4ª edição
IBM Security Forum

Desmistificando os Managed Security Services
(Security Operations Center Services)

Fernando Guimarães

MSS Global Architect

feguima@br.ibm.com

Agenda

- ***SOC** – construir ou contratar? Que **aspectos** considerar ?*
- *O **Portfólio** de Serviços MSS da IBM*
- *Visão integrada: Portal **Virtual-SOC***

SOC - construir ou contratar?

- Preciso **estruturar** um processo formal para gerenciamento e monitoramento de minha infraestrutura de segurança.

- **O que fazer?**
  - Construir a estrutura **internamente** ou;
  - Adquirir o serviço através de **MSSPs** ?

Que Aspectos Considerar

- *build x buy...*

  - Cobertura **24x7**
  - Alocação da **Equipe de Segurança**
  - **Escopo**
  - **Redução de custos** da Infraestrutura tecnológica
  - **Processos Internos** estruturados
  - *Experiência em* ***Outsourcing***

Cobertura 24x7

- Ao estabelecer o requisito de monitoramento 24x7, pretendo:
  - Contratar,
    - treinar continuamente, manter políticas de retenção, estrutura organizacional própria, 6 analistas por posto

OU

  - Deixar isso tudo a cargo do MSS Provider

Alocação da Equipe de Segurança

- **Sua organização:**
  - Possui **carência de pessoas** capacitadas em segurança da informação ?
  - Deseja que os **recursos existentes mantenham o foco** em atividades **estratégicas** (ex, definição de políticas de segurança, avaliação periódica de risco ou investigação de incidentes internos) ?

A contratação de um MSSP:

- Irá **retirar a carga operacional** relativa ao gerenciamento e monitoração dos componentes de segurança dos ombros de sua equipe.
- **Reduzirá os custos** relacionados à contratação e treinamento.
- **Liberará a equipe de segurança** para atividades de maior valor agregado.

Escopo

- **Um típico MSSP é capaz de ofertar a gestão dos seguintes processos de segurança:**
  - Monitoramento e Gerenciamento **remotos**
  - Recentemente alguns passaram a ofertar guarda de **logs** e **notificação** de eventos de segurança – **sem** gerenciar ou monitorar**.**
- Um típico MSSP **NÃO** oferta:
  - Implantação das **correções das vulnerabilidades** dos equipamentos **não gerenciados**
  - **Recuperação dos desastres** gerados pelos incidentes.
- **Cliente** **autoriza mudanças** em configuração dos dispositivos sob gerência

Redução de custos da Infraestrutura tecnológica

- Sem diferença significativa nos custos relacionados aos **componentes de segurança**.

- A **redução de custo é grande** em ferramentas de back-office:
  - *trouble-tickets*, correlação de eventos, geradores de relatórios , portal-web, storage, backup-offline, etc...
  - O MSSP reduz o custo para o cliente final em função da **escala** e **compartilhamento** no uso destas ferramentas.

Processos Internos estruturados

– Sua organização tem o processo de **respostas à incidentes estruturado ?**

  - Se sim, será capaz de aproveitar todos os benefícios de um conhecimento mais rápido e profundo de potenciais incidentes de segurança.

  - **Não ter este processo** estruturado internamente **reduz os benefícios à empresa** quanto a contratação de um MSSP.

Experiência em Outsourcing

- Outsourcing = **abrir mão** de determinados controles em prol da **eficiência/eficácia** e da ***expertise*** oferecida pelo provedor de serviço.

- O Outsourcing de segurança traz, por vezes, o **sentimento de estar abrindo mão** de controles importantes da organização.

- Você já tem **experiência em outsourcing** de outras tarefas operacionais? ex, gerenciamento de redes, servidores –

⮱ então sua experiência tornará mais simples a tarefa de gerir um outsourcing da infraestrutura de segurança.

