Nova Prestech.net

Consultoria e Soluções em Informática

GTS

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

NOVA PRESTECH.NET

Nova Prestech.net

Consultoria e Soluções em Informática

GTS

Agenda:

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

NOVA PRESTECH.NET

Nova Prestech.net

GTS

Tríade - Segurança da Informação

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

Nova Prestech.net

Uma novo olhar sobre a Segurança da Informação

Nova Prestech.net

GTS

Framework de Segurança da Informação

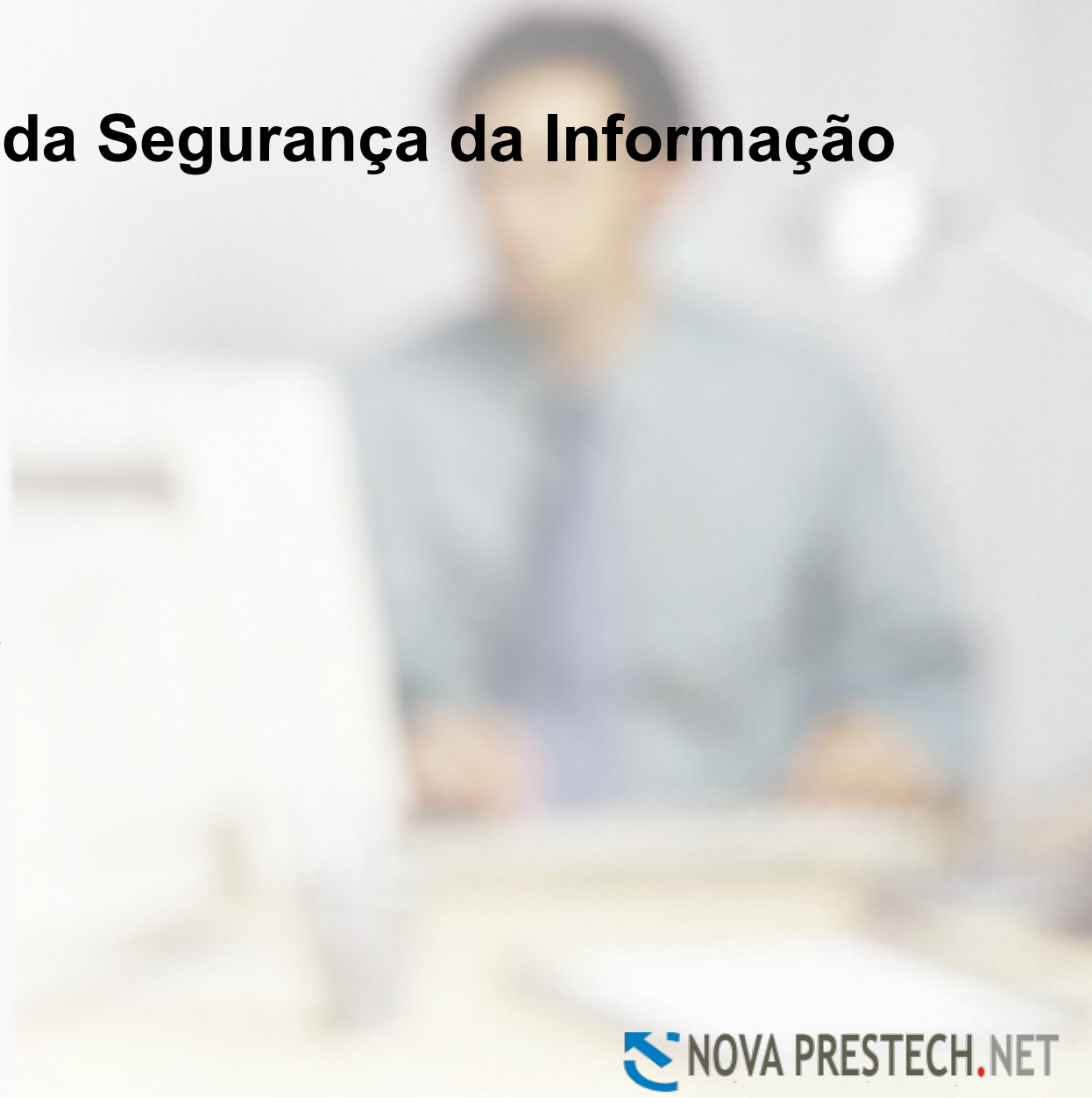
NOVA PRESTECH.NET

