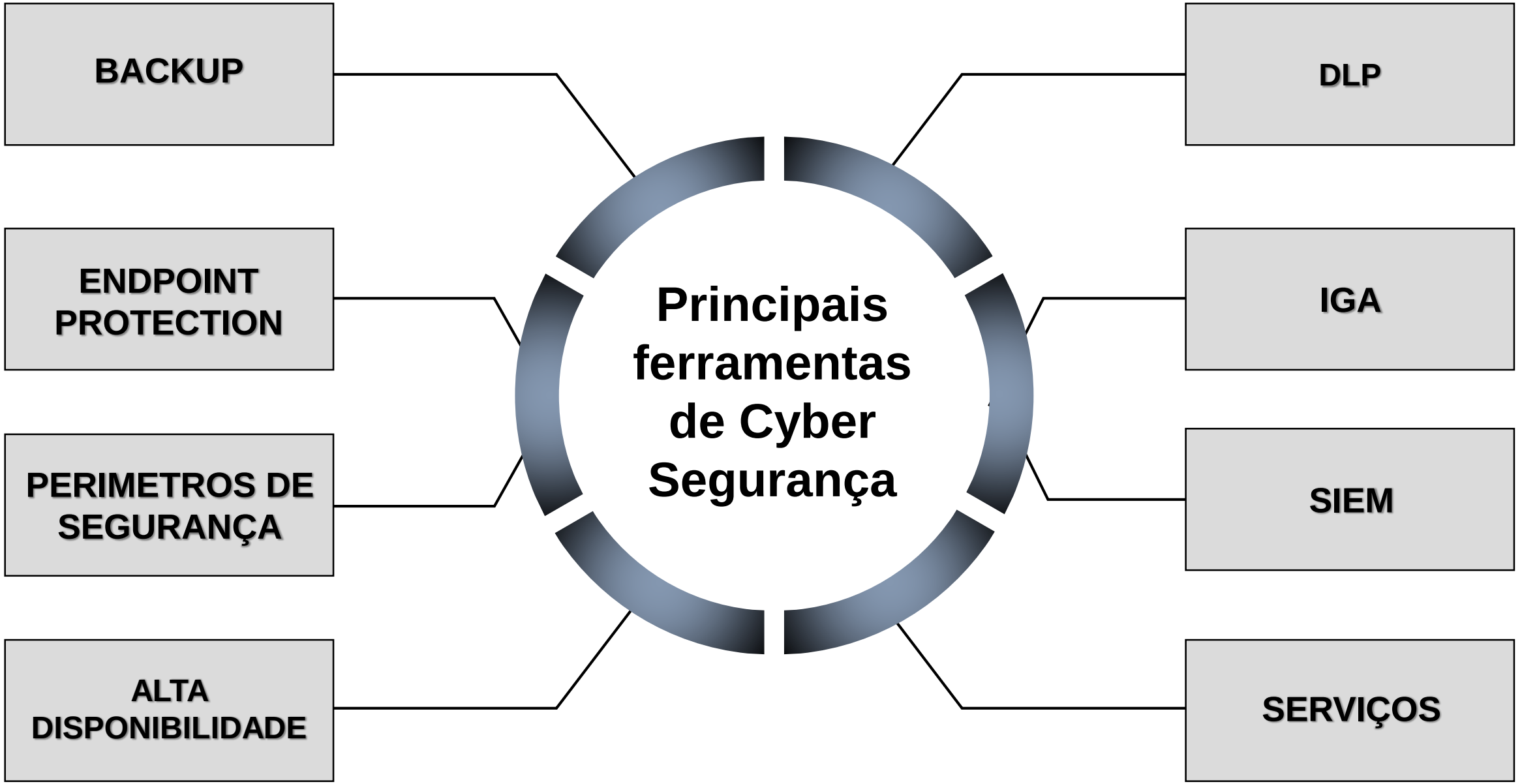
COGEF
Comissão de Gestão Fazendária

Segurança na Prática

Ferramentas e Soluções

Bruno de Souza Lovatti


BACKUP
ENDPOINT PROTECTION
PERIMETROS DE SEGURANÇA
ALTA DISPONIBILIDADE
Principais ferramentas de Cyber Segurança
DLP
IGA
SIEM
SERVIÇOS

BACKUP

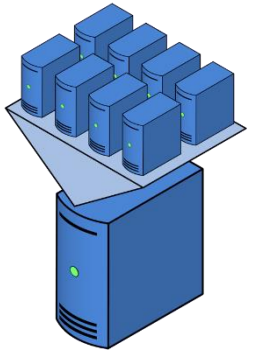
BACKUP

	+ Prós	- Contras
On Premise 	• Maior visibilidade; • Sensação de Controle; • Maior Flexibilidade;	• Riscos mais próximos; • Maior custo para escalar e gerenciar;
Cloud 	• Risco Distribuído; • Melhor segurança; • Mais escalável e menor custo;	• Confiar em Terceiros; • Risco de interrupção da Nuvem;

AGENTES DE BACKUP ESPECIALIZADOS

Servidor de Arquivos

Banco de Dados



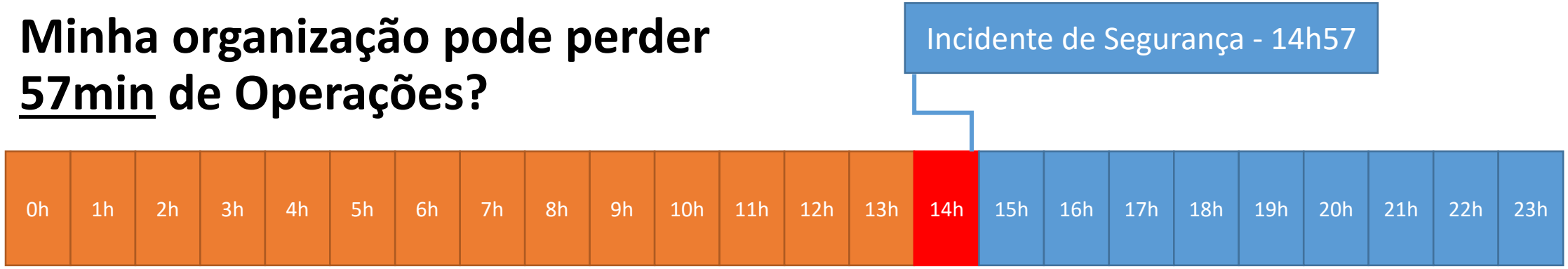
Ambiente Virtual

BACKUP

RPO: Recovery Point Objective.

