

Nova Prestech.net

Consultoria e Soluções em Informática

The logo consists of the letters 'GTS' in a bold, red, sans-serif font. Each letter has a white outline and a slight drop shadow, giving it a 3D appearance.

Gerenciamento de Segurança da Informação com Software Livre

<http://www.prestech.com.br>

Victor Batista da Silva Santos

victor@prestech.com.br

+55 21 8762-6977

+55 21 3622-1600

Rua Francisco Manuel 99/A

Benfica – Rio de Janeiro, RJ

Fax: (21) 3860-7510

CEP 20911-270

Agenda:

- Conceitos
- Motivação
- Técnicas e Ferramentas
- Conscientização
- Conclusão

Confidencialidade

- Assegurar que a informação é acessível somente por aqueles devidamente autorizados

Integridade

- Salvaguardar a veracidade e complementariedade da informação bem como os seus métodos de processamento

Disponibilidade

- Assegurar que quem devidamente autorizado tem acesso á informação e bens associados sempre que necessário

Uma novo olhar sobre a Segurança da Informação

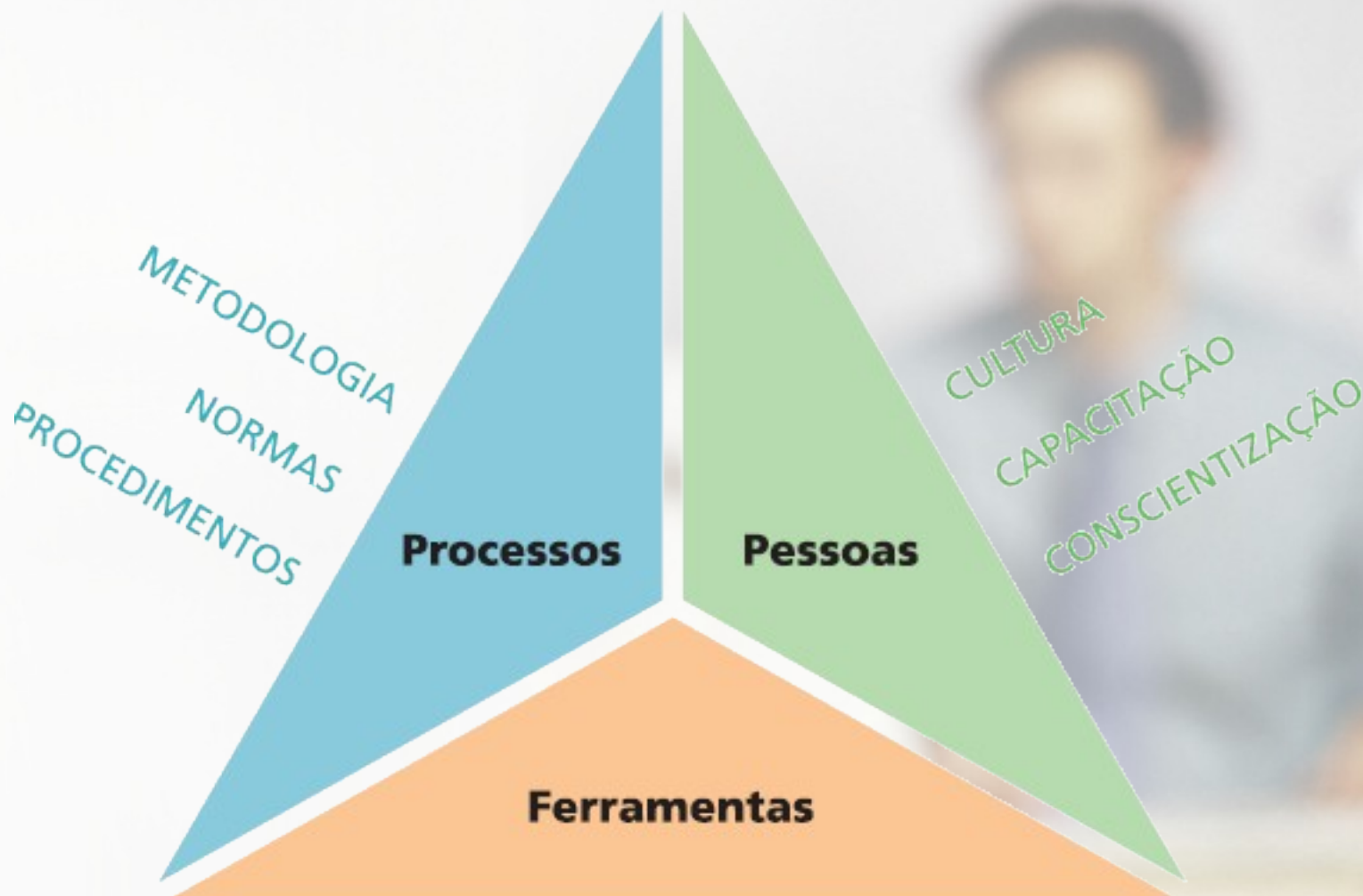
Mudança de abordagem



Nova Prestech.net

GTS

Framework de Segurança da Informação



RECURSOS FÍSICOS E LÓGICOS

Pessoas: O elo fraco da Segurança da Informação

- Palestras Educativas
- Ciclo de treinamentos
- Cartilhas de Segurança
- Cartazes