Nova Prestech.net

Framework de Segurança da Informação

GTS

Pessoas: O elo fraco da Segurança da Informação



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

NOVA PRESTECH.NET

Nova Prestech.net

Framework de Segurança da Informação

GTS

Processos: O Controle de Segurança da Informação

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

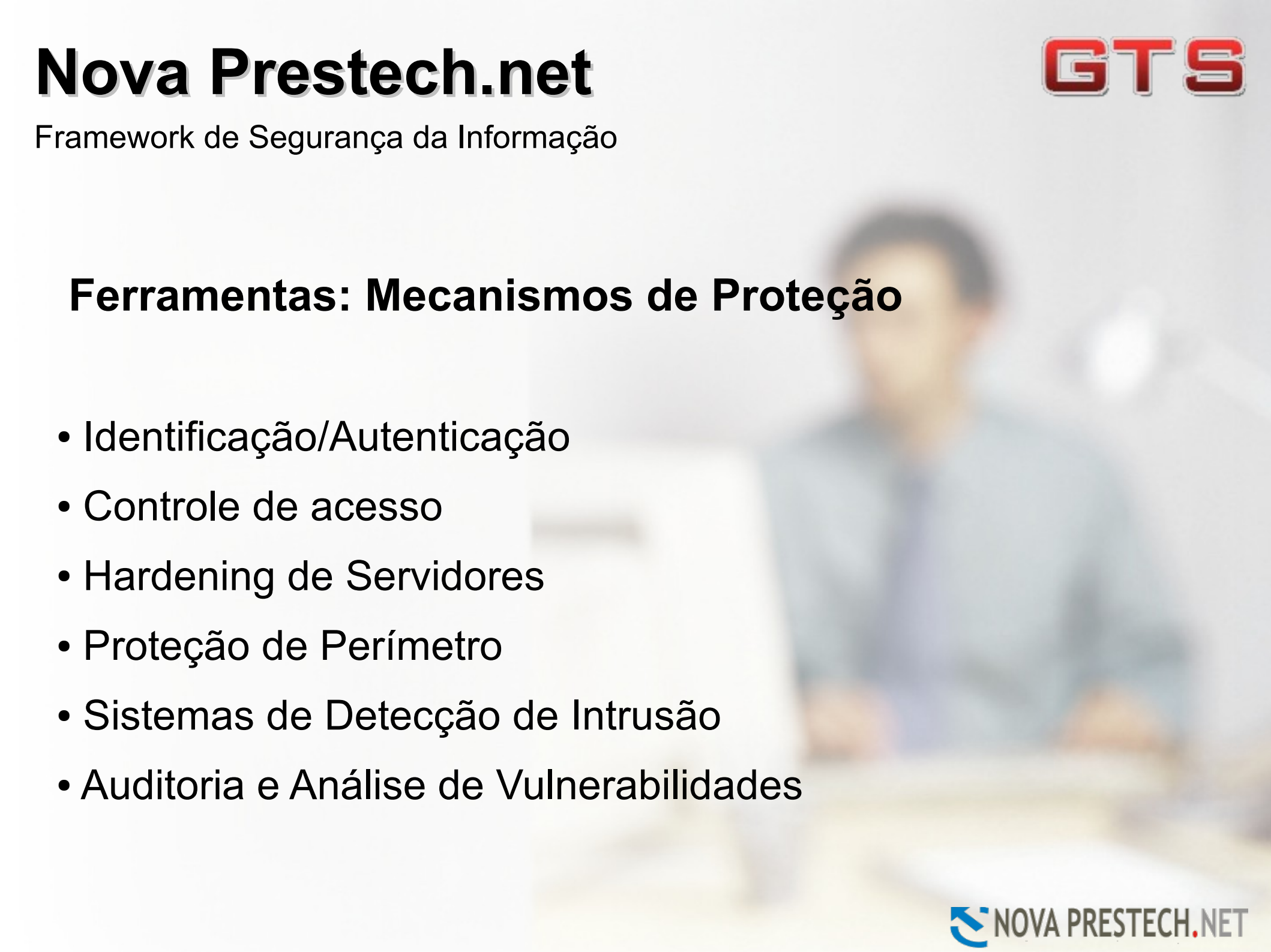
Nova Prestech.net

Framework de Segurança da Informação

GTS

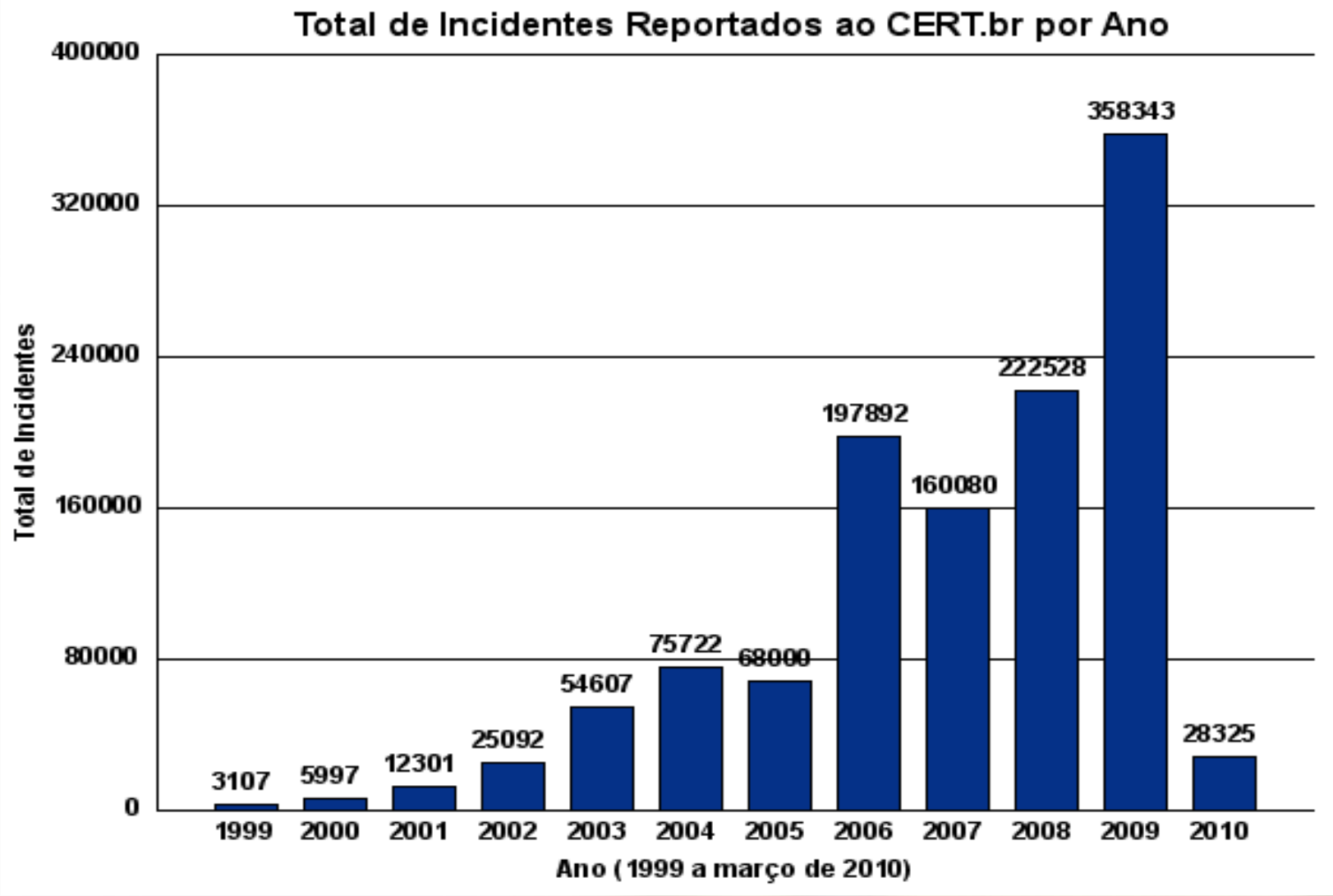
Ferramentas: Mecanismos de Proteção

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