- Qual a margem de perda de dados que uma empresa pode ter sem afetar as operações?

Minha organização pode perder <u>57min</u> de Operações?

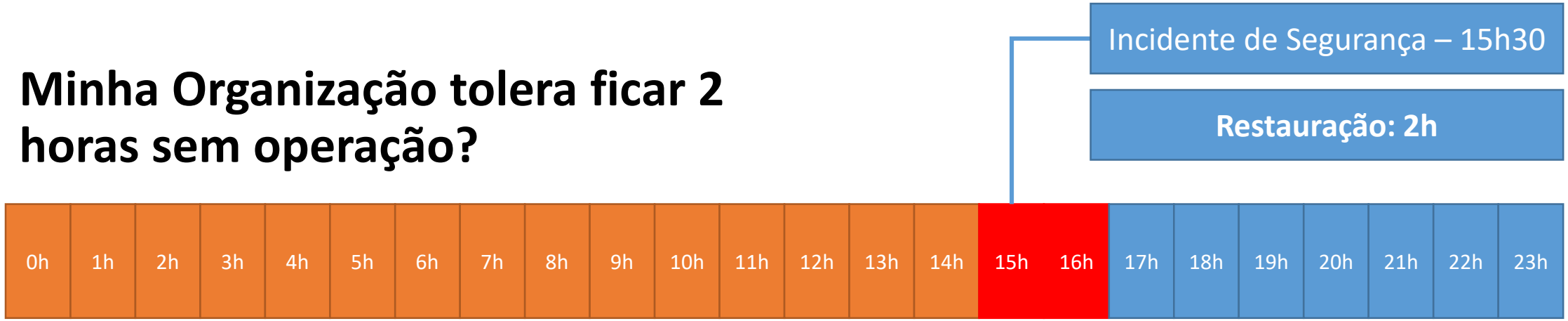


BACKUP

RTO: Recovery Time Objective

- Qual período máximo de tempo que o sistema levará retornar?

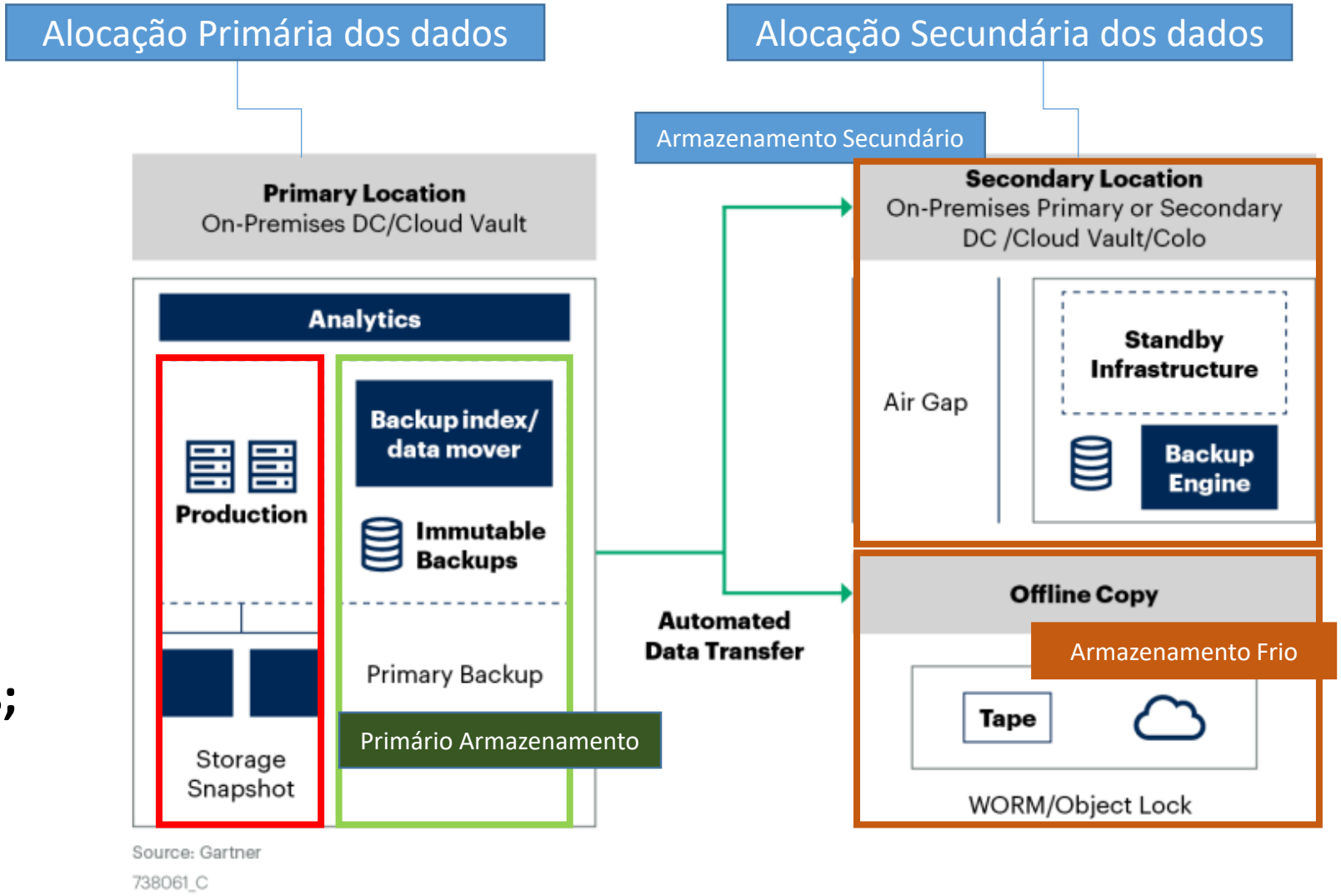
Minha Organização tolera ficar 2 horas sem operação?



BACKUP

Abordagem Moderna:

- **Local Primário:**
- **Local Secundário;**
- **Imutabilidade dos dados;**



Gartner

ENDPOINT PROTECTION


O ANTIVÍRUS ESTÁ MORTO
Symantec (2014).

ENDPOINT PROTECTION

Endpoint Next Generation
Soluções mais modernas no mercado.

A.V - Antivírus:

Software baseado em Assinatura de Arquivos.

