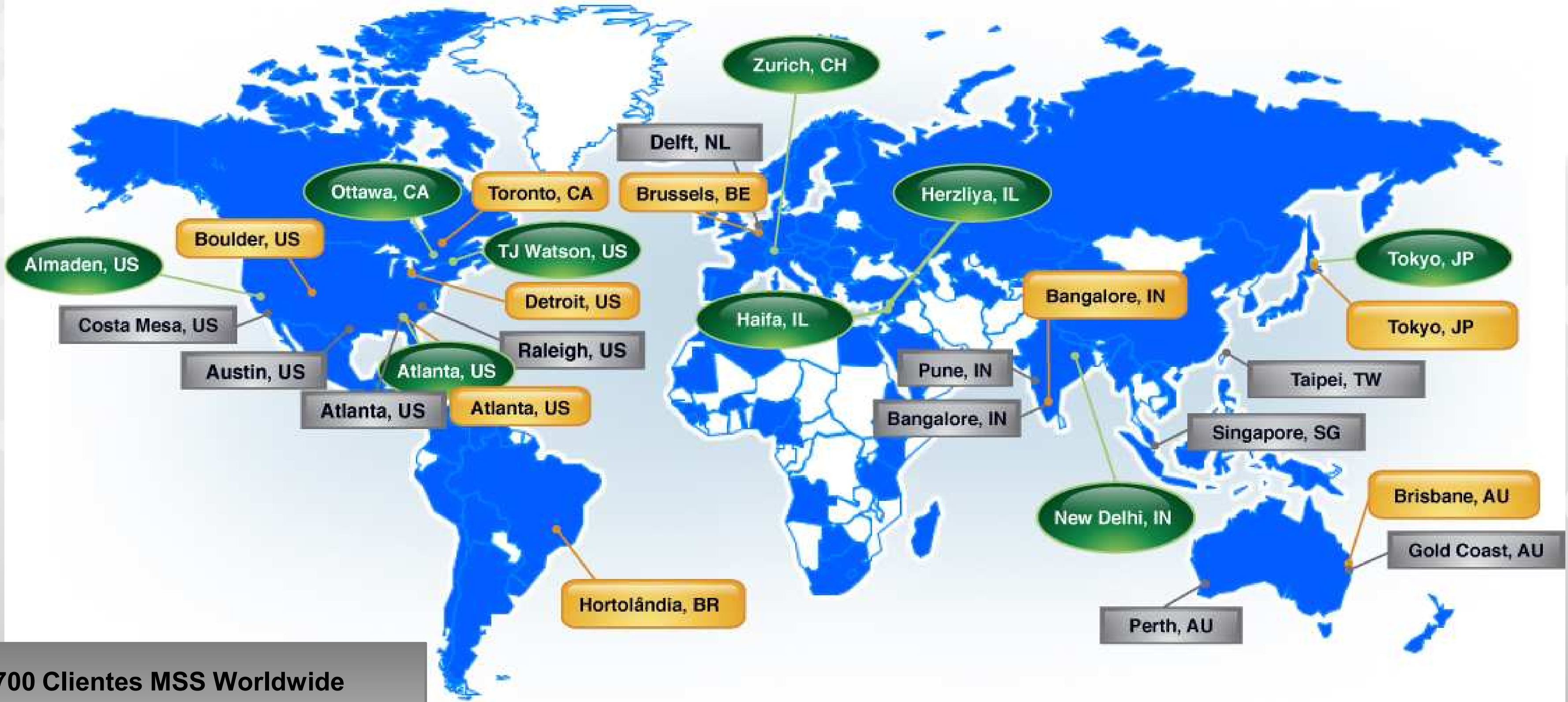
Otras consideraciones importantes…

- **¡¡Atención!! No** existe ***SOC in a BOX*** (aunque algunos proveedores de productos SIEM traten de convencerte de ello…)
  - SOC es… **Personas** capacitadas + **Procesos** bien definidos y probados + **Tecnología**
  - Por lo tanto: Al comparar costos de MSS versus SOC interno, **piense en:**
    - Infraestructura **Tecnológica**: Producto SIEM + HW + Servicios de implantación y personalización + infraestructura de DR
    - Definición e implantación de **procesos**
    - Costos de **personal**: contratación + capacitación constante + retención

Los Managed Security Services de IBM

Infraestructura Global Integrada

9 SOCs + 9 Security Research Centers + 11 Security Solution Development Centers + 133 Países + +900 Consultores + +600 Especialistas de campo + 4.500 Security Delivery Experts + +400 Analistas de Operaciones de Seguridad



- +3.700 Clientes MSS Worldwide
- +13 Mil Millones de Eventos/Día
- X-Force

Portafolio de Servicios MSS

CPE Managed Security Services

- Managed Firewall Services
- Managed Secure Web Gateway
- Managed IPS and IDS Services
- Managed UTM Services
- Managed Protection Services for Networks and Servers

Cloud Security Services

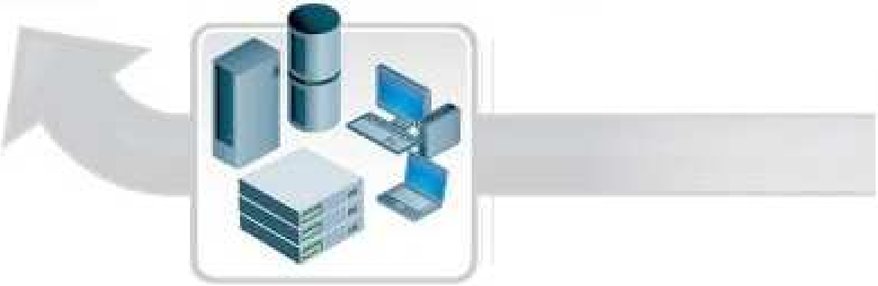
- Vulnerability Management Services
- Security Event and Log Management Services
- Hosted Application Security Services
- Hosted Email Security Services
- Mobile Security Services

Soporte a distintos vendors y equipos

"Full-Services"

CPE Managed Security Services

- Managed Firewall Services
- Managed Secure Web Gateway
- Managed IPS and IDS Services
- Managed UTM Services
- Managed Protection Services for Networks and Servers



