GTS - Grupo de Trabalho em Segurança de Redes - 23ª Reunião

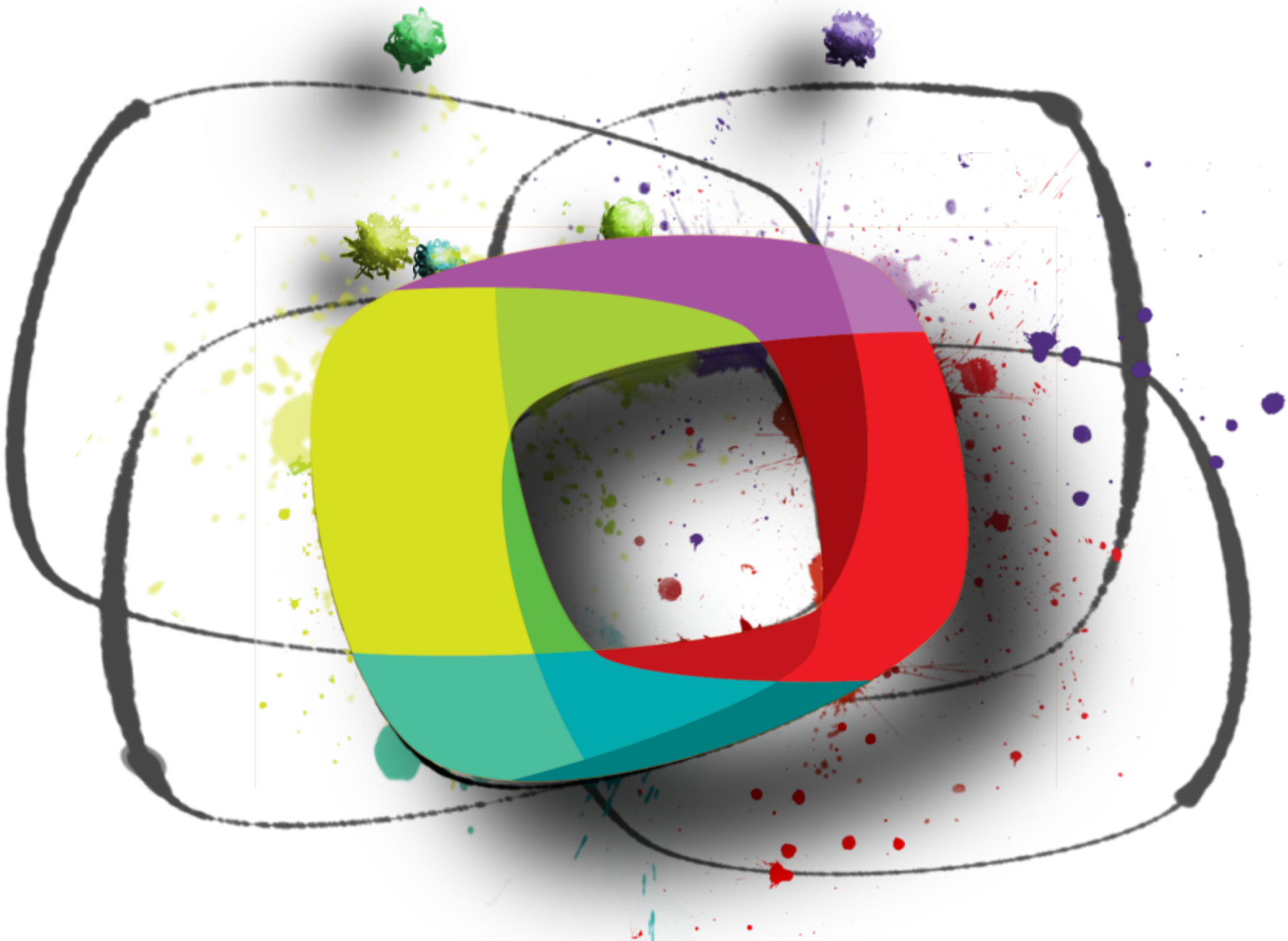
GESTÃO DE RISCOS COM BASE NO MONITORAMENTO DE AMEAÇAS

Leandro Bennaton
✉ leandro.bennaton@corp.terra.com.br
Twitter: @bennaton

Carlos H. Borella Jr.
✉ carlos.borella@corp.terra.com.br

Eleven Paths

terra



LEANDRO BENNATON

- Chief Security Officer responsável por Segurança e Conformidade de sistemas para LatAm, USA e Espanha na empresa **TERRA**
- Chief Security Ambassador na **ELEVEN PATHS**

Pós-Graduado em Gerenciamento de Segurança da Informação

Palestrante internacional de Segurança

Atuação nos grupos de trabalho de:
AntiSpam, Qualidade da Banda Larga e IPv6 conduzidos pelo Comitê Gestor Internet Brasil.

terra

CARLOS H. BORELLA JR.

- Security & Compliance Consultant responsável pelas avaliações de Segurança Tecnológica, Auditoria e Compliance para Latino América, Estados Unidos e Espanha na empresa **TERRA**

Pós-Graduado em Segurança da Informação e MBA em Gestão de Tecnologia

Certificações Internacionais:

CISSP, CISA, BS Lead Auditor (ISO/IEC 27001)

