



IBM Security Forum
Soluções para um ambiente seguro

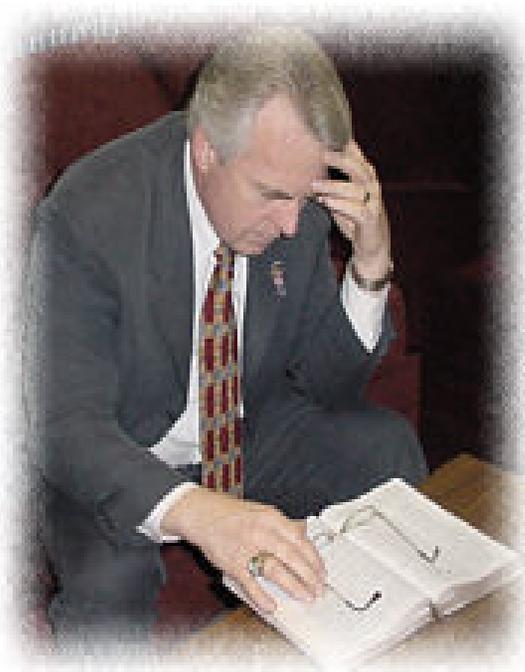
Managed Security Services
Reduzindo custos operacionais de segurança de
forma garantida e eficaz

Fernando Guimarães – MSS Global Architect
feguima@br.ibm.com



AGENDA

- Os Desafios dos Gestores de Segurança da Informação
- Os Serviços Oferecidos pela IBM ISS
- Como o MSS da IBM ISS pode lhe ajudar
- Portal Virtual-SOC



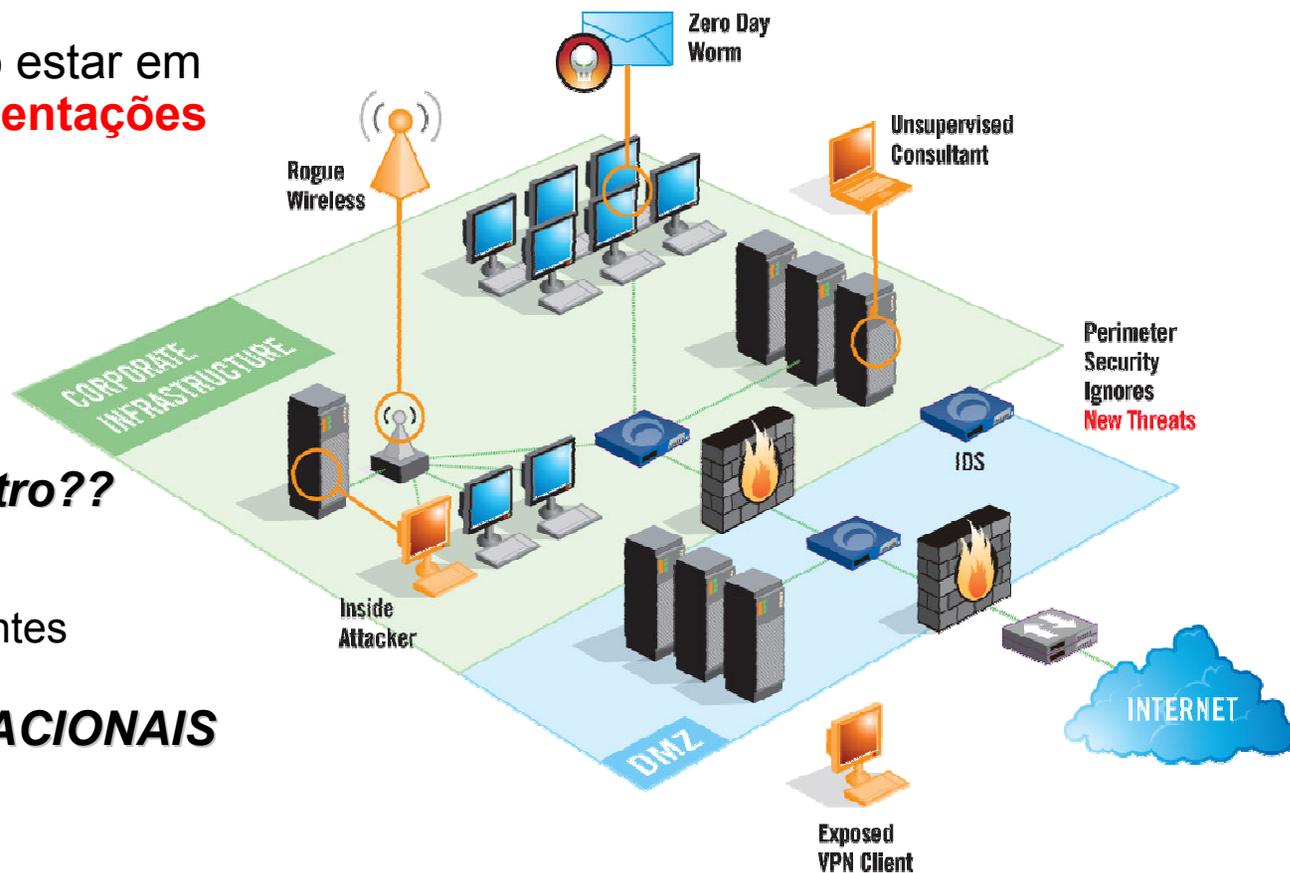
Os Desafios dos Gestores de Segurança da Informação