- *Multivendor* *(IBM, Cisco, Juniper, Checkpoint, etc.)*
- *Supervisión de Eventos*
  - *Sistema de Analistas calificados+Procesos*
  - *Notificación de incidentes*
  - *SLAs*
- *Gestión de las Plataformas*
  - *Updates y Patches*
  - *Backup Diario*
  - *Device Health y Disponibilidad*
- *Almacenamiento de Logs hasta por 7 años*
- *Portal Virtual-SOC*
- *Servicio 24/7/365*

Cloud Services

- Modelo IaaS SaaS
- Vulnerability Mgmt Service (VMS)
  - Internal & External
  - Vulnerability Remediation Workflow
  - PCI ASV (Approved Scanning Vendor)
- Security Event & Log Management (SELM)
  - Syslog, Universal Logging Agent (ULA)
  - Alertas Automatizadas
- Application Security
  - Analisis Pre-producción / Producción
- Email Security
  - AV, AS, Content Protection
  - Sin instalación de HW/SW
- Mobile Security
  - AV, AS, VPN, App Control, device lock/wipe, backup

Cloud Security Services

Vulnerability Management Services

Security Event and Log Management Services

Hosted Application Security Services

Hosted Email Security Services

Mobile Security Services

Modelos de Asociación Virtual SOC

	Sales	Partner Sales Geo	Standard IBM Portafolio	Custom Portafolio	Co-branded Portal	Helpdesk (First Call)	Tier 1-3 Service Delivery	SOC Mgmt Systems	XPS Systems
Business Partner	Shared	In-Country	IBM	n/a	n/a	IBM	IBM	IBM	IBM Shared
MSS Integrated Alliance Partner	Partner	Global	Partner	Optional	Optional	Partner	IBM	IBM	IBM Shared
MSS Shared Delivery	Partner	Global	Partner	Partner	Partner	Partner	Partner	Partner	IBM Shared
MSS Shared Delivery w/ Dedicated XPS	Partner	Global	Partner	Partner	Partner	Partner	Partner	Partner	IBM Dedicated

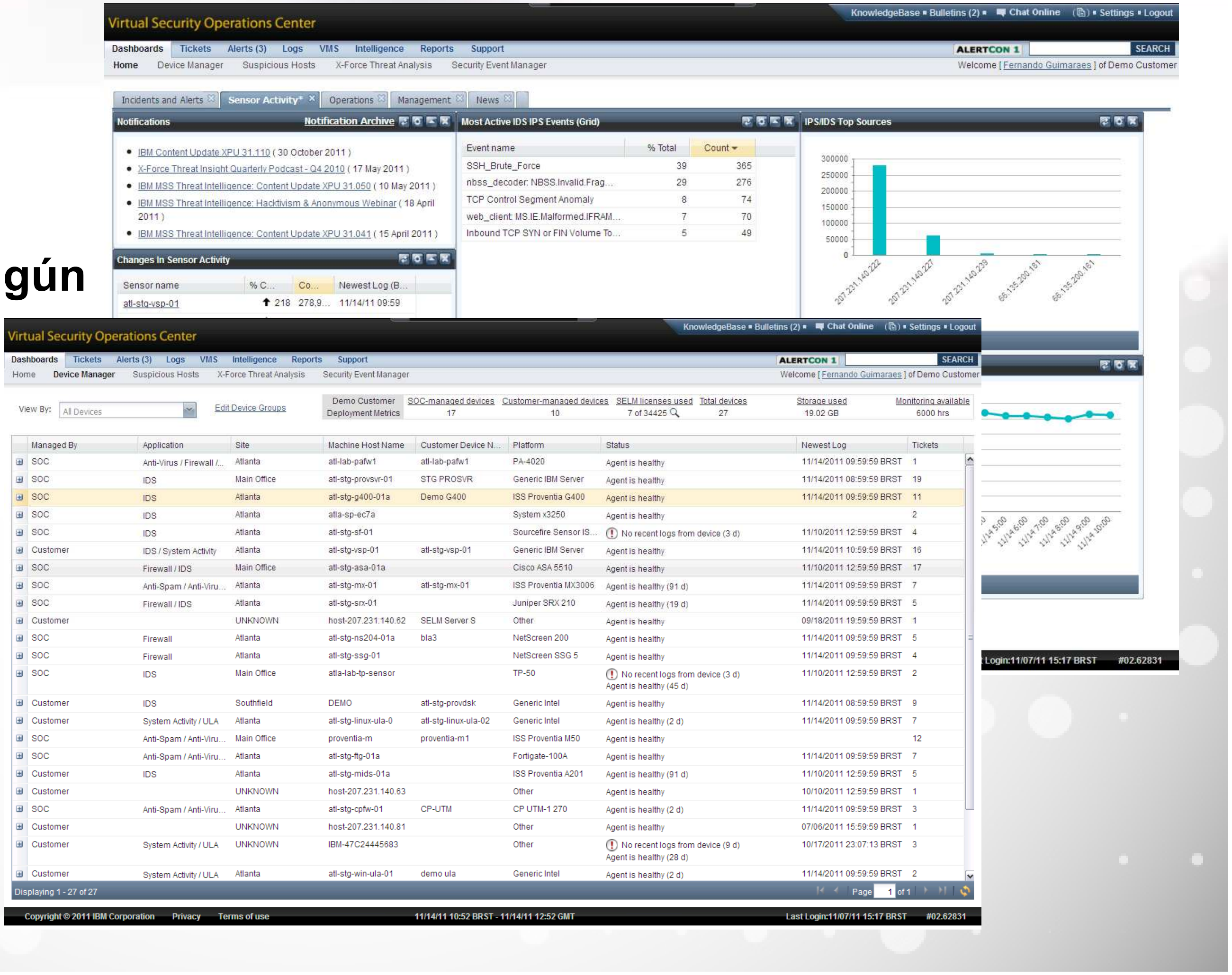
Visión Integrada y Centralizada

Portal Virtual-SOC

Security
Intelligence
Customer Portal
NEWS & RESEARCH
Current Internet Security Assessment
24/7
Protection

Portal Virtual SOC

- Visión **Centralizada**
- Visión **Consolidada**
- **100% web-based**: ningún equipo en el cliente



Notifications

- IBM Content Update XPU 31.110 (30 October 2011)
- X-Force Threat Insight Quarterly Podcast - Q4 2010 (17 May 2011)
- IBM MSS Threat Intelligence: Content Update XPU 31.050 (10 May 2011)
- IBM MSS Threat Intelligence: Hacktivism & Anonymous Webinar (18 April 2011)
- IBM MSS Threat Intelligence: Content Update XPU 31.041 (15 April 2011)

