

SpotLight

Sistema de Detecção,
Monitorização e
Isolamento a Intrusão

Bruno Castro
Edmundo Monteiro

7 de Novembro 2005





Índice

1. Introdução

- a. Estado da Nação
- b. CIA Triad
- c. Modelo de Segurança
- d. Segurança Defensiva

2. HoneyPot e HoneyNet

3. Objectivos *versus* Arquitectura

4. Arquitectura do SpotLight

- a. SpotLight
- b. HoneyWall

5. Avaliação

- a. Disponibilidade de Serviço
- b. Aprendizagem
- c. Conhecimento das Fragilidades
- d. Recolha de Evidências

6. Resultados Finais

7. Conclusões

8. Trabalho Futuro





1. Introdução

A “segurança informática” é um requisito fundamental para o suporte da tecnologia Internet.

Os limites da segurança informática são os limites da Internet. E não existe indivíduo ou empresa fora dos limites e necessidades da segurança informática.

“A Segurança Perfeita é um Mito!”

Não existe sistema, aplicacional ou tecnológico, completamente seguro. A conectividade implica sempre uma exposição ao risco e um consequente risco associado.

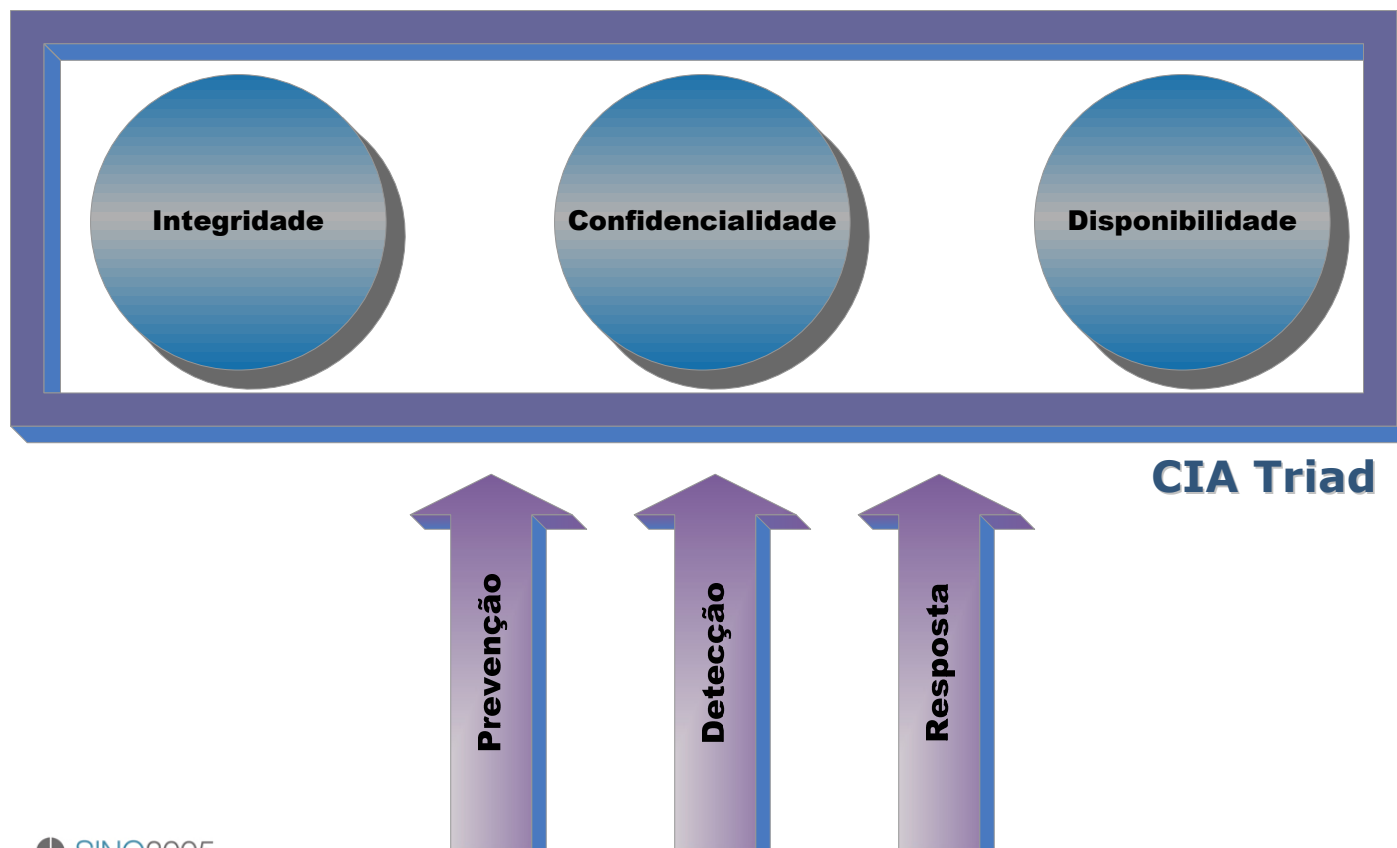
Este, foi um dos princípios no qual o desenvolvimento do **SpotLight** se baseou.