O Ambiente Atual de Segurança da Informação

- Ambiente **complexo** = **Altos custos** de gerenciamento/monitoração
- Riscos crescentes por não estar em conformidade com **regulamentações**



Onde foi parar o perímetro??

- **VPN's**, Wireless
- Terceiros, parceiros, clientes

MUDANÇAS ORGANIZACIONAIS

- Novos negócios, novas aplicações
- **Fusões** e aquisições



Muita coisa para tratar...

Ambiente **Multi-Vendor**

- ISS, CheckPoint, Cisco, Juniper, Symantec, McAfee, TrendMicro, 3com and more...

Operações **Distribuídas**

- Recursos distribuídos, escritórios remotos, equipes remotas.

Sobrecarga de Informações...Logs e Eventos de Segurança

- Firewalls & IDS/IPS
 - Facilmente mais de 10GB de dados por semana
 - Podem gerar centenas de alertas em 1 único dia





Tenho que Gerenciar e Monitorar isso Tudo!

Custos Altos

- Requer cobertura 24x7x365 (6 – 9 técnicos por posto)
- Requer ferramentas sofisticadas (**e caras!!**) para análise precisa das ameaças
- Requer boas instalações físicas e sistemas de suporte redundantes

Requer Equipe com Skills sofisticados e constantemente treinada

- Analistas capacitados para detecção e investigação de incidentes
- Analistas preparados para responder e resolver emergências
- Treinamento e política de retenção contínua

Inteligência

- Conhecimento das últimas ameaças, virus, worms, etc...
- Compreensão dos mais sofisticados métodos de ataque
- PESQUISA, PESQUISA, PESQUISA...





Você Conhece esta Empresa ?

- **Não instalou** todos os produtos de segurança adquiridos no último ano.
- Possui **recursos limitados** para operar seu ambiente de segurança.
- Não possui equipe e/ou **capacitação** para gerenciar a solução de segurança recém adquirida.
- Quer **focar sua equipe** de segurança de TI em projetos/atividades estratégicas.
- Está sendo pressionada pela alta gerência para:
 - **Mostrar rapidamente o valor** dos investimentos feitos em segurança.
 - **Redução** imediata dos **custos** de operação de TI
- Precisa aderir às **regulamentações**.