Compara a assinatura do Malware

N.G.A.V - Antivírus:

Novas características como controle USB, Firewall de Host e Anti-Intrusão.

EPP - Endpoint Protection Platform:

Plataforma adiciona DLP e detecção avançadas.

EDR – Endpoint Detection and Response:

Detecta e contem incidentes de segurança de modo pró ativo, contendo a ameaça na pré infecção.

XDR – Extended Detection and Response:

Unifica o Gerenciamento de segurança integrando e correlacionando as ferramentas de proteção.

PROGRESSÃO DO ENDPOINT SECURITY

SEFAZ-ES

Projeto para contratação de Solução de Endpoint Protection:

- EPP - Endpoint Protection Platform;
- EDR – Endpoint Detection and Response;
- DLP – Data Loss Prevention.

Desktops

Servidores

Storage NAS

DLP

DATA LOSS PREVECTION (DLP)

Definição: DLP é uma tecnologia de inspeção de conteúdos e analise contextual dos dados tráfegos pelos Serviços Computacionais da Organização.

Enterprise: Solução completa de DLP.

Integrated: Soluções de Segurança que possuem sistema de DLP integrados.

DATA LOSS PREVECTION (DLP)

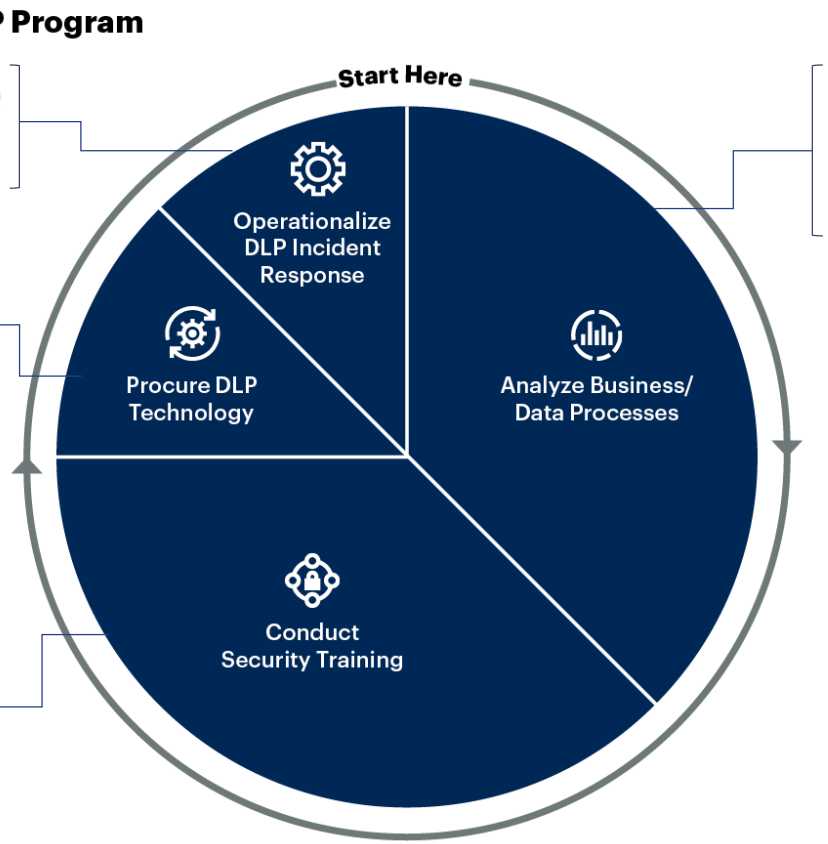
- Permite visibilidade do uso e movimentação de dados;
- Aplicação dinâmica de políticas de segurança com base no conteúdo e no contexto no momento das ações nos dados.
- Aborda ameaças na perda de dados inadvertida ou acidental;
- Exposição de dados confidenciais;
- Implementando monitoramento, alerta, aviso, bloqueio e outros recursos de correção.

DATA LOSS PREVECTION (DLP)

Implementar um processo de Resposta a Incidentes.

Implementar uma tecnologia DLP mais aos processos organizacionais.

Implementar treinamentos a respeito de privacidade risco. #LGPD



Alinhar estrategicamente os requisitos do negócios que o DLP deve atender.

Source: Gartner
749040_C

Gartner

DATA LOSS PREVECTION (DLP)

- Programas de **DLP imaturos são sistematicamente inundados com violações recorrentes e reincidentes**, o que contribui para o desperdício de tempo e recursos.

- Os programas DLP são frequentemente implementados como uma tecnologia de **“definir e esquecer”** sem desenvolvimento contínuo.

DATA LOSS PREVECTION (DLP)

