Defesas contra ameaças

Prevenção, Detecção e Resposta a Intrusões

Arquitetura de Segurança

- Organização de um sistema de forma a ter atendidos seus requisitos de segurança
  - Foco da parte inicial do curso
- Baseado no uso de ”ferramentas básicas de segurança”
  - autenticação de usuário
  - controle de acesso
  - criptografia
  - ...
- Mas... atacantes buscarão subverter a arquitetura de segurança e comprometer os requisitos de segurança

Defesas

- Foco nas ferramentas que permitem combater ataques
  - Parte do princípio que o ataque vai acontecer – mesmo com uma boa arquitetura de segurança
- Possíveis abordagens contra ataques
  - Prevenir
  - Detectar
  - Responder

Exemplos

- Prevenção (limite entre defesa e arquitetura)
  - Filtro de tráfego por Firewal
    - Reduz possibilidade de ataque contra host, aplicação ou sistema
- Detecção
  - Sistemas de Detecção de Intrusão
    - Permite que atividade maliciosa seja identificada na rede
- Resposta
  - Bloqueio automático de IP
    - Impede que um ataque em execução prossiga e tenha sucesso

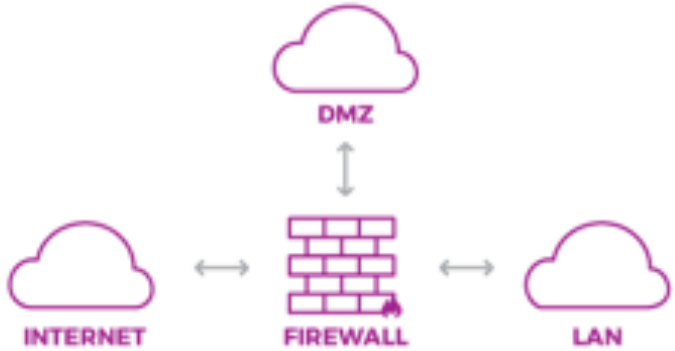
Alguns exemplos de ferramentas de defesa

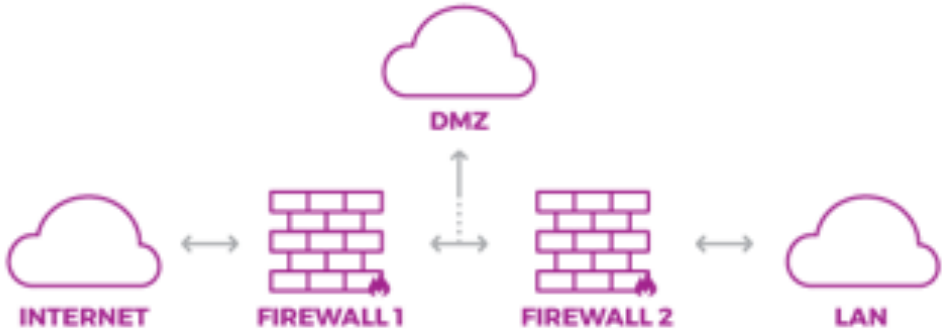
- Firewall
- Sistema de Detecção de Intrusão (IDS)
- Sistema de Prevenção de Intrusão (IPS)
- Sistema de Gerenciamento de Eventos e Informações de Segurança (SIEM)
- Threat Hunting

Firewall

- Ferramenta básica para proteção de perímetro de rede
- Isola segmentos mais "críticos" da rede das áreas menos seguras
- Pode ser pensado como um "filtro" que retém pacotes que não atendem às regras e políticas de segurança
- Tipos de regras evoluem com o tempo
  - Filtro de pacote (IP de origem ou porta de destino)
  - Filtro de estado de sessão (análise de conexão TCP)
  - Gateway de aplicação (análise de protocolos FTP e HTTP)
  - Deep inspection, firewall UTM, host-based firewall
- Firewall moderno agrega muitas funcionalidades de segurança