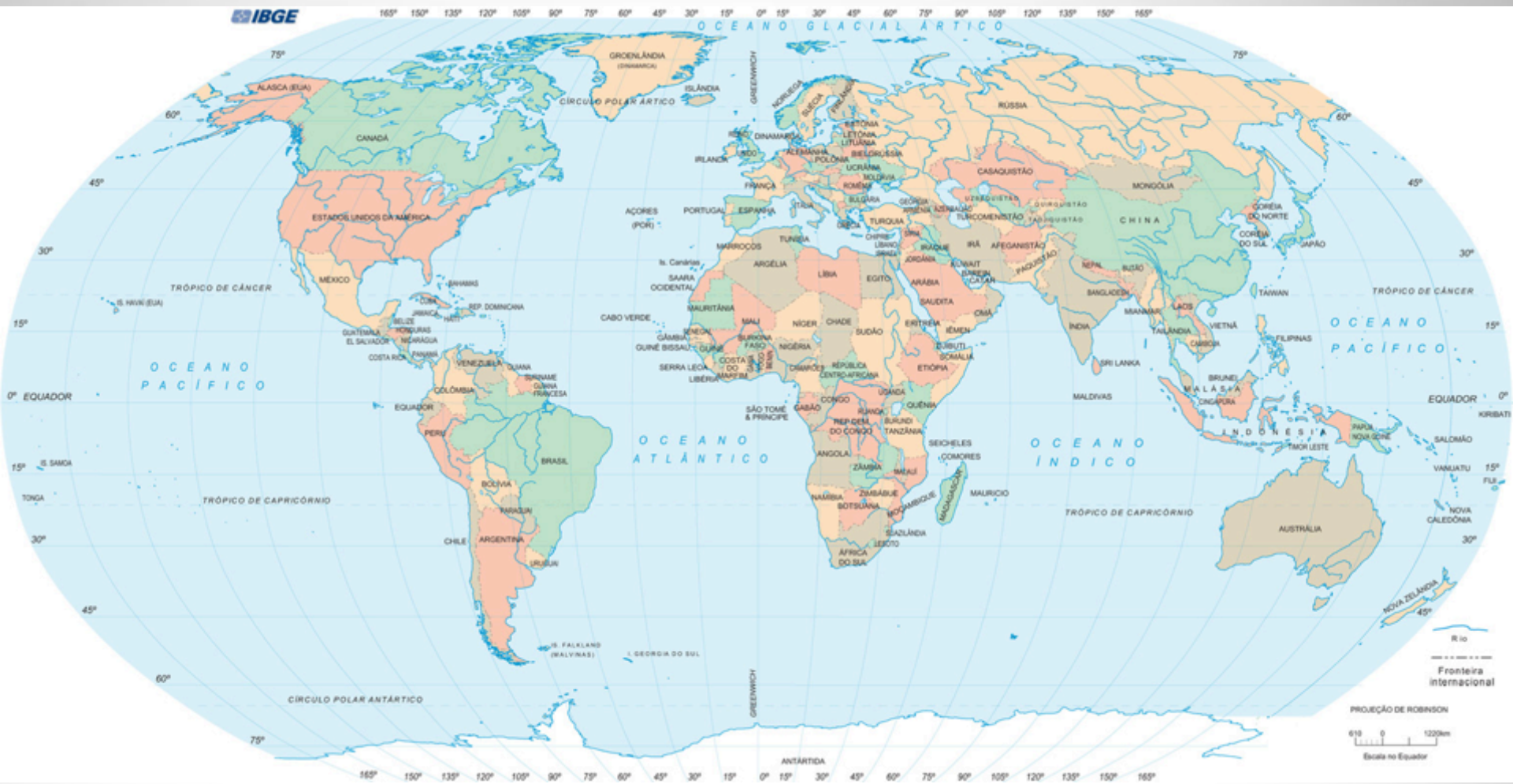
Criado em 1999, o Terra é referências em conteúdo digital em países de língua hispânica e portuguesa

Além dos 17 países da América Latina, está presente nos Estados Unidos e Espanha

terra

ATUAÇÃO – SECURITY & COMPLIANCE

terra



Equipe **GLOBAL** com sede em SP, responsável por Argentina, **Brasil**, Chile, Colômbia, **Estados Unidos**, **Espanha**, México e Peru

terra

ATIVIDADES – SECURITY & COMPLIANCE

- ❑ Requerimentos Legais
- ❑ Controle de Acesso
- ❑ Auditoria e Conformidade
- ❑ Segurança Física
- ❑ Gestão de Incidentes
- ❑ Fraudes
- ❑ Segurança Tecnológica
- ❑ Politicas & Normas
- ❑ Conscientização
- ❑ Proteção da Marca

Segurança

Atenção a postura!

Esta área deve ser **consultiva**!

terra

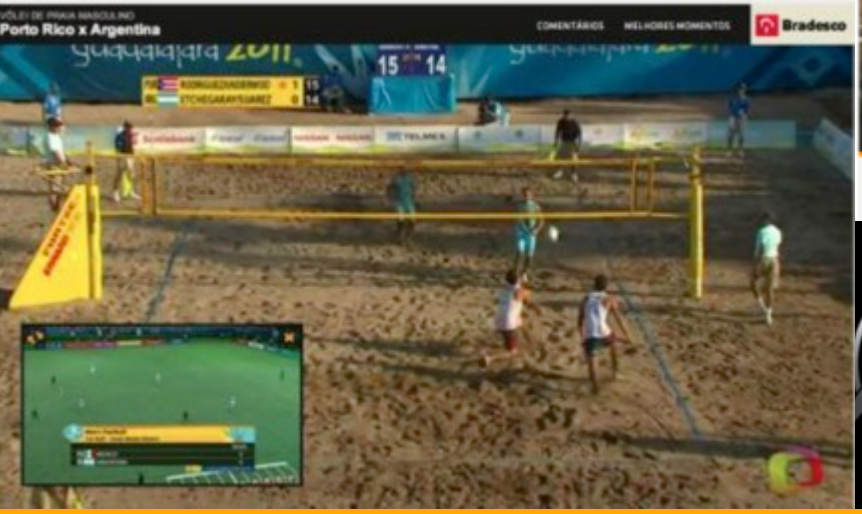
AGENDA

- Desafios
- Ambiente
- Metodologia
  - Análise de Vulnerabilidades
  - Aplicações
  - Classificação Criticidade
- Projeto → Processo
- Gestão de Riscos
- Resultados
- Monitoramento