Most Active IDS IPS Events (Grid)

Event name	% Total	Count
SSH_Brute_Force	39	365
nbss_decoder: NBSS.Invalid.Frag...	29	276
TCP Control Segment Anomaly	8	74
web_client: MS.IE.Malformed.IFRAM...	7	70
Inbound TCP SYN or FIN Volume To...	5	49

Changes In Sensor Activity

Sensor name	% C...	Co...	Newest Log (B...
atl-stg-vsp-01	↑ 218	278,9...	11/14/11 09:59

Demo Customer Deployment Metrics	SOC-managed devices	Customer-managed devices	SELM licenses used	Total devices	Storage used	Monitoring available
	17	10	7 of 34425	27	19.02 GB	6000 hrs

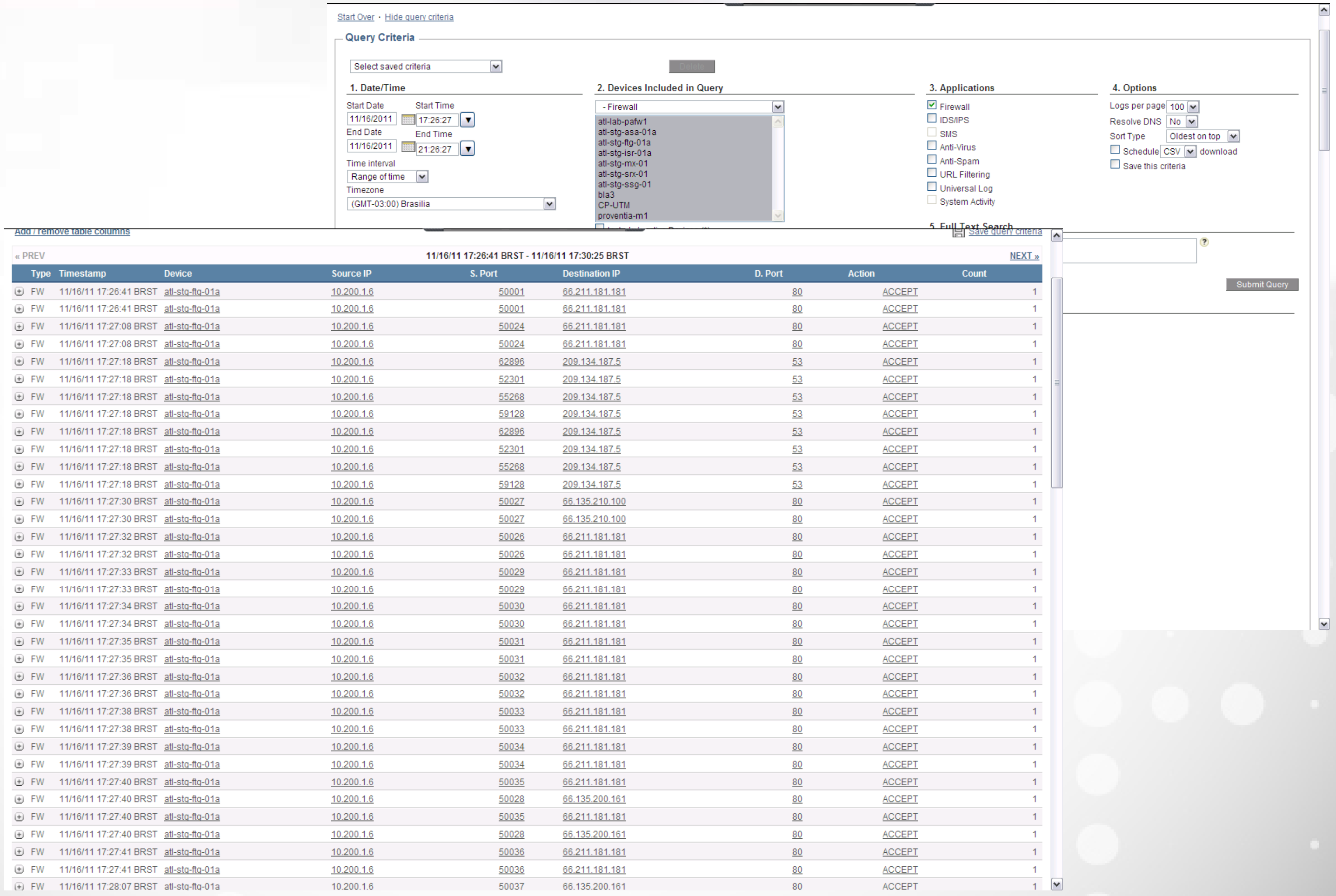
Managed By	Application	Site	Machine Host Name	Customer Device N...	Platform	Status	Newest Log	Tickets
SOC	Anti-Virus / Firewall /...	Atlanta	atl-lab-pafw1	atl-lab-pafw1	PA-4020	Agent is healthy	11/14/2011 09:59:59 BRST	1
SOC	IDS	Main Office	atl-stg-provsvr-01	STG PROSVR	Generic IBM Server	Agent is healthy	11/14/2011 08:59:59 BRST	19
SOC	IDS	Atlanta	atl-stg-g400-01a	Demo G400	ISS Proventia G400	Agent is healthy	11/14/2011 09:59:59 BRST	11
SOC	IDS	Atlanta	atla-sp-ec7a		System x3250	Agent is healthy		2
SOC	IDS	Atlanta	atl-stg-sf-01		Sourcefire Sensor IS...	(!) No recent logs from device (3 d)	11/10/2011 12:59:59 BRST	4
Customer	IDS / System Activity	Atlanta	atl-stg-vsp-01	atl-stg-vsp-01	Generic IBM Server	Agent is healthy	11/14/2011 10:59:59 BRST	16
SOC	Firewall / IDS	Main Office	atl-stg-asa-01a		Cisco ASA 5510	Agent is healthy	11/10/2011 12:59:59 BRST	17
SOC	Anti-Spam / Anti-Viru...	Atlanta	atl-stg-mx-01	atl-stg-mx-01	ISS Proventia MX3006	Agent is healthy (91 d)	11/14/2011 09:59:59 BRST	7
SOC	Firewall / IDS	Atlanta	atl-stg-srx-01		Juniper SRX 210	Agent is healthy (19 d)	11/14/2011 09:59:59 BRST	5
Customer		UNKNOWN	host-207.231.140.62	SELM Server S	Other	Agent is healthy	09/18/2011 19:59:59 BRST	1
SOC	Firewall	Atlanta	atl-stg-ns204-01a	bla3	NetScreen 200	Agent is healthy	11/14/2011 09:59:59 BRST	5
SOC	Firewall	Atlanta	atl-stg-ssg-01		NetScreen SSG 5	Agent is healthy	11/14/2011 09:59:59 BRST	4
SOC	IDS	Main Office	atla-lab-tp-sensor		TP-50	(!) No recent logs from device (3 d) Agent is healthy (45 d)	11/10/2011 12:59:59 BRST	2
Customer	IDS	Southfield	DEMO	atl-stg-provdsk	Generic Intel	Agent is healthy	11/14/2011 08:59:59 BRST	9
Customer	System Activity / ULA	Atlanta	atl-stg-linux-ula-0	atl-stg-linux-ula-02	Generic Intel	Agent is healthy (2 d)	11/14/2011 09:59:59 BRST	7
SOC	Anti-Spam / Anti-Viru...	Main Office	proventia-m	proventia-m1	ISS Proventia M50	Agent is healthy		12
SOC	Anti-Spam / Anti-Viru...	Atlanta	atl-stg-ftg-01a		Fortigate-100A	Agent is healthy	11/14/2011 09:59:59 BRST	7
Customer	IDS	Atlanta	atl-stg-mids-01a		ISS Proventia A201	Agent is healthy (91 d)	11/10/2011 12:59:59 BRST	5
Customer		UNKNOWN	host-207.231.140.63		Other	Agent is healthy	10/10/2011 12:59:59 BRST	1
SOC	Anti-Spam / Anti-Viru...	Atlanta	atl-stg-cpfw-01	CP-UTM	CP UTM-1 270	Agent is healthy (2 d)	11/14/2011 09:59:59 BRST	3
Customer		UNKNOWN	host-207.231.140.81		Other	Agent is healthy	07/06/2011 15:59:59 BRST	1
Customer	System Activity / ULA	UNKNOWN	IBM-47C24445683		Other	(!) No recent logs from device (9 d) Agent is healthy (28 d)	10/17/2011 23:07:13 BRST	3
Customer	System Activity / ULA	Atlanta	atl-stg-win-ula-01	demo ula	Generic Intel	Agent is healthy (2 d)	11/14/2011 09:59:59 BRST	2

