PRODESP
Tecnologia da Informação

PRODESP ISG 9001 27001 20000 14001

Redução de incidentes através da identificação, análise e correção de vulnerabilidades

André Braga

Thiago B. Santana

CSIRT / Laboratório Forense Digital
Divisão de Continuidade e Riscos

GOVERNO DO ESTADO
DE SÃO PAULO

Agenda

- Histórico e estrutura do CSIRT
- Escopo de atuação
- Estatísticas ANTES da implantação
- Vulnerabilidades em estações e servidores
- Dificuldades e desafios
- Soluções desenvolvidas pelo time
- Estatísticas APÓS a implantação
- Novo cenário e evolução


PRODESP
Tecnologia da Informação
PRODESP
ISO
9001
27001
20000
14001
PRODESP

- Data Center de 800m2
- 3 salas-cofre
- 3 Mainframes com capacidade para processar cerca de 3.7 bilhões de instruções por segundo
- Cerca de 2.200 servidores instalados, mais de 1.700 virtuais
- 180 Tb de armazenamento
- Backup - Sistema robótico: 1,3 Petabytes
- Faturamento: R$ 546,1 milhões (2012)
- Usina própria de energia

PRODESP
Tecnologia da Informação

PRODESP ISO 9001 27001 20000 14001

PRODESP

PRODESP
Tecnologia da Informação

PRODESP ISG 9001 27001 20000 14001

PRODESP

acessa sp

708 postos e 616 municípios atendidos

Acessa SP recebe prêmio de US$ 1 milhão da Fundação Bill & Melinda Gates

BLOG DA GESTÃO, BLOG DO ACESSA, DESTAQUES, NOTÍCIAS · EM 19 DE AGOSTO DE 2013 · 5 COMENTÁRIOS · *TAGGED WITH: ACESSASP, INCLUSÃO DIGITAL, PRÊMIO, SINGAPURA; FUNDAÇÃO BILL & MELINDA GATTES*

O Acessa São Paulo foi premiado nesta segunda-feira (19/8), em Cingapura, pela Fundação Bill & Melinda Gates. O prêmio, que está em sua 14ª edição, pode ser considerado o Nobel da inclusão digital, reconhecendo esforços inovadores em todo o mundo para conectar pessoas à informação por meio do acesso gratuito a computadores e à internet, abrindo oportunidades de bem-estar econômico e social. O Acessa SP concorreu com outras 300 candidaturas de 56 países.

Prêmio de US$ 1 milhão foi concedido em cerimônia em Cingapura

Acessa SP em números

Atendimentos: 71.403.944
Cadastros: 2.702.562
Postos ativos: 708
Em implantação: 182
Municípios atendidos: 616