Nova Prestech.net

Motivação

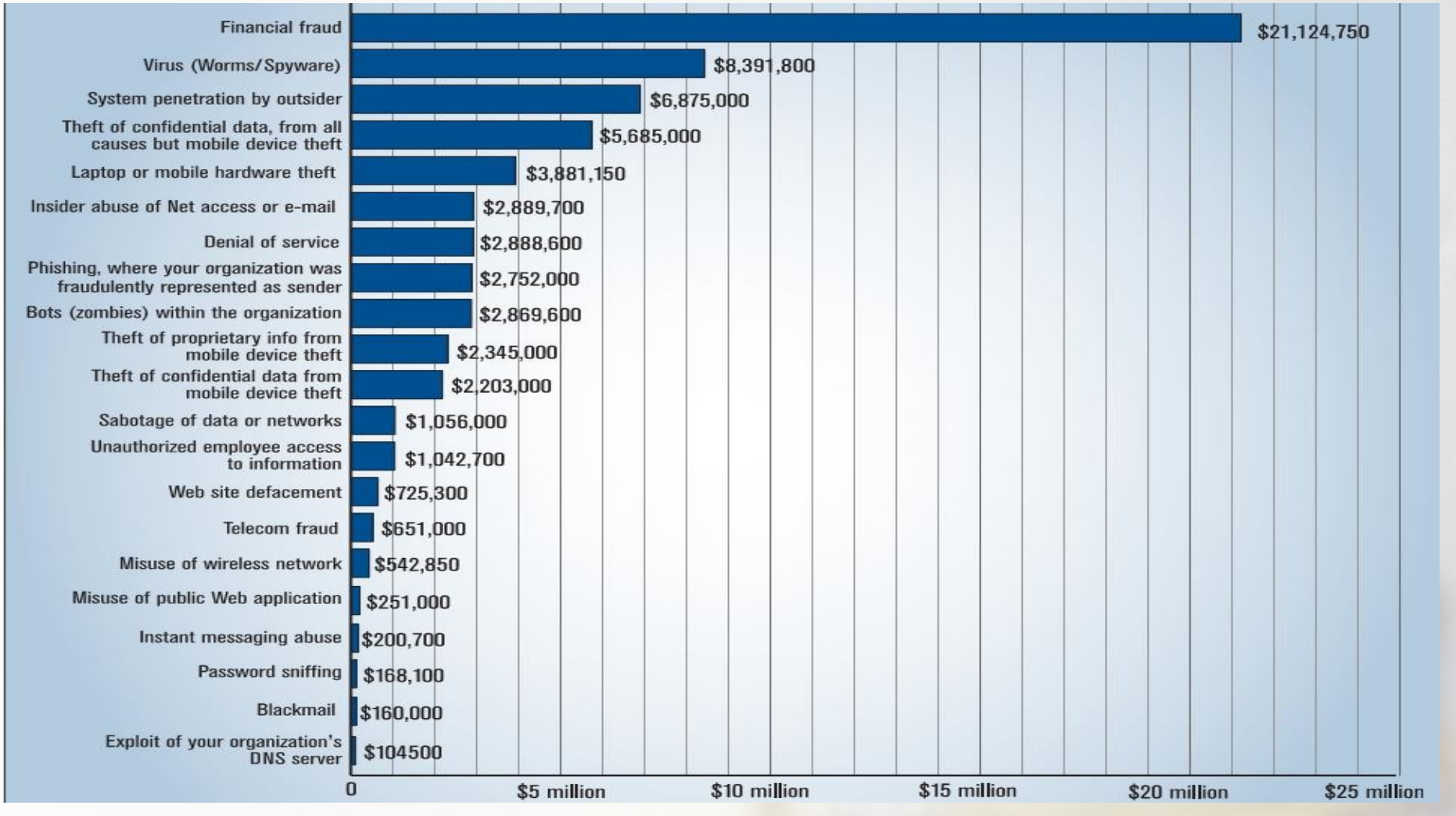


Nova Prestech.net

Motivação

Nova Prestech.net

Motivação



Nova Prestech.net

Incidentes de Segurança da Informação

GTS

Incidentes de segurança :

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

Nova Prestech.net

NBR ISO/IEC 27002 – Código de Prática para a Gestão de Segurança da Informação

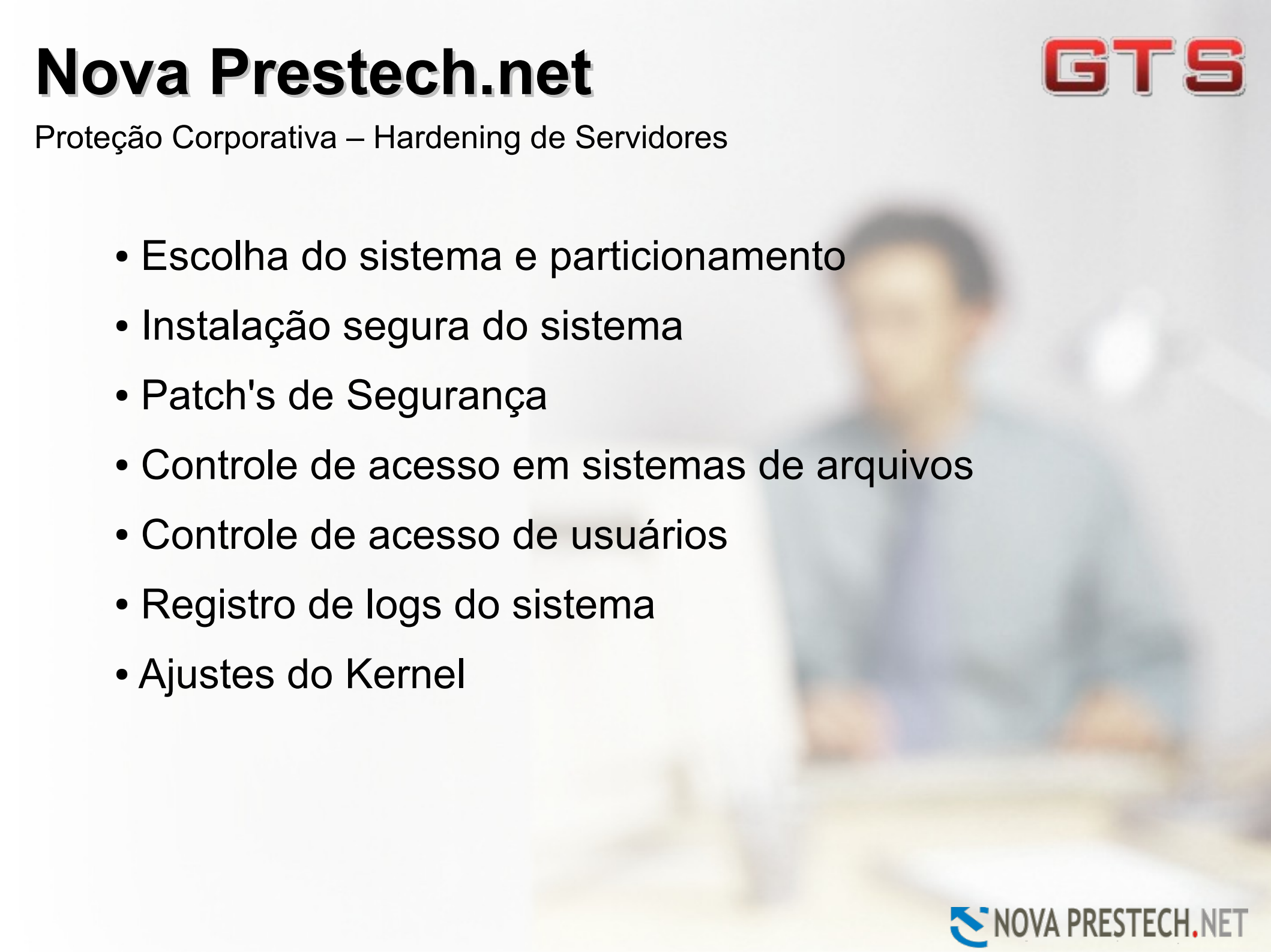
Norma que apresenta uma guia de boas práticas em segurança da informação, orientando e apresentando recomendações para implementações de controles.