1. Introdução *(continuação)*

Actualmente, e no decorrer do constante aparecimento de novas ameaças, as organizações apresentam uma abordagem de segurança estruturada em três áreas distintas:





1. Introdução *(continuação)*

"A segurança é baseada em pessoas, e as pessoas cometem erros."

Independentemente das medidas preventivas, tecnológicas ou processos implementados na organização, é garantido que existirá uma falha de segurança algures no tempo. Assim, é fundamental uma rápida detecção e resposta ao eventual incidente, valorizando a componente de detecção numa abordagem de segurança corporativa.

Uma detecção eficaz é preponderante para a manutenção do nível de segurança de uma organização, garantindo a disponibilidade e competitividade do negócio em causa.





1. Introdução *(continuação)*

"Tradicionalmente a segurança informática tem sido unicamente defensiva!"

Os processos de implementação de segurança nas organizações, baseiam o seu âmbito em mecanismos singularmente defensivos





2. HoneyPot e HoneyNet

Os sistemas de HoneyPot ou HoneyNet podem ser considerado como ferramentas de aprendizagem e recolha de informação sobre a comunidade *hacker*.

Lance Spitzner, membro e fundador do grupo de investigação HoneyNet Project, apresenta a sua definição do termo "HoneyPot" do seguinte modo:

"A security resource who's value lies in being probed, attacked or compromised."