CHALLENGES

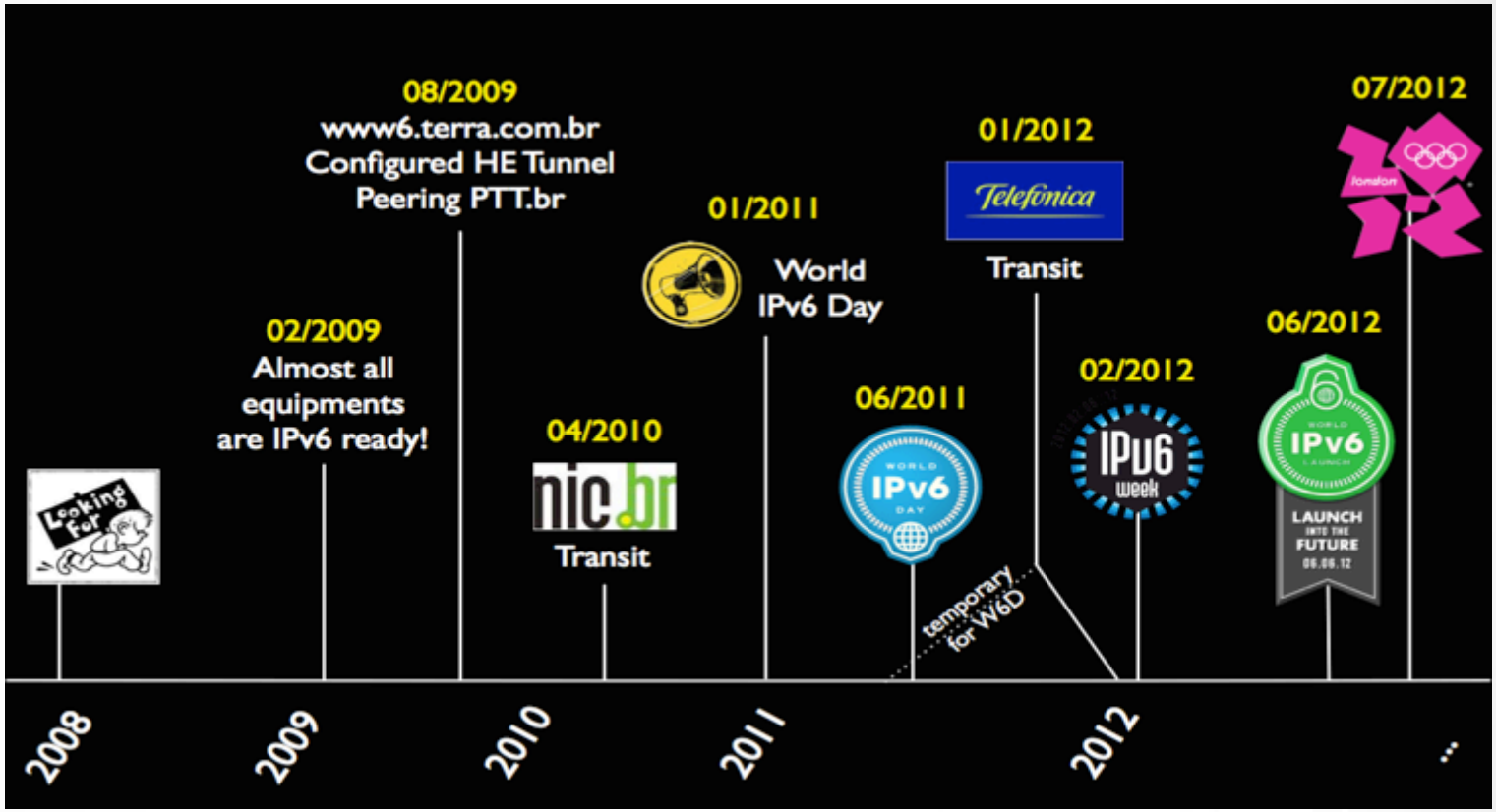
terra

TRANSMISSÕES AO VIVO



terra

IMPLEMENTAÇÃO IPV6



terra

For better security, think like a bad guy

terra

superfície
ataques

Contas de E-mails (*spammers*)

E-commerce (cartões de créditos)

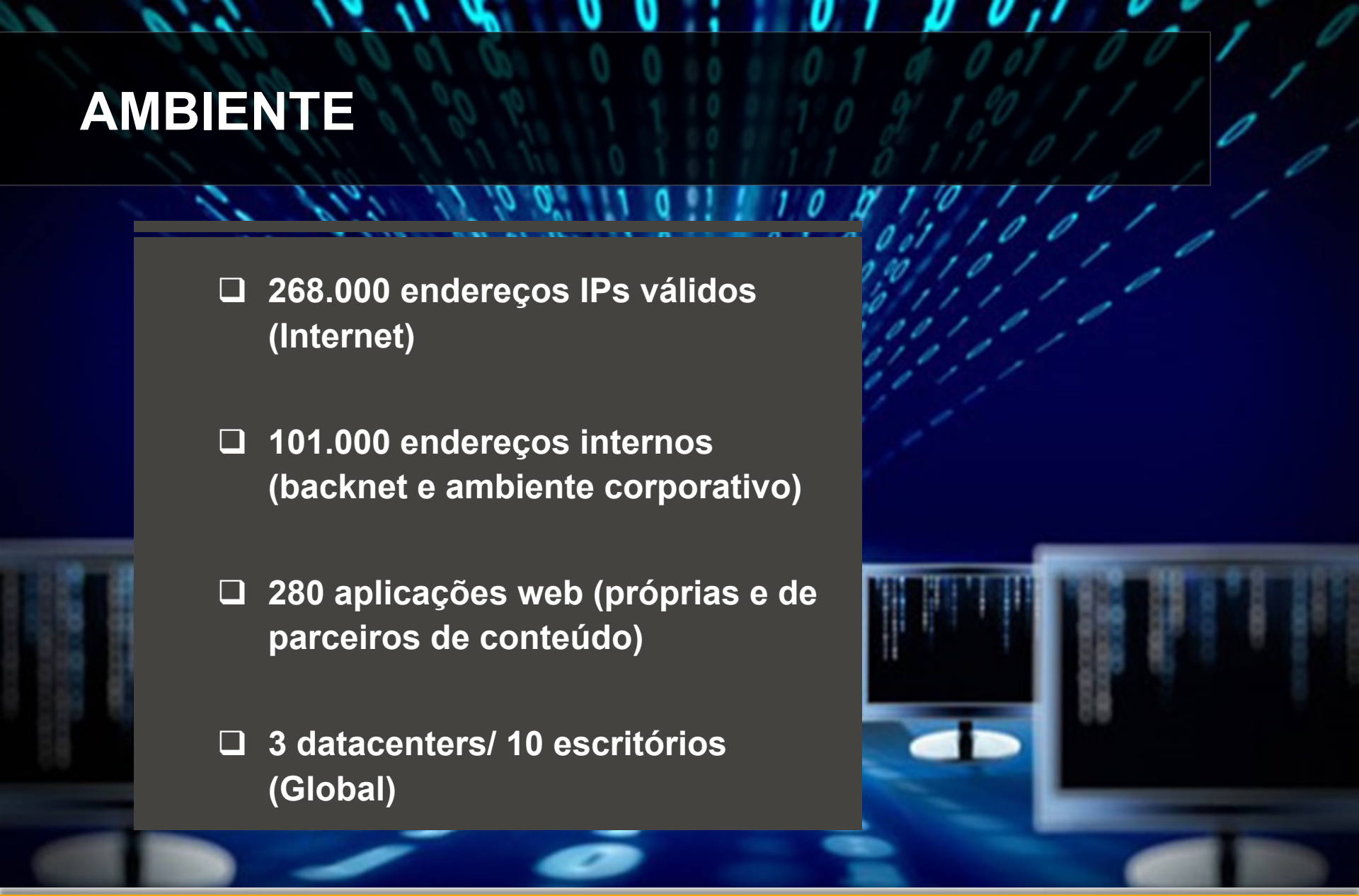
Base de Clientes (informações cadastrais)

Visibilidade e Abrangência (volume de acesso)

Hospedagem (*fake pages*)

AMBIENTE

- 268.000 endereços IPs válidos (Internet)
- 101.000 endereços internos (backnet e ambiente corporativo)
- 280 aplicações web (próprias e de parceiros de conteúdo)
- 3 datacenters/ 10 escritórios (Global)