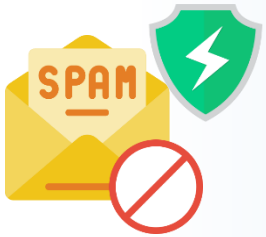
Desktops

Servidores

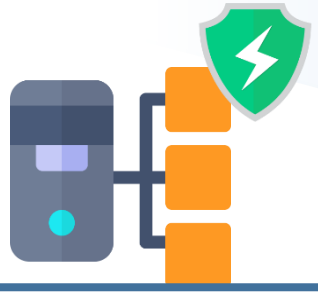
WAF

Firewall

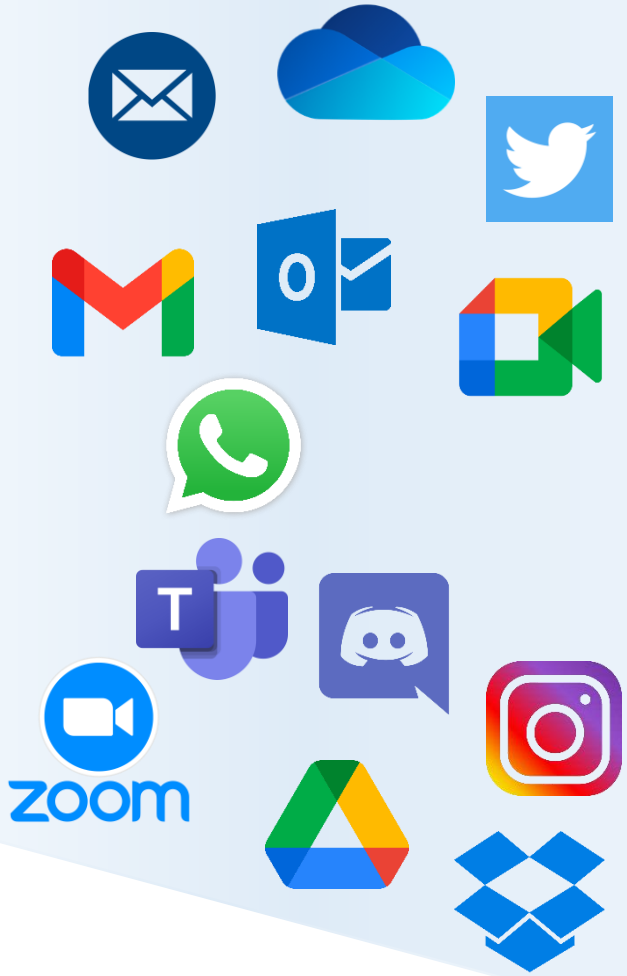
Antispam



Proxy



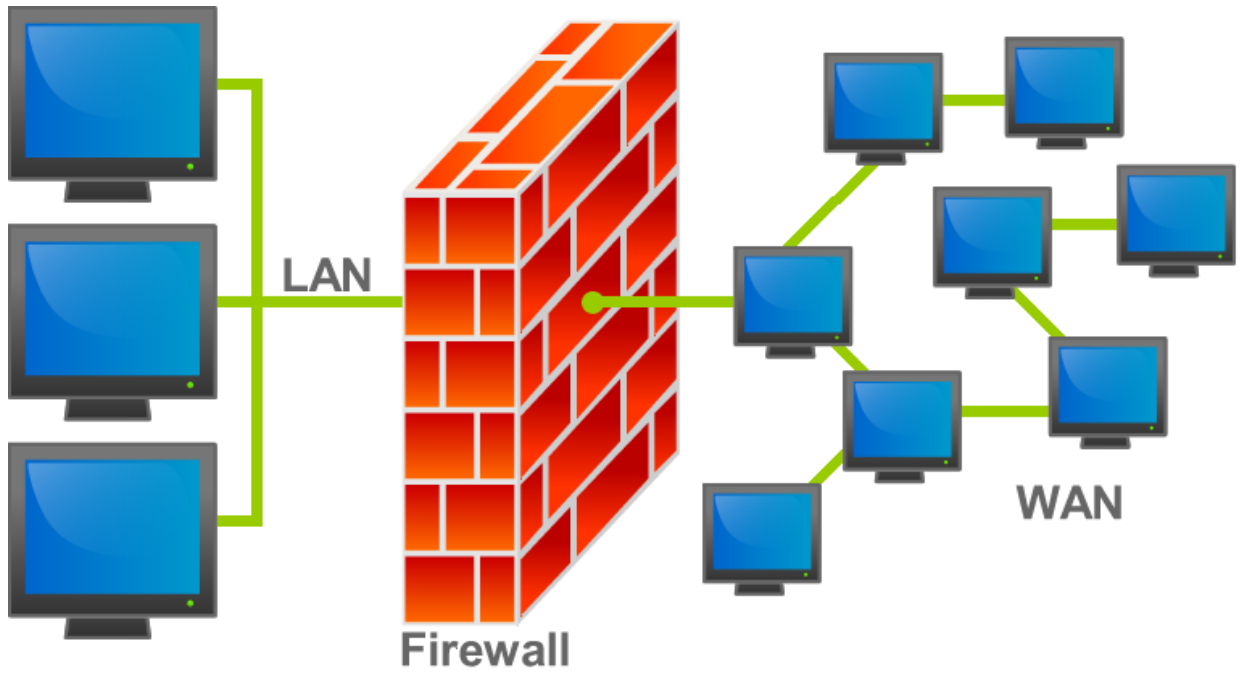
Nuvem de Serviços



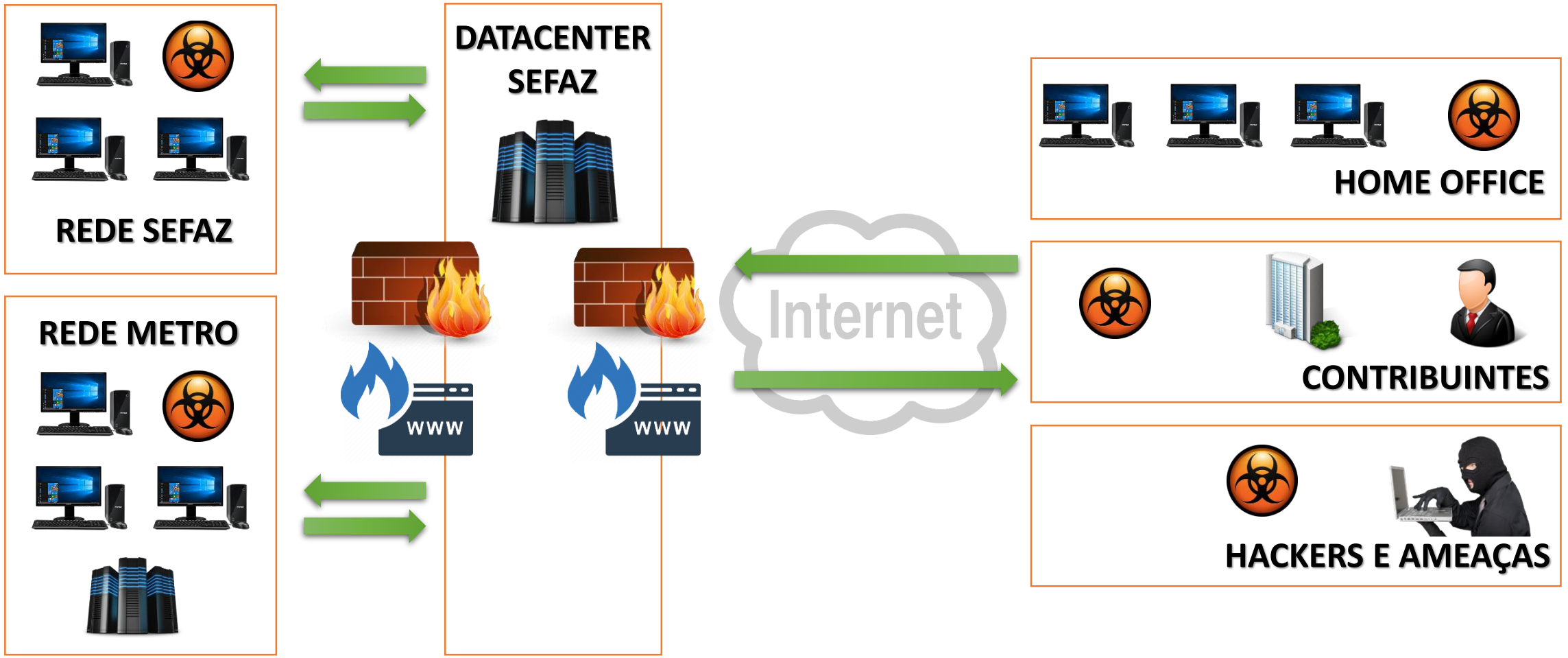
PROTEÇÃO DE PERÍMETROS

PROTEÇÃO DE PERÍMETROS

- Proteção de Perímetro tradicional;
- Firewall protegendo a Rede Interna;
- **Não atende** mais aos requisitos dos Negócios;



