Prime

CCS-A

Arquitetura de Segurança Corporativa – Parte 1

O que é Arquitetura de Segurança Corporativa?

- Arquitetura se preocupa em garantir que os elementos possam trabalhar de forma confiável e segura.
- Arquitetos corporativos:
  - Estabelecem um checklist padronizado para seus sistemas;
  - Definem configurações e interfaces para sistemas trabalhando em conjunto.
- A arquitetura orienta as pessoas a fazer escolhas de configuração.

Gerenciamento de Configuração

- Essencial para proteger o sistema usando a configuração especifica para uma implementação.
- Importante monitorar e proteger contra alterações de configuração.
- Cada empresa define padrões e estruturas.
- Três principais guias:
  - Benchmark dos fabricantes do software;
  - Benchmark do governo;
  - Benchmark do Center for Internet Security (CIS) https://www.cisecurity.org/cis-benchmarks/

Diagramas

- Usados em especificações de arquitetura para comunicar como a empresa está configurada.
- Diagramas gráficos são usados pois:

São mais fáceis de seguir;

Imagens fornecem acesso imediato a informações;

Deixam mais fácil entender as relações das listas de especificações.

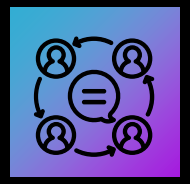
Configuração de Linha de Base

- Ponto de partida para as avaliações de linha de base.
- Presente desde a criação de um sistema.
- Exige atualização.
- Permite enxergar mudanças não autorizadas. Ex:
  - Permissões;
  - Na infraestrutura da rede.

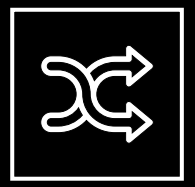
Funcionamento da Linha de Base

- Funcionamento da linha de base:
  - Configuração do sistema;
  - Medição da linha de base;
  - Correção dos problemas;
  - Declaração de configuração do sistema.
- Mudanças na linha de base podem ser positivas ou negativas.
  - Diminuindo os riscos;
  - Aumentando os riscos.

Convenções de Nomenclatura Padrão



Importantes em uma empresa para que haja clareza e compreensão na comunicação.



Se vários servidores forem nomeados de forma aleatória, isso dificulta a correção.

Elimina erros e promove comunicação clara. Ex:

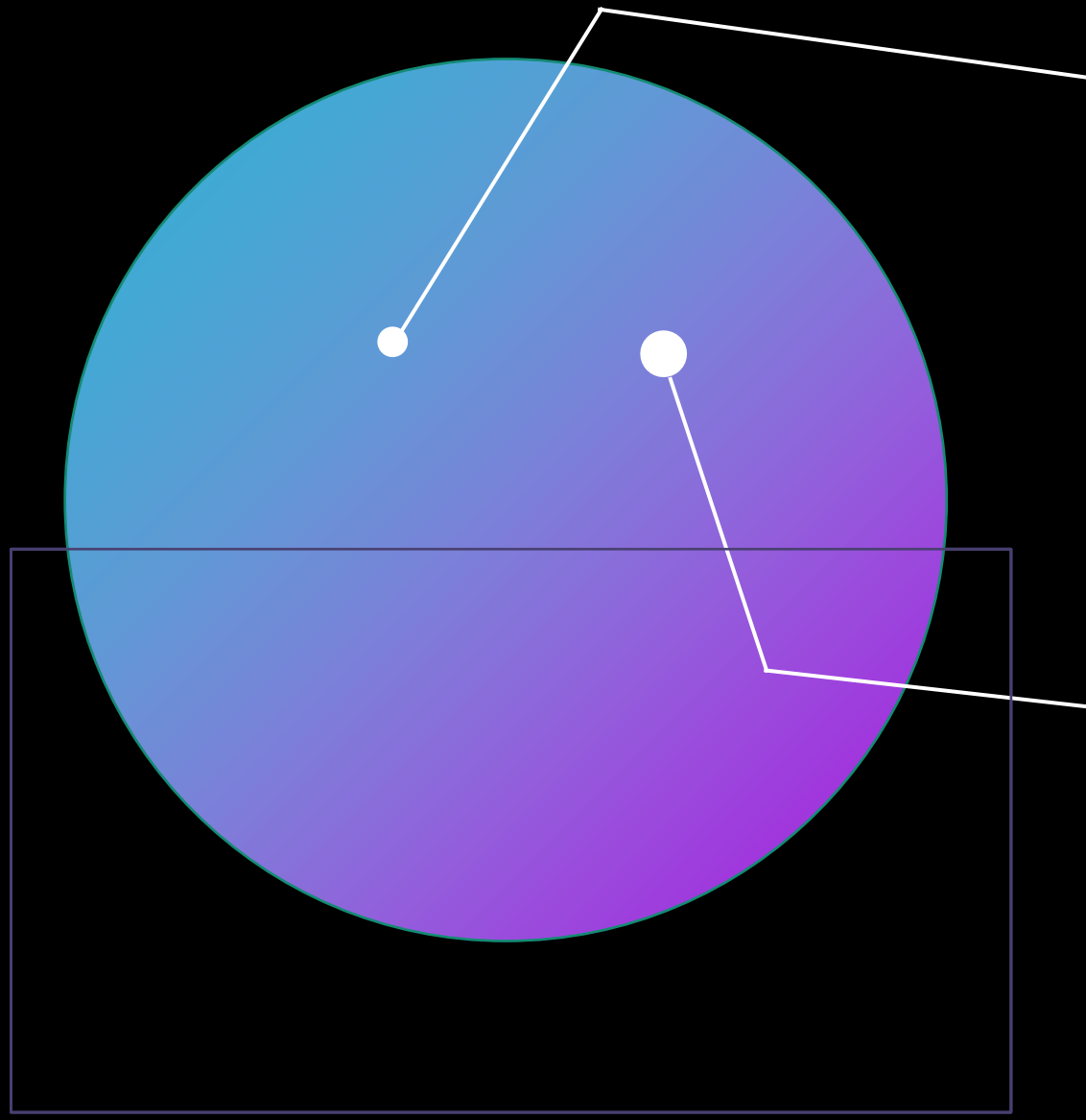
- @adriano.martins
- @ama
- @a.martins
- @antonio

