nic.br cgi.br | cert.br

ANBIMA
27 de maio de 2021
On-line

MISP para Compartilhamento de Informações e IoCs

cert.br nic.br cgi.br

Introdução às Atividades do CERT.br

cert.br nic.br cgi.br

Serviços Prestados à Comunidade

Gestão de Incidentes

- Coordenação
- Análise Técnica
- Suporte à Mitigação e Recuperação

Consciência Situacional

- Aquisição de Dados
  - *Honeypots* Distribuídos
  - SpamPots
  - *Threat feeds*
- Compartilhamento das Informações

Transferência de Conhecimento

- Conscientização
  - Desenvolvimento de Boas Práticas
  - Cooperação, Eventos e Reuniões (*Outreach*)
- Treinamento
- Aconselhamento Técnico e Político

Filiações e Parcerias:

FIRST Improving Security Together MEMBER

ACCREDITED BY TI TRUSTED INTRODUCER

APWG RESEARCH PARTNER www.antiphishing.org

CARNEGIE MELLON UNIVERSITY SOFTWARE ENGINEERING INSTITUTE

SEI Partner Network

HN/P

Criação:

Agosto/1996: CGI.br publica o relatório "Rumo à Criação de uma Coordenadoria de Segurança de Redes na Internet Brasil"[1]

Junho/1997: CGI.br cria o CERT.br (à época chamado NBSO – *NIC BR Security Office*), com base nas recomendações do relatório[2]

[1] https://cert.br/sobre/estudo-cgibr-1996.html | [2] https://nic.br/pagina/gts/157

Missão

Aumentar os níveis de segurança e de capacidade de tratamento de incidentes das redes conectadas à Internet no Brasil.

Público Alvo (*Constituency*)

Redes que utilizam recursos administrados pelo NIC.br

- endereços IP ou ASNs alocados ao Brasil
- domínios sob o ccTLD .br

Governança

Mantido pelo **NIC.br** – Núcleo de Informação e Coordenação do .br

- todas as atividades são sustentadas pelo registro de domínios .br

O NIC.br é o **braço executivo do CGI.br** – Comitê Gestor da Internet no Brasil

- entidade multissetorial
- responsável por coordenar e integrar as iniciativas e serviços da Internet no País

https://cert.br/sobre/
https://cert.br/sobre/filiacoes/
https://cert.br/about/rfc2350/

TLP:WHITE

Foco do CERT.br nestes 22 anos:
Aumentar a Capacidade Nacional de Tratamento de Incidentes

Nenhum grupo ou estrutura única conseguirá fazer sozinho a segurança ou a resposta a incidentes

Comunidade Nacional

- Auxiliar na análise técnica e facilitar o tratamento de incidentes por outros CSIRTs
- Ações junto a setores chave, para criação e treinamento de Grupos de Tratamento de Incidentes de Segurança (CSIRTs)
- Gerar massa crítica para possibilitar a cooperação e melhora na segurança das redes
- Ter uma visão sobre as principais tendências de ataques no Brasil

Comunidade Internacional

- Estabelecer relações de confiança
  - facilitar a comunicação em casos de incidentes
  - dar acesso a informações que ajudem a comunidade local
- Influenciar os padrões e certificações sendo construídos para CSIRTs
- Levar a visão nacional aos fóruns pertinentes

Cooperação Internacional: **Construção de Confiança**

TLP:WHITE

FIRST

Fórum existe desde 1992

- membro desde 2002

É uma Rede Global de CSIRTs

- fomenta a cooperação
- acesso a times e especialistas do mundo todo

Destaques da Participação:

- Coordenação de conteúdo do padrão *FIRST CSIRT Services Framework*
- *Co-chair* do *Membership Committee* e do *Security Lounge SIG*
- *Chair* da Conferência 2020
- Viabilização da parceria entre o FIRST e o LACNIC
  - CERT.br é *co-host* dos TCs e Simpósios na região