Displaying 1 - 27 of 27

Copyright © 2011 IBM Corporation   Privacy   Terms of use   11/14/11 10:52 BRST - 11/14/11 12:52 GMT   Last Login:11/07/11 15:17 BRST   #02.62831

Búsquedas Customizadas

- En equipos de **distintos vendors**



Start Over · Hide query criteria

Query Criteria

Select saved criteria

1. Date/Time

Start Date: 11/16/2011 Start Time: 17:26:27
End Date: 11/16/2011 End Time: 21:26:27
Time interval: Range of time
Timezone: (GMT-03:00) Brasilia

2. Devices Included in Query

- Firewall
atl-lab-pafw1
atl-stg-asa-01a
atl-stg-ftg-01a
atl-stg-isr-01a
atl-stg-mx-01
atl-stg-srx-01
atl-stg-ssg-01
bla3
CP-UTM
proventia-m1

3. Applications

☑ Firewall
☐ IDS/IPS
☐ SMS
☐ Anti-Virus
☐ Anti-Spam
☐ URL Filtering
☐ Universal Log
☐ System Activity

4. Options

Logs per page: 100
Resolve DNS: No
Sort Type: Oldest on top
☐ Schedule CSV download
☐ Save this criteria

5. Full Text Search

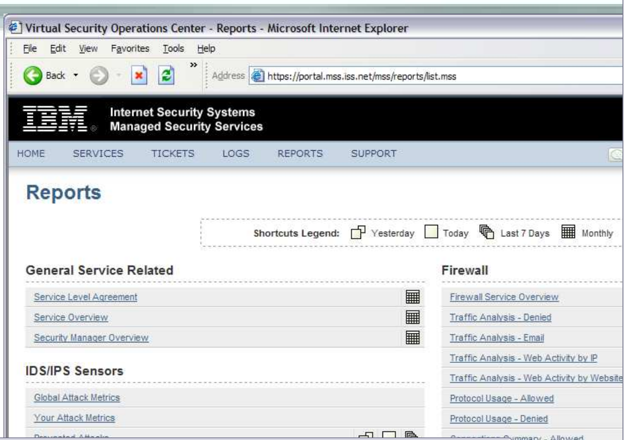
11/16/11 17:26:41 BRST - 11/16/11 17:30:25 BRST