PRODESP
Tecnologia da Informação

PRODESP ISO 9001 27001 20000 14001

PRODESP

poupa tempo

39 postos e 33 milhões de atendimentos em 2012

PRODESP
Tecnologia da Informação

PRODESP
ISO
9001
27001
20000
14001

CSIRT PRODESP

PRODESP
Tecnologia da Informação

PRODESP ISO 9001 27001 20000 14001

ESCOPO CSIRT PRODESP

IntraGOV

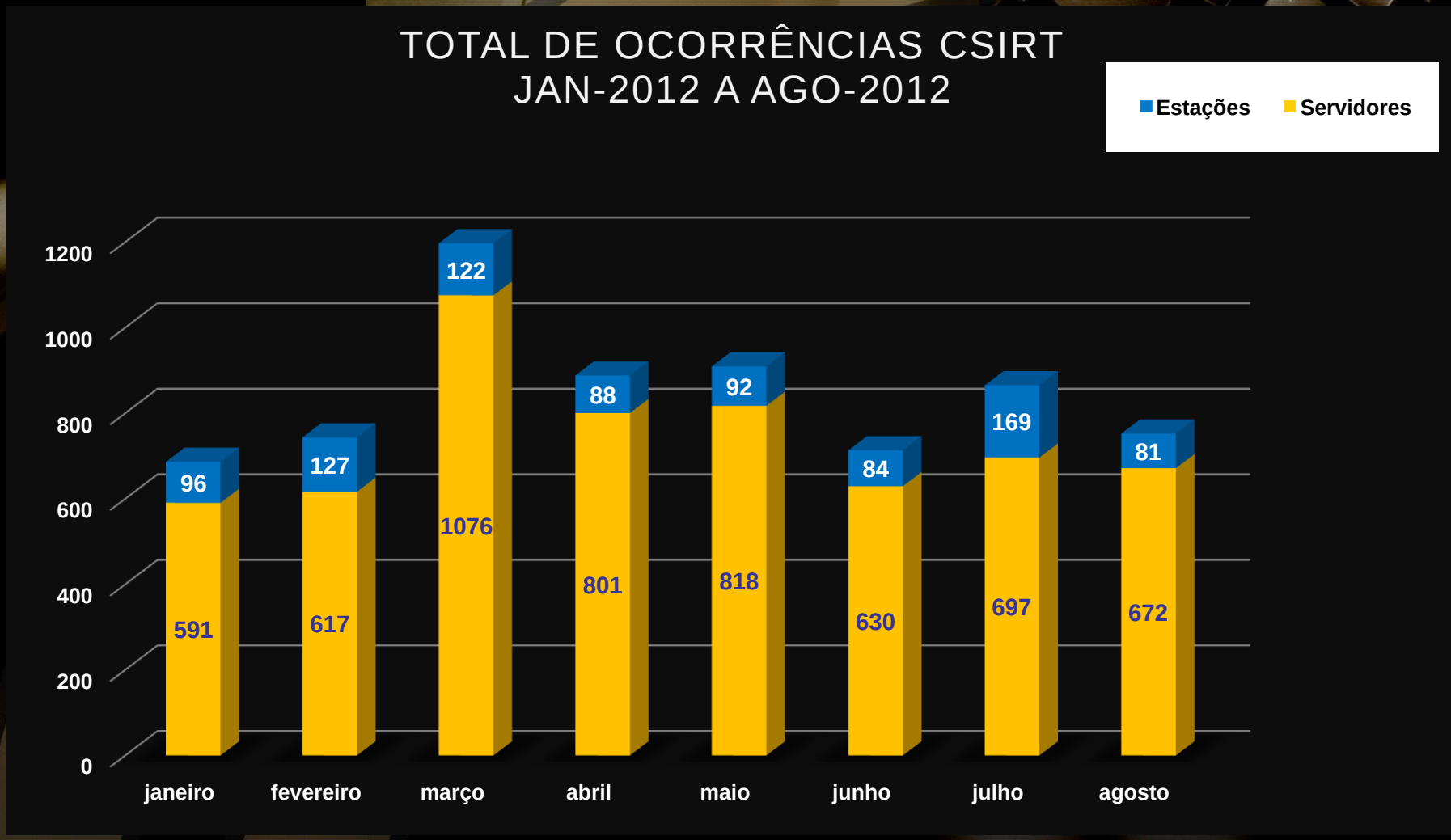
Mais de 15 mil links de acesso

AS GESP
(ASN 28637)

SP.GOV.BR
Mais de 2,5 mil domínios

Antes da Implantação

Servidores + Estações de Trabalho



Tipos de Ocorrências

- Desfiguração de páginas
- Malwares
- Ataques, Varreduras (portscans), Negação de Serviço (DoS), Brute Force, etc.
- Hospedagem de ferramentas maliciosas
- SPAM/Phishing
- Violação de Legislação
- Violação de Políticas e Normas
- Incidentes de Segurança
- Fraudes, Vazamentos de Informação
- Resposta a Ofícios Judiciais