BS7799 – ISO/IEC 17799 – ISO/IEC 27002

Nova Prestech.net

GTS

Proteção Corporativa – Hardening de Servidores



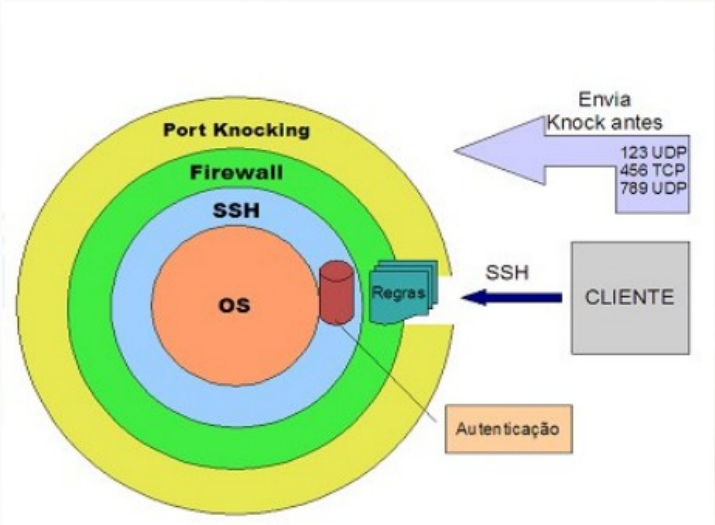
- Escolha do sistema e particionamento
- Instalação segura do sistema
- Patch's de Segurança
- Controle de acesso em sistemas de arquivos
- Controle de acesso de usuários
- Registro de logs do sistema
- Ajustes do Kernel

Nova Prestech.net

GTS

Indentificação/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)



Nova Prestech.net

GTS

Controle de Acesso

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

Nova Prestech.net

Proteção de Perímetro de Rede

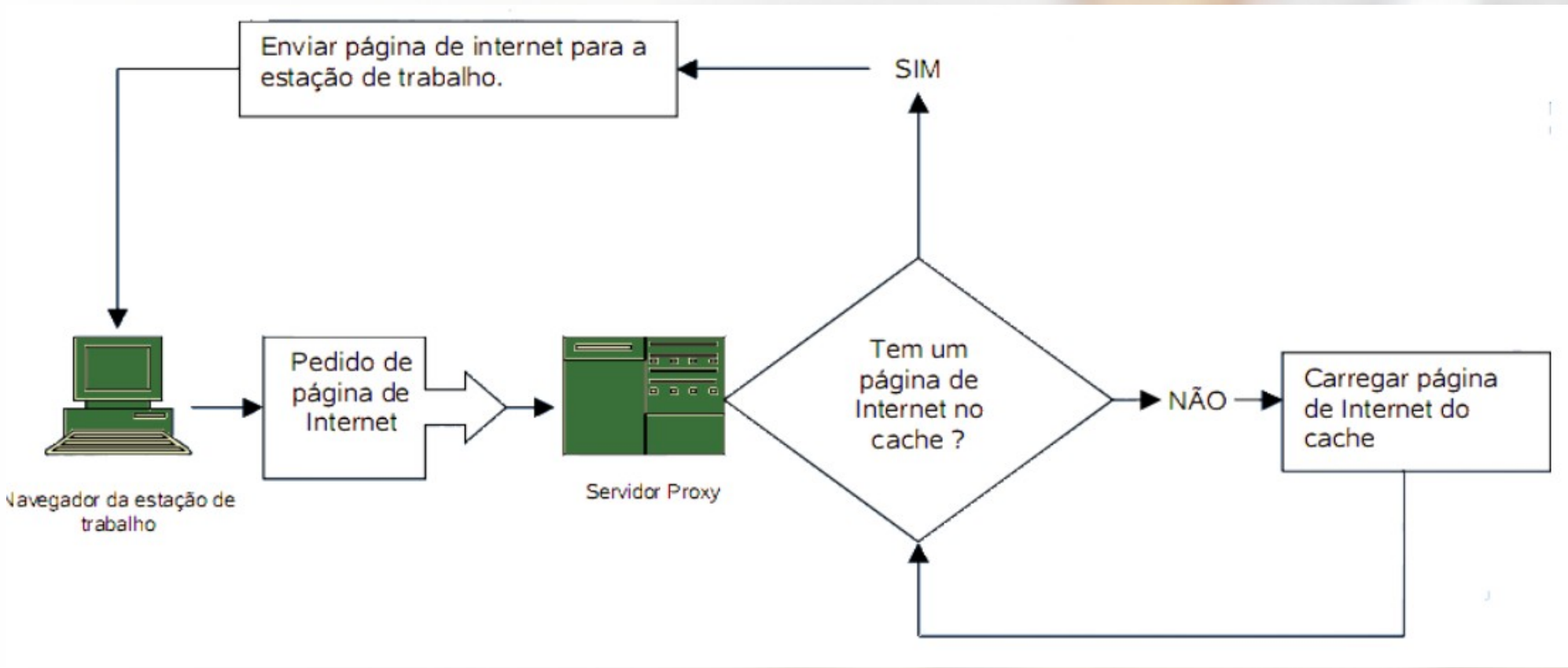
Controle de Tráfego (Firewall – Iptables):