PROTEÇÃO DE PERÍMETROS

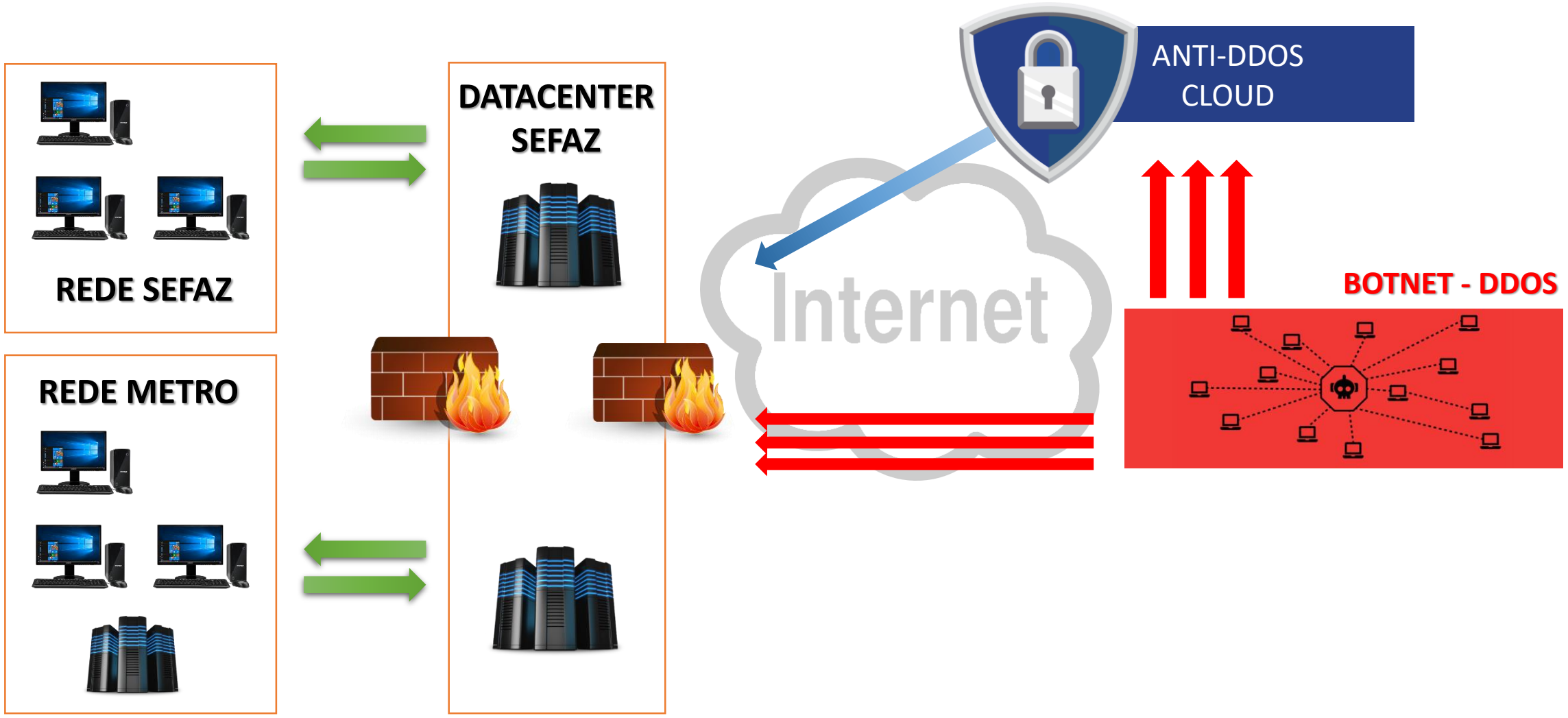


PROTEÇÃO DE PERÍMETROS

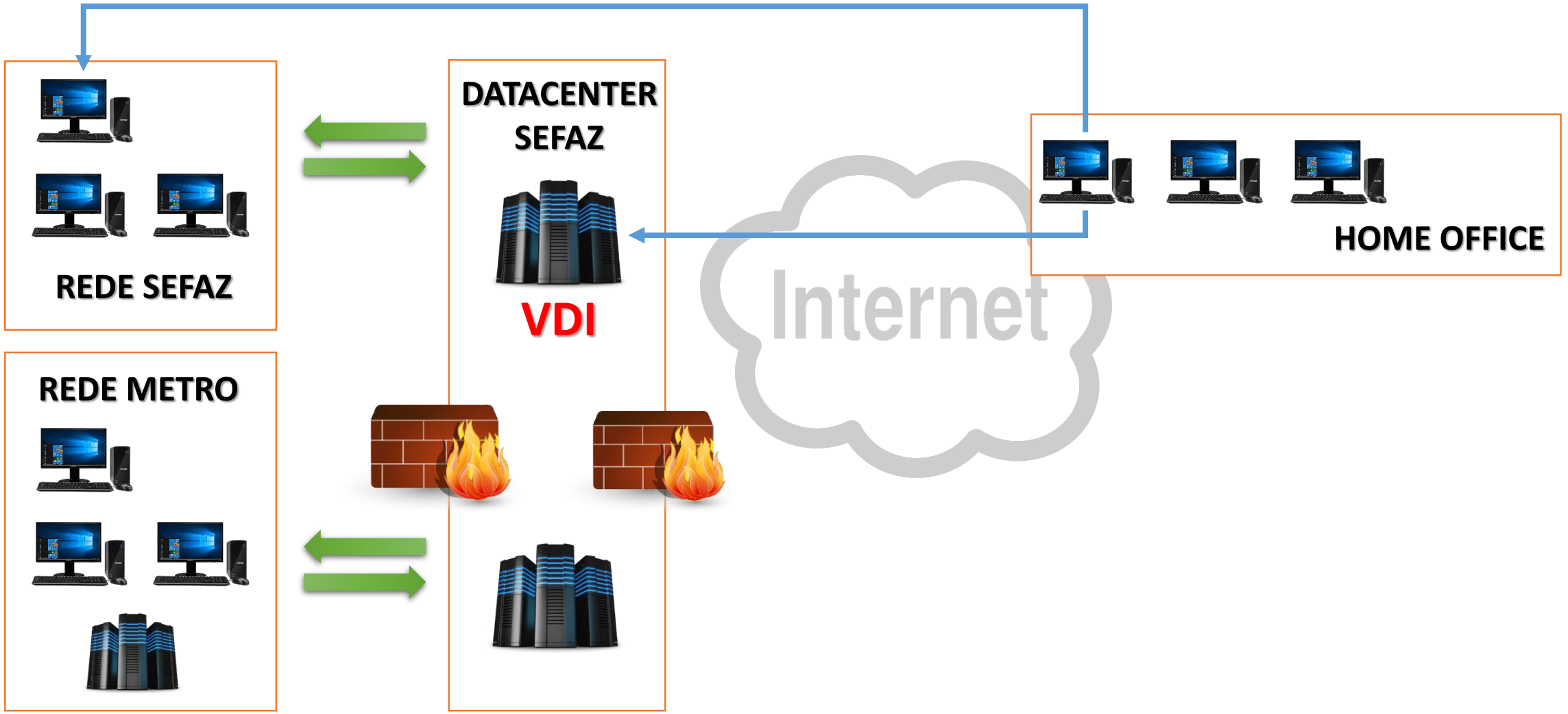
- **Firewall:** Serviço responsável por filtragem do tráfego de rede, oriundo de vários locais internos (intranet) ou externos (internet);