The Honeynet
P R O J E C T

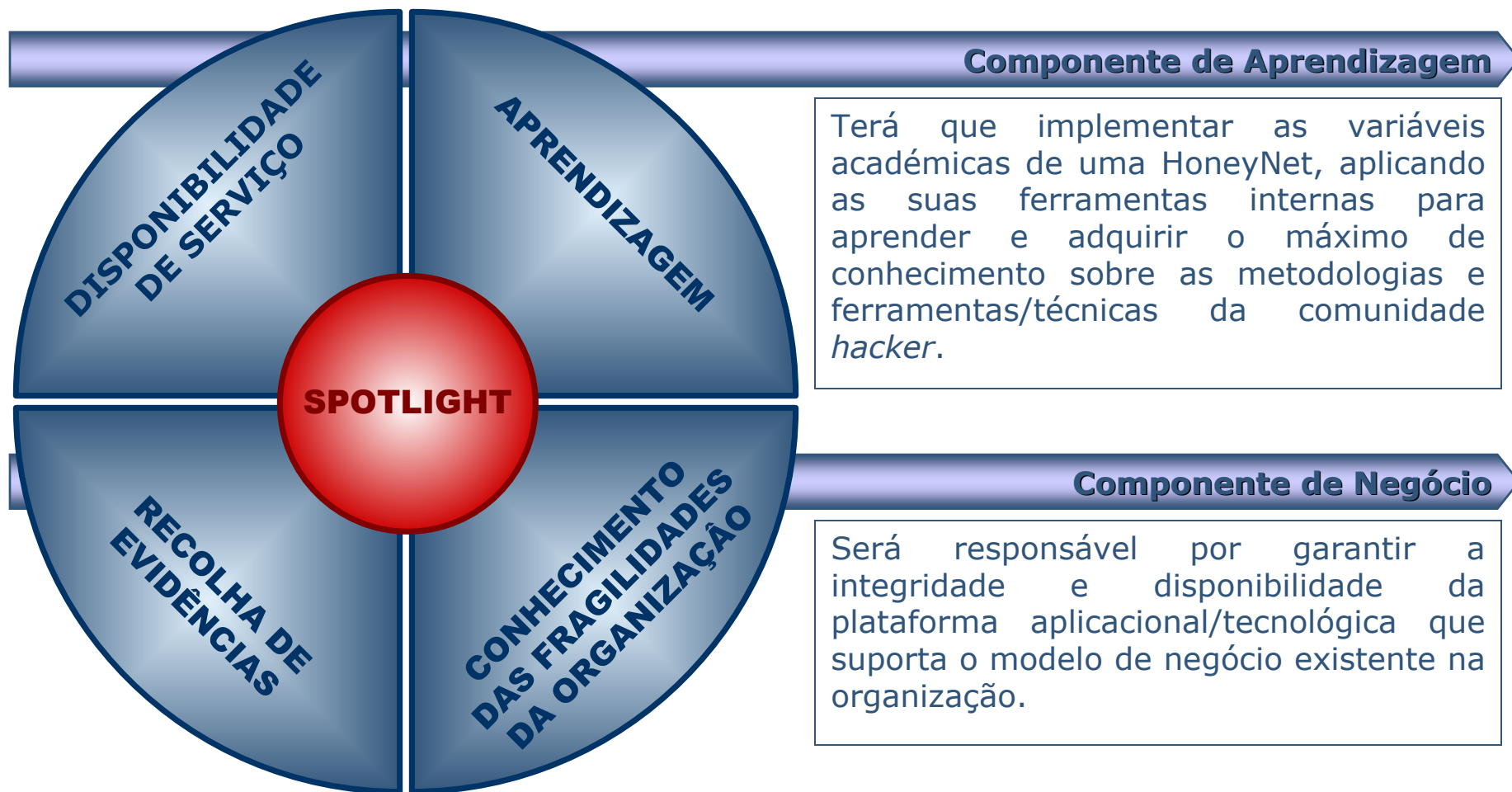
A abordagem típica, prende-se com o desenvolvimento de uma *armadilha* conceptual integrada num ambiente devidamente estruturado com o único objectivo de caçar *hackers* em plena acção.

O presente trabalho, **SpotLight**, propõe uma plataforma tecnológica e aplicacional, baseada nos conceitos funcionais de uma *HoneyNet Generation II*, acrescido de algumas das principais funcionalidades das *Virtual HoneyNet*.