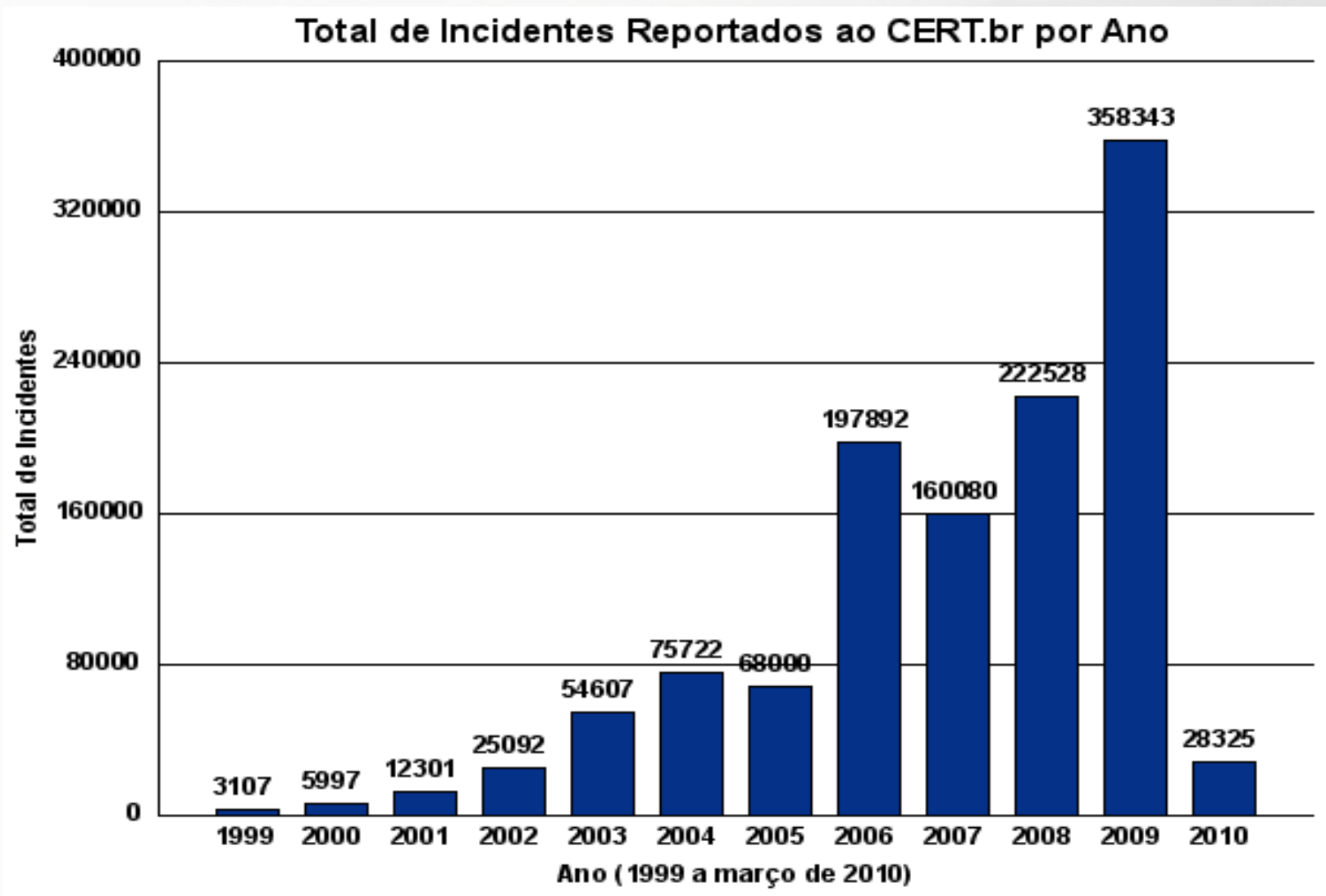
Processos: O Controle de Segurança da Informação

- Política de Segurança da Informação
- Política de Uso Aceitável
- Adequação a Normas de Segurança: 27001 e 27002