- **WAF:** Web Application Firewall, seu foco principal é a Proteção das Aplicações e Serviços disponibilizados na Internet, contra ataques de injeção.

PROTEÇÃO DE PERÍMETROS



PROTEÇÃO DE PERÍMETROS



SEFAZ-ES

Projetos e Soluções:

- Firewall de Borda (Em funcionamento);
- Proxy – Controle de Navegação;
- Firewall de Aplicação (Em funcionamento);
- Aquisição de VDI (em Licitação);

SERVIÇOS DE SEGURANÇA

SOC: SECURITY OPERATIONS CENTER

SoC

Abrange as pessoas, processos, tecnologias e serviços;

Identificar e gerenciar a exposição a ameaças;

Prevenir, detectar e responder a incidentes de segurança cibernética.

SecOps

Objetiva compreensão proativa dos riscos de negócios

Visibilidade dos riscos do negócio;
Ambientes, usuários e ativos;
Compreensão das ameaças;

Os recursos eficazes devem ser automatizados.

Automação de segurança para operações mais consistentes.

CSIRT - COMPUTER SECURITY INCIDENT AND RESPONSE TEAM

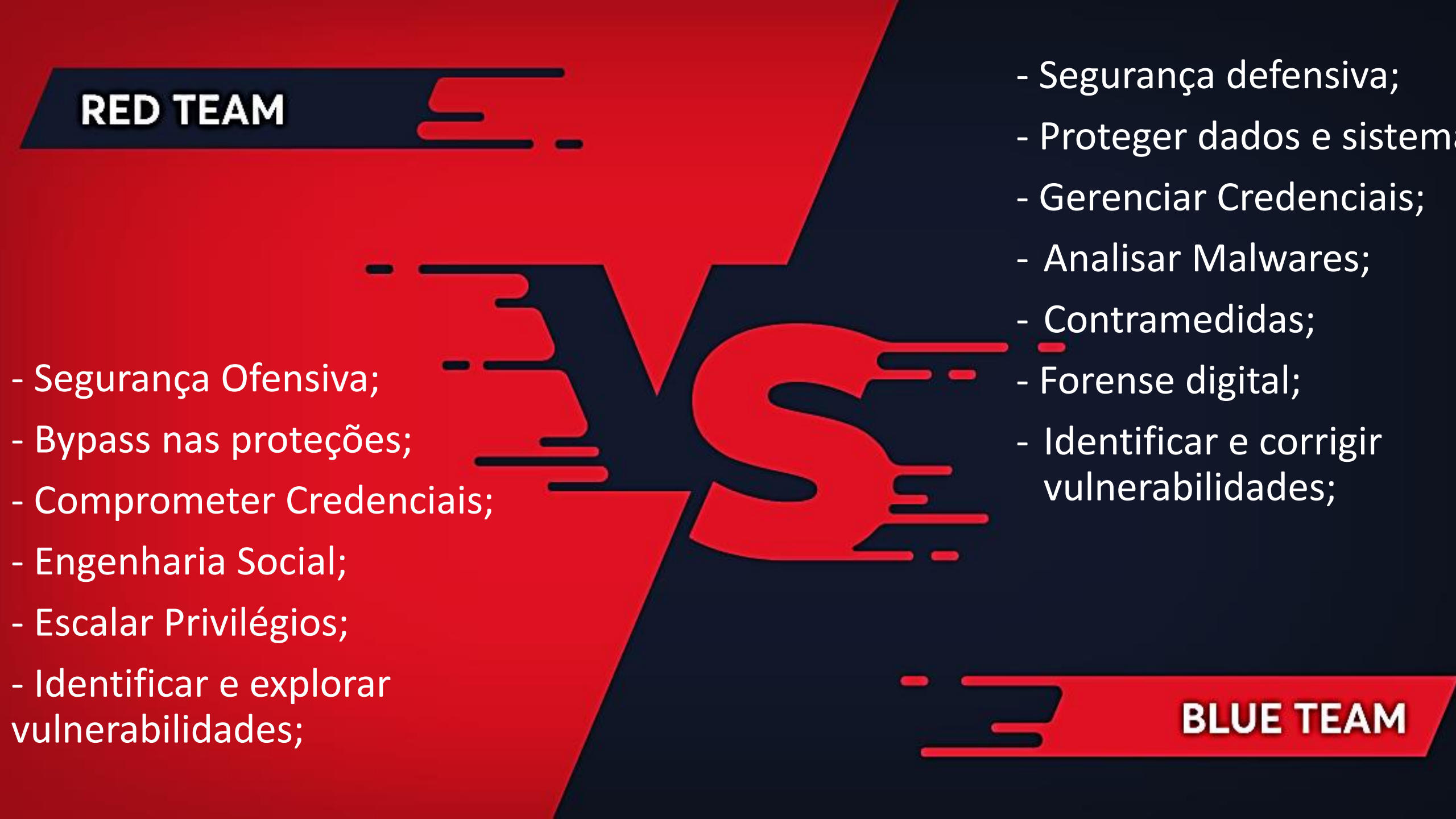
Equipe de especialistas para receber, analisar e **responder a incidentes de segurança;**

SoC, Terceirizados ou grupo especial de trabalho ou comissão;

Equipe multidisciplinar conforme a necessidade da Área de Negócio afetada.