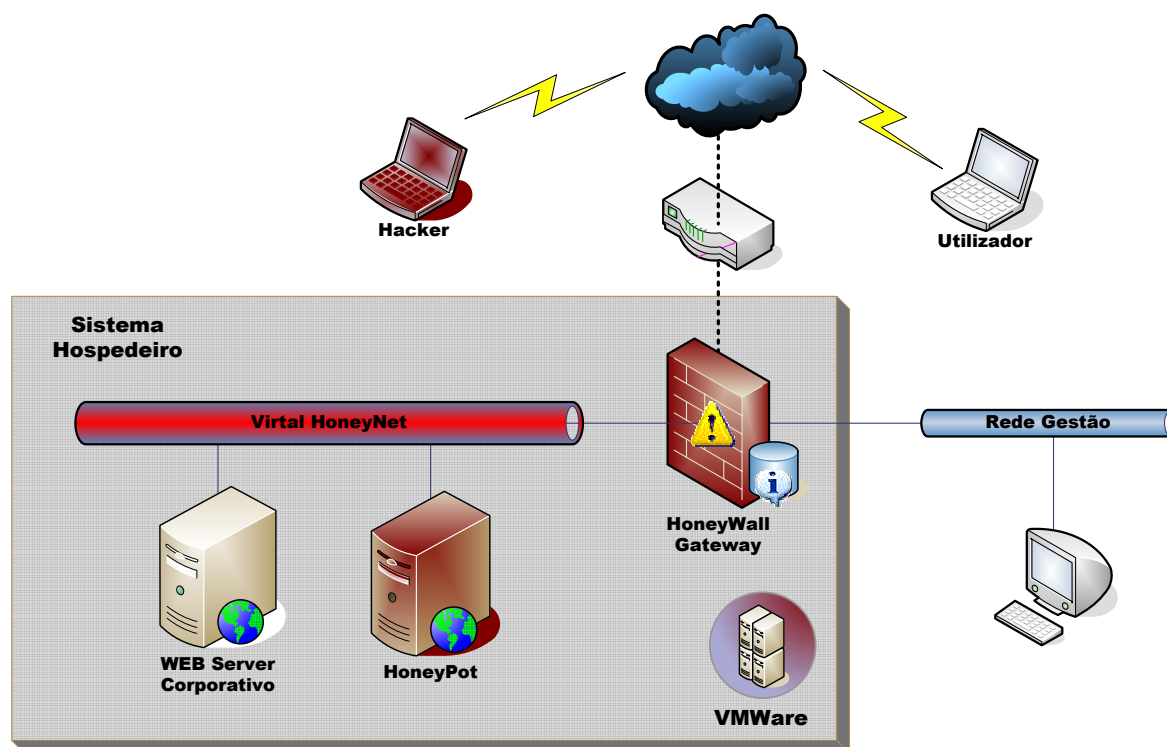
3. Objectivos *versus* Arquitectura





4. Arquitectura do SpotLight

A arquitectura do SpotLight foi desenvolvida com o intuito de ser simples, dinâmica e extremamente versátil, de acordo com o ambiente que a rodeia.



SISTEMAS VIRTUAIS

❑ HoneyWall

A HoneyWall é o centro nevrálgico do SpotLight. Podemos considerá-la como o “cérebro” da arquitectura desenvolvida no âmbito deste projecto. A totalidade de processamento e análise de tráfego é da sua inteira responsabilidade.

❑ HoneyPot

O HoneyPot apresenta-se como o sistema responsável por “simular” o sistema corporativo, ao receber os ataques oriundos do exterior (em modelo de HoneyPot).

❑ Servidor WEB Corporativo

Este sistema representa o recurso de valor corporativo para a organização.





A HoneyWall é o centro nevrálgico do SpotLight. Podemos considerá-la como o “cérebro” da arquitectura desenvolvida no âmbito deste projecto. A totalidade de processamento e análise de tráfego é da sua inteira responsabilidade.





5. Avaliação

Disponibilidade de Serviço

Grau de Cumprimento do
Objectivo Proposto

Níveis de Avaliação: A/B/C/D

A-



Resultados Obtidos em Fase de *Piloto*

- ✓ Detecção de um número elevado de ataques automatizados e sistematizados por gamas de endereçamento IP na rede interna do fornecedor/ISP.
- ✓ Detectado um conjunto bastante alargado de ferramentas de *scanning*, que de uma forma automatizada, pesquisam por sistemas vulneráveis a determinadas falhas de segurança (vulnerabilidades).
- ✓ A prestação (A-) é devida essencialmente à simplicidade aplicada sobre o modelo funcional, permitindo estabelecer um tempo de resposta no processamento de dados bastante razoável, com um índice de falsos positivos reduzido no decorrer do processo de identificação da legitimidade do tráfego.