Solução

- Desenvolvimento interno de ferramenta de monitoramento e gestão de vulnerabilidades nas estações de trabalho que geram incidentes (SG7)
- Implantação de ferramenta gestão de vulnerabilidades nos servidores, baseada no OWASP
- Soluções integradas com o sistema de chamados (tickets)
- Baixo custo de implantação e ambos hospedados em apenas 1 servidor

SG7

- Gestão de blindagem das estações e da segurança dos aplicativos homologados
- Disponibiliza um banco de dados para softwares de risco
- Redução de custos com o tratamento e quantidade de incidentes internos
- Baixo custo de desenvolvimento e implantação

PRODESP
Tecnologia da Informação

PRODESP ISO 9001 27001 20000 14001

SG7

SG7

- Mapeamento completo das estações de trabalho por setores
- Mapeamento dos usuários por setores (relação de permissões de dispositivos, pastas, acessos)
- Relação de softwares A SEREM avaliados por gestores
- Relação de softwares JÁ avaliados por gestores
- Relação de softwares de risco (não permitidos), homologados e desconhecidos (para avaliação ou homologação)

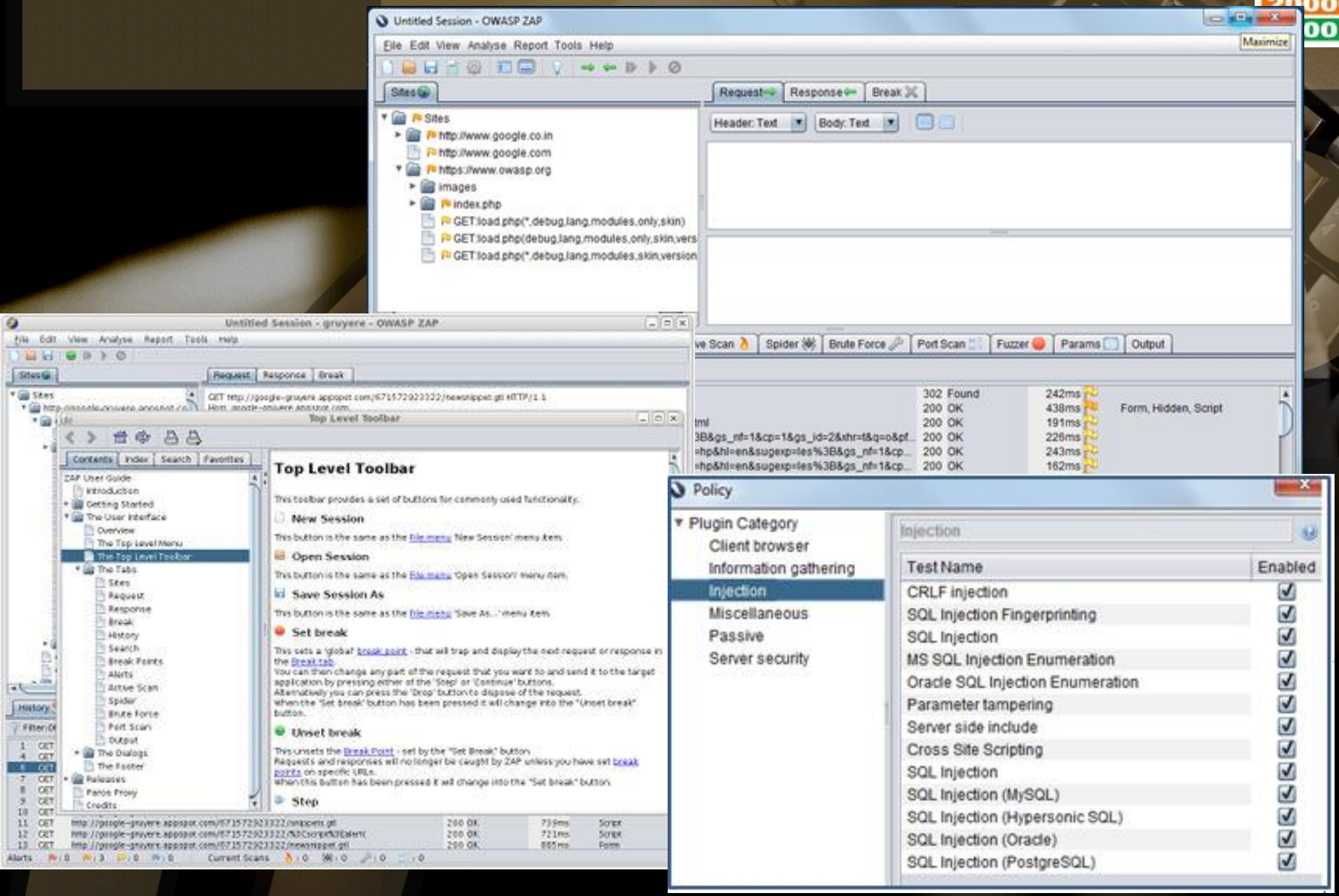
Análise de Vulnerabilidades

- Scan realizado nos domínios e portais
- Compara as 10 vulnerabilidades mais comuns (TOP 10 OWASP) e outras (Infraestrutura e outras vulnerabilidades)