PENTEST E VULNERABILIDADES

- **Segurança Proativa;**
- Analise de Vulnerabilidades;
- Hackers Éticos;
- Segurança em Profundidade;
- Testes Controlados;

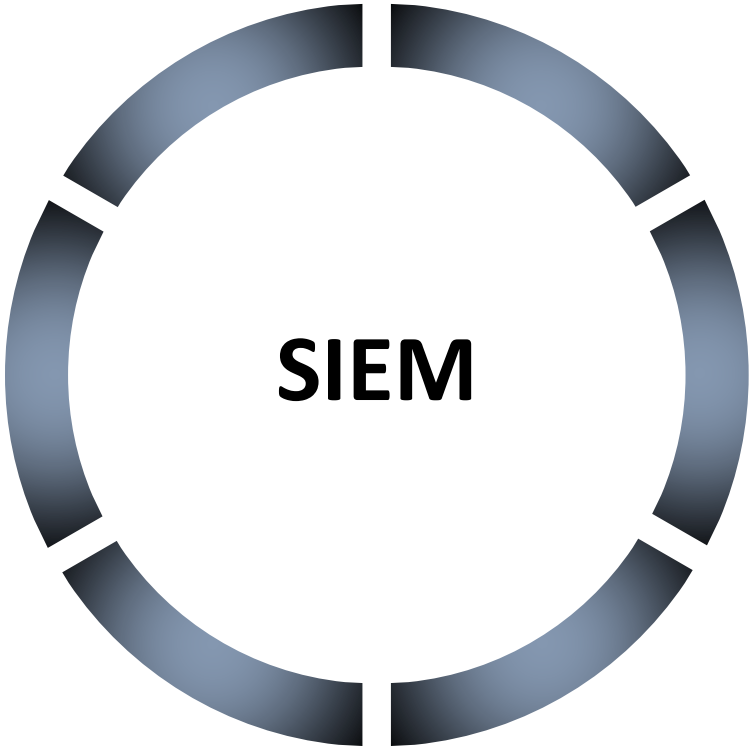

RED TEAM
- Segurança Ofensiva;
- Bypass nas proteções;
- Comprometer Credenciais;
- Engenharia Social;
- Escalar Privilégios;
- Identificar e explorar vulnerabilidades;
VS
- Segurança defensiva;
- Proteger dados e sistem
- Gerenciar Credenciais;
- Analisar Malwares;
- Contramedidas;
- Forense digital;
- Identificar e corrigir vulnerabilidades;
BLUE TEAM

MSS - MANAGEMENT SECURITY SERVICES

Variedade de Serviços Operacionais de Gerenciamento de Segurança:

- Contratação de SOC;
- Gerenciamento das Ferramentas de Segurança do cliente;
- Maturidade e equipes especializadas;
- Monitoramento 24h;
- Compartilhamento de Conhecimento;
- Resposta a Incidentes;
- Avaliação e Gerenciamento de Exposição;