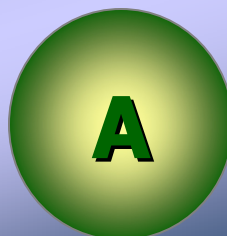


5. Avaliação *(continuação)*

Aprendizagem

Grau de Cumprimento do Objectivo Proposto

Níveis de Avaliação: A/B/C/D



Resultados Obtidos em Fase de *Piloto*

- ✓ Através do módulo de captação de pacotes de tráfego, correlacionado com assinaturas de ataques conhecidos foi possível reconhecer e identificar inúmeras tentativas de intrusão oriundas directamente da Internet.
- ✓ À medida que foram sendo publicadas novas vulnerabilidades, foi notório que no espaço de dias houve uma alteração substancial no comportamento da Internet com o SpotLight, tendo sido reportado várias tentativas de *scanning* e/ou exploração sobre portos específicos associados às novas vulnerabilidades.
- ✓ O SpotLight acabou por funcionar como um barómetro comportamental da comunidade *hacker*, detectando as alterações comportamentais da comunidade à medida que as novas vulnerabilidades iam sendo tornadas públicas.





5. Avaliação *(continuação)*

Conhecimento das Fragilidades

Grau de Cumprimento do
Objectivo Proposto

B+

Níveis de Avaliação: A/B/C/D



Resultados Obtidos em Fase de *Piloto*

- ✓ O SpotLight, através da sua capacidade de aprendizagem, conseguiu compreender rapidamente, quais as vulnerabilidades existentes no sistema corporativo mais emergentes e “apetecíveis” para a comunidade *hacker*.
- ✓ Apesar de terem sido detectadas algumas vulnerabilidades amplamente conhecidas, foram descobertas algumas possíveis e eventuais falhas de segurança, que para além de não serem ainda reconhecidas, poderão vir tornar-se ameaças graves num futuro próximo.
- ✓ Tendo o piloto durado alguns meses, bastou um espaço temporal de dias, para que o conjunto de vulnerabilidades disponibilizadas no SpotLight, desde logo identificadas, fossem exploradas e comprometidas na sua totalidade.