	Type	Timestamp	Device	Source IP	S. Port	Destination IP	D. Port	Action	Count
⊕	FW	11/16/11 17:26:41 BRST	atl-stg-ftg-01a	10.200.1.6	50001	66.211.181.181	80	ACCEPT	1
⊕	FW	11/16/11 17:26:41 BRST	atl-stg-ftg-01a	10.200.1.6	50001	66.211.181.181	80	ACCEPT	1
⊕	FW	11/16/11 17:27:08 BRST	atl-stg-ftg-01a	10.200.1.6	50024	66.211.181.181	80	ACCEPT	1
⊕	FW	11/16/11 17:27:08 BRST	atl-stg-ftg-01a	10.200.1.6	50024	66.211.181.181	80	ACCEPT	1
⊕	FW	11/16/11 17:27:18 BRST	atl-stg-ftg-01a	10.200.1.6	62896	209.134.187.5	53	ACCEPT	1
⊕	FW	11/16/11 17:27:18 BRST	atl-stg-ftg-01a	10.200.1.6	52301	209.134.187.5	53	ACCEPT	1
⊕	FW	11/16/11 17:27:18 BRST	atl-stg-ftg-01a	10.200.1.6	55268	209.134.187.5	53	ACCEPT	1
⊕	FW	11/16/11 17:27:18 BRST	atl-stg-ftg-01a	10.200.1.6	59128	209.134.187.5	53	ACCEPT	1
⊕	FW	11/16/11 17:27:18 BRST	atl-stg-ftg-01a	10.200.1.6	62896	209.134.187.5	53	ACCEPT	1
⊕	FW	11/16/11 17:27:18 BRST	atl-stg-ftg-01a	10.200.1.6	52301	209.134.187.5	53	ACCEPT	1
⊕	FW	11/16/11 17:27:18 BRST	atl-stg-ftg-01a	10.200.1.6	55268	209.134.187.5	53	ACCEPT	1
⊕	FW	11/16/11 17:27:18 BRST	atl-stg-ftg-01a	10.200.1.6	59128	209.134.187.5	53	ACCEPT	1
⊕	FW	11/16/11 17:27:30 BRST	atl-stg-ftg-01a	10.200.1.6	50027	66.135.210.100	80	ACCEPT	1
⊕	FW	11/16/11 17:27:30 BRST	atl-stg-ftg-01a	10.200.1.6	50027	66.135.210.100	80	ACCEPT	1
⊕	FW	11/16/11 17:27:32 BRST	atl-stg-ftg-01a	10.200.1.6	50026	66.211.181.181	80	ACCEPT	1
⊕	FW	11/16/11 17:27:32 BRST	atl-stg-ftg-01a	10.200.1.6	50026	66.211.181.181	80	ACCEPT	1
⊕	FW	11/16/11 17:27:33 BRST	atl-stg-ftg-01a	10.200.1.6	50029	66.211.181.181	80	ACCEPT	1
⊕	FW	11/16/11 17:27:33 BRST	atl-stg-ftg-01a	10.200.1.6	50029	66.211.181.181	80	ACCEPT	1
⊕	FW	11/16/11 17:27:34 BRST	atl-stg-ftg-01a	10.200.1.6	50030	66.211.181.181	80	ACCEPT	1
⊕	FW	11/16/11 17:27:34 BRST	atl-stg-ftg-01a	10.200.1.6	50030	66.211.181.181	80	ACCEPT	1
⊕	FW	11/16/11 17:27:35 BRST	atl-stg-ftg-01a	10.200.1.6	50031	66.211.181.181	80	ACCEPT	1
⊕	FW	11/16/11 17:27:35 BRST	atl-stg-ftg-01a	10.200.1.6	50031	66.211.181.181	80	ACCEPT	1
⊕	FW	11/16/11 17:27:36 BRST	atl-stg-ftg-01a	10.200.1.6	50032	66.211.181.181	80	ACCEPT	1
⊕	FW	11/16/11 17:27:36 BRST	atl-stg-ftg-01a	10.200.1.6	50032	66.211.181.181	80	ACCEPT	1
⊕	FW	11/16/11 17:27:38 BRST	atl-stg-ftg-01a	10.200.1.6	50033	66.211.181.181	80	ACCEPT	1
⊕	FW	11/16/11 17:27:38 BRST	atl-stg-ftg-01a	10.200.1.6	50033	66.211.181.181	80	ACCEPT	1
⊕	FW	11/16/11 17:27:39 BRST	atl-stg-ftg-01a	10.200.1.6	50034	66.211.181.181	80	ACCEPT	1
⊕	FW	11/16/11 17:27:39 BRST	atl-stg-ftg-01a	10.200.1.6	50034	66.211.181.181	80	ACCEPT	1
⊕	FW	11/16/11 17:27:40 BRST	atl-stg-ftg-01a	10.200.1.6	50035	66.211.181.181	80	ACCEPT	1
⊕	FW	11/16/11 17:27:40 BRST	atl-stg-ftg-01a	10.200.1.6	50028	66.135.200.161	80	ACCEPT	1
⊕	FW	11/16/11 17:27:40 BRST	atl-stg-ftg-01a	10.200.1.6	50035	66.211.181.181	80	ACCEPT	1
⊕	FW	11/16/11 17:27:40 BRST	atl-stg-ftg-01a	10.200.1.6	50028	66.135.200.161	80	ACCEPT	1
⊕	FW	11/16/11 17:27:41 BRST	atl-stg-ftg-01a	10.200.1.6	50036	66.211.181.181	80	ACCEPT	1
⊕	FW	11/16/11 17:27:41 BRST	atl-stg-ftg-01a	10.200.1.6	50036	66.211.181.181	80	ACCEPT	1
⊕	FW	11/16/11 17:28:07 BRST	atl-stg-ftg-01a	10.200.1.6	50037	66.135.200.161	80	ACCEPT	1

SERVICE & RISK MANAGEMENT FORUM 2011

Informes

- Más de 20 tipos de **informes**
- Pueden generarse en HTML, CSV y PDF



Virtual Security Operations Center - Reports - Microsoft Internet Explorer

Address: https://portal.mss.iss.net/mss/reports/list.mss

Internet Security Systems
Managed Security Services

HOME · SERVICES · TICKETS · LOGS · REPORTS · SUPPORT

Reports

Shortcuts Legend: Yesterday · Today · Last 7 Days · Monthly

General Service Related

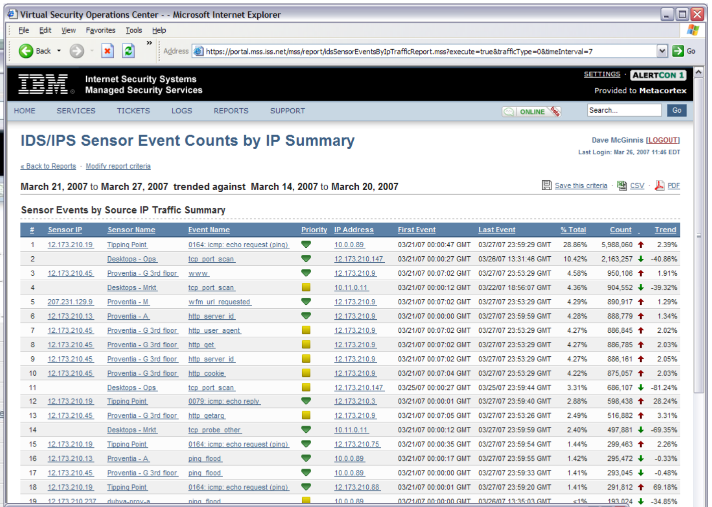
- Service Level Agreement
- Service Overview
- Security Manager Overview

IDS/IPS Sensors

- Global Attack Metrics
- Your Attack Metrics

Firewall

- Firewall Service Overview
- Traffic Analysis - Denied
- Traffic Analysis - Email
- Traffic Analysis - Web Activity by IP
- Traffic Analysis - Web Activity by Website
- Protocol Usage - Allowed
- Protocol Usage - Denied