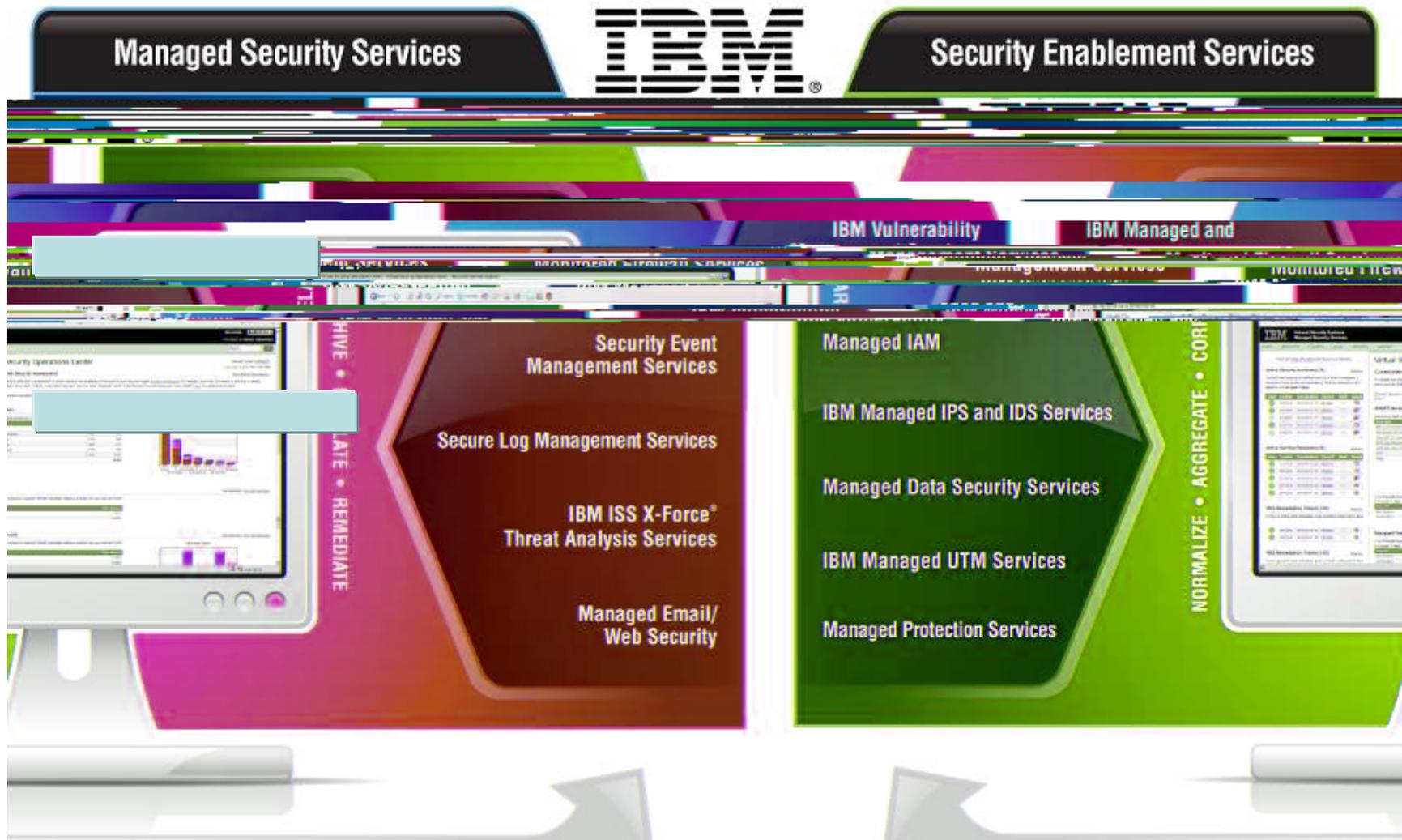


Os Serviços de Gerenciamento de Segurança “MSS” da IBM ISS





Virtual Security Operations Center (VSOC)





Abrangência e Expertise Global





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

IBM Internet Security Systems Managed Security Services

ALERTCON 3

Virtual Security Operations Center

Current Internet Security Assessment

IDS/IPS Sensors

Managed Firewalls

Bulletins

Type	Created	Last Updated	Ticket ID	Notify	Status
...	03/29/07	03/29/07 16:47	0438703
...	03/29/07	03/29/07 16:47	0438704
...	03/29/07	03/29/07 16:47	0438705
...	03/29/07	03/29/07 16:47	0438706
...	03/29/07	03/29/07 16:47	0438707

Type	Created	Last Updated	Ticket ID	Notify	Status
...	03/29/07	03/29/07 14:34	0337484
...	03/29/07	03/29/07 16:47	0438708
...	03/29/07	03/29/07 16:37	0399345
...	03/29/07	03/29/07 16:37	0438709
...	03/29/07	03/29/07 22:48	0399348

Device	Asset ID	Status	IP Value	IP Source
0301001	0300001	...	1	1
0301002	7000000	...	1	1
0301003	0300001	...	1	1
0301004	7000000	...	1	1
0301005	0300001	...	1	1

Item	Count	Value
Unlabeled Registration	17,125	3,268
Unlabeled users IP ID	17,000	8,000
Unlabeled users	1,175	4,18
Unlabeled users	3,000	700
Unlabeled users	17,000	7,14
TOTAL	38,300	13,062