- 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

Nova Prestech.net

Proteção de Perímetro de Rede

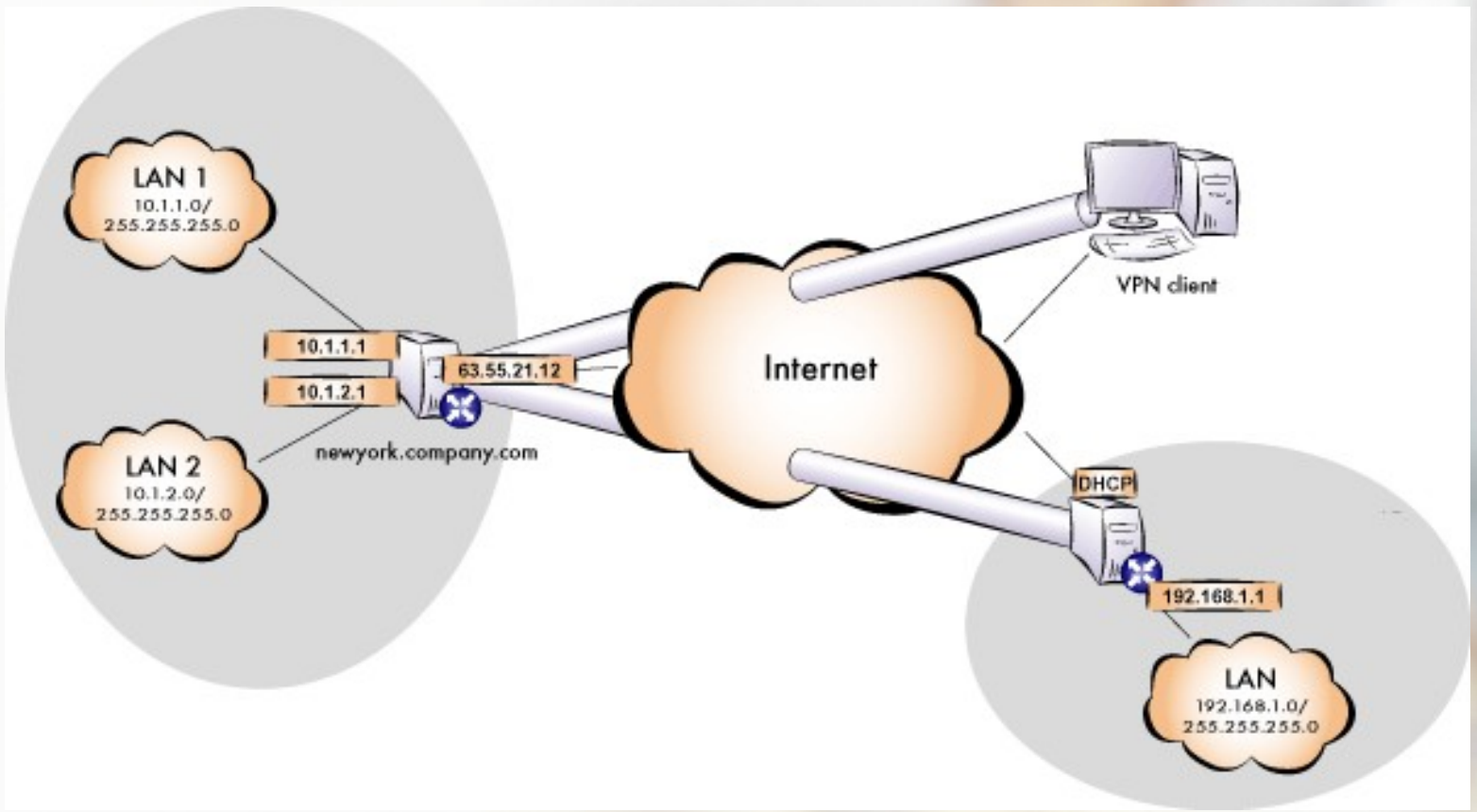
Controle de Conteúdo Web (Proxy – Squid):



Nova Prestech.net

Proteção de Perímetro de Rede

Rede Virtual Privada (VPN – OpenVPN):



Nova Prestech.net

Sistemas de Detecção de Intrusão

GTS

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

Nova Prestech.net

Sistemas de Detecção de Intrusão

GTS

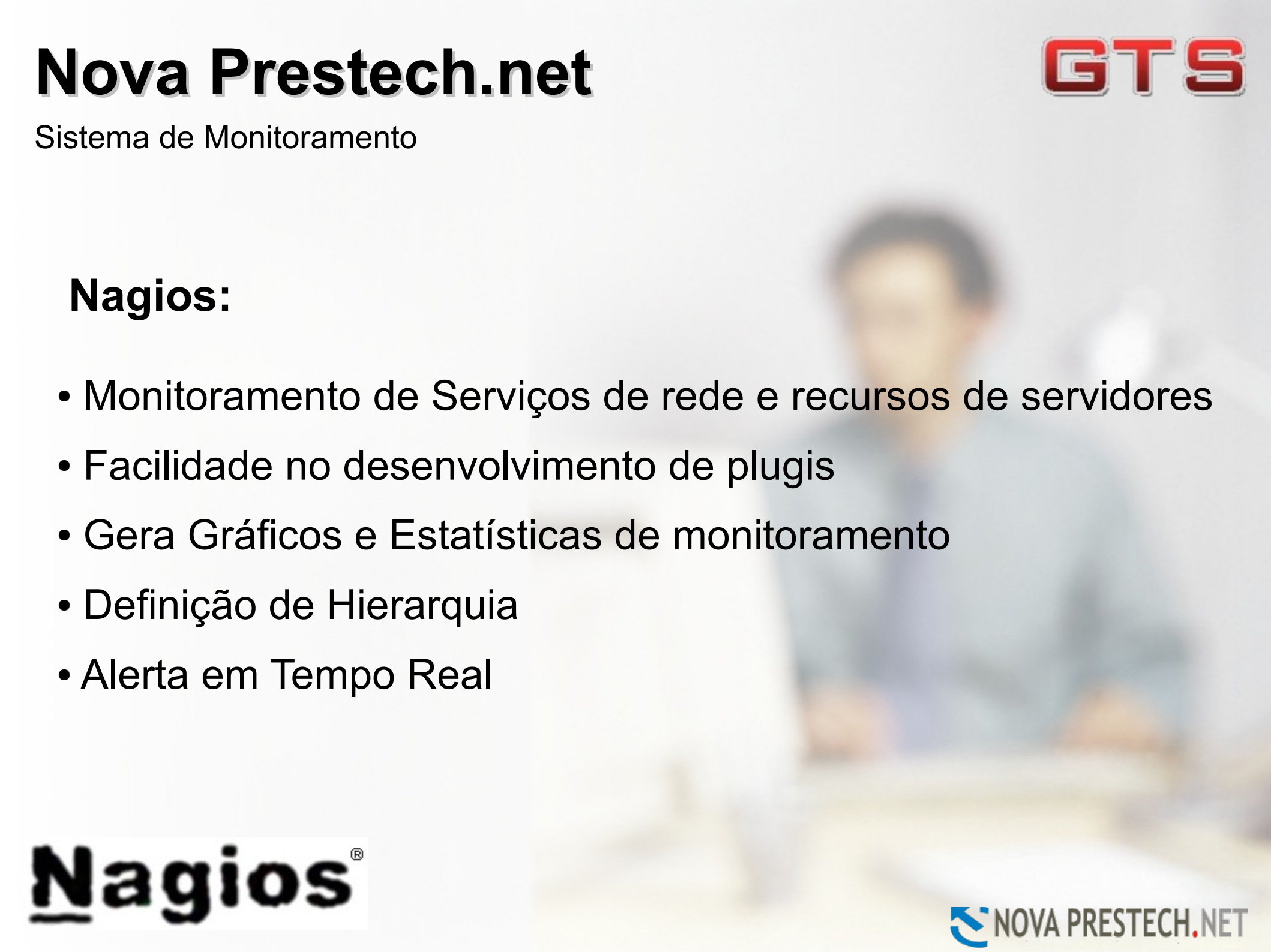
OSSEC:

- 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

Nova Prestech.net

GTS

Sistema de Monitoramento



Nagios:

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

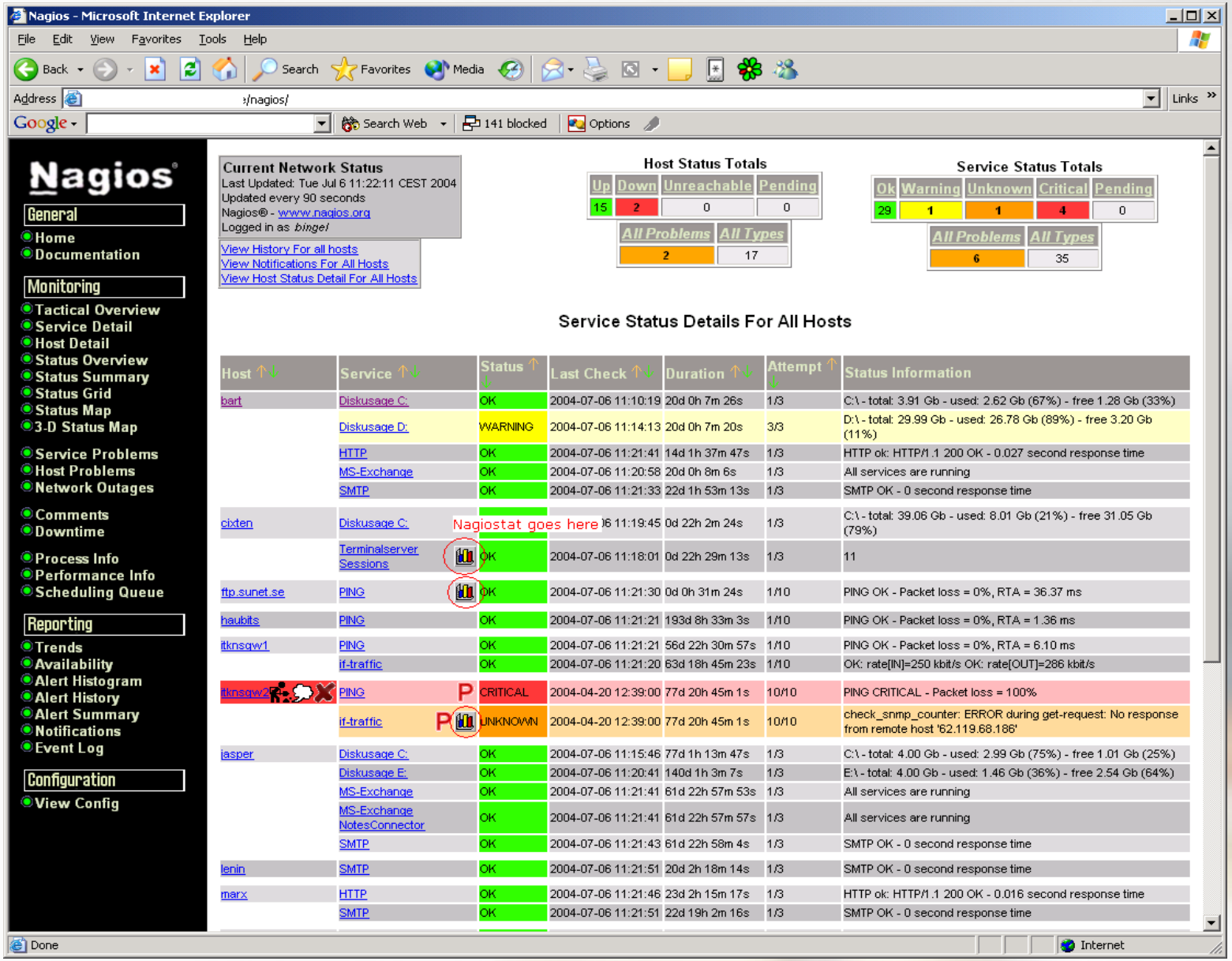
Nagios®

NOVA PRESTECH.NET

Nova Prestech.net

GTS

Nagios



NOVA PRESTECH.NET

Nova Prestech.net

GTS

Gerenciamento de Segurança

OSSIM:

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

Nova Prestech.net

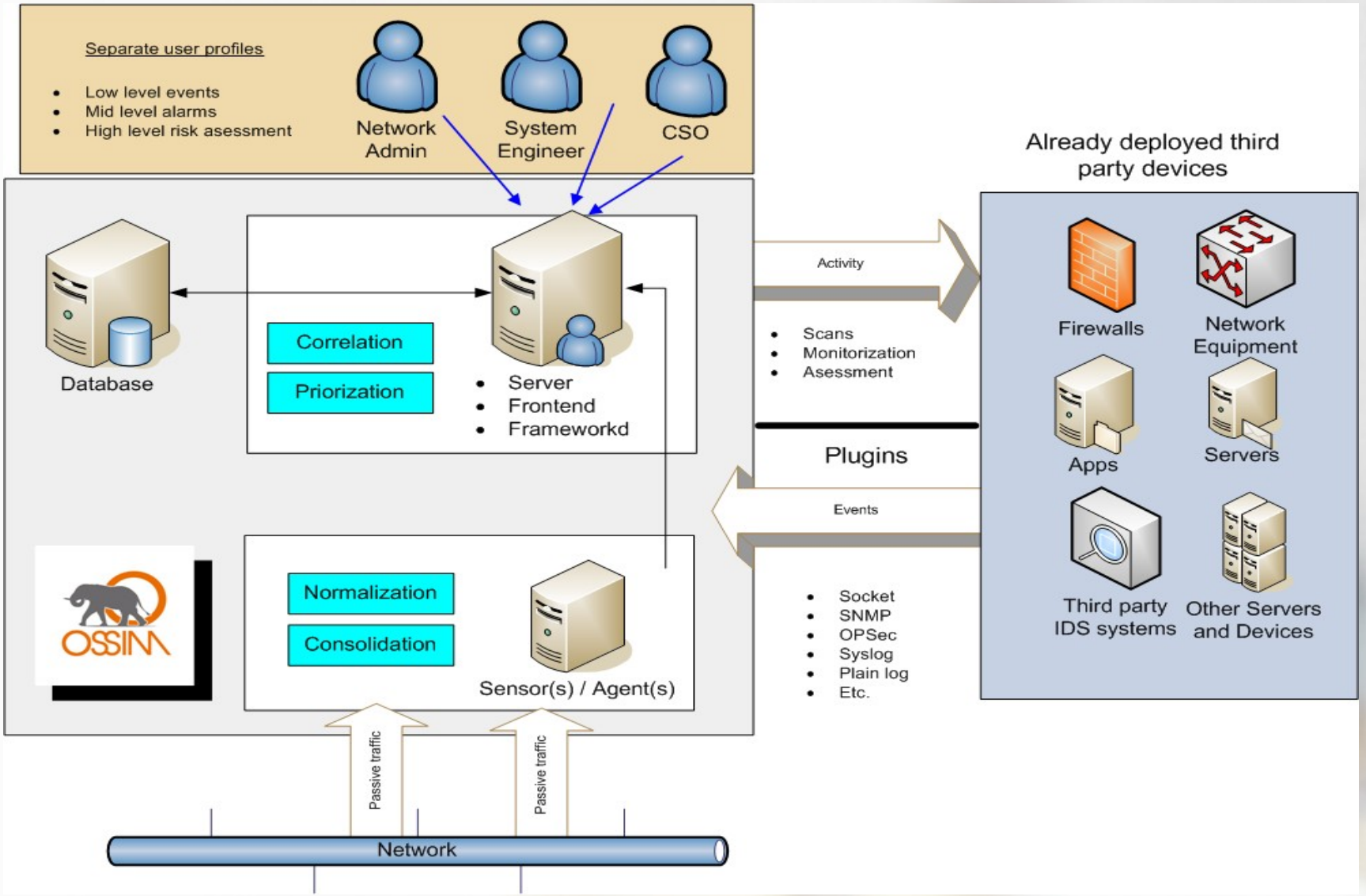
OSSIM – Open Source Security Information Management