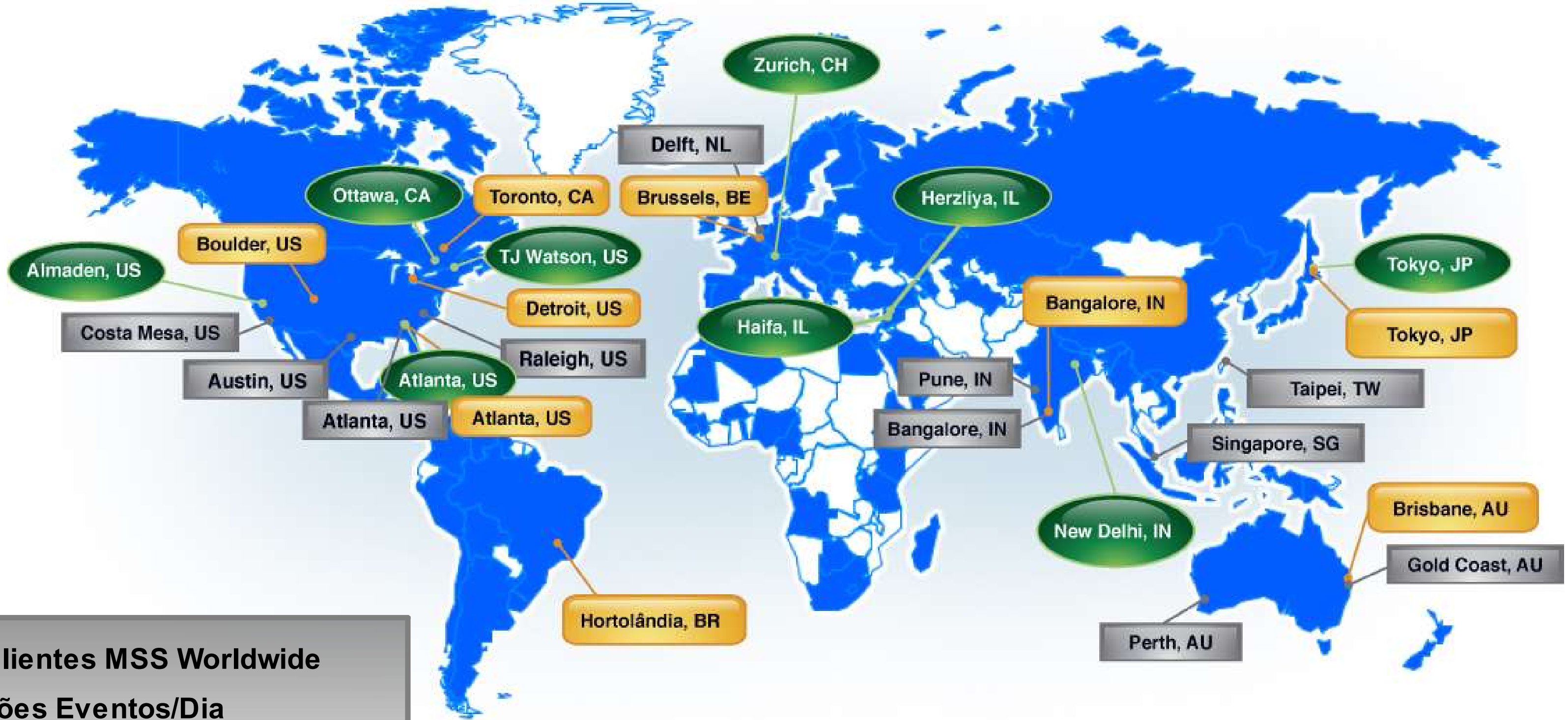
Outras importantes considerações…

- **Atencão**!! **Não** existe *SOC in a BOX* (apesar de alguns fornecedores de produtos SIEM tentarem te convencer disso…)
  - SOC é… **Pessoas** capacitadas + **Processos** bem definidos e testados + **Tecnologia**
  - Portanto: Ao comparar custos de MSS versus SOC interno, **pense nisso:**
    - Infra **Tecnológica**: Produto SIEM + HW + Serviços de implantação e customização + infra de DR
    - Definição e implantação de **processos**
    - Custos de **pessoal**: contratação + treinamento constante + retenção

Os Managed Security Services da IBM

Infraestrutura 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 Operação de Segurança



- +3,700 Clientes MSS Worldwide
- +13 Bilhões Eventos/Dia
- X-Force

Portfólio de Serviços MSS

CPE Managed Security Services

- Managed and Monitored 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 Management Services
- Secure Log Management Services
- IBM ISS X-Force® Threat Analysis Services
- Managed E-mail Security
- Managed Web Security

Suporte a distintos vendores e equipamentos

“Full-Services”