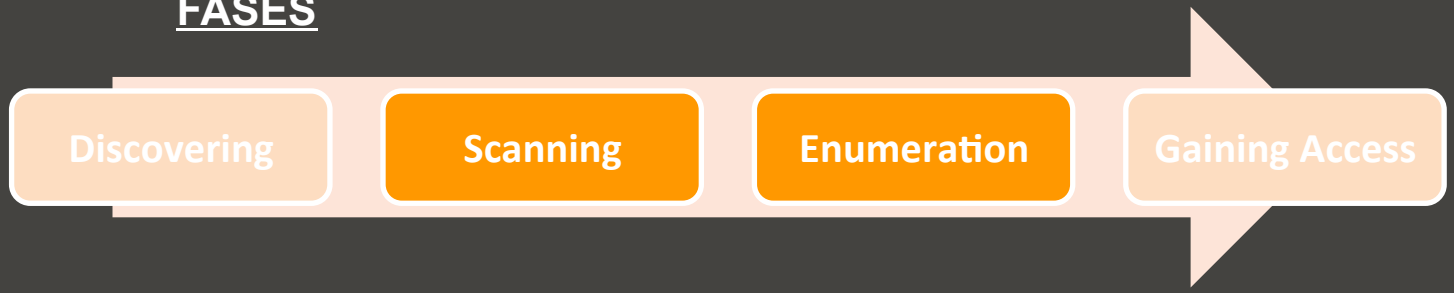
terra

METODOLOGIA – Análise de Vulnerabilidades

GreyBox

Utilização de credenciais legitimas, visando a validação das permissões de acesso e autorização estão em conformidade com as necessidades de negócio.

FASES



- Destaque para as fases de Scanning e Enumeration;
- No geral, a fase de Gaining Access, é realizada em aplicações onde há a necessidade de comprovar o impacto de vulnerabilidades críticas.

METODOLOGIA - Aplicações

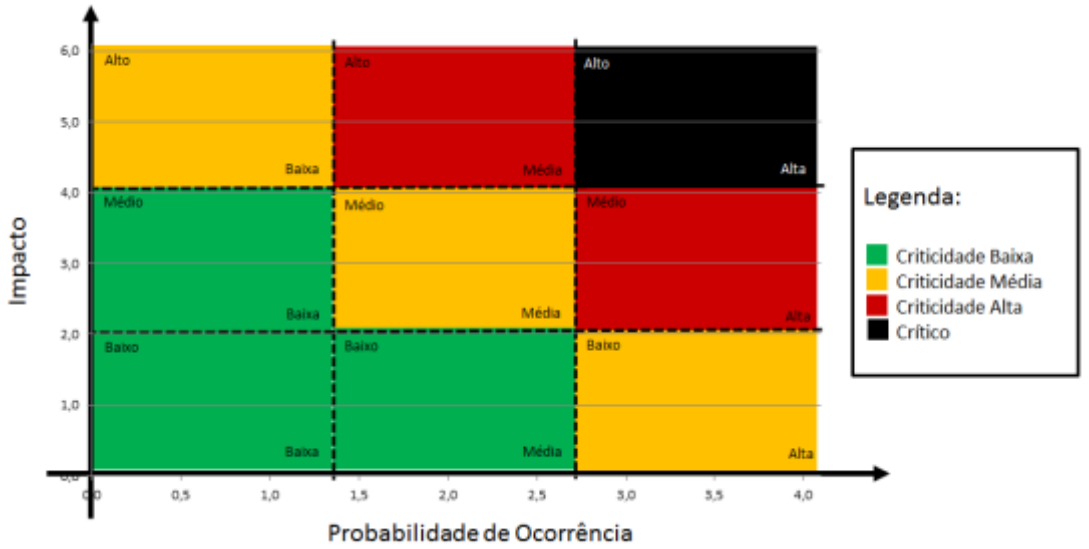
- Testes realizados com base nos 66 controles apresentados pelo OWASP TESTING GUIDE (v3.0):
  - Information Gathering
  - Configuration Management Testing
  - Business Logic Testing
  - Authentication Testing
  - Authorization testing
  - Session Management Testing
  - Data Validation Testing
  - Denial of Service Testing
  - Web Services Testing
  - Ajax Testing

METODOLOGIA – Classificação Criticidade

Calculadora CVSS2

Probabilidade de Ocorrência	Vetor de Acesso	Remoto	4,0
	Complexidade de Acesso	Baixa	
	Autenticação	Nenhuma	
Impacto	Confidencialidade	Completa	6,0
	Integridade	Completa	
	Disponibilidade	Completa	
	BASE SCORE	10,0	

Fator de Risco/Criticidade	
0.0	Nenhum
0.1 - 3.9	Baixo
4.0 - 6.9	Médio
7.0 - 9.9	Alto
10.0	Crítico