Ferramentas:

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

Nova Prestech.net

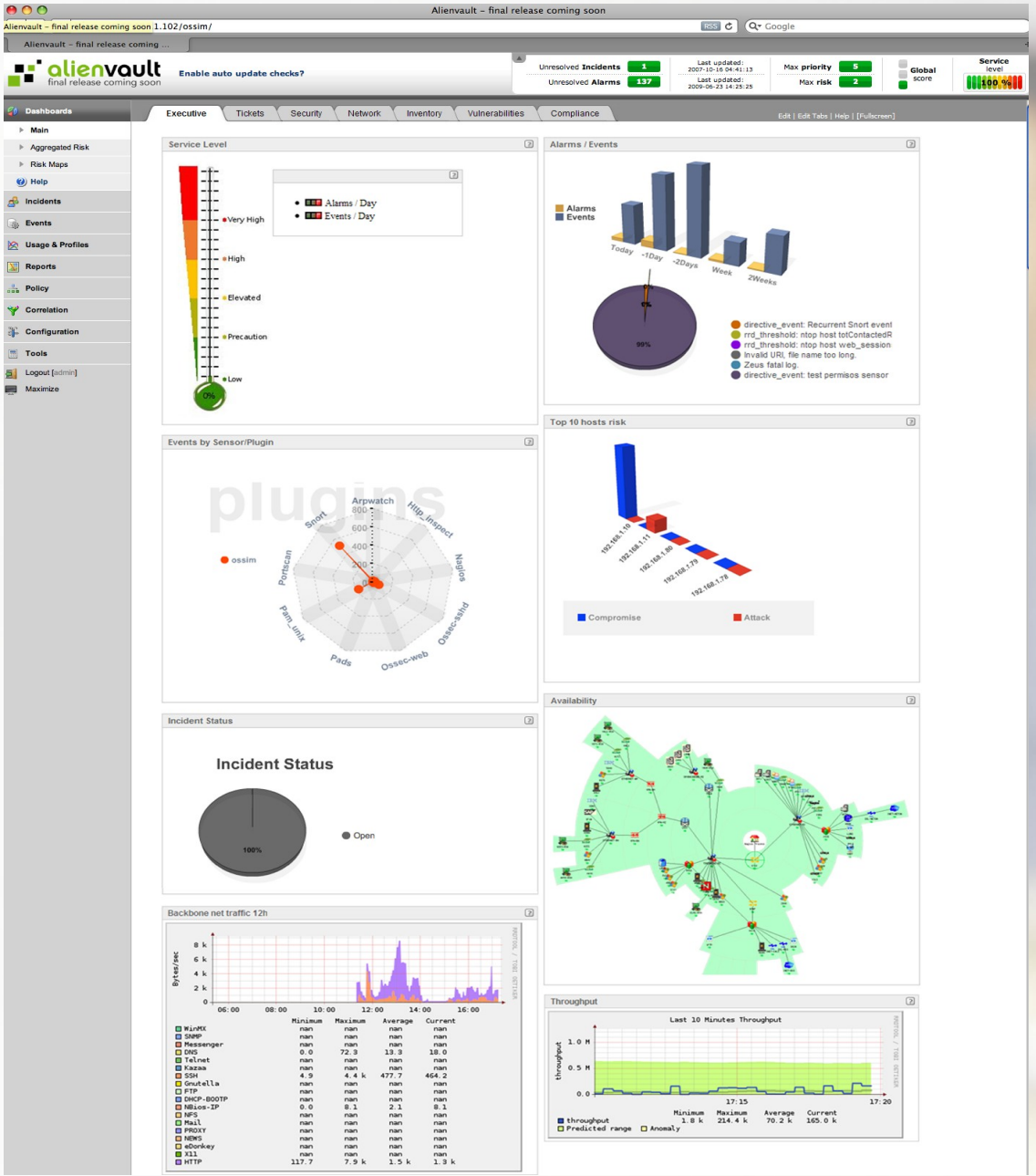
OSSIM – Open Source Security Information Management