Classe IP e Notação CIDR

- A configuração inclui diagramas físicos e lógicos.
- Planeje sua configuração para manter uma segmentação lógica da rede.
- O endereço real é composto de duas partes:
  - Rede;
  - Host.
- Existem dois esquemas de endereçamento:
  - Classe A/B/C;
  - Notação CIDR (fácil compreender como a rede é disposta).
- O Gerenciamento de Configuração permite padrões compreensíveis e esquemas IP seguros.

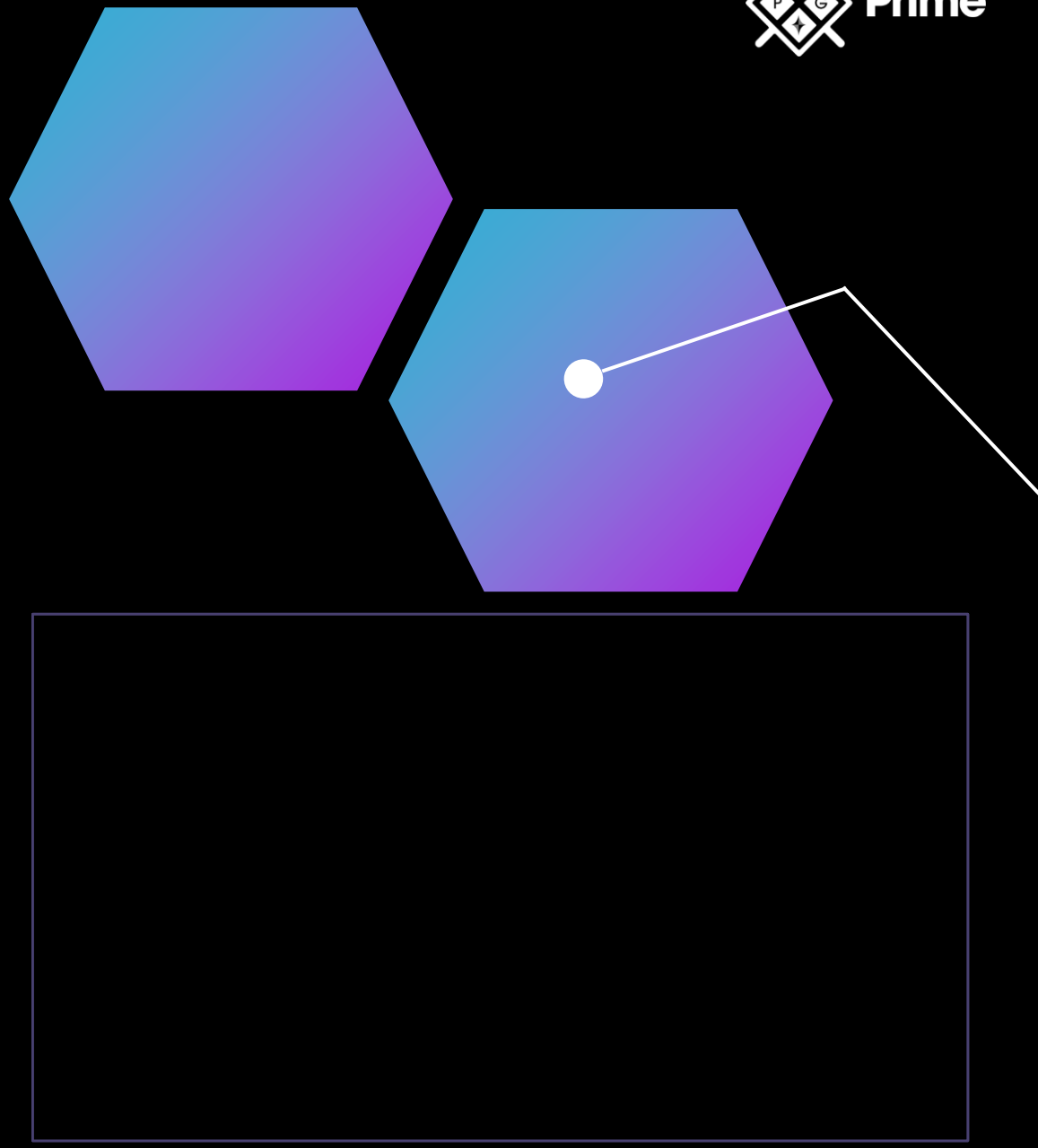
Soberania de Dados

- Dados são regidos pelas leis do país em que os dados residem.
- Tipo relativamente novo de legislação (Nuvem e Big Data).
- Várias empresas mudaram suas estratégias e ofertas para cumprir a soberania de dados.
  - Exemplo: LinkedIn na Rússia.
- Orienta decisões em origem multinacional.
- As leis de soberania de dados se aplicam a um país específico.
- Para uma empresa cumprir a lei, os dados da nuvem devem estar em seu país.



Proteção de Dados

- Conjunto de:
  - Políticas e leis;
  - Procedimentos;
  - Ferramentas (criptografia);
  - Arquiteturas.
- Dados do cliente e confidenciais precisam de proteção.
- O dado é o elemento mais importante para proteção da empresa.
- Ações tomadas para proteger dados = Segurança de dados, como tokenização, mascaramento etc.



Prevenção Contra Perda de Dados (DLP)

- Soluções de prevenção contra perda de dados e vazamento (e-mail, BD, USB e Nuvem).