Virtual Security Operations Center - - Microsoft Internet Explorer

Address: https://portal.mss.iss.net/mss/report/idsSensorEventsByIpTrafficReport.mss?execute=true&trafficType=0&timeInterval=7

Internet Security Systems
Managed Security Services

SETTINGS · ALERTCON 1
Provided to Metacortex

HOME · SERVICES · TICKETS · LOGS · REPORTS · SUPPORT

IDS/IPS Sensor Event Counts by IP Summary

Dave McGinnis [LOGOUT]
Last Login: Mar 26, 2007 11:46 EDT

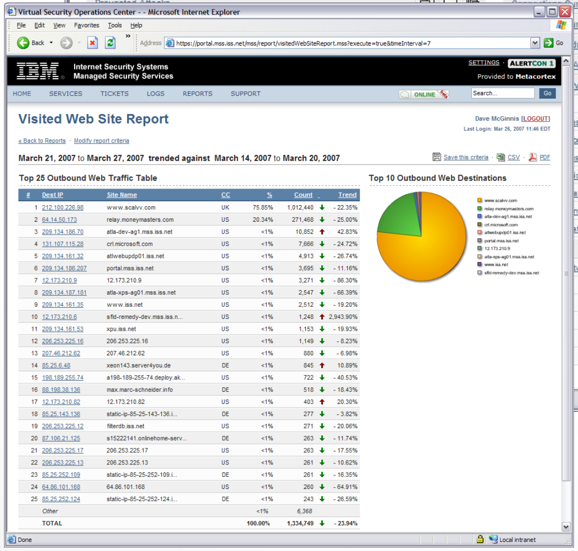
« Back to Reports · Modify report criteria

March 21, 2007 to March 27, 2007 trended against March 14, 2007 to March 20, 2007

Save this criteria · CSV · PDF

Sensor Events by Source IP Traffic Summary

#	Sensor IP	Sensor Name	Event Name	Priority	IP Address	First Event	Last Event	% Total	Count		Trend
1	12.173.210.19	Tipping Point	0164: icmp: echo request (ping)	🟩	10.0.0.89	03/21/07 00:00:47 GMT	03/27/07 23:59:29 GMT	28.86%	5,988,060	↑	2.39%
2		Desktops - Ops	tcp_port_scan	🟩	12.173.210.147	03/21/07 00:00:27 GMT	03/26/07 13:31:46 GMT	10.42%	2,163,257	↓	-40.86%
3	12.173.210.45	Proventia - G 3rd floor	www	🟩	12.173.210.9	03/21/07 00:07:02 GMT	03/27/07 23:53:29 GMT	4.58%	950,106	↑	1.91%
4		Desktops - Mrkt	tcp_port_scan	🟨	10.11.0.11	03/21/07 00:00:12 GMT	03/22/07 18:56:07 GMT	4.36%	904,552	↓	-39.32%
5	207.231.129.9	Proventia - M	wfm_url_requested	🟩	12.173.210.9	03/21/07 00:07:02 GMT	03/27/07 23:53:29 GMT	4.29%	890,917	↑	1.29%
6	12.173.210.13	Proventia - A	http_server_id	🟩	12.173.210.9	03/21/07 00:00:00 GMT	03/27/07 23:59:59 GMT	4.28%	888,779	↑	1.34%
7	12.173.210.45	Proventia - G 3rd floor	http_user_agent	🟨	12.173.210.9	03/21/07 00:07:02 GMT	03/27/07 23:53:29 GMT	4.27%	886,845	↑	2.02%
8	12.173.210.45	Proventia - G 3rd floor	http_get	🟨	12.173.210.9	03/21/07 00:07:02 GMT	03/27/07 23:53:29 GMT	4.27%	886,785	↑	2.03%
9	12.173.210.45	Proventia - G 3rd floor	http_server_id	🟨	12.173.210.9	03/21/07 00:07:02 GMT	03/27/07 23:53:29 GMT	4.27%	886,161	↑	2.05%
10	12.173.210.45	Proventia - G 3rd floor	http_cookie	🟨	12.173.210.9	03/21/07 00:07:04 GMT	03/27/07 23:53:29 GMT	4.22%	875,057	↑	2.03%
11		Desktops - Ops	tcp_port_scan	🟨	12.173.210.147	03/25/07 00:00:27 GMT	03/25/07 23:59:44 GMT	3.31%	686,107	↓	-81.24%
12	12.173.210.19	Tipping Point	0079: icmp: echo reply	🟩	12.173.210.3	03/21/07 00:00:01 GMT	03/27/07 23:59:40 GMT	2.88%	598,438	↑	28.24%
13	12.173.210.45	Proventia - G 3rd floor	http_getarg	🟨	12.173.210.9	03/21/07 00:07:05 GMT	03/27/07 23:53:26 GMT	2.49%	516,882	↑	3.31%
14		Desktops - Mrkt	tcp_probe_other	🟩	10.11.0.11	03/21/07 00:00:12 GMT	03/27/07 23:59:59 GMT	2.40%	497,881	↓	-69.35%
15	12.173.210.19	Tipping Point	0164: icmp: echo request (ping)	🟩	12.173.210.75	03/21/07 00:00:35 GMT	03/27/07 23:59:54 GMT	1.44%	299,463	↑	2.26%
16	12.173.210.13	Proventia - A	ping_flood	🟩	10.0.0.89	03/21/07 00:00:17 GMT	03/27/07 23:59:55 GMT	1.42%	295,472	↓	-0.33%
17	12.173.210.45	Proventia - G 3rd floor	ping_flood	🟩	10.0.0.89	03/21/07 00:00:00 GMT	03/27/07 23:59:33 GMT	1.41%	293,045	↓	-0.48%
18	12.173.210.19	Tipping Point	0164: icmp: echo request (ping)	🟩	12.173.210.88	03/21/07 00:00:01 GMT	03/27/07 23:59:20 GMT	1.41%	291,812	↑	69.18%
19	12.173.210.237	dubya-proxy-a	ping_flood	🟨	10.0.0.89	03/21/07 00:00:00 GMT	03/26/07 13:35:03 GMT	<1%	193,024	↓	-34.85%
										↓	-90.99%



Virtual Security Operations Center - - Microsoft Internet Explorer

Address: https://portal.mss.iss.net/mss/report/visitedWebSiteReport.mss?execute=true&timeInterval=7