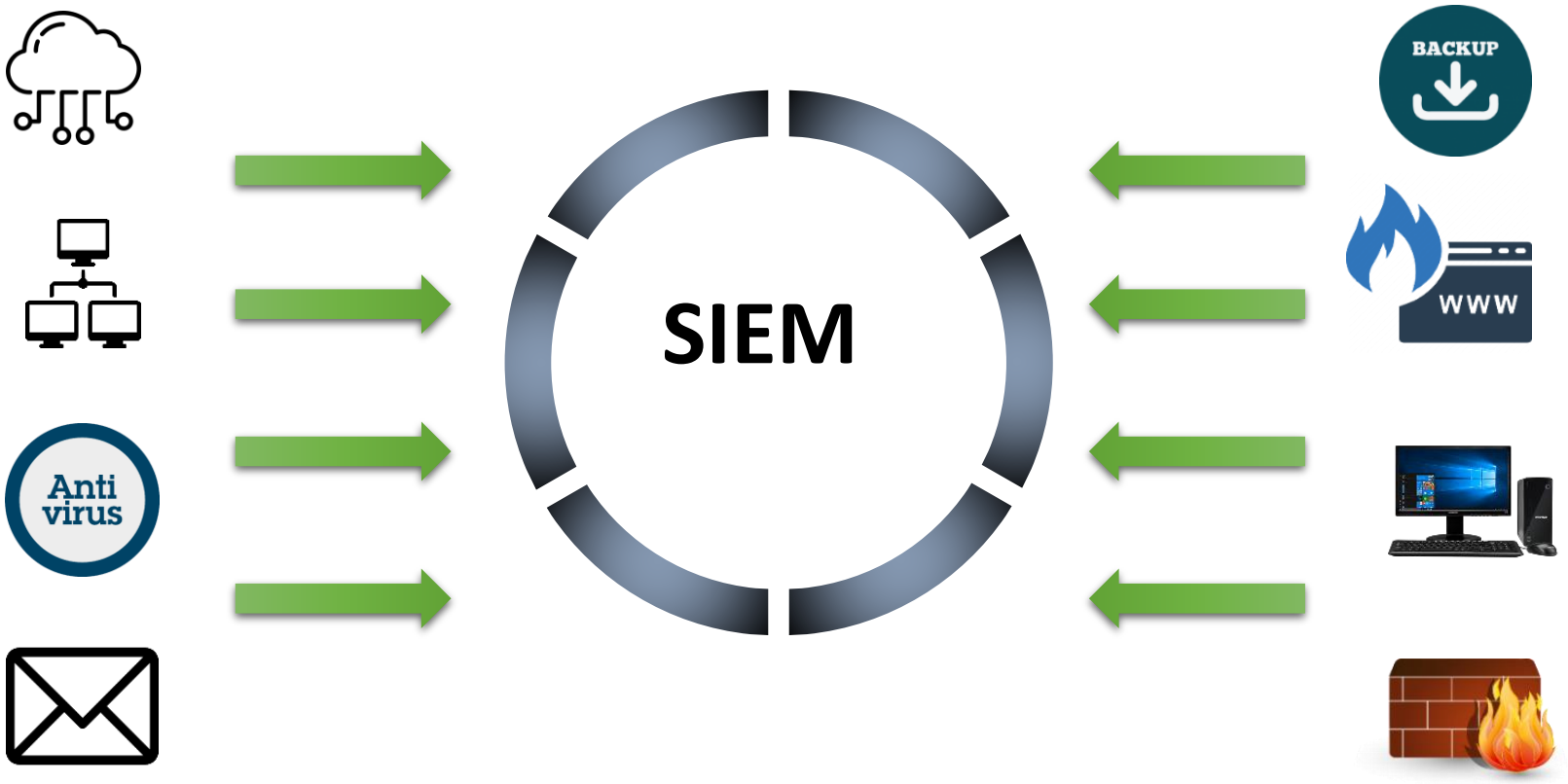
SIEM



- Coleta de LOGs;
- Análise de LOGs (I.A);
- Correlação de Eventos;
- Forense;
- Compliance (PCI, BACEN, HIPAA);
- Auditoria;
- Alertas e Monitoramento;
- Dashboards;
- Retenção de LOGs (Compliance);

SIEM

- **Security Information and Event Management – SIEM;**



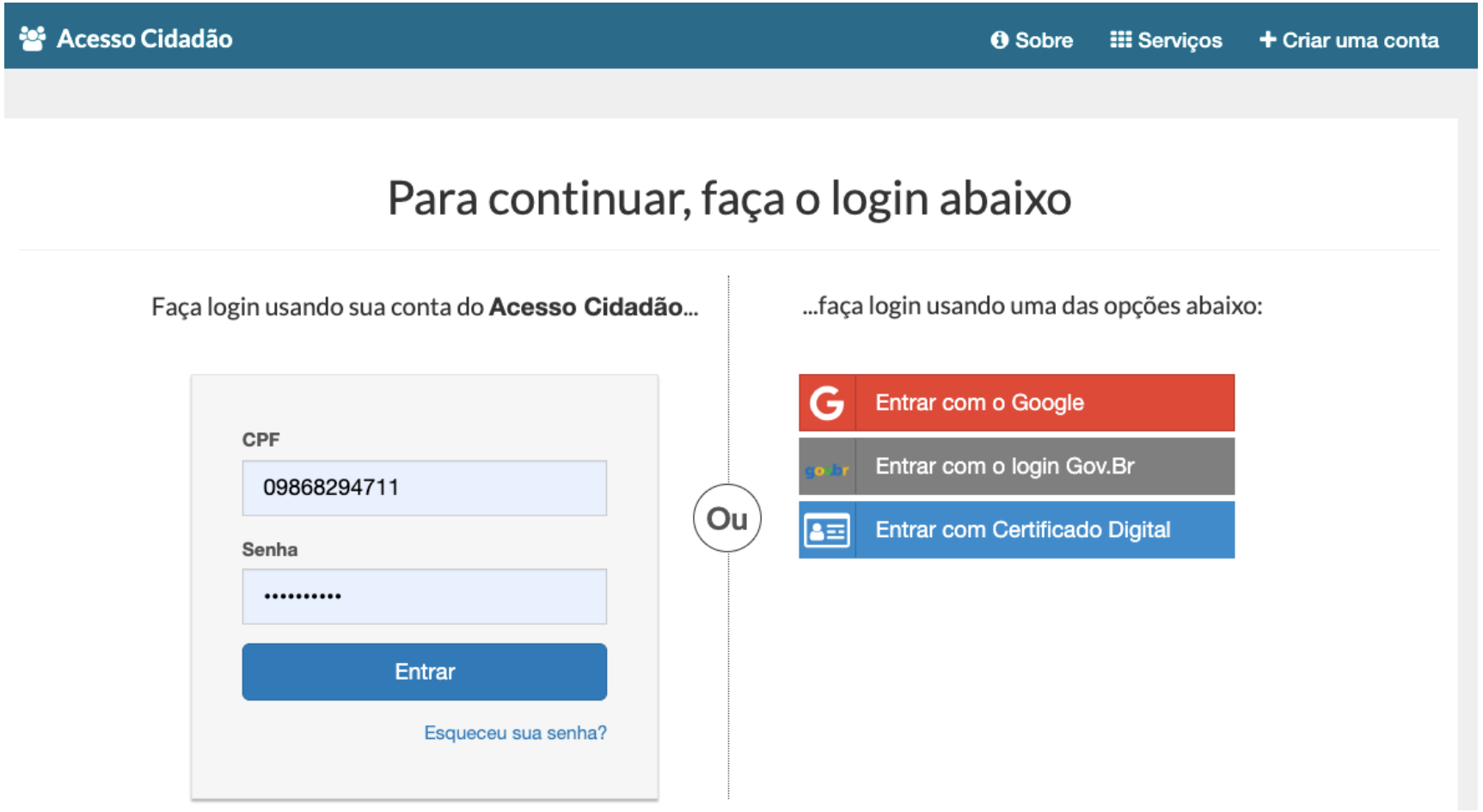
SEFAZ-ES

Projeto para contratação de Serviços de:

- Gestão de Incidentes de Segurança da Informação e SOC;
- Gestão de Vulnerabilidades e Conformidade;
- Monitoramento De Ataques Cibernéticos;
- Segurança Ofensiva e testes Periódicos De Invasão;
- SIEM – Gerenciamento de LOGs com Inteligência Artificial.

IGA

IGA – IDENTITY GOVERNANCE E ADMINISTRATION



Depois

TI
GESTÃO!

MSS
CONTRATADO!

SOC
OPERAÇÃO!

CSIRT
DEFINIDO!

RED TEAM vs BLUE TEAM
ATUANDO!

SEGURANÇA DE PERIMETRO – ATUALIZADA!

SIEM
MONITORANDO!

IGA - IMPLANTADO

ENDPOINT PROTECTION

DLP - IMPLANTADO

Negócio da SEFAZ

BACKUP
FUNCIONAL E TESTADO

COGEF
Comissão de Gestão Fazendária

Nunca estamos 100% seguros.
Mas devemos estar 100% preparados.

COGEF
Comissão de Gestão Fazendária

OBRIGADO!

Bruno de Souza Lovatti