ameaças

vulnerabilidades

conhecidas

desconhecidas

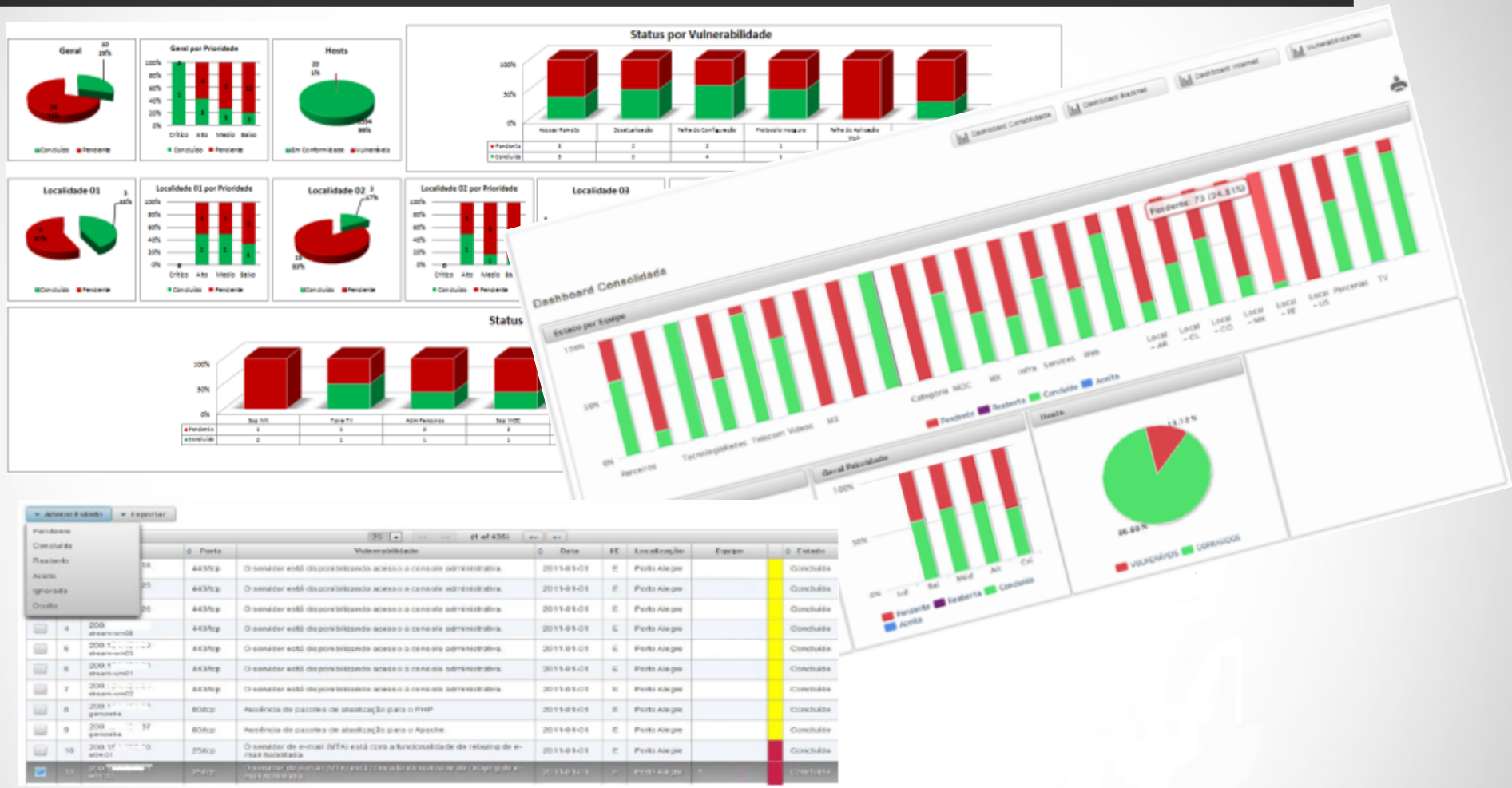
terra

PROJETO → PROCESSO

- Projeto em fases
(Externo, Interno e Aplicações)
- Cronograma e Comunicação
- Reporte executivos com informações relevantes
- Plataforma Web, em real time

terra

PROJETO → PROCESSO



PROJETO → PROCESSO

Ponto 03 **Criticidade Alta**	Os servidores web estão suscetíveis a uma vulnerabilidade no cabeçalho *Range* e *Request-Range* devido à utilização de uma versão desatualizada do Apache.		
IP da Máquina/ Nome da Máquina			
Impacto	Alto	**Probabilidade**	Alta
Recomendação	Atualizar o Apache para a versão 2.2.21 ou superior. Adicionalmente, é possível realizar algumas configurações alternativas, até que o servidor seja atualizado, conforme referência abaixo: http://mail-archives.apache.org/mod_mbox/httpd-announce/201108.mbox/%3C20110826103531.998348F82@minotaur.apache.org%3E		
Referências	CVE: CVE-2011-3192		

Os servidores web estão utilizando versões do Apache anterior à 2.2.20, as quais estão suscetíveis a ataques de *DoS* (*Denial of Service*) devido uma vulnerabilidade na forma como o Apache manipula o cabeçalho *HTTP*.

Esta vulnerabilidade permite que um atacante realize uma série de requisições com sobreposição de intervalos no cabeçalho *HTTP* (mais especificamente no cabeçalho *Range* ou *Request-Range*) resultando em uma sobrecarga no consumo de CPU e de memória, causando assim a paralisação do serviço. Já há um *exploit* publicado, além de terem sido notificados ataques, ao redor do mundo, que exploram esta vulnerabilidade.

Ponto 01 **Crítico**	As aplicações encontram-se vulneráveis a *Blind SQL Injection*.		
Site/ *URL*			
Impacto	Alto	**Probabilidade**	Alta
Recomendação	Evitar o uso de interpretadores externos sempre que possível, aproveitando que diversos *shell commands* e alguns *system calls* existam em bibliotecas específicas de linguagem que executam as mesmas funções sem envolver o interpretador de *Shell* do sistema operacional, e consequentemente, evita os riscos relacionados com o uso deste processo. Quando não for possível evitar o uso de interpretadores (ex. chamadas para *backend databases*), é fundamental validar os dados para garantir que não existe nenhum argumento malicioso que possa ser processado. Outra opção recomendada é a estruturação de requisições de forma a garantir que os parâmetros fornecidos são tratados como dados, ao invés de conteúdo executável, o que não elimina, mas reduz significativamente a possibilidade de ocorrência destas vulnerabilidades.		
Referência	http://www.owasp.org/index.php/Blind_SQL_Injection http://www.owasp.org/index.php/Guide_to_SQL_Injection http://www.owasp.org/index.php/Reviewing_Code_for_SQL_Injection		

A aplicação analisada está vulnerável a *Blind SQL Injection*. O *SQL* é a linguagem usada por bancos de dados para realizar consultas e alterar dados. Esta vulnerabilidade ocorre devido à possibilidade de um atacante inserir uma série de instruções *SQL* dentro de uma consulta (*query*) através da manipulação das entradas de dados de uma aplicação. Um usuário mal-intencionado pode explorar está vulnerabilidade de *SQL Injection* para alterar de formá maliciosa os comandos que são passados ao banco de dados, com isso, é possível ler ou alterar dados que normalmente não poderiam ser lidos e alterados.

Abaixo listamos os formulários vulneráveis a *Injection*:

/novosite/categoriacidades.cfm
/novosite/detail.cfm
/novosite/galerianova.cfm
/novosite/postnew.cfm
/novosite/reservas_p1.cfm

Foram realizados ataques automatizados e manuais visando à extração de informações sensíveis do banco de dados que suporta a aplicação.

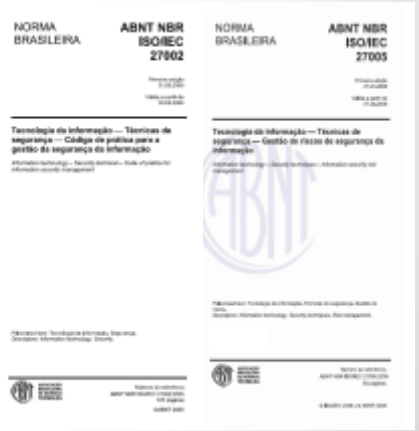
O primeiro passo foi levantar os nomes das tabelas existentes e, em seguida, consultar os dados de algumas tabelas, conforme ilustramos a seguir:

terra

terra

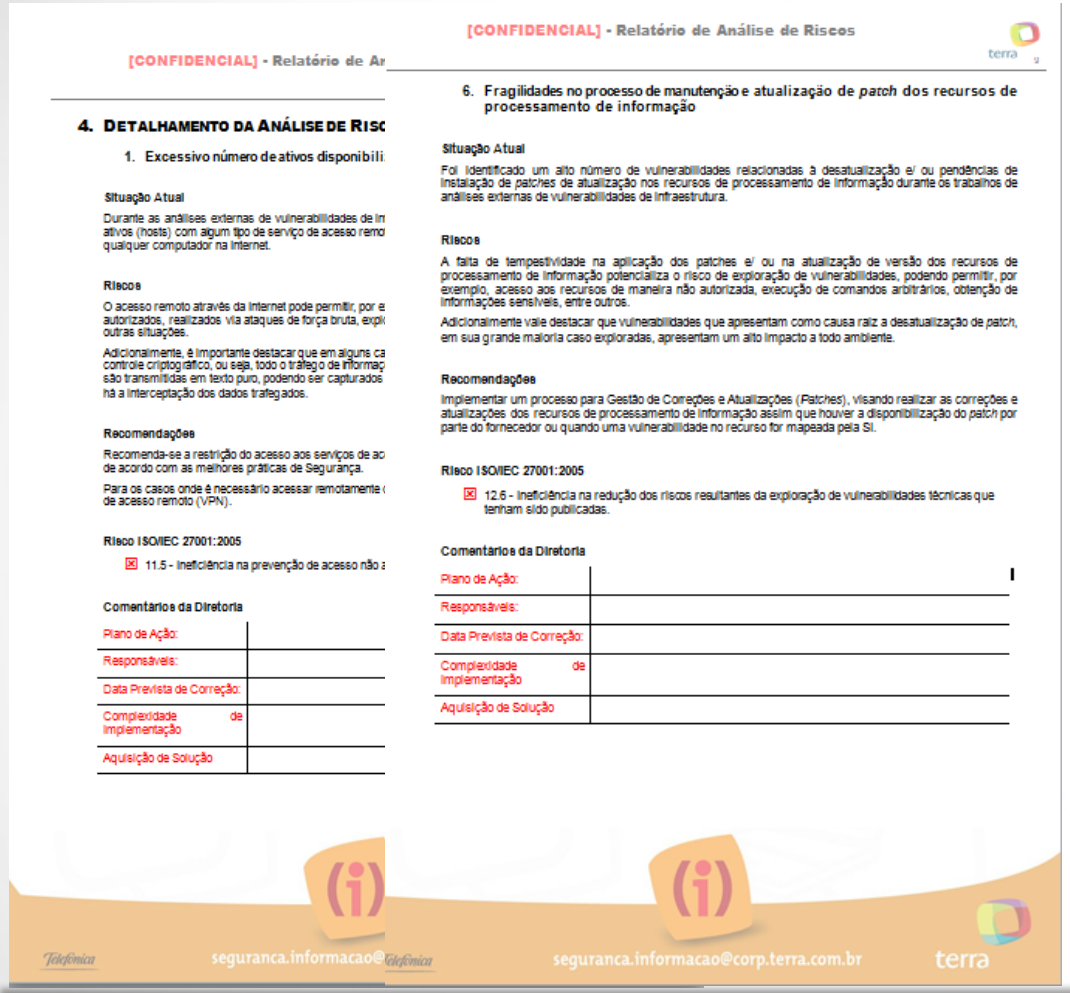
GESTÃO de RISCOS

- Transformar o “tecniques” em linguagem de negócio
- Apoio do CEO, CTO, direção
- Maior envolvimento de áreas de Tecnologia
- Métricas, Indicadores do PLR
- Mapa de Riscos Tecnológicos
  (atualização Trimestral/ reunião Semestral)



terra

GESTÃO de RISCOS



[CONFIDENCIAL] - Relatório de Análise de Riscos

terra

4. DETALHAMENTO DA ANÁLISE DE RISC

1. Excessivo número de ativos disponibili

Situação Atual

Durante as análises externas de vulnerabilidades de In
ativos (hosts) com algum tipo de serviço de acesso remo
qualquer computador na Internet.

Riscos

O acesso remoto através da Internet pode permitir, por e
autorizados, realizados via ataques de força bruta, explo
outras situações.

Adicionalmente, é importante destacar que em alguns ca
controle criptográfico, ou seja, todo o tráfego de informaç
são transmitidas em texto puro, podendo ser capturados
há a interceptação dos dados trafegados.

Recomendações

Recomenda-se a restrição do acesso aos serviços de ac
de acordo com as melhores práticas de Segurança.

Para os casos onde é necessário acessar remotamente
de acesso remoto (VPN).

Risco ISO/IEC 27001:2005

☒ 11.5 - Ineficiência na prevenção de acesso não a

Comentários da Diretoria

Plano de Ação:	
Responsáveis:	
Data Prevista de Correção:	
Complexidade de Implementação	
Aquisição de Solução	

[CONFIDENCIAL] - Relatório de Análise de Riscos

terra

6. Fragilidades no processo de manutenção e atualização de *patch* dos recursos de processamento de informação

Situação Atual

Foi identificado um alto número de vulnerabilidades relacionadas à desatualização e/ ou pendências de instalação de *patches* de atualização nos recursos de processamento de informação durante os trabalhos de análises externas de vulnerabilidades de infraestrutura.

Riscos

A falta de tempestividade na aplicação dos patches e/ ou na atualização de versão dos recursos de processamento de informação potencializa o risco de exploração de vulnerabilidades, podendo permitir, por exemplo, acesso aos recursos de maneira não autorizada, execução de comandos arbitrários, obtenção de informações sensíveis, entre outros.

Adicionalmente vale destacar que vulnerabilidades que apresentam como causa raiz a desatualização de *patch*, em sua grande maioria caso exploradas, apresentam um alto impacto a todo ambiente.

Recomendações

Implementar um processo para Gestão de Correções e Atualizações (*Patches*), visando realizar as correções e atualizações dos recursos de processamento de informação assim que houver a disponibilização do *patch* por parte do fornecedor ou quando uma vulnerabilidade no recurso for mapeada pela SI.

Risco ISO/IEC 27001:2005

☒ 12.6 - Ineficiência na redução dos riscos resultantes da exploração de vulnerabilidades técnicas que tenham sido publicadas.

Comentários da Diretoria

Plano de Ação:	
Responsáveis:	
Data Prevista de Correção:	
Complexidade de Implementação	
Aquisição de Solução	

Telefônica seguranca.informacao@ Telefônica seguranca.informacao@corp.terra.com.br terra

Legenda:	Impacto			
RB Risco Baixo RM Risco Médio RA Risco Alto		RM	RA	RA
		RB	RM	RA
		RB	RB	RM
		Probabilidade		