Internet Security Systems
Managed Security Services

SETTINGS · ALERTCON 1
Provided to Metacortex

HOME · SERVICES · TICKETS · LOGS · REPORTS · SUPPORT

Visited Web Site Report

Dave McGinnis [LOGOUT]
Last Login: Mar 26, 2007 11:46 EDT

« Back to Reports · Modify report criteria

March 21, 2007 to March 27, 2007 trended against March 14, 2007 to March 20, 2007

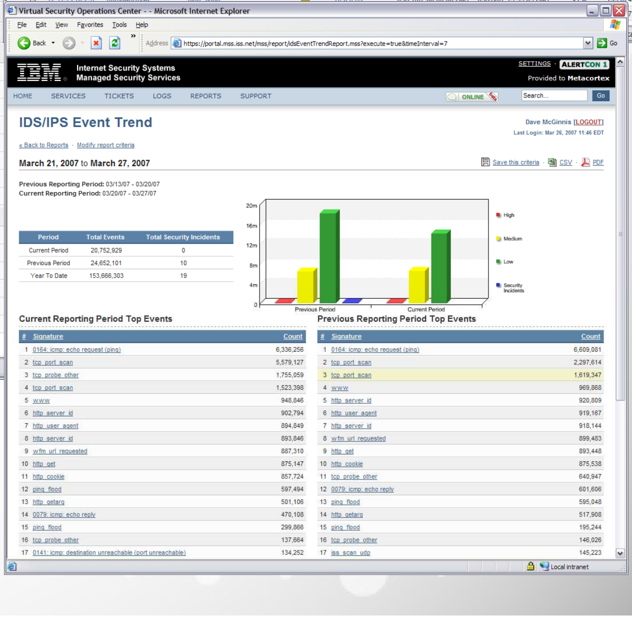
Save this criteria · CSV · PDF

Top 25 Outbound Web Traffic Table

#	Dest IP	Site Name	CC	%	Count		Trend
1	212.100.226.98	www.scalvv.com	UK	75.85%	1,012,440	↓	- 22.35%
2	64.14.50.173	relay.moneymasters.com	US	20.34%	271,468	↓	- 25.00%
3	209.134.186.70	atla-dev-ag1.mss.iss.net	US	<1%	10,852	↑	42.83%
4	131.107.115.28	crl.microsoft.com	US	<1%	7,666	↓	- 24.72%
5	209.134.161.32	atlwebupdp01.iss.net	US	<1%	4,913	↓	- 26.74%
6	209.134.186.207	portal.mss.iss.net	US	<1%	3,695	↓	- 11.16%
7	12.173.210.9	12.173.210.9	US	<1%	3,271	↓	- 86.30%
8	209.134.187.181	atla-xps-ag01.mss.iss.net	US	<1%	2,547	↓	- 66.39%
9	209.134.161.35	www.iss.net	US	<1%	2,512	↓	- 19.20%
10	12.173.210.6	sfld-remedy-dev.mss.iss.n...	US	<1%	1,248	↑	2,943.90%
11	209.134.161.53	xpu.iss.net	US	<1%	1,153	↓	- 19.93%
12	206.253.225.16	206.253.225.16	US	<1%	1,149	↓	- 8.23%
13	207.46.212.62	207.46.212.62	US	<1%	880	↓	- 6.98%
14	85.25.6.48	xeon143.server4you.de	DE	<1%	845	↑	10.89%
15	198.189.255.74	a198-189-255-74.deploy.ak...	US	<1%	722	↓	- 40.53%
16	88.198.38.136	max.marc-schneider.info	DE	<1%	518	↓	- 18.43%
17	12.173.210.82	12.173.210.82	US	<1%	403	↑	20.30%
18	85.25.143.136	static-ip-85-25-143-136.i...	DE	<1%	277	↓	- 3.82%
19	206.253.225.12	filterdb.iss.net	US	<1%	271	↓	- 20.06%
20	87.106.21.125	s15222141.onlinehome-serv...	DE	<1%	263	↓	- 11.74%
21	206.253.225.17	206.253.225.17	US	<1%	263	↓	- 17.55%
22	206.253.225.13	206.253.225.13	US	<1%	261	↓	- 10.62%
23	85.25.252.109	static-ip-85-25-252-109.i...	DE	<1%	261	↓	- 16.35%
24	64.86.101.168	64.86.101.168	US	<1%	260	↓	- 64.91%
25	85.25.252.124	static-ip-85-25-252-124.i...	DE	<1%	243	↓	- 26.59%
	Other			*<1%*	*6,368*		
	TOTAL			**100.00%**	**1,334,749**	↓	**- 23.94%**

Top 10 Outbound Web Destinations

Done



Virtual Security Operations Center - - Microsoft Internet Explorer

Address: https://portal.mss.iss.net/mss/report/idsEventTrendReport.mss?execute=true&timeInterval=7

Internet Security Systems
Managed Security Services

SETTINGS · ALERTCON 1
Provided to Metacortex

HOME · SERVICES · TICKETS · LOGS · REPORTS · SUPPORT

IDS/IPS Event Trend

Dave McGinnis [LOGOUT]
Last Login: Mar 26, 2007 11:46 EDT

« Back to Reports · Modify report criteria

March 21, 2007 to March 27, 2007

Save this criteria · CSV · PDF

Previous Reporting Period: 03/13/07 - 03/20/07
Current Reporting Period: 03/20/07 - 03/27/07

Period	Total Events	Total Security Incidents
Current Period	20,752,929	0
Previous Period	24,652,101	10
Year To Date	153,666,303	19

Current Reporting Period Top Events

#	Signature	Count
1	0164: icmp: echo request (ping)	6,336,256
2	tcp_port_scan	5,579,127
3	tcp_probe_other	1,755,059
4	tcp_port_scan	1,523,398
5	www	948,846
6	http_server_id	902,794
7	http_user_agent	894,849
8	http_server_id	893,846
9	wfm_url_requested	887,310
10	http_get	875,147
11	http_cookie	857,724
12	ping_flood	597,494
13	http_getarg	501,106
14	0079: icmp: echo reply	470,108
15	ping_flood	299,866
16	tcp_probe_other	137,664
17	0141: icmp: destination unreachable (port unreachable)	134,252

Previous Reporting Period Top Events

#	Signature	Count
1	0164: icmp: echo request (ping)	6,609,081
2	tcp_port_scan	2,297,614
3	tcp_port_scan	1,619,347
4	www	969,868
5	http_server_id	920,809
6	http_user_agent	919,167
7	http_server_id	918,144
8	wfm_url_requested	899,483
9	http_get	893,448
10	http_cookie	875,538
11	tcp_probe_other	640,947
12	0079: icmp: echo reply	601,606
13	ping_flood	595,048
14	http_getarg	517,908
15	ping_flood	195,244
16	tcp_probe_other	146,026
17	iss_scan_udp	145,223

Local intranet

¡Beneficios Claros!