Source IP	Total Sessions
207.231.120.0	68215
12.172.212.0	68626
12.172.212.81	43072
12.2.0.22	14024
207.174.186.12	21726



Portal Ticket Manager

- Sistema de **Trouble-ticket** integrado
- Usado tanto para comunicação com o **SOC** quanto para uso **interno** do cliente

The screenshot displays the Portal Ticket Manager interface. At the top, there is a navigation bar with links for HOME, SERVICES, TICKETS, LOGS, REPORTS, and SUPPORT. A search bar is located on the right. The main content area is divided into several sections:

- Custom Query:** A sidebar on the left with filters for Ticket ID, Customer Ticket ID, Ticket Type (All), Start Date (05/02/2006), End Date (05/02/2006), and Timezone (EST).
- Security & Service Related Tickets:** A central dashboard showing 'Open Security Incidents' and 'Open Service Requests' in table format.

Type	Date/Time	Ticket ID	Issue	Event Name	Last Modified Date	Status	Priority	Rpt.
SI - Security Incident	04/29/06 22:11	0701738	SI - Security Incident		05/01/06 15:53	Open	Low	
SI - Security Incident	04/29/06 21:05	0701737	SI - Security Incident		04/30/06 08:33	Open	Low	
SI - Security Incident	04/29/06 00:39	0701705	SI - Security Incident		04/29/06 09:13	Open	Low	
SI Suspicious Activity	01/25/05 16:53	7113867	SI Suspicious Activity			Open	Low	
- VMS Remediation Tickets:** A section at the bottom of the dashboard with a similar table structure.
- Ticket Details:** A large panel on the right showing the details of a selected ticket (Ticket Number: 0701737).
 - Service Ticket:** Includes fields for Assigned To (Tom Anderson), Created On (04/29/06 21:05), Last Modified On (04/30/06 08:33), File Attachments (0 files), Status (New), Resolution (), Priority (Low), and Notification Status (No).
 - Issue Details:** Reason for Escalation: 'The XPS Alert System has detected anomalous activity on one of your sensors.' Issue Code: 'SI - Security Incident', Device Name: 'meta-portal-mids1 (proventia-0)'. Includes fields for Attack Name, Src. IP, and Dest. IP.
 - Alert Issue:** Sweeps Alert, Alert Status: Normalized.
 - AI Analysis Period:** Apr 29, 2006 20:00 EDT to Apr 29, 2006 20:59 EDT.
 - Sensor Profile:** A table showing activity levels for various sensors.

	Baseline Profile	Current Hour 00:00 - 00:59	Previous Hour 23:00 - 23:59	Four Hour 20:00 - 23:59
Low	31426	94098	5812	5815
Medium	10700	36103	2924	2919
High	0	0	0	0
Total	42126	130201	8736	8734
 - Trigger Explanation:** 'Alert triggered due to a statistical deviation in activity for the Current Hour compared to the Previous Hour. Sweeps events increased by 2,100,700%'.
 - Event Analysis Report:** Apr 29, 2006 16:00 EDT to Apr 29, 2006 20:59 EDT.



Informação na ponta dos dedos

HOME SERVICES TICKETS LOGS REPORTS SUPPORT SEARCH: Go

Active Analyzer - Event Name View Dave McGinnis [\[LOGOUT\]](#)
Last Login: May 03, 2006 09:33 EDT

[Go to Default View](#) · [Modify query criteria](#) Selected view: **Event Name View** ▼

May 03, 2006 13:00:00 to May 03, 2006 14:48:06 [Auto-refresh](#) · [Refresh now](#)