CPE Managed Security Services

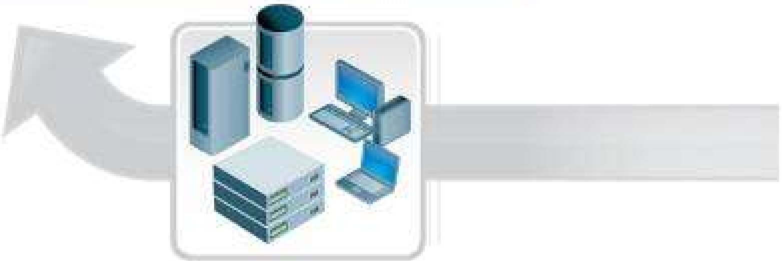
Managed and Monitored Firewall Services

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..)*
- *Monitoração de Eventos*
  - *Sistema AI+Analistas qualificados +Processos*
  - *Notificação de incidentes*
  - *SLAs*
- *Gerência das Plataformas*
  - *Updates e Patches*
  - *Backup Diário*
  - *Device Health e Disponibilidade*
- *Arquivamento de Logs por até 07 anos*
- *Consultas, relatórios , gráficos, Sistema de TT, informações de segurança no Portal Virtual-SOC*
- *Serviço 24/7/365*

Cloud Services

- Modelo **IaaS SaaS**
- **Vulnerability Mgmt Service (VMS)**
  - Internal & External Vulnerability Assessments
  - Vulnerability Remediation Workflow
- **Security Event & Log Management (SELM)**
  - Syslog, Universal Logging Agent (ULA)
  - On Site Aggregation, Compressão, Criptografia
  - Alertas Automatizados (SLA Select)
- **Email Security**
  - Anti-Virus, Anti-Spam, Content Protection
  - Sem instalação de HW/SW
- Inclui Serviço de informações de Segurança XFTAS

Cloud Security Services

Vulnerability Management Services

Security Event Management Services

Secure Log Management Services

IBM ISS X-Force® Threat Analysis Services

Managed E-mail Security

Managed Web Security

Modelos de Parceria Virtual SOC

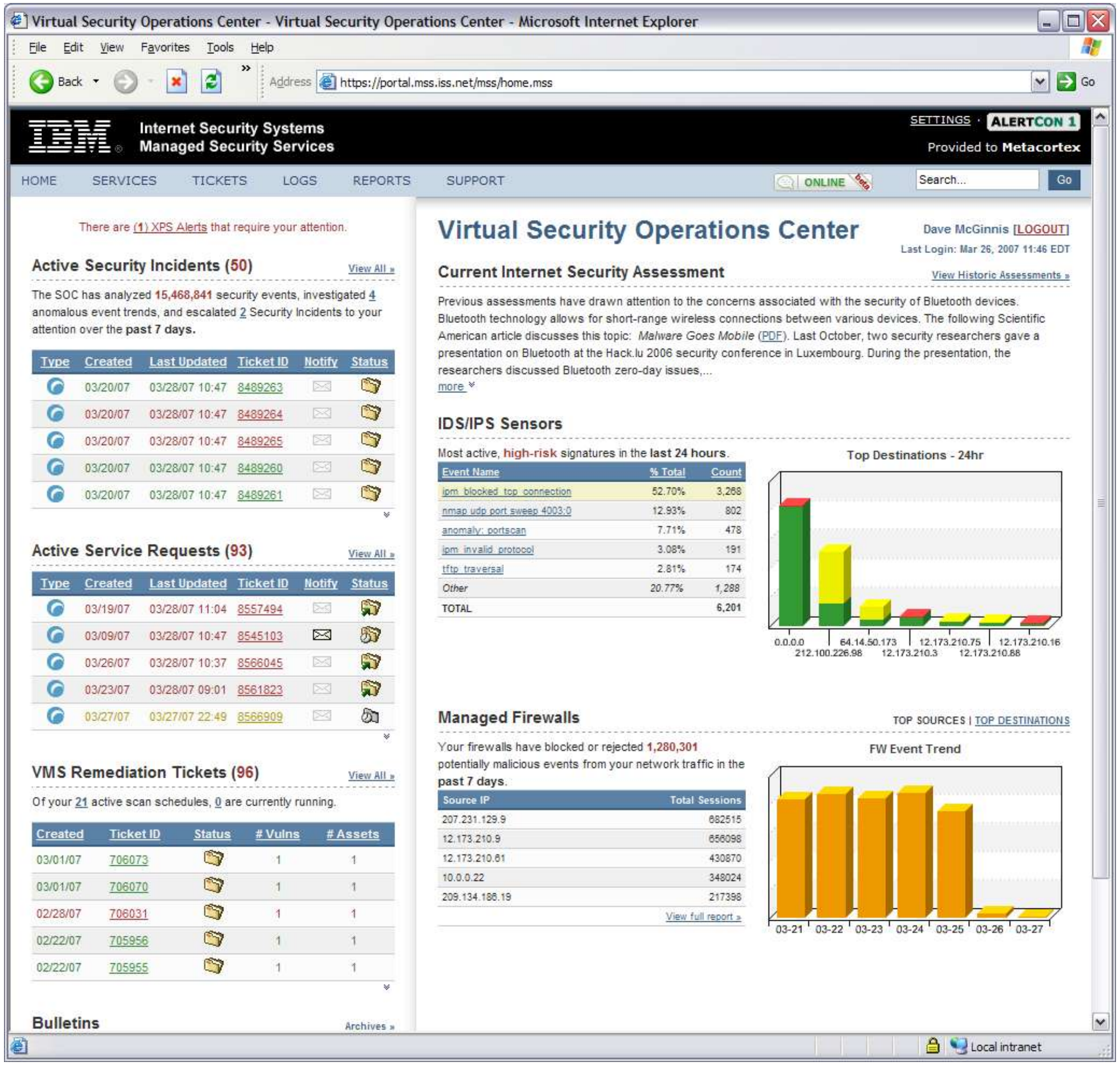
	Sales	Partner Sales Geo	Standard IBM Portfolio	Custom Portfolio	Co-branded Portal	Helpdesk (First Call)	Tier 1-3 Service Delivery	SOC Mgmt Systems	XPS Systems
Business Partner	Shared	In-Country	IBM	n/a	n/a	IBM	IBM	IBM	IBM Shared
MSS Integrated Alliance Partner	Partner	Global	Partner	Optional	Optional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