terra

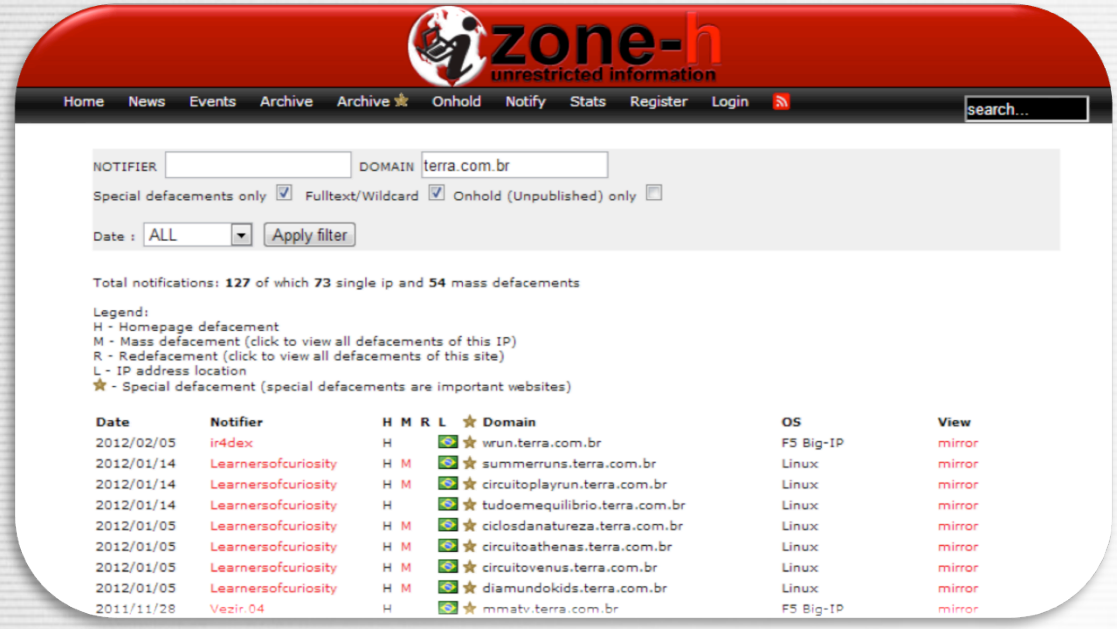
RESULTADOS

- ✓ +11.000 vulnerabilidades tratadas
- ✓ Melhor nível de proteção
- ✓ Não há *defacement* desde mar/12
- ✓ Percepção dos executivos da importância de SI e Governança
- ✓ Aumento da maturidade e cultura da Segurança da Informação

terra

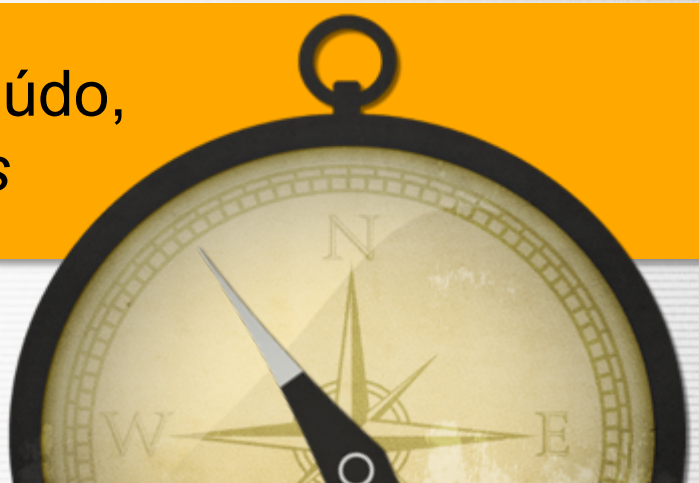
MONITORAMENTO

Defacements



Acompanhar notificação de domínios vítimas de Defacement

Atenção especial aos Parceiros de Conteúdo, foco na autopromoção de grupos *hackers*



terra

MONITORAMENTO

Malwares

Acompanhar notificação

domínios do Terra

relacionados a *Malwares*

Grande desafio no mapeamento e identificação, nos casos onde o *malware ou* problema está na Publicidade.

terra

MONITORAMENTO

From: "ctir@ctir.gov.br" <ctir@ctir.gov.br>
Subject: [CTIR Gov BR #57256] SMTP Abuse [parc-smtp02-tna-mia.terra.com|208.84.247.225]
Date: February 27, 2014 at 11:00:02 AM GMT-3
To: "abuse@terra.com" <abuse@terra.com>, "Eng. Redes" <eng.redes@corp.terra.com.br>
Cc: "soc@us-cert.gov" <soc@us-cert.gov>

Manager,

After analyzing incident (Phishing), we've detected that:
1. A machine with the IP address [208.84.247.225] probably hosts/relays a phishing message (see below).
2. We kindly request you to verify this occurrence since this machine could be compromised or abused.
3. This message was sent to the network's registered technical, administrative and contact, but if you are not

Trojan Detected – Please Shut Down! – [ATS #11019] – IP: 177.53.152.51 Domain: n...

RSA Anti-Fraud Command Center

Sent: quarta-feira, 3 de outubro de 2012 07:02
To: Terra – Abuse
Cc: Leandro Bennaton

[ATS ID - 11019]

PayPal 5146.2

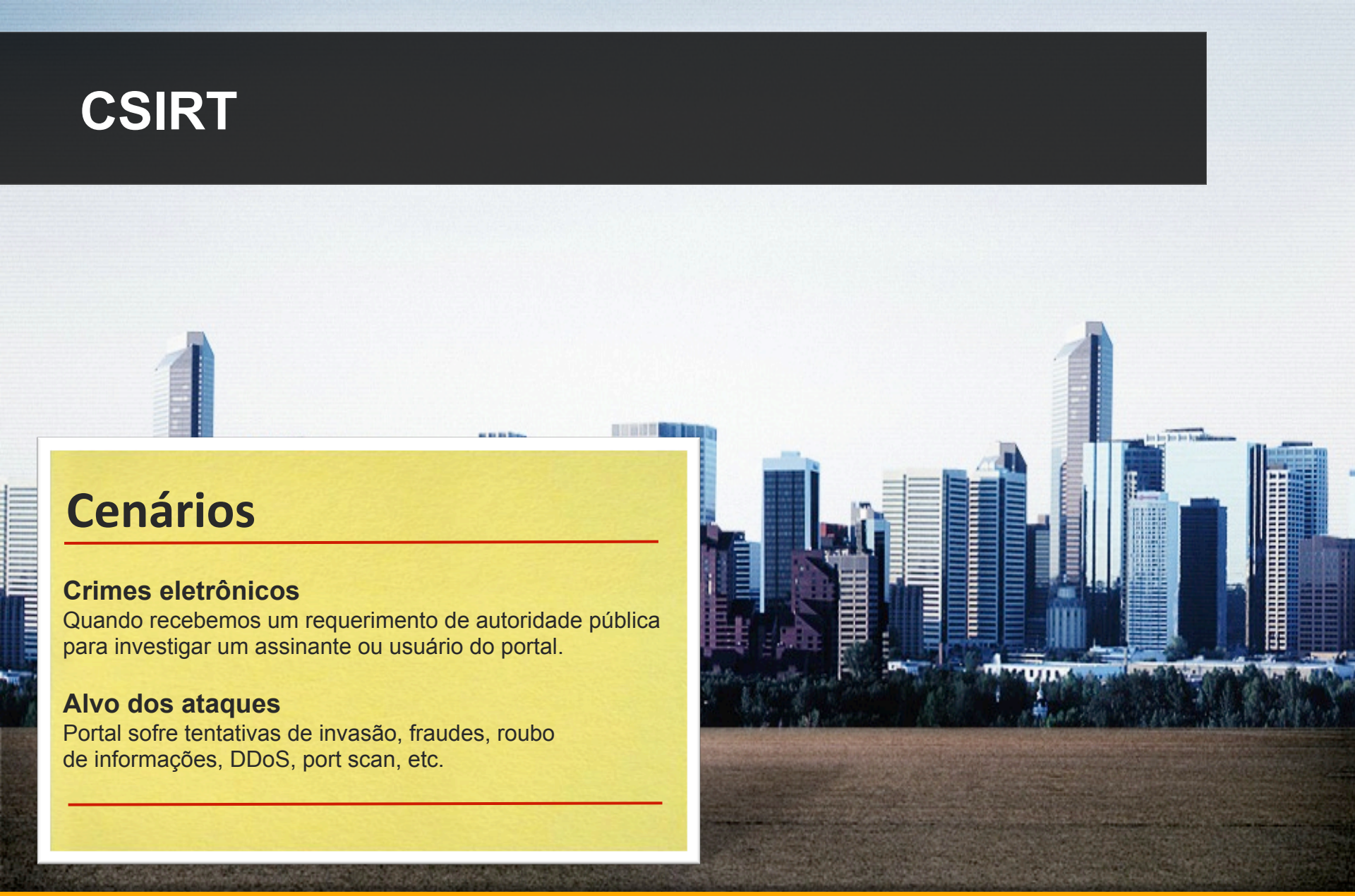
Dear Team, Please be advised that it is likely an empty page will appear when accessing the URL below. The resource under this URL is used by machines infected with a Trojan. The content is designed to remain undetected, thus an empty page or a fake error message may appear. Please take the necessary steps in order to disable this fraudulent URL. We appreciate your cooperation. RSA Security – Anti Trojan Team