- São realizadas cerca de 20 análises/semana

PRODESP
Tecnologia da Informação

Análise de Vulnerabilidades

PRODESP ISO 9001 27001 20000 001



Análise de Vulnerabilidades

- POC da solução – Julho/2012 - Dezembro/2012 (4 soluções testadas)
- 3 profissionais do time de CSIRT dedicados na ferramenta
- Acesso ao ambiente previamente autorizado pelo cliente
- Envia e analisa cerca de 5000 pacotes por hora
- Relatório detalhado com recomendações de correção

Relatório Detalhado

3. DETALHES DAS VULNERABILIDADES

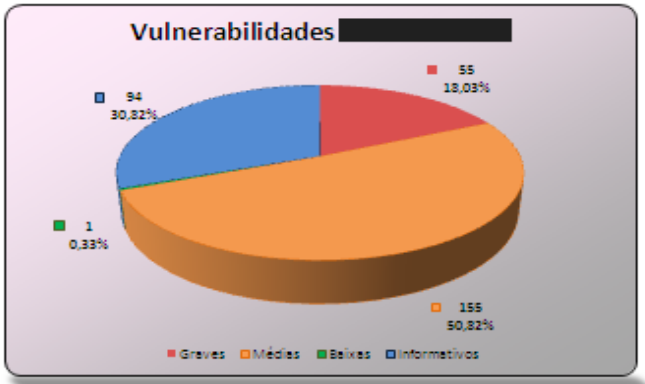
Na análise executada pelo CSIRT em 2[redacted], onde estes testes abordaram buscas intrusivas e testes de profundidade, gerando mais de 200 mil pacotes enviados para a URLs e mais de 500 MB de logs de capturas para análise. Houve um agendamento prévio com a equipe de TI [redacted]ara a varredura do servidor de hostname [redacted], onde monitoraram todos os passos e acessos das técnicas usadas.

Vulnerabilidades encontradas

Abaixo segue número de vulnerabilidades na página que foi requerida:

- https:/[redacted].sp.gov.br/

  Foram encontradas 305 vulnerabilidades na página [redacted].sp.gov.br, sendo elas:



55 vulnerabilidades graves de SQL Injection:

URLs Afetadas	Qtde
/administracao/download/dnl_templ1.asp	1
/administracao/download/dnl_templ2.asp	1
/administracao/download/dnl_templ3.asp	1
/administracao/download/dnl_templ5.asp	1
/administracao/download/dnl_templ6.asp	1
/administracao/formularios/download.asp	1
/administracao/formularios/listaqem.asp	4
/administracao/listatel_ninovamatricula.asp	1
/administracao/sc/psqsc.asp	1
/comunicacao/clipping/clpbusca_imgpop.asp	2
/comunicacao/clipping/clpbusca_principal.asp	2
/comunicacao/slsnoticias/headlines.asp	1
/eng_obras/expansao/centro/fotos/default.asp	2
/eng_obras/expansao/centro/fotos/view.asp	1
/gestcorp/galeria/foto_thumb.asp	1
/manutencao/forum/active.asp	1
/manutencao/portal_clm_app/cautelas/cautelas.asp	1
/manutencao/portal_clm_app/fotograf/asistemas_distribuicao.asp	1
/manutencao/portal_clm_app/fotograf/asistemas_material.asp	1
/manutencao/portal_clm_app/termomfalhas_periodo.asp	2
/manutencao/portal_mr_app/termomfalhas_periodo.asp	6
/manutencao/portal_mr_app/termomfalhas_periodocombois.asp	1
/operacao/dop/relatorios/media_pass_emb.asp	1
/operacao/dop/relatorios/media_pass_paq.asp	1
/operacao/dop/relatorios/melhoresmarcas.asp	1
/operacao/dop/relatorios/mov_est_mes.asp	1
/operacao/dop/relatorios/movtransf.asp	1
/operacao/frota/principal.asp	1
/operacao/portalcco/bilheteeletronico/carregaralax.asp	1
/operacao/rede_cotm/estacao.asp	1
/operacao/rop/cons/rop_blitz_det.asp	1
/patrimonio/documentos_tecnicos/localizadoctec.asp	1
/rh/beneficios/convenioeducar/resultados.asp	2
/rh/desenv_organizacional/feedbackpositivo/detalhe_elo.asp	1
/rh/desenv_organizacional/feedbackpositivo/feedbackpos_cons.asp	4
/rh/desenv_organizacional/profissional_destaque/popup_facilitador.asp	1
/rh/galeriarh/default.asp	2
/rh/selecaointerna/listaresultados.asp	1

Relatório Detalhado

Descrição da Vulnerabilidade: O SQL Injection ou injeção no SQL é uma vulnerabilidade que ocorre em aplicações web. O principal motivo de vulnerabilidades de SQL ocorrerem são erros de validação de desenvolvimento, onde não são feitos os tratamentos necessários das variáveis que serão passadas pelos métodos GET ou POST, isto permite o atacante injetar diretamente na URL ou formulários, comandos arbitrários de SQL para consulta, modificação ou exclusão de tabelas, colunas e valores. A linguagem (SQL Structured Query Language) é uma linguagem nativa que será utilizada em todos os serviços como MySQL, MSSQL, Postgre, Oracle, entre outras.

Cada campo é chamado de tuplas, as tuplas são onde os dados ficarão armazenados de acordo com o seu tipo e o tipo da coluna que foi definida, ou seja, não é possível armazenar em um campo de uma tabela que foi definido como inteiro e armazenar chars.

Correção: A correção sugerida aborda a validação de campos e variáveis. É necessário executar filtros de metacaracteres nas entradas do código que efetua interação com o Banco de Dados. Os comandos OPTIONS, GET, HEAD, DELETE, PUT, COPY, MOVE, DROP também foram aceitos pelo servidor mediante comandos arbitrários. Convém também revisar as URLs que estão nas pastas do servidor se estão em desuso, removendo-as.