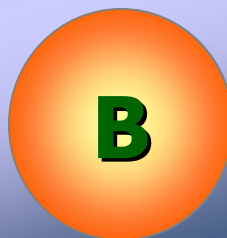


5. Avaliação *(continuação)*

Recolha de Evidências

Grau de Cumprimento do Objectivo Proposto

Níveis de Avaliação: A/B/C/D



Resultados Obtidos em Fase de *Piloto*

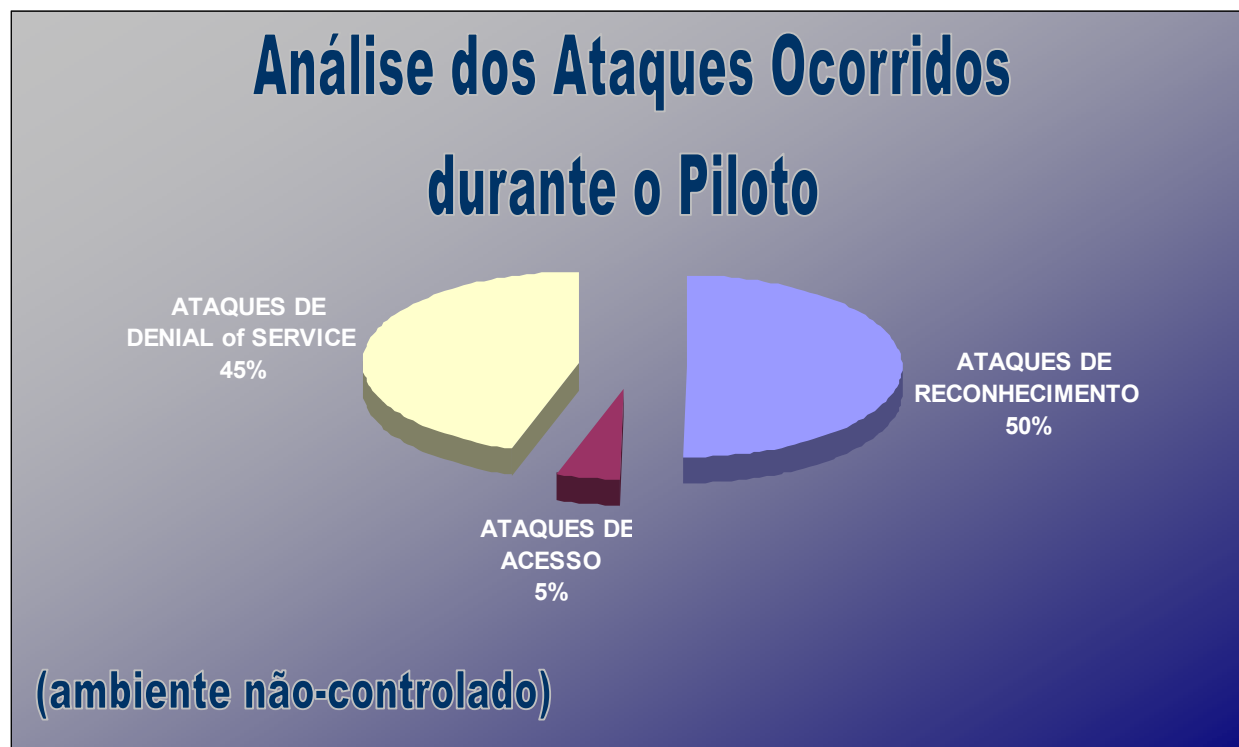
- ✓ No decorrer do piloto, a base de dados de informação do SpotLight foi crescendo exponencialmente, permitindo analisar ao detalhe todo o percurso de um determinado *hacker* durante e após a tentativa de intrusão.
- ✓ Houve oportunidade de enumerar e identificar um conjunto bastante extenso, e de grande dimensão, de eventuais *hackers*, com registos evidentes e detalhados dos ataques destinados e concretizados sobre o HoneyPot.
- ✓ Como tem sido comum no decorrer das iniciativas da comunidade *hacker*, muitos dos eventuais atacantes, foram identificados como possíveis "terceiras entidades", que estariam infectados com algum *worm* que estaria a originar massivamente ataques aleatórios sobre determinadas a rede pública.





6. Resultados Finais

A análise e classificação das actividades maliciosas detectadas no decorrer do piloto do SpotLight, foram categorizados em três categorias distintas de ataques informáticos: ataques de reconhecimento, ataques de acesso, ataques *DoS*.





6. Resultados Finais *(continuação)*

ATAQUES DE RECONHECIMENTO				
Ataque	Período	Tentativas	Origens	Tipo de Ataque
PortScan	3 meses	439	214	Não-Controlado
	N/A	78	1	Controlado
FingerPrint	3 meses	321	211	Não-Controlado
	N/A	78	1	Controlado
PortTool - Microsoft Windows NT 4.0 / 2000 Predictable LPC Message Identifier Multiple Vulnerabilities	N/A	1	1	Controlado





6. Resultados Finais *(continuação)*

ATAQUES DE ACESSO (<i>buffer overflow</i>)				
Vulnerabilidade	Período	Tentativas	Origens	Tipo de Ataque
MS Windows RPCSS Multi-thread Race Condition Vulnerability	N/A	1	1	Controlado
MS RPCSS DCOM Interface Long Filename Heap Corruption Vulnerability	N/A	3	1	Controlado
MS Windows Workstation Service Remote Buffer Overflow Vulnerability	N/A	1	1	Controlado
Microsoft Windows Locator Service Buffer Overflow Vulnerability	3 meses	24	10	Não-Controlado
	N/A	1	1	Controlado
Microsoft Windows Server Message Block Handlers Remote Buffer Overflow Vulnerability	N/A	1	1	Controlado
Microsoft IIS Executable File Parsing Vulnerability	3 meses	45	19	Não-Controlado
	N/A	1	1	Controlado
Microsoft IIS Chunked Encoding Transfer Heap Overflow Vulnerability	N/A	1	1	Controlado
Microsoft Internet Explorer Content Advisor File Handling Buffer Overflow Vulnerability	N/A	1	1	Controlado
Microsoft IIS CodeBrws.ASP Source Code Disclosure Vulnerability	N/A	1	1	Controlado
Microsoft Windows Media Services NSIISlog.DLL Remote Buffer Overflow Vulnerability	N/A	1	1	Controlado