- DLP envolve vários controles de segurança contra vazamento intencional ou acidentalmente.
- Evita que dados confidenciais saiam da rede de repente.
- Monitoramento DLP a nível empresarial relata atividades em:
  - Sistemas centralizados na empresa;
  - DLP de empresas especializadas.
- Projetar tais soluções faz parte de uma empresa moderna.

Mascaramento

- Oculta dados substituindo valores alterados.
- Utiliza:
  -  Embaralhamento de caracteres;
  -  Criptografia;
  -  Substituição de palavras e caracteres;
  -  Redigir elementos fisicamente (*).
- É possível criar conjuntos de dados para teste e carregar *honeypots* com dados utilizáveis ainda falsos.

Criptografia

Melhor solução para segurança dos dados.

Não podem ser lidos por uma parte não autorizada.

Uso de técnicas para impedir que pessoas sem acesso leiam os dados.

- É preciso:
  - Criptografar os dados de forma correta;
  - Garantir que aplicativos de negócios sejam configurados para ler os dados.
- Faz parte do esquema geral da arquitetura corporativa.

Em Repouso

- Os dados confidenciais devem protegidos, seja armazenado em um disco ou em um banco de dados.
- Dados podem ser armazenados em vários formatos:
  - ASCII;
  - XML;
  - JavaScript Object Notation (JSON);
  - Banco de dados.
- Dados em repouso exigem proteção, conforme seu valor.
- Melhor meio de proteção: **criptografia.**

Dados em Trânsito/Movimento

- Os elementos de dados precisam ser:

Compartilhados;