Referências de Pesquisa:

https://www.owasp.org/index.php/Injection_Flaws

http://www.wisec.it/en/Docs/and_more_sql_injection.pdf

https://sparrow.ece.cmu.edu/group/731-s11/readings/anley-sql-inj.pdf

Amostra do teste para SQL Injection:

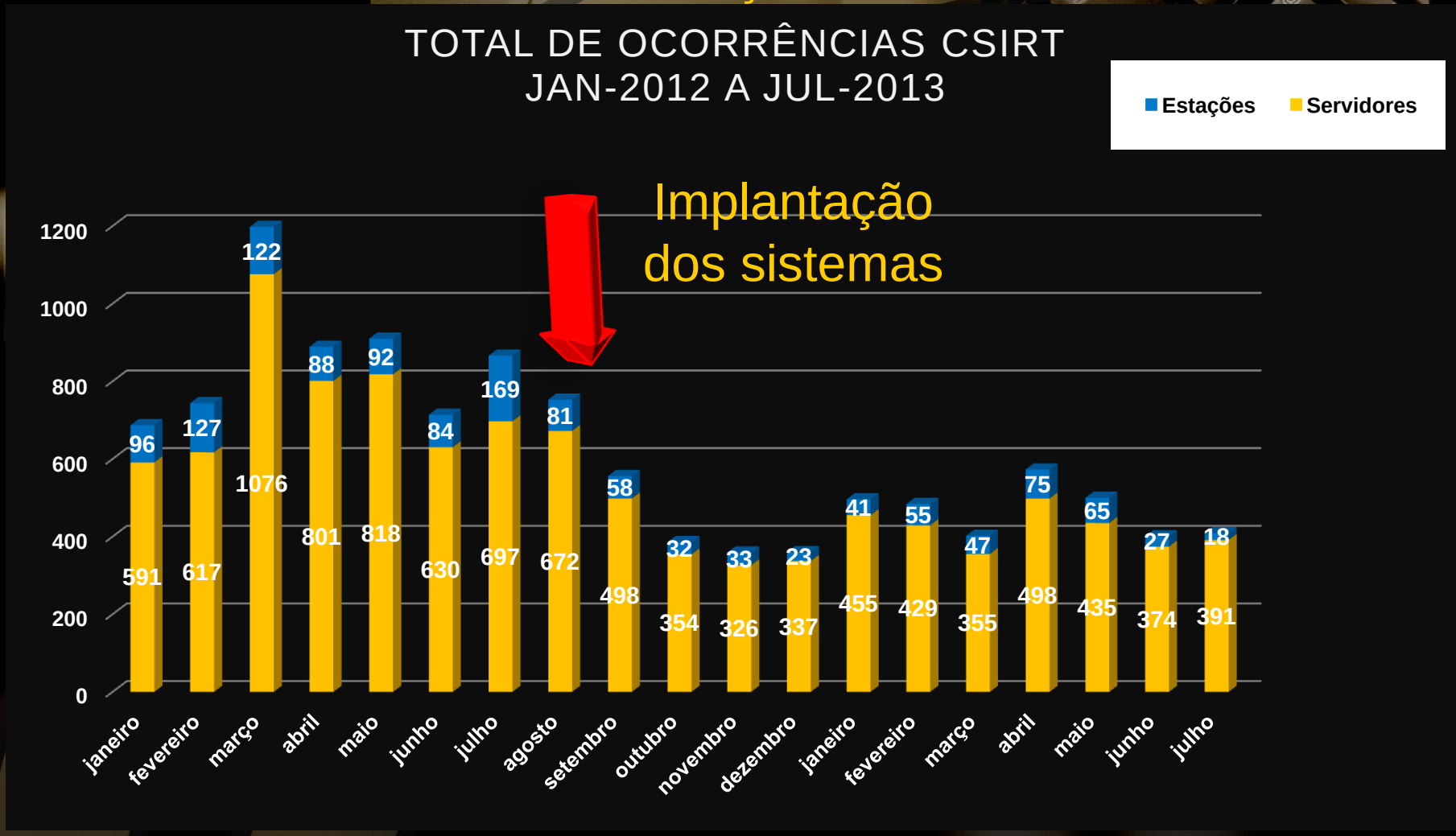
```
URL encoded GET input subcat was set to -1 or 45 = 45
Request headers
GET /administracao/download/dnl_templ1.asp?subcat=-1%20or%2045%20%3d%2045 HTTP/1.1
X-Requested-With: XMLHttpRequest
(line truncated) ...MLLPOBBMH;
ASPSESSIONIDQATASDSB=OHGDPBLAELGPAFCCGAEAHPPA; ASPSESSIO-
NIDQCTDSCTB=NPGNGELAJBPOLJBAPIHLLPKI; fcspersistslider1=2; ASPSESSIONID-
QCRCTDSA=PLHNMLNABCIGDGMOAFLFDGCH;
ASPSESSIONIDSATASBRD=EMHNMLNAKCINGEJDKPDLAPMP; ASPSES-
SIONIDSCTCSATA=BKOLIKLABPOFAFMJMOGABIC L;
ASPSESSIONIDSATDRBQC=BHOJPMLAHOBFEDONMHFAHIMJ;
ASPSESSIONIDSARAQDTA=MFIFOLNADODJDPENHFGOBGMJ; ASPSESSIO-
NIDSATCSAQC=DAJNDIOAPIHKMKOLPMBHKMFL;

ASPSESSIONIDSCRCTCTA=COOFJKLALHAMIHGOCBFDHKJN; ASPSESSIO-
NIDSCTDRCSB=BKCBBAMAGPCCKKEHPAOOMLDH
Host: [redacted]sp.gov.br
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Accept: */*
Authorization: ~~~~~
```