6. Resultados Finais *(continuação)*

ATAQUES DE DENIAL of SERVICE (<i>buffer overflow</i>)				
Vulnerabilidade	Período	Tentativas	Origens	Tipo de Ataque
Microsoft Windows RPCSS DCOM Interface Denial of Service Vulnerability	3 meses	21	8	Não-Controlado
	N/A	1	1	Controlado
Microsoft Windows RPC Service Denial of Service Vulnerability	3 meses	21	8	Não-Controlado
	N/A	1	1	Controlado
Microsoft Windows Messenger Service Buffer Overrun Vulnerability	N/A	1	1	Controlado
Microsoft Windows ASN.1 Library Bit String Processing Integer Handling Vulnerability	N/A	1	1	Controlado
Microsoft Windows RPC Service Denial of Service Vulnerability	3 meses	12	8	Não-Controlado
	N/A	1	1	Controlado
Microsoft IIS Unspecified Remote Denial Of Service Vulnerability	N/A	1	1	Controlado
Microsoft IIS WebDAV Denial of Service Vulnerability	N/A	1	1	Controlado
Microsoft XML Parser Remote Denial of Service Vulnerability	N/A	1	1	Controlado





6. Resultados Finais *(continuação)*

ATAQUES DE DENIAL OF SERVICE (<i>worms</i>)				
Vulnerabilidade	Período	Tentativas	Origens	Tipo de Ataque
W32.Blaster.Worm - Microsoft Windows DCOM RPC Interface Buffer Overrun Vulnerability	3 meses	361	210	Não-Controlado
	N/A	6	1	Controlado
W32.Sasser.Worm - Microsoft Windows LSASS Buffer Overrun Vulnerability	3 meses	172	39	Não-Controlado
	N/A	1	1	Controlado
Microsoft Windows RPC Service Denial of Service Vulnerability	3 meses	72	34	Não-Controlado
	N/A	1	1	Controlado
W32.CodeBlue.Worm - Microsoft IIS and PWS Extended Unicode Directory Traversal Vulnerability	3 meses	23	12	Não-Controlado
	N/A	1	1	Controlado





7. Conclusões

As conclusões sobre os resultados obtidos, e a respectiva análise da performance funcional e operacional do próprio SpotLight, foram baseados nas interacções existentes no decorrer do *piloto* (numa janela temporal de três meses).

Como conclusão, foi evidente que o SpotLight cumpriu, e para além das expectativas iniciais, os objectivos originalmente propostos para este projecto. Foi notório como a abordagem apresentada pelo SpotLight, veio modificar alguns dos conceitos mais tradicionais do mundo da segurança informática.