Ferramentas: Mecanismos de Proteção

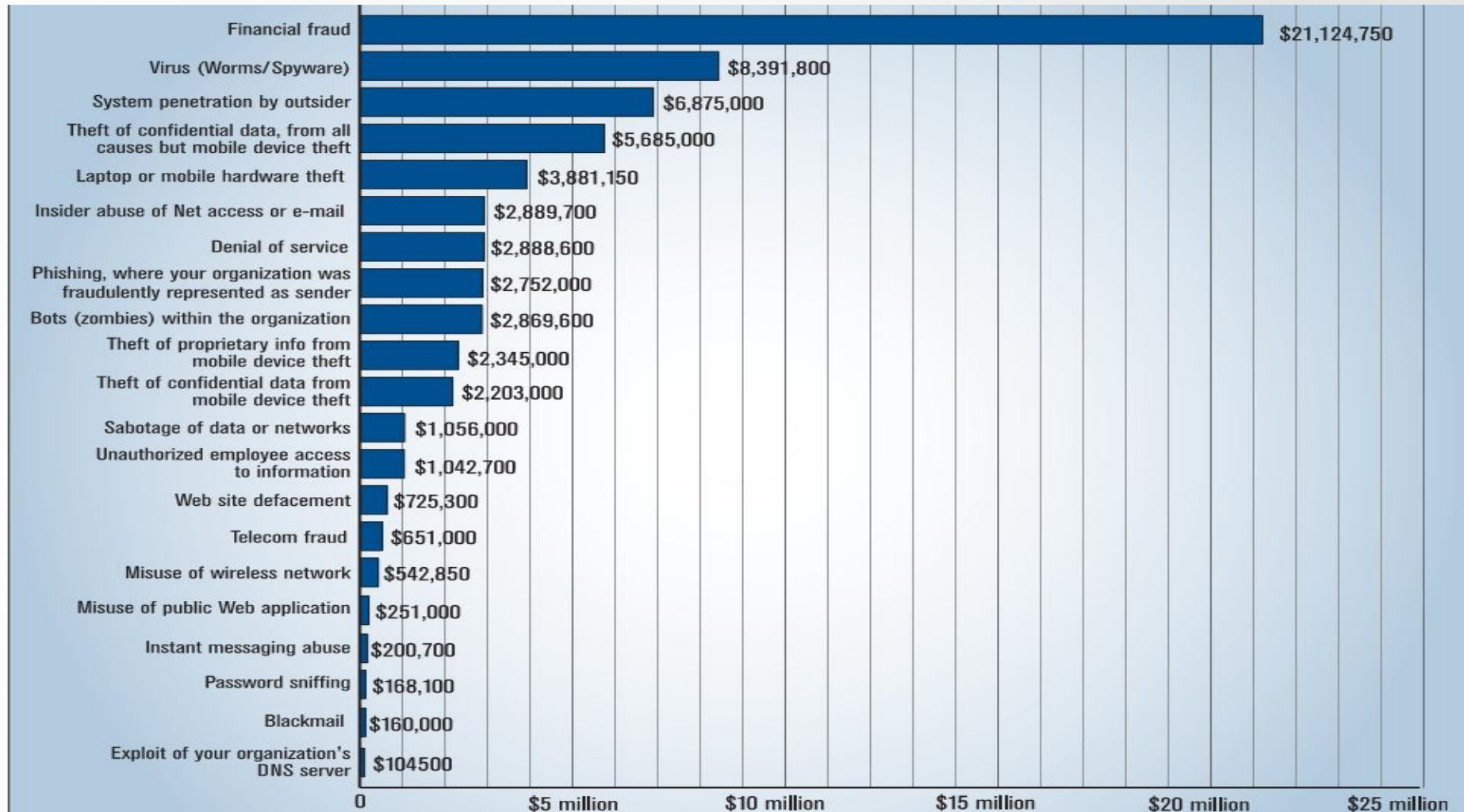
- Identificação/Autenticação
- Controle de acesso
- Hardening de Servidores
- Proteção de Perímetro
- Sistemas de Detecção de Intrusão
- Auditoria e Análise de Vulnerabilidades

Motivação





Motivação



Incidentes de segurança :

- Impactam diretamente na receita das Organizações
- Abalam a confiança dos clientes
- Afetam negativamente o relacionamento com parceiros

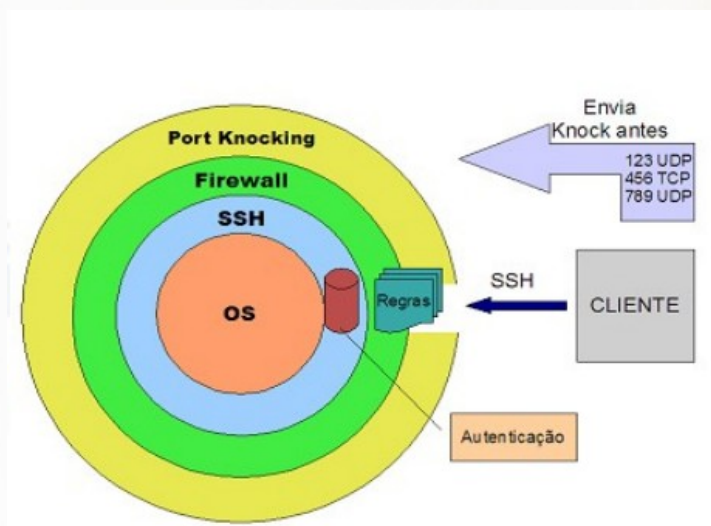
Norma que apresenta uma guia de boas práticas em segurança da informação, orientando e apresentando recomendações para implementações de controles.