Event Name	Priority ▲	%	Count	Sources	Destinations	First Event	Last Event
IPM_Blocked_TCP_Connection	▲	<1%	2,210	2	19	05/03/06 01:30:49 GMT	05/03/06 02:21:50 GMT
Nmap_UDP_Port_Sweep_4003:0	▲	<1%	760	1	26	05/03/06 01:25:51 GMT	05/03/06 01:34:04 GMT
SQL_SSRP_Slammer_Worm	▲	<1%	252	65	62	05/03/06 00:02:54 GMT	05/03/06 14:32:55 GMT
IPM_Invalid_Protocol	▲	<1%	234	1	1	05/03/06 01:01:32 GMT	05/03/06 01:20:25 GMT
UDP_Port_Sweep_4001:0	▲	<1%	124	1	24	05/03/06 01:25:59 GMT	05/03/06 01:38:45 GMT
Tftp_Passwd_File_5509:0	▲	<1%	75	1	23	05/03/06 01:29:21 GMT	05/03/06 01:37:43 GMT
SQL_SSRP_StackBo	▲	<1%	53	33	39	05/03/06 00:12:24 GMT	05/03/06 14:28:40 GMT
SSH_Deattack_IO	▲	<1%	48	1	26	05/03/06 01:35:44 GMT	05/03/06 02:22:52 GMT
Email_Pipe	▲	<1%	43	1	1	05/03/06 01:29:17 GMT	05/03/06 01:33:10 GMT
TFTP_Passwd_File	▲	<1%	34	1	9	05/03/06 01:36:10 GMT	05/03/06 01:42:11 GMT
TFTP_Traversal	▲	<1%	34	1	9	05/03/06 01:36:10 GMT	05/03/06 01:42:11 GMT
SSH_Brute_Force	▲	<1%	28	2	9	05/03/06 00:01:17 GMT	05/03/06 01:40:42 GMT
Cisco_TFTPD_Directory_Traversal.5510:0	▲	<1%	23	1	23	05/03/06 01:29:21 GMT	05/03/06 01:37:31 GMT
Syphillis_Scan_Request	▲	<1%	15	1	14	05/03/06 01:39:35 GMT	05/03/06 01:55:40 GMT
Win_MessengerPopup_Bo	▲	<1%	15	1	14	05/03/06 01:39:02 GMT	05/03/06 01:48:55 GMT
Telnet_Linker_Bug	▲	<1%	14	1	2	05/03/06 01:29:51 GMT	05/03/06 01:29:52 GMT
TCP_Hijack_3250:0	▲	<1%	11	4	5	05/03/06 00:51:12 GMT	05/03/06 14:03:09 GMT
Dtspcd_Overflow	▲	<1%	10	1	1	05/03/06 01:35:50 GMT	05/03/06 01:35:51 GMT
FW1_Auth_As_Local	▲	<1%	8	1	6	05/03/06 01:39:28 GMT	05/03/06 02:21:28 GMT
MSRPC_RemoteActivate_Bo	▲	<1%	8	1	1	05/03/06 01:34:34 GMT	05/03/06 01:34:34 GMT
LPRng_Format_String	▲	<1%	5	1	1	05/03/06 01:34:44 GMT	05/03/06 01:34:45 GMT
statd_dot_dot_6188:0	▲	<1%	3	1	3	05/03/06 01:31:36 GMT	05/03/06 01:36:31 GMT
SMB_Samba_Transaction2_bo	▲	<1%	1	1	1	05/03/06 01:38:38 GMT	05/03/06 01:38:38 GMT

- Visualização de eventos em **REAL-TIME**



Consultas históricas dos logs armazenados

- Armazenamento por até **07 anos !!**

Virtual Security Operations Center Log Query Microsoft Internet Explorer

Internet Security Systems
Managed Security Services

Log Query

Query Criteria

1. Date/Time

2. Devices Included in Query

3. Log Types

4. Options

5. Full Text Search

K. Filter

NOTE: Separate multiple filters with commas (e.g., "192.168.1.1, 192.168.0.2")

Action

Source IP

Destination IP

Protocol

Port

Firewall

IDS/IPS

Event Type

Log per page

Row per page

Sort Type

Search Query



*Como o MSS da IBM ISS
pode lhe ajudar*



Como podemos ajudá-lo

Resultados para o Negócio

- **Integrando** seu ambiente *multi-vendor* e provendo uma **visão centralizada** de suas condições de segurança em tempo-real.
- Auxiliando na **conformidade** com regulamentações
 - Cobre 6 das 12 categorias PCI: Install firewalls, protect stored data, encrypt data, restrict data access, track and monitor access, test system regularly.
- Mostrando rapidamente o retorno do investimento – **baixo custo** de implantação / **curtíssimo tempo** de implantação
- Protegendo sua **marca/reputação**