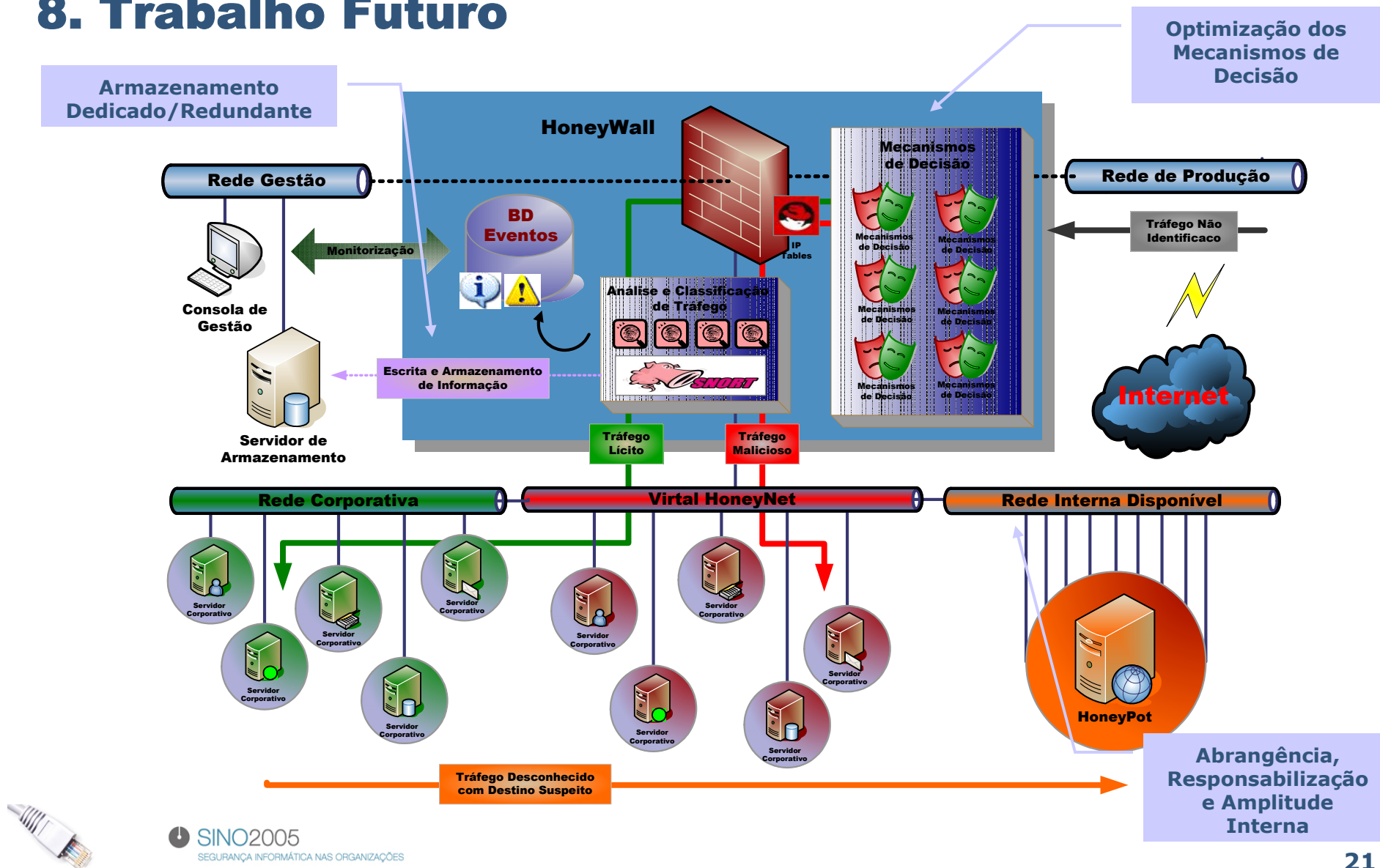
- ❑ Na intenção de analisar o estado actual do mundo da Internet, o SpotLight conseguiu funcionar como barómetro comportamental da comunidade *hacker*.
- ❑ Na perspectiva de negócio, e através da sua arquitectura dinâmica e reactiva, possibilitou uma defesa rigorosa e incondicional sobre as várias plataformas corporativas que sustentam o “negócio” da organização.
- ❑ Na componente académica, o SpotLight permitiu um “estudo” detalhado das metodologias e técnicas utilizadas pela comunidade *hacker* actual.

O SpotLight não pode ser considerado como uma solução em versão final ou *release*...





8. Trabalho Futuro





Q&A ?

Obrigado.

bcastro@visionware.pt