Rede de CSIRTs Nacionais

Existe desde 2006

Fórum para discussão de assuntos específicos para grupos de responsabilidade nacional

- CERT.br e CTIR Gov são membros

Maiores parceiros do CERT.br:

CERT/CC	US-CERT	CERT.at
NCSC-NL	NCSC-FI	CERT.LV
JPCERT/CC	NISC JP	HKCERT
TWCERT/CC		

LAC-CSIRTs

Reunião de Grupos de Resposta a Incidentes de Segurança (CSIRTs) da região da América Latina e o Caribe – ocorre durante o LACNIC

Conscientização:
Portal InternetSegura.br

TLP:WHITE

Conscientização:
Materiais sob Licença Creative Commons

TLP:WHITE

TLP:WHITE

CSIRTs no Brasil:
Criação de Uma Comunidade Atuante

Foco

- Criar/aproximar CSIRTs (Grupos de Tratamento de Incidentes de Segurança) no Brasil
- Possuir profissionais preparados para resolver os problemas de segurança no país

Fórum Brasileiro de CSIRTs

- Evento anual para profissionais da área de Tratamento de Incidentes
- *Workshops* sobre assuntos específicos

Lista de CSIRTs Brasileiros

- https://cert.br/csirts/brasil/

Fomento à adoção de MISP

- https://cert.br/misp/

Cursos de Gestão de Incidentes

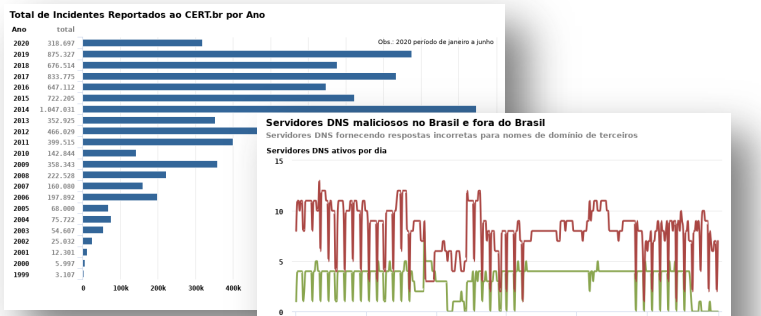
Ministra os cursos do *CERT® Division, do SEI/Carnegie Mellon,* desde 2004:

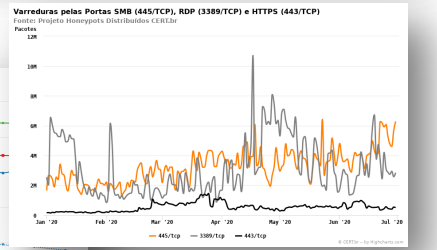
- 3 cursos, 1900+ alunos
- https://cert.br/cursos/