BS7799 – ISO/IEC 17799 – ISO/IEC 27002

- Escolha do sistema e particionamento
- Instalação segura do sistema
- Patch's de Segurança
- Controle de acesso em sistemas de arquivos
- Controle de acesso de usuários
- Registro de logs do sistema
- Ajustes do Kernel

Identificação/Autenticação

- Controle de privilégios (**PAM – su**)
- OTP - One Time Password (**opie**)
- Senhas diferentes por serviço (**PAM – dotfile**)
- TCPWrappers (**hosts.deny, hosts.allow**)
- Port Knockig (**Knockd / Fwknop**)

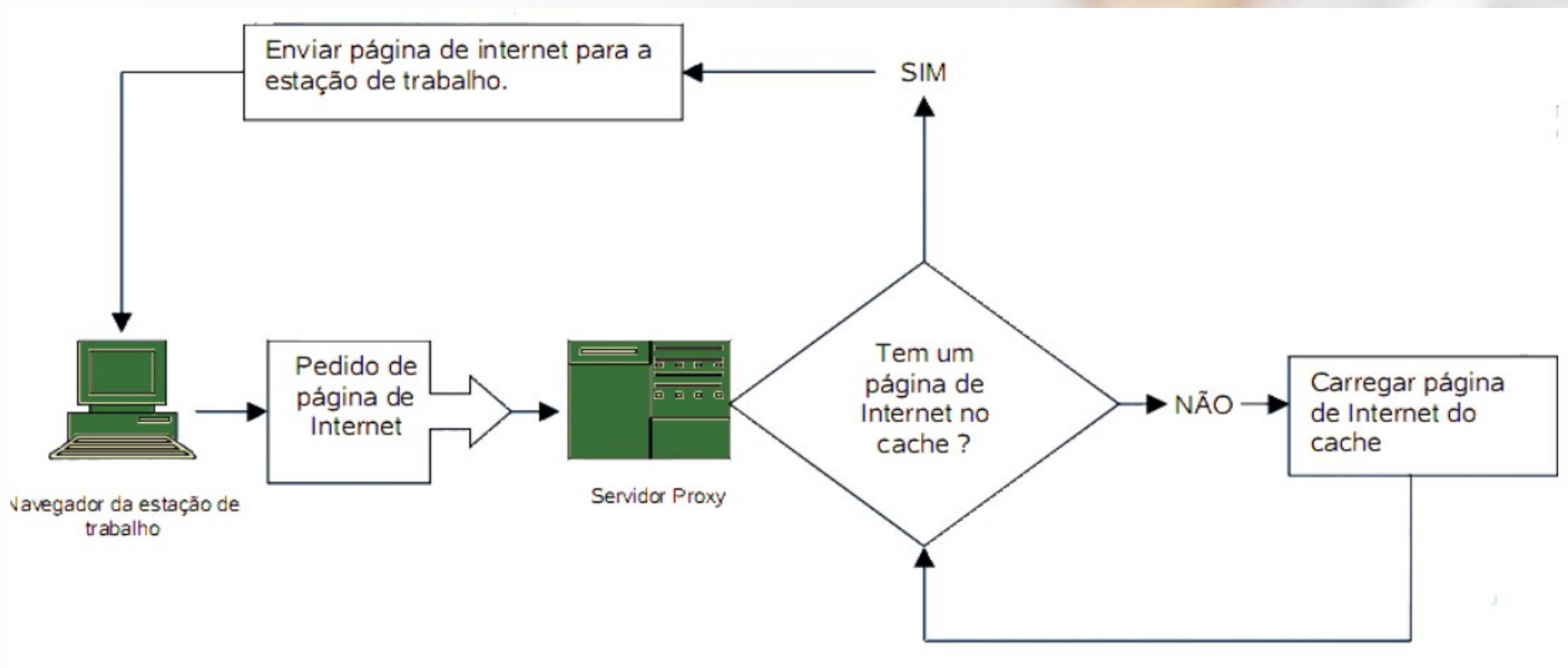


- Controle de Permissões (**chmod e chown**)
- Definição de Atributos Especiais (**chattr**)
- Listas de Controle de Acesso (**ACL Posix**)
- Conexão remota criptografada (**OpenSSH - SShTEST**)
- Política de Senhas e acesso a recursos (**PAM**)