Nova Prestech.net

GTS

OSSIM – Open Source Security Information Management

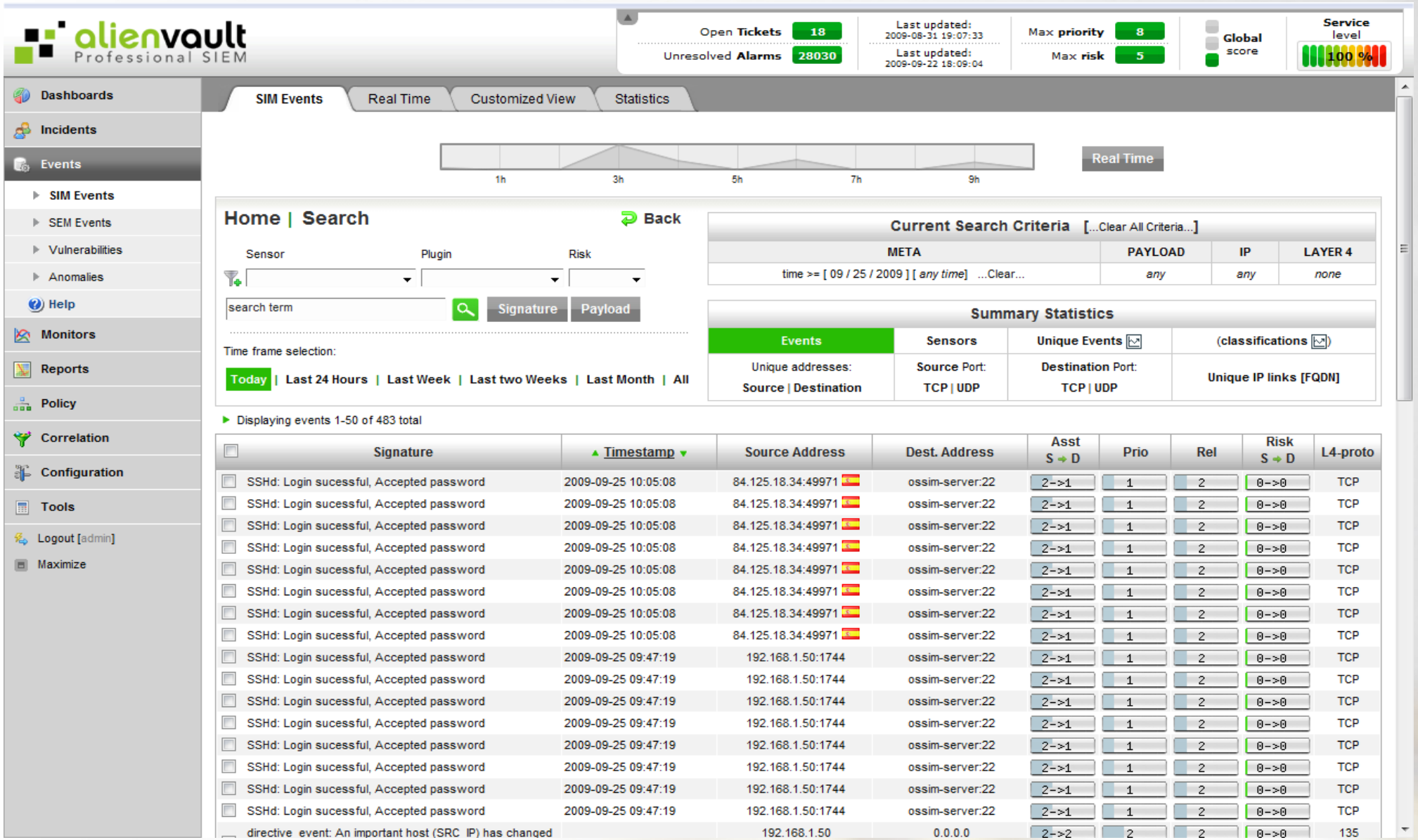


NOVA PRESTECH.NET

Nova Prestech.net

GTS

OSSIM – Open Source Security Information Management

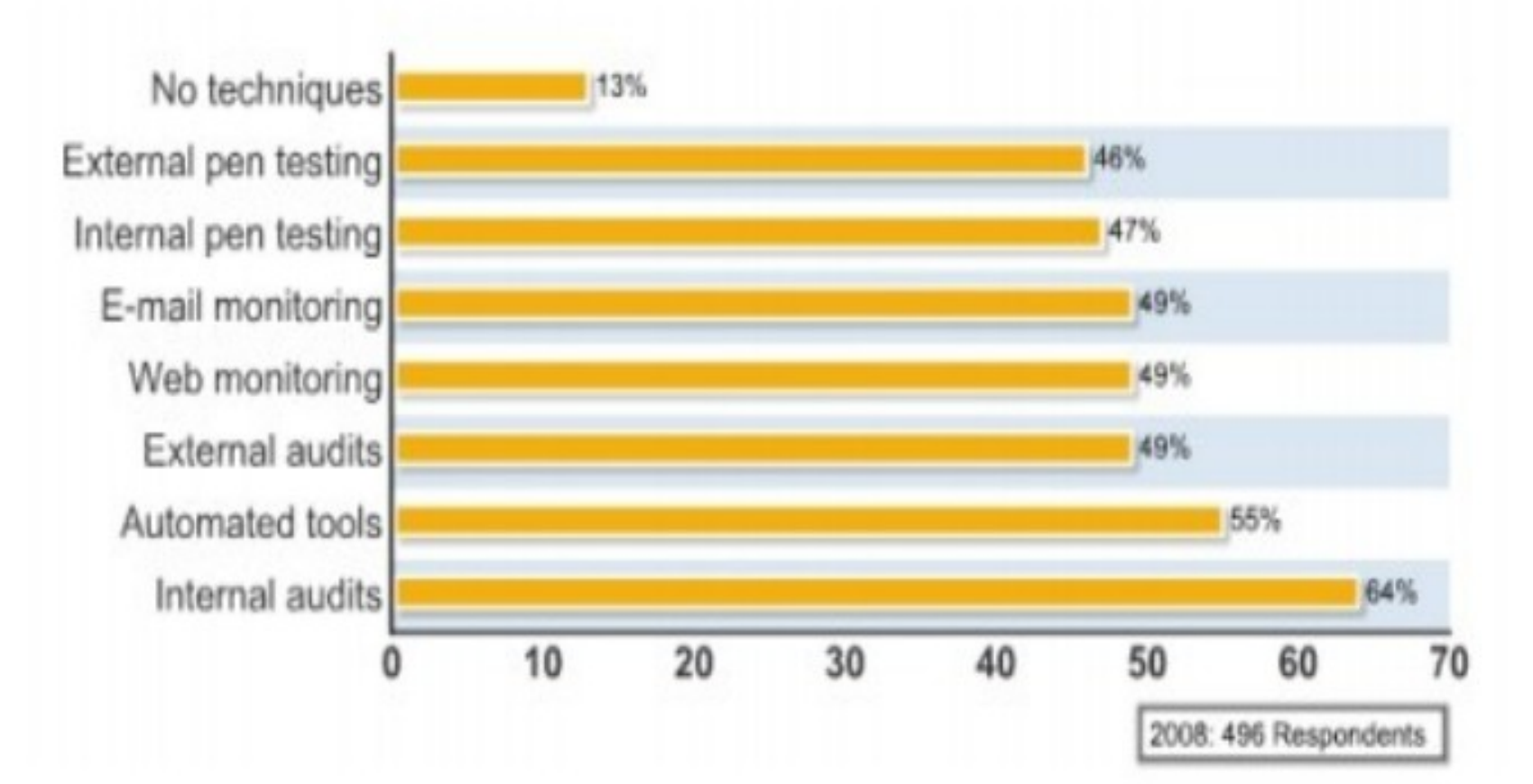


NOVA PRESTECH.NET

Nova Prestech.net

Auditoria e Analise de Vulnerabilidades

Técnicas Utilizadas para avaliação de Segurança:



Nova Prestech.net

Consultoria, Soluções e Treinamento

GTS

Como devemos nos adaptar ?

NOVA PRESTECH.NET

Nova Prestech.net

Preocupação com a Segurança da Informação

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

Nova Prestech.net

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”

Nova Prestech.net

Consultoria e Soluções em informática

GTS

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 !!!!

Nova Prestech.net

GTS

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

NOVA PRESTECH.NET