Como podemos ajudá-lo

Redução de Custos

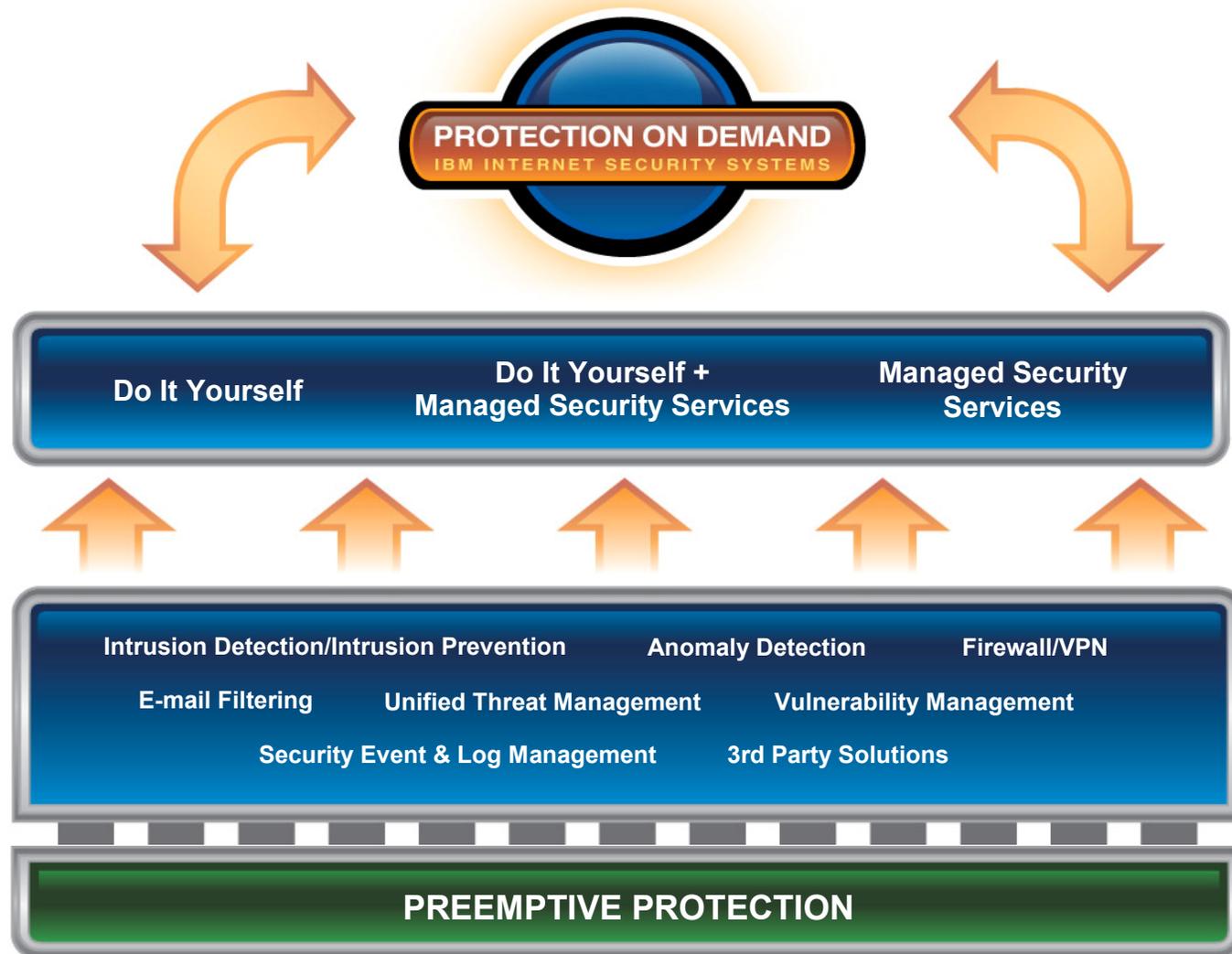
- Evitando **investimento** em recursos e tecnologias adicionais
- Reduzindo seu **custos** operacionais
- Reduzindo **perdas** por incidentes de segurança





Proteção *On Demand*

- **Flexibilidade**
- **Modularidade**
- **Otimização dos custos** de contratação





Obrigado!

IBM Security Forum
Soluções para um ambiente seguro

Fernando Guimarães
feguima@br.ibm.com



Exemplos PCI

- PCI 1.1.1 - A formal process for approving and testing all external network connections and changes to the firewall configuration – **Managed Firewall Service**
- PCI 6.2 - Establish a process to identify newly discovered security vulnerabilities. **Vulnerability Management Service, X-Force Threat Analysis Service**
- Implement automated audit trails for all system components to reconstruct:
 - PCI 10.2.4 - Invalid logical access attempts. **Security Event & Log Management Service (SELM)**
 - PCI 10.2.7 - Creation and deletion of system-level objects. **SELM Service**