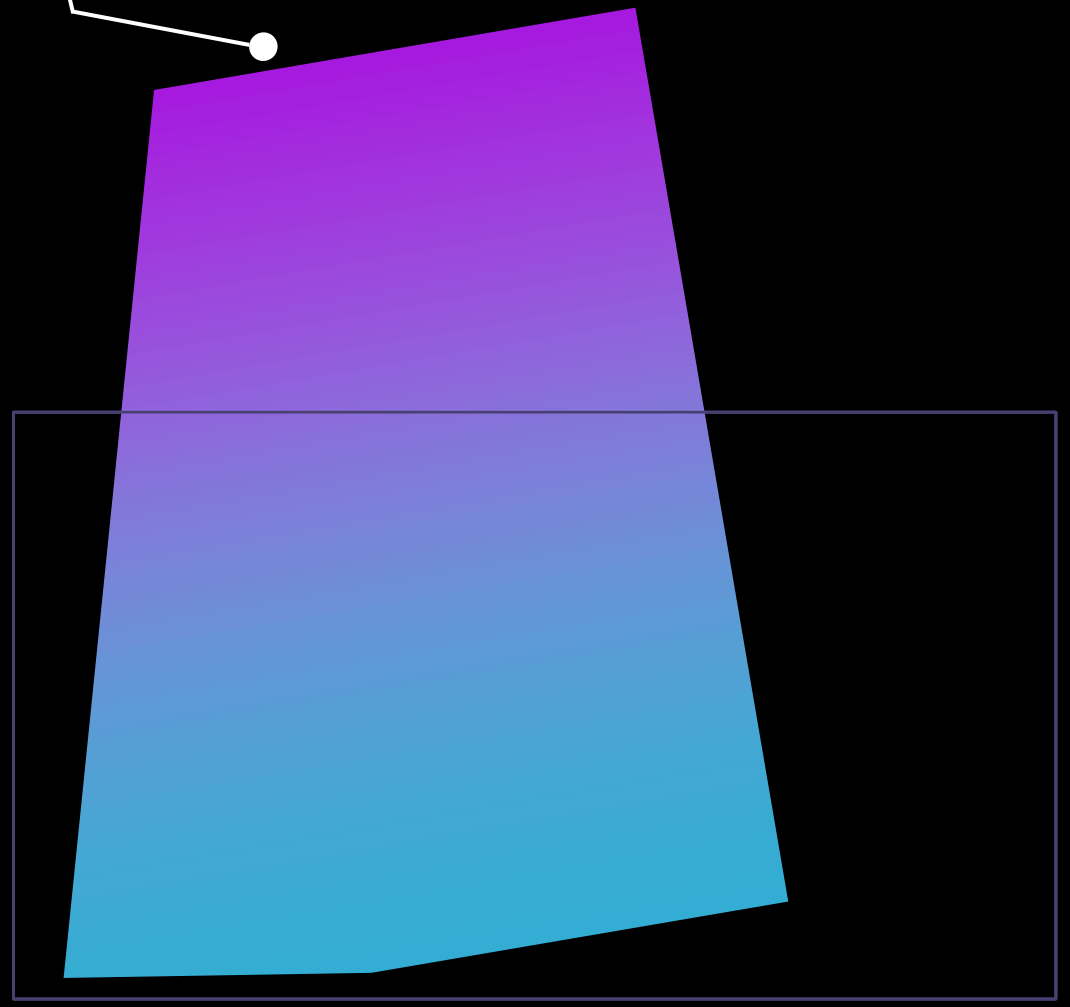
Movidos entre os sistemas;

Protegidos.

Método mais comum: **criptografia.**

Em Processamento

- Proteção durante o processamento até que as informações sejam realmente lidas.
- Dados que estão sendo usados.
- Proposta mais complicada do que proteger em trânsito ou no armazenamento.
- Não é prático realizar operações em dados criptografados.
- Outros meios precisam ser tomados para proteção dos dados.



Tokenização

- Uso de valor aleatório para substituir um elemento de dados com significado rastreável.

Exemplo: Processo de aprovação do cartão de crédito.

- Usado em vários sistemas de transmissão de dados.

Protege informações confidenciais;

Mantém as características desejadas de não repúdio (mapeando valores).

- Não é a mesma coisa que criptografia.

Gerenciamento de Direitos

- Sistematiza regras e ordem para os usuários sobre objetos digitais.
- No nível de arquivo existe, por exemplo:
  - Opções de leitura;
  - Gravação;
  - Outras opções de controle de acesso.
- Termo usado para descrição de cenários a vários tipos de arquivos.
  - Reprodução;
  - Cópia;
  - Edição;
  - Salvamento.
- DRM: direitos de copiar, editar, reproduzir e salvar mídias no dispositivo.

OBRIGADO!

ARQUITETURA DE SEGURANÇA CORPORATIVA – PARTE 1