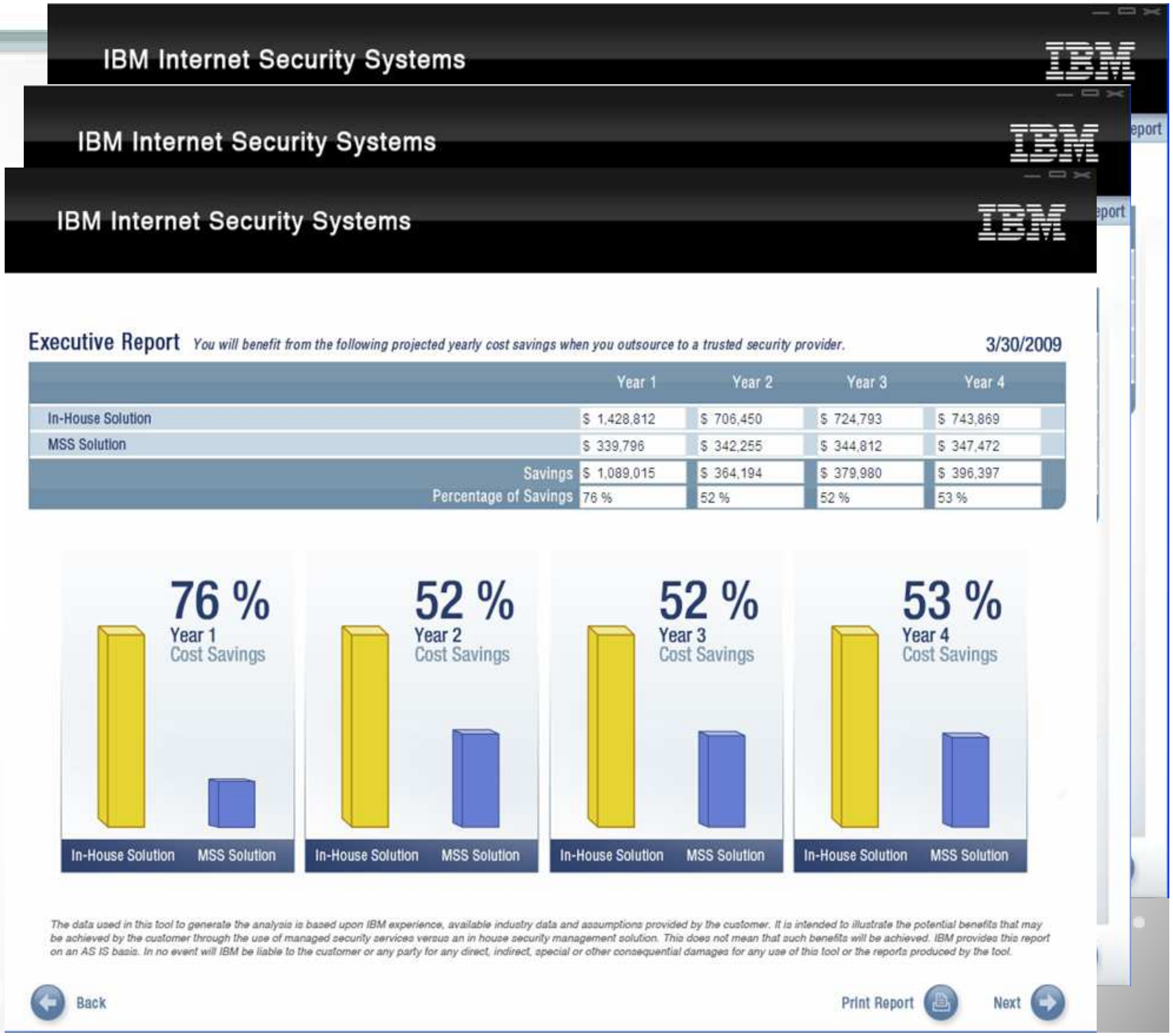
- *Resultados para el Negocio*
  - **Integración** del entorno *multivendor*
  - **Visión centralizada** en tiempo real
  - Exhibe rápidamente el retorno de la inversión
    - **bajo costo** de implementación
    - **muy rápida** implementación

¡Beneficios Claros!

•*Reducción de Costos*

- Evita ***inversiones*** en recursos y tecnologías adicionales
- Reduce los ***costos*** operacionales
- Reduce las ***pérdidas*** por incidentes de seguridad

¡¡¡Utilice el IBM TCO Tool!!!



IBM Internet Security Systems

IBM Internet Security Systems

IBM Internet Security Systems

Executive Report *You will benefit from the following projected yearly cost savings when you outsource to a trusted security provider.* 3/30/2009

	Year 1	Year 2	Year 3	Year 4
In-House Solution	$ 1,428,812	$ 706,450	$ 724,793	$ 743,869
MSS Solution	$ 339,796	$ 342,255	$ 344,812	$ 347,472
Savings	$ 1,089,015	$ 364,194	$ 379,980	$ 396,397
Percentage of Savings	76 %	52 %	52 %	53 %

The data used in this tool to generate the analysis is based upon IBM experience, available industry data and assumptions provided by the customer. It is intended to illustrate the potential benefits that may be achieved by the customer through the use of managed security services versus an in house security management solution. This does not mean that such benefits will be achieved. IBM provides this report on an AS IS basis. In no event will IBM be liable to the customer or any party for any direct, indirect, special or other consequential damages for any use of this tool or the reports produced by the tool.

Si no recuerda nada más…

Reducción de Costos

Simplificación de la gestión de infraestructuras complejas

Protección de su negocio / marca / reputación

Muchas Gracias México!

Fernando Guimarães

feguima@br.ibm.com

Referencias:

http://www-935.ibm.com/services/us/en/it-services/managed-security-services.html

http://www.csoonline.com/article/220328/guidelines-for-choosing-to-outsource-security-management?page=1