Visão Integrada e Centralizada

Portal Virtual-SOC

Portal Virtual SOC

- Visão Centralizada
- Visão Consolidada
- 100% web-based: nenhum equipamento no cliente


Virtual Security Operations Center - Virtual Security Operations Center - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address https://portal.mss.iss.net/mss/home.mss
Go
IBM
Internet Security Systems
Managed Security Services
SETTINGS · ALERTCON 1
Provided to Metacortex
HOME SERVICES TICKETS LOGS REPORTS SUPPORT
ONLINE beta
Search...
Go
Local intranet

There are (1) XPS Alerts that require your attention.

Active Security Incidents (50)

View All »

The SOC has analyzed 15,468,841 security events, investigated 4 anomalous event trends, and escalated 2 Security Incidents to your attention over the **past 7 days.**

Type	Created	Last Updated	Ticket ID	Notify	Status
	03/20/07	03/28/07 10:47	8489263	✉	
	03/20/07	03/28/07 10:47	8489264	✉	
	03/20/07	03/28/07 10:47	8489265	✉	
	03/20/07	03/28/07 10:47	8489260	✉	
	03/20/07	03/28/07 10:47	8489261	✉	

Active Service Requests (93)

View All »

Type	Created	Last Updated	Ticket ID	Notify	Status
	03/19/07	03/28/07 11:04	8557494	✉	
	03/09/07	03/28/07 10:47	8545103	✉	
	03/26/07	03/28/07 10:37	8566045	✉	
	03/23/07	03/28/07 09:01	8561823	✉	
	03/27/07	03/27/07 22:49	8566909	✉	

VMS Remediation Tickets (96)

View All »

Of your 21 active scan schedules, 0 are currently running.

Created	Ticket ID	Status	# Vulns	# Assets
03/01/07	706073		1	1
03/01/07	706070		1	1
02/28/07	706031		1	1
02/22/07	705956		1	1
02/22/07	705955		1	1

Bulletins

Archives »

Virtual Security Operations Center

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

Current Internet Security Assessment

View Historic Assessments »

Previous assessments have drawn attention to the concerns associated with the security of Bluetooth devices. Bluetooth technology allows for short-range wireless connections between various devices. The following Scientific American article discusses this topic: *Malware Goes Mobile* (PDF). Last October, two security researchers gave a presentation on Bluetooth at the Hack.lu 2006 security conference in Luxembourg. During the presentation, the researchers discussed Bluetooth zero-day issues,...
more

IDS/IPS Sensors

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

Event Name	% Total	Count
ipm_blocked_tcp_connection	52.70%	3,268
nmap udp port sweep 4003:0	12.93%	802
anomaly: portscan	7.71%	478
ipm_invalid_protocol	3.08%	191
tftp_traversal	2.81%	174
Other	*20.77%*	*1,288*
TOTAL		6,201

Top Destinations - 24hr

Managed Firewalls

TOP SOURCES | TOP DESTINATIONS

Your firewalls have blocked or rejected 1,280,301 potentially malicious events from your network traffic in the **past 7 days**.