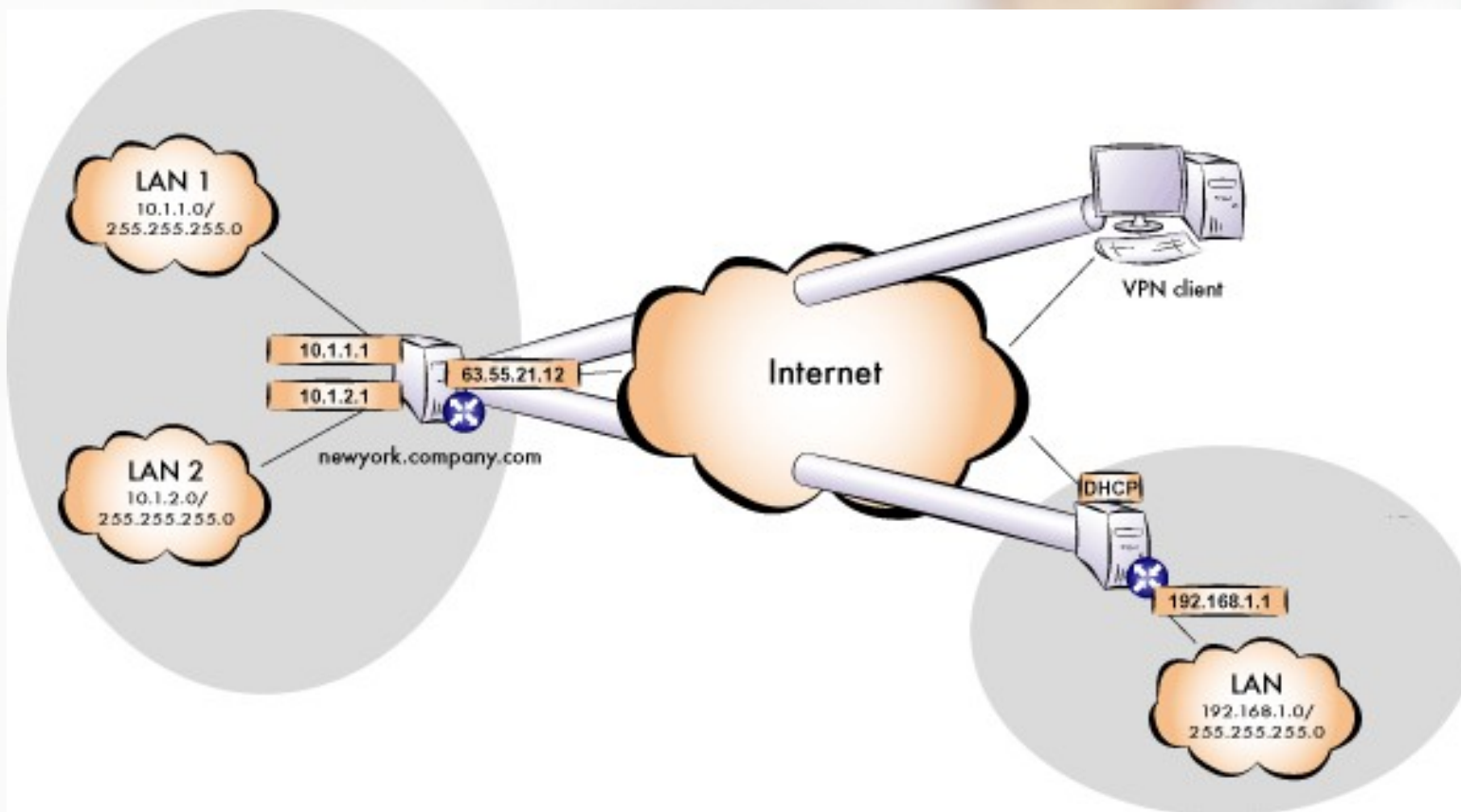
Controle de Tráfego (**Firewall – Iptables**):

- iptables -A INPUT, OUTPUT, FORWARD
--source IP/MASCARA (-s, --src)
--sport PORTA
--destination (-d, --dst)
--dport
--protocol TCP, UDP
-m (--state, --multiport, etc)
-j ACCEPT, DENY

Controle de Conteúdo Web (Proxy – Squid):



Rede Virtual Privada (VPN – OpenVPN):



Snort:

- Análise de tráfego em tempo real
- Registro de Pacotes IP
- Análise de Protocolo
- Notificação de alertas em tempo real
- Baseado em regras e assinaturas



OSSEC:

- Análise de logs
- Verificação de integridade do sistema
- Detecção de Rootkits
- Alerta e resposta ativa (Regras de Firewall – TCP Wrappers)
- Monitoramento de registros do Windows



Nagios:

- Monitoramento de Serviços de rede e recursos de servidores
- Facilidade no desenvolvimento de plugins
- Gera Gráficos e Estatísticas de monitoramento
- Definição de Hierarquia
- Alerta em Tempo Real