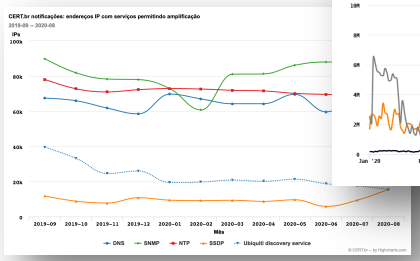
SEI Partner Network

TLP:WHITE

Compartilhamento de Indicadores para Consciência Situacional







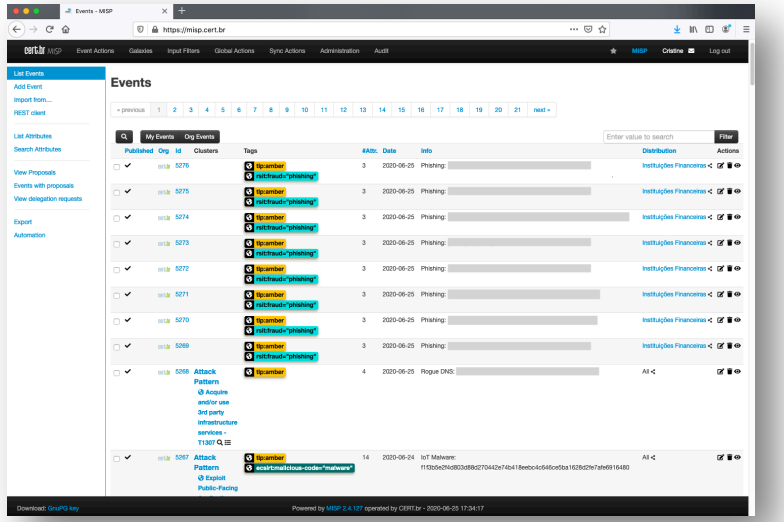
Estatísticas Públicas

https://cert.br/stats/

Notificações de Incidentes

Honeypots e *Threat Feeds*

Notificações para os Sistemas Autônomos



Compartilhamento de indicadores via MISP

https://cert.br/misp/

MISP para Compartilhamento de Informações e IoCs

cert.br nic.br cgi.br

MISP – Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing

TLP:WHITE

O que é o MISP

– uma plataforma de software livre para compartilhamento de dados de inteligência de ameaças
https://www.misp-project.org/

– um conjunto de padrões abertos para compartilhamento destas informações
https://www.misp-standard.org

Utilização de MISP ao redor do mundo em comunidades específicas

– *ENISA eCSIRT network*
– *TF-CSIRT Trusted Introducer*
– FIRST – *Forum of Incident Response and Security Teams*
– Redes setoriais de CSIRTs na Holanda e Sérvia
– Interpol

Uso de MISP no Brasil

Atividades promovidas pelo CERT.br

Treinamentos presenciais

- *Workshop* MISP, junto ao Fórum Brasileiro de CSIRTs em 2019 e 2020
- *Workshop* para a Febraban

Página dedicada ao MISP

https://cert.br/misp/

- Passo-a-passo de instalação e operação na página do CERT.br

  https://cert.br/misp/tutorial-ubuntu/

  https://cert.br/docs/palestras/certbr-workshop-misp2020.pdf
- Lista de discussão

  https://listas.cert.br/mailman/listinfo/misp-br

Setores utilizando MISP

- Acadêmico
- Energia
- Financeiro
- Governo
- Operadores de redes

O CERT.br compartilha os seguintes indicadores

- Servidores DNS maliciosos (todos)
- Binários e Comando e Controle de *botnets* IoT (todos)
- *Phishing* (setor financeiro)
- Amplificadores usados em ataques DDoS (operadores de redes)

Uso do MISP de maneira automatizada

cert.br nic.br cgi.br

REST API

O MISP tem uma REST API que possibilita:

- gerenciar (adicionar, atualizar e remover) eventos
- gerenciar atributos
- gerenciar *tags*
- gerenciar organizações
- gerenciar usuários
- submeter *sightings*
- obter estatísticas de atributos/*tags*
- etc

Referências: https://www.circl.lu/doc/misp/automation/

Exemplo de consulta utilizando curl

Buscando eventos publicados no último dia:

```
curl \
-d '{"returnFormat":"json","publish_timestamp":"1d"}' \
-H "Authorization: authkey" \
-H "Accept: application/json" \
-H "Content-type: application/json" \
-X POST https://<FQDN>/events/restSearch
```

PyMISP

O PyMISP é a biblioteca Python oficial utilizada para acessar o MISP através da sua REST API.

Com o PyMISP é possível:

- Adicionar, buscar, atualizar, publicar e apagar eventos
- Adicionar ou remover *tags*
- Adicionar atributos
- Fazer *upload*/*download* de binários
- Atualizar *sightings*
- Pesquisar por palavras chaves e por atributos

Referências:

https://www.circl.lu/doc/misp/pymisp/
https://pymisp.readthedocs.io/en/latest/
https://www.misp-project.org/tools/#libraries-to-access-the-misp-api

Obrigado

cristine@cert.br jessen@cert.br

Notificações para: cert@cert.br @certbr

www.cert.br

nic.br cgi.br

www.nic.br | www.cgi.br