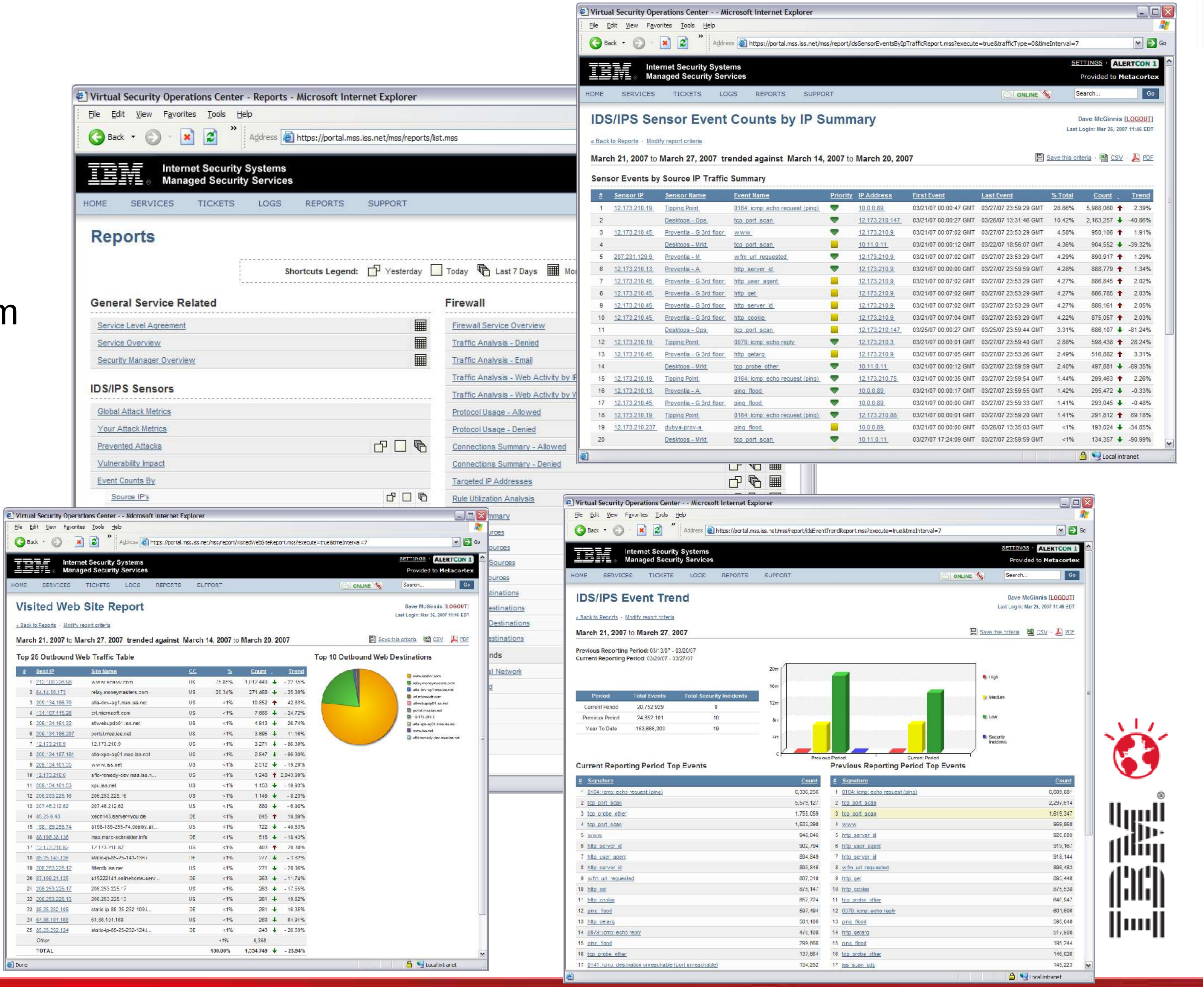
Source IP	Total Sessions
207.231.129.9	682515
12.173.210.9	656098
12.173.210.61	430870
10.0.0.22	348024
209.134.186.19	217398