Firewall - topologias

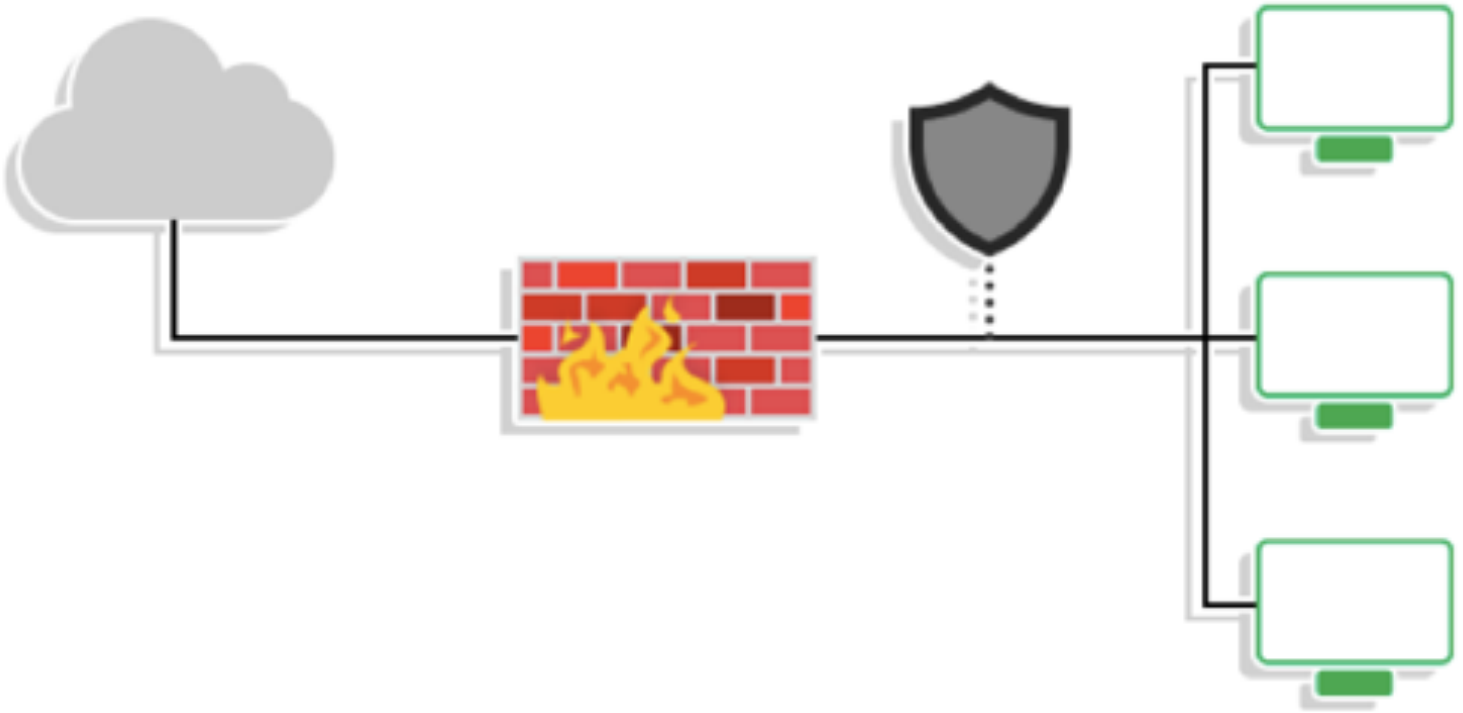




Sistema de Detecção de Intrusão (IDS)

- Monitora host, sistema ou rede
- Busca por indícios de atividade maliciosa ou violação de política/requisitos de segurança
- Tem uma visão tipicamente "local" da segurança
- Postura passiva – apenas detecta intrusão

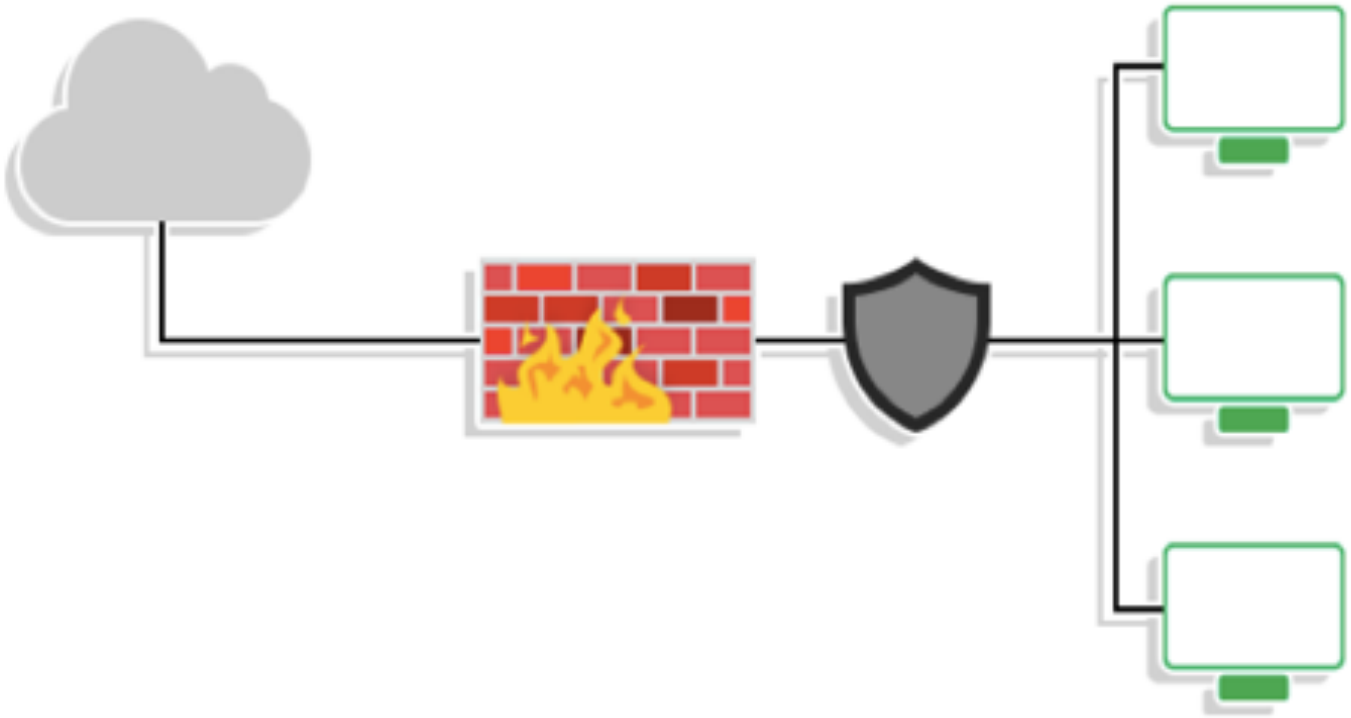
Sistema de Detecção de Intrusão (IDS)