Nagios - Microsoft Internet Explorer

Address: /nagios/

Google Search Web 141 blocked Options

Current Network Status

Last Updated: Tue Jul 6 11:22:11 CEST 2004
 Updated every 90 seconds
 Nagios@ - www.nagios.org
 Logged in as: *bingel*

[View History For all hosts](#)
[View Notifications For All Hosts](#)
[View Host Status Detail For All Hosts](#)

Host Status Totals

Up	Down	Unreachable	Pending
15	2	0	0

All Problems	All Types
2	17

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
29	1	1	4	0

All Problems	All Types
6	35

Service Status Details For All Hosts

Host	Service	Status	Last Check	Duration	Attempt	Status Information
bart	Diskusage_C.	OK	2004-07-06 11:10:19	20d 0h 7m 26s	1/3	C:\ - total: 3.91 Gb - used: 2.62 Gb (67%) - free 1.28 Gb (33%)
	Diskusage_D.	WARNING	2004-07-06 11:14:13	20d 0h 7m 20s	3/3	D:\ - total: 29.99 Gb - used: 26.78 Gb (89%) - free 3.20 Gb (11%)
	HTTP	OK	2004-07-06 11:21:41	14d 1h 37m 47s	1/3	HTTP ok: HTTP/1.1 200 OK - 0.027 second response time
	MS-Exchange	OK	2004-07-06 11:20:58	20d 0h 8m 6s	1/3	All services are running
	SMTP	OK	2004-07-06 11:21:33	22d 1h 53m 13s	1/3	SMTP OK - 0 second response time
cixten	Diskusage_C.	OK	2004-07-06 11:19:45	0d 22h 2m 24s	1/3	C:\ - total: 39.06 Gb - used: 8.01 Gb (21%) - free 31.05 Gb (79%)
	Terminalserver Sessions	OK	2004-07-06 11:18:01	0d 22h 29m 13s	1/3	11
ftp.sunet.se	PING	OK	2004-07-06 11:21:30	0d 0h 31m 24s	1/10	PING OK - Packet loss = 0%, RTA = 36.37 ms
haubits	PING	OK	2004-07-06 11:21:21	193d 8h 33m 3s	1/10	PING OK - Packet loss = 0%, RTA = 1.36 ms
itknsqw1	PING	OK	2004-07-06 11:21:21	56d 22h 30m 57s	1/10	PING OK - Packet loss = 0%, RTA = 6.10 ms
	if-traffic	OK	2004-07-06 11:21:20	63d 18h 45m 23s	1/10	OK: rate[IN]=250 kbit/s OK: rate[OUT]=286 kbit/s
itknsqw2	PING	CRITICAL	2004-04-20 12:39:00	77d 20h 45m 1s	10/10	PING CRITICAL - Packet loss = 100%
	if-traffic	UNKNOWN	2004-04-20 12:39:00	77d 20h 45m 1s	10/10	check_snmp_counter: ERROR during get-request: No response from remote host '62.119.68.186'
jasper	Diskusage_C.	OK	2004-07-06 11:15:46	77d 1h 13m 47s	1/3	C:\ - total: 4.00 Gb - used: 2.99 Gb (75%) - free 1.01 Gb (25%)
	Diskusage_E.	OK	2004-07-06 11:20:41	140d 1h 3m 7s	1/3	E:\ - total: 4.00 Gb - used: 1.46 Gb (36%) - free 2.54 Gb (64%)
	MS-Exchange	OK	2004-07-06 11:21:41	61d 22h 57m 53s	1/3	All services are running
	MS-Exchange NotesConnector	OK	2004-07-06 11:21:41	61d 22h 57m 57s	1/3	All services are running
	SMTP	OK	2004-07-06 11:21:43	61d 22h 58m 4s	1/3	SMTP OK - 0 second response time
lenin	SMTP	OK	2004-07-06 11:21:51	20d 2h 18m 14s	1/3	SMTP OK - 0 second response time
marx	HTTP	OK	2004-07-06 11:21:46	23d 2h 15m 17s	1/3	HTTP ok: HTTP/1.1 200 OK - 0.016 second response time
	SMTP	OK	2004-07-06 11:21:51	22d 19h 2m 16s	1/3	SMTP OK - 0 second response time

Nagios

General

- Home
- Documentation

Monitoring

- Tactical Overview
- Service Detail
- Host Detail
- Status Overview
- Status Summary
- Status Grid
- Status Map
- 3-D Status Map

- Service Problems
- Host Problems
- Network Outages

- Comments
- Downtime

- Process Info
- Performance Info
- Scheduling Queue

Reporting

- Trends
- Availability
- Alert Histogram
- Alert History
- Alert Summary
- Notifications
- Event Log

Configuration

- View Config

OSSIM:

- Framework Open Source
- Agrega as principais ferramentas de segurança
- Integração e correlação de dados
- Permite uma visão detalhada sobre os ativos de rede