View full report »

FW Event Trend

Relatórios

- Mais de 20 tipos de **relatórios**
- Podem ser gerados em HTML, CSV e PDF



Virtual Security Operations Center - - Microsoft Internet Explorer

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

IBM Internet Security Systems Managed Security Services — SETTINGS · ALERTCON 1 — Provided to Metacortex

HOME · SERVICES · TICKETS · LOGS · REPORTS · SUPPORT · ONLINE · Search... · Go

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-prov-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%
20		Desktops - Mrkt	tcp_port_scan	▼	10.11.0.11	03/27/07 17:24:09 GMT	03/27/07 23:59:59 GMT	<1%	134,357 ↓	-90.99%

Local intranet

Virtual Security Operations Center - Reports - Microsoft Internet Explorer

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

IBM Internet Security Systems Managed Security Services

HOME · SERVICES · TICKETS · LOGS · REPORTS · SUPPORT

Reports

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

General Service Related

- Service Level Agreement
- Service Overview
- Security Manager Overview

IDS/IPS Sensors

- Global Attack Metrics
- Your Attack Metrics
- Prevented Attacks
- Vulnerability Impact
- Event Counts By
  - Source IP's

Firewall

- Firewall Service Overview
- Traffic Analysis - Denied
- Traffic Analysis - Email
- Traffic Analysis - Web Activity by IP
- Traffic Analysis - Web Activity by W
- Protocol Usage - Allowed
- Protocol Usage - Denied
- Connections Summary - Allowed
- Connections Summary - Denied
- Targeted IP Addresses
- Rule Utilization Analysis
- mmary
- urces
- ources
- Sources
- ources
- tinations
- estinations
- Destinations
- estinations
- nds
- l Network
- d

Virtual Security Operations Center - - Microsoft Internet Explorer

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

IBM Internet Security Systems Managed Security Services — SETTINGS · ALERTCON 1 — Provided to Metacortex

HOME · SERVICES · TICKETS · LOGS · REPORTS · SUPPORT · ONLINE · Search... · Go

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 ↓	- 72.35%
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 ↑	42.33%
4	131.107.115.28	crl.microsoft.com	US	<1%	7,666 ↓	- 24.72%
5	209.134.161.32	allwebupdp01.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	sflc-remedy-dev.mss.iss.n...	US	<1%	1,240 ↑	2,943.90%
11	209.134.161.53	xpu.iss.net	US	<1%	1,150 ↓	- 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	85.25.6.43	xeon143.server4you.de	DE	<1%	845 ↑	10.59%
15	198.189.255.74	a198-189-255-74.deploy.ak...	US	<1%	722 ↓	- 40.53%
16	66.198.36.136	max.marc-schneider.info	DE	<1%	518 ↓	- 18.43%
17	12.173.210.82	12.173.210.82	US	<1%	403 ↑	70.30%
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 · Local intranet

Virtual Security Operations Center - - Microsoft Internet Explorer

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

IBM Internet Security Systems Managed Security Services — SETTINGS · ALERTCON 1 — Provided to Metacortex

HOME · SERVICES · TICKETS · LOGS · REPORTS · SUPPORT · ONLINE · Search... · Go

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	153,686,303	19

Current Reporting Period Top Events

#	Signature	Count
1	0104: icmp: echo request (ping)	6,330,256
2	tcp_port_scan	5,579,127
3	tcp_probe_other	1,755,059
4	tcp_port_scan	1,523,398
5	www	940,046
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	0104: icmp: echo request (ping)	6,009,001
2	tcp_port_scan	2,297,614
3	tcp_port_scan	1,619,347
4	www	969,868
5	http_server_id	920,009
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

Benefícios claros!