Sistema de Prevenção de Intrusão (IPS)

- Sistemas que detectam ameaças e previnem o desenvolvimento dos ataques identificados
  - Pode ser visto como um IDS com capacidade de resposta
- Pode executar várias ações
  - Terminar uma conexão TCP
  - Bloquear endereços IP ou contas de usuário
  - Remover conteúdos maliciosos
  - ...
- É posicionado de forma diferente de um IDS
  - Na prática, "em série" com as comunicações

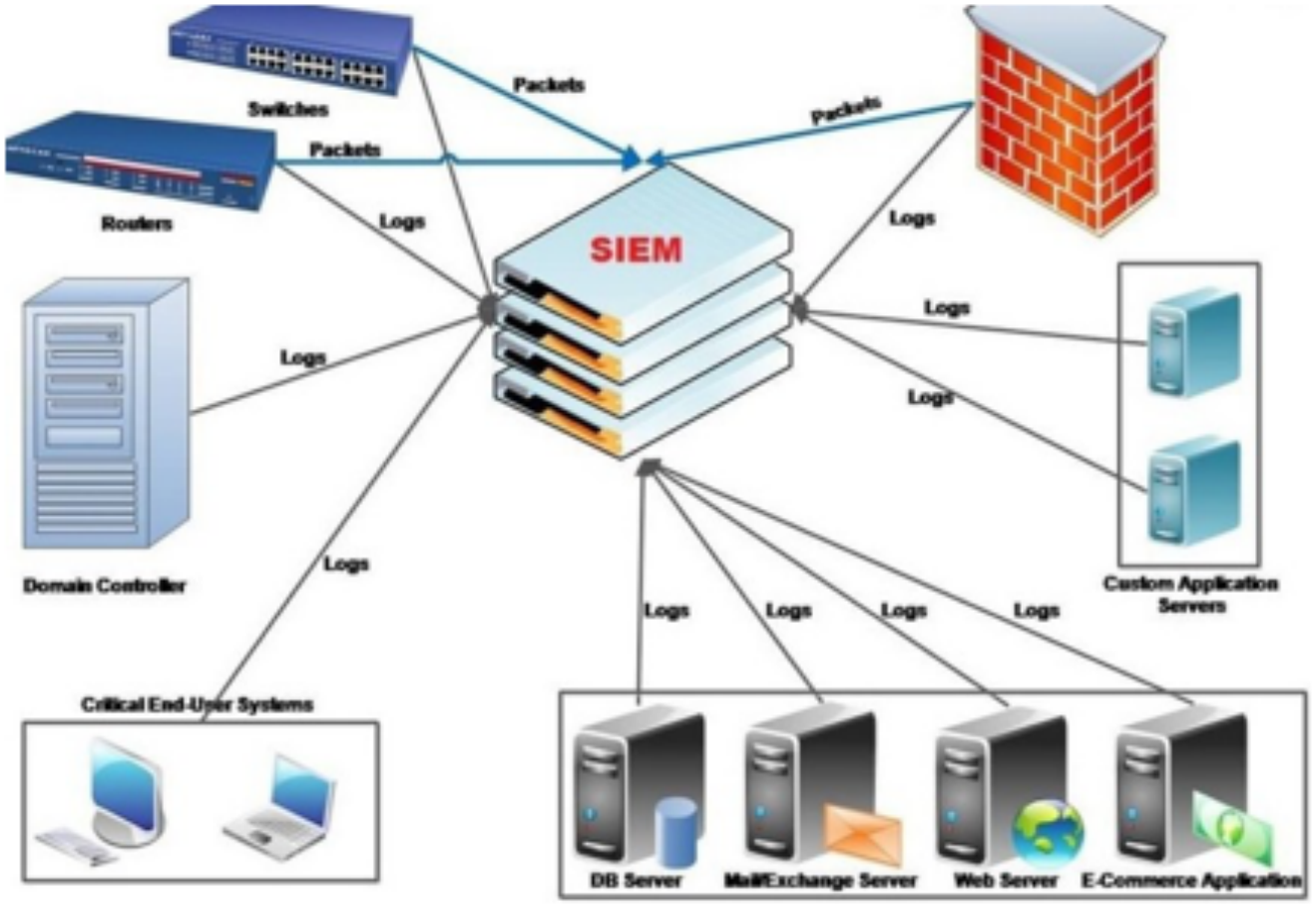
Sistema de Prevenção de Intrusão (IPS)