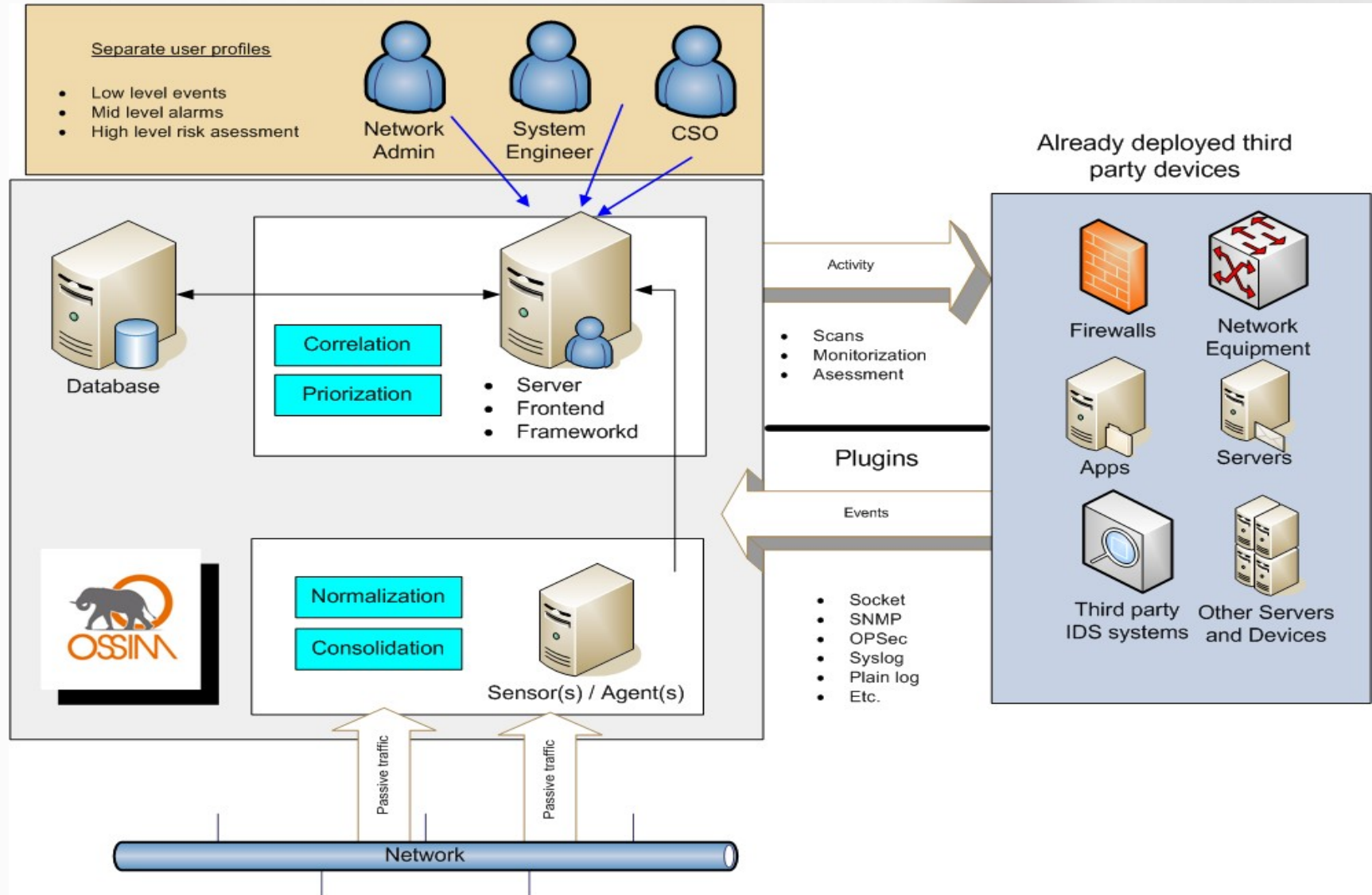
Ferramentas:

- Nessus
- Snort
- Nagios
- OCS-NG
- OSSEC
- NTOP
- Pads
- Entre outras

Nova Prestech.net



OSSIM – Open Source Security Information Management



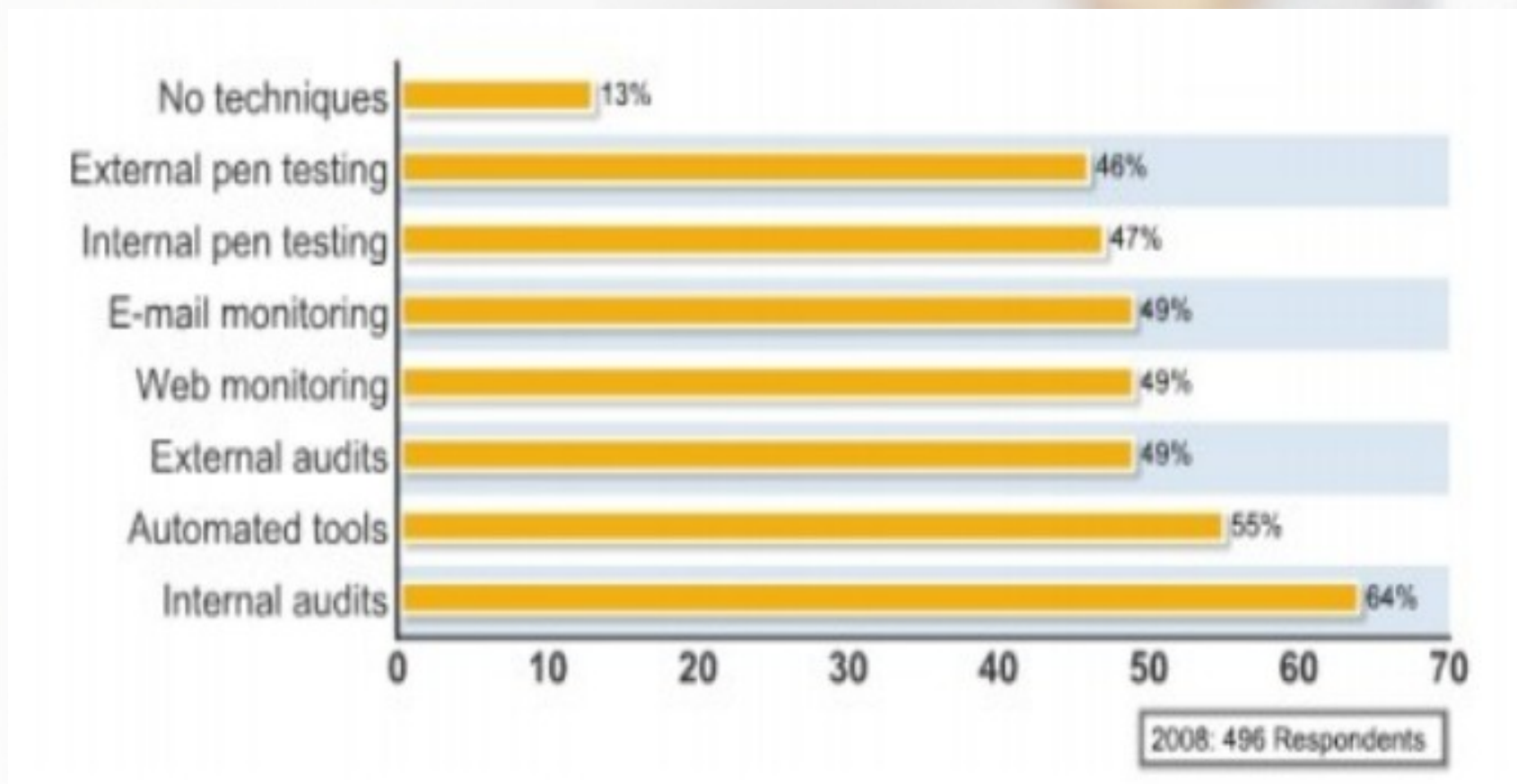
Nova Prestech.net



OSSIM – Open Source Security Information Management



Técnicas Utilizadas para avaliação de Segurança:



Como devemos nos adaptar ?



- Entendermos a natureza dos ataques é fundamental
- Novas tecnologias trazem consigo novas vulnerabilidades
- Novas formas de ataque são criadas a cada dia
- Aumento de conectividade resulta em novas possibilidades
- Ataques direcionados x Ataques Oportunísticos
- A Defesa é muito mais complexa do que o Ataque
- Não subestimar o aumento dos crimes digitais

Quebra dos Mitos sobre segurança da Informação

- “Isso nunca acontecerá conosco”
- “Nunca fomos atacados, não precisamos de segurança”
- “Utilizamos o melhores sistemas”
- “Não dá para gastar com segurança agora”
- “Ninguém vai descobrir esta falha de segurança”
- “Vamos deixar funcionando, depois resolvemos”
- “Segurança é um luxo para quem tem dinheiro”

Conclusões :

- É necessário que se mude o olhar sobre a S.I.
- Controles de Segurança se fazem necessários
- Não basta só implementar mecanismos tem que avaliar
- Uma cultura de segurança na empresa é essencial
- Não se iluda com a falsa sensação de segurança
- A Tecnologia não é uma panacéia !!!!



BRIGADO

<http://www.prestech.com.br>

Victor Batista da Silva Santos

victor@prestech.com.br

+55 21 8762-6977

+55 21 3622-1600

Rua Francisco Manuel 99/A
Benfica – Rio de Janeiro, RJ
Fax: (21) 3860-7510
CEP 20911-270