Abuse

- CTIR
- CSIRT
- Serviços

terra

CSIRT



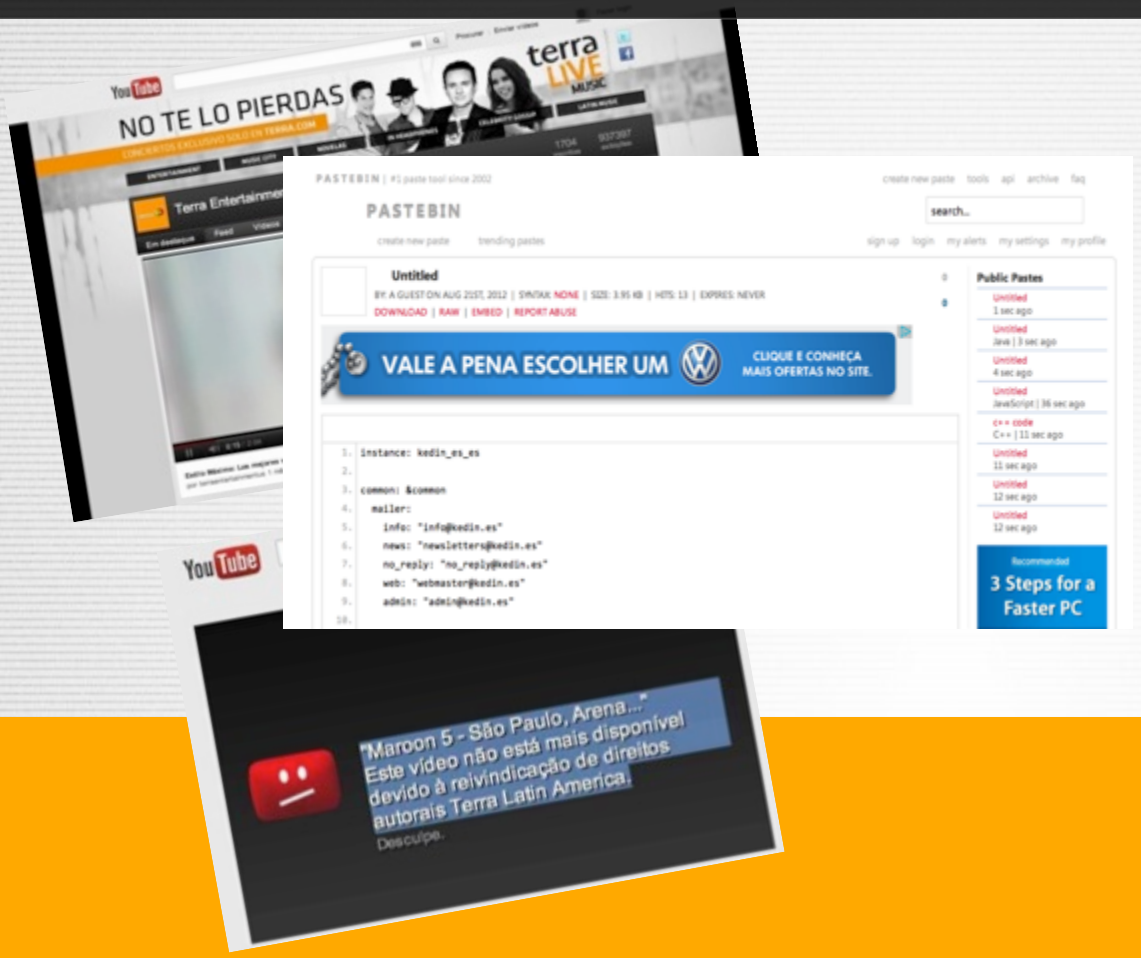
Cenários

Crimes eletrônicos
Quando recebemos um requerimento de autoridade pública para investigar um assinante ou usuário do portal.

Alvo dos ataques
Portal sofre tentativas de invasão, fraudes, roubo de informações, DDoS, port scan, etc.

terra

MONITORAMENTO



Marca

Brand Protection

Acompanhar a marca

(Pastebin, Youtube, etc)

terra

MONITORAMENTO

Marca

nokterra.com	Ativo - 200 - OK
positivterraceapartmentbarcelona.com	Inativo - 404 - Not Found
puidukodafranceterrasses.com	Inativo - 404 - Not Found
rhterra.com	Inativo - Connection Error
rousselet-terrassement.com	Ativo - 301 - Moved Permanently
sonorachemical.com	Ativo - 200 - OK
sonorataxhelp.com	Ativo - 200 - OK
superterradx.com	Ativo - 200 - OK
terra-studios.com	Ativo - 200 - OK
terracaptura.com	Ativo - 200 - OK
terracecentralapartmentbarcelona.com	Inativo - 404 - Not Found
terradaxis.com	Ativo - 200 - OK
terradiciclismo.com	Ativo - 200 - OK
terradomis.com	Inativo - Connection Error

terra

segurança da informação

Leandro Bennaton
✉ leandro.bennaton@corp.terra.com.br
@bennaton

Carlos Borella
✉ carlos.borella@corp.terra.com.br

Obrigado!

terra