155 vulnerabilidades médias, sendo que todas elas são de HTML sem proteção contra CSRF - Cross-Site Request Forgery.

URLs Afetadas	Qtde
/	1
/administracao/ap_rd/geral/leftmenu.asp	1
/administracao/formularios/default.asp	1
/administracao/listatel_n/default.asp (9da5267e0cd74cc7dc270f81f2b15f4b)	2
/administracao/listatel_n/novamatricula.asp	1
/administracao/meioambiente/fale.asp	1
/administracao/sc/psqsc.asp	1
/administracao/sistema_normativo/default.asp	1
/comum/library/asp/calendario.asp	1
/comunicacao/clipping/cl/pbusca_pesq.asp	1
/comunicacao/enquete/enquetehome.htm	1
/comunicacao/jornalcptm/2011_01_jan/jornal.asp (4de9fbcaf4a2071bf2ba0db519ed0ac1)	1
/comunicacao/slsnoticias/add_comment.asp (98284aceff1d0a83c2f4d90f0fe270a5d)	1
/comunicacao/slsnoticias/add_comment.asp (e89d86cca77a25fe6314acb004ee255a)	1
/comunicacao/slsnoticias/add_comment.asp (f32386d781773d8a292b642f9b51650fe)	1

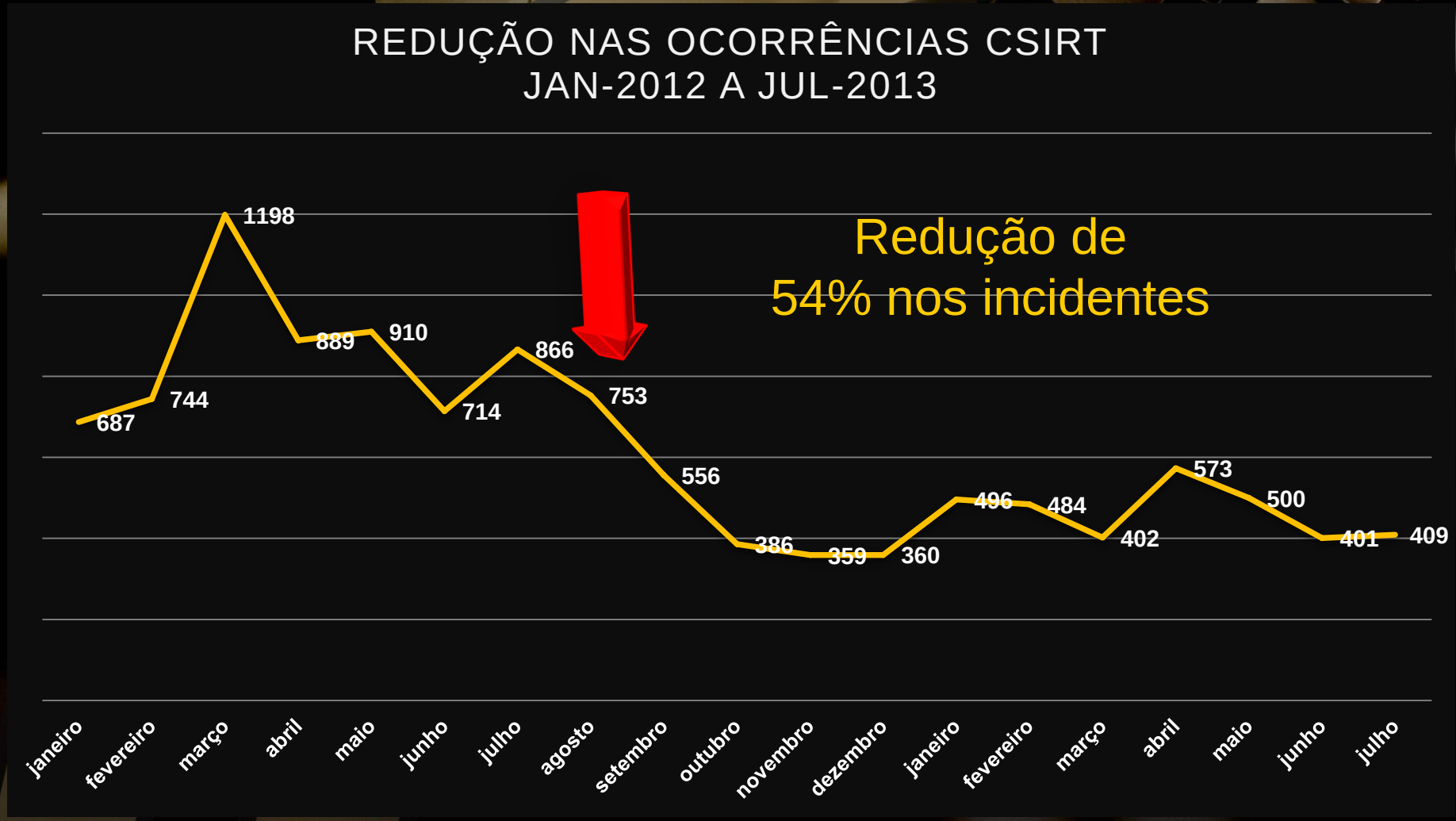
Após a Implantação

Servidores + Estações de Trabalho



Após a Implantação

Servidores + Estações de Trabalho



Desafios e Dificuldades

- Ausência de ferramentas de Inteligência
- Tempo de aquisição de ferramentas (média 2 anos)
- Estigma de que CSIRT é só reativo
- Justificar PoC de ferramentas
- Apoio de parceiros (Infra, Desenvolvimento e Rede Local)
- Capacitação da equipe
- Manutenção e implantação de ferramentas opensource

Conclusão

- 2012
  - 42 desfigurações
  - Análises de Vulnerabilidade reativas
  - POC de soluções de mercado
- 2013
  - 14 desfigurações (até 16/09)
  - Análise de Vulnerabilidade proativas – Foco Data Center
  - Lean Six Sigma e GT de Segurança da Informação
  - Criação de um novo serviço: Análise de Vulnerabilidade Técnica
- 2014
  - Análise de Vulnerabilidade nas páginas externas

Obrigado!

André Braga
abraga@sp.gov.br
(11) 2845-6801

Thiago B. Santana
tbsantana@sp.gov.br
(11) 2845-6344

cso@sp.gov.br
csirt@sp.gov.br
INOC: 28637*800