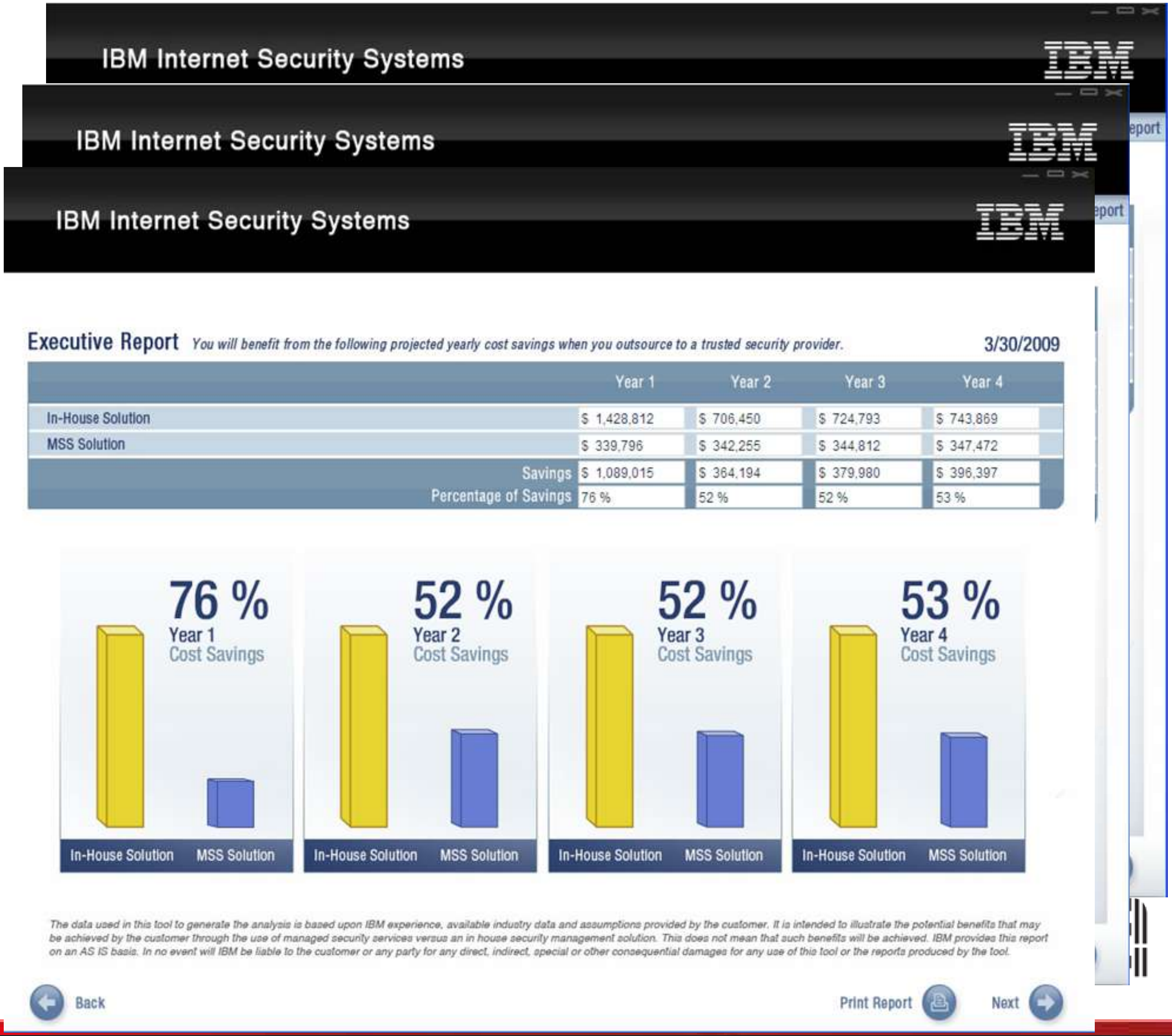
- *Resultados para o Negócio*

  - **Integrando** o ambiente *multi-vendor*
  - **Visão centralizada** em tempo-real.
  - Mostrando rapidamente o retorno do investimento
    - **baixo custo** de implantação
    - **curtíssimo tempo** de implantação

Benefícios claros!

- ***Redução de Custos***
  - Evitando ***investimento*** em recursos e tecnologias adicionais
  - Reduzindo os ***custos*** operacionais
  - Reduzindo ***perdas*** por incidentes de segurança

Use o 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.

Se não lembrar de mais nada…

Redução de Custos

Simplificação da gestão de infraestrutura complexa

Proteção do seu negócio / marca / reputação

Obrigado!

Fernando Guimarães

feguima@br.ibm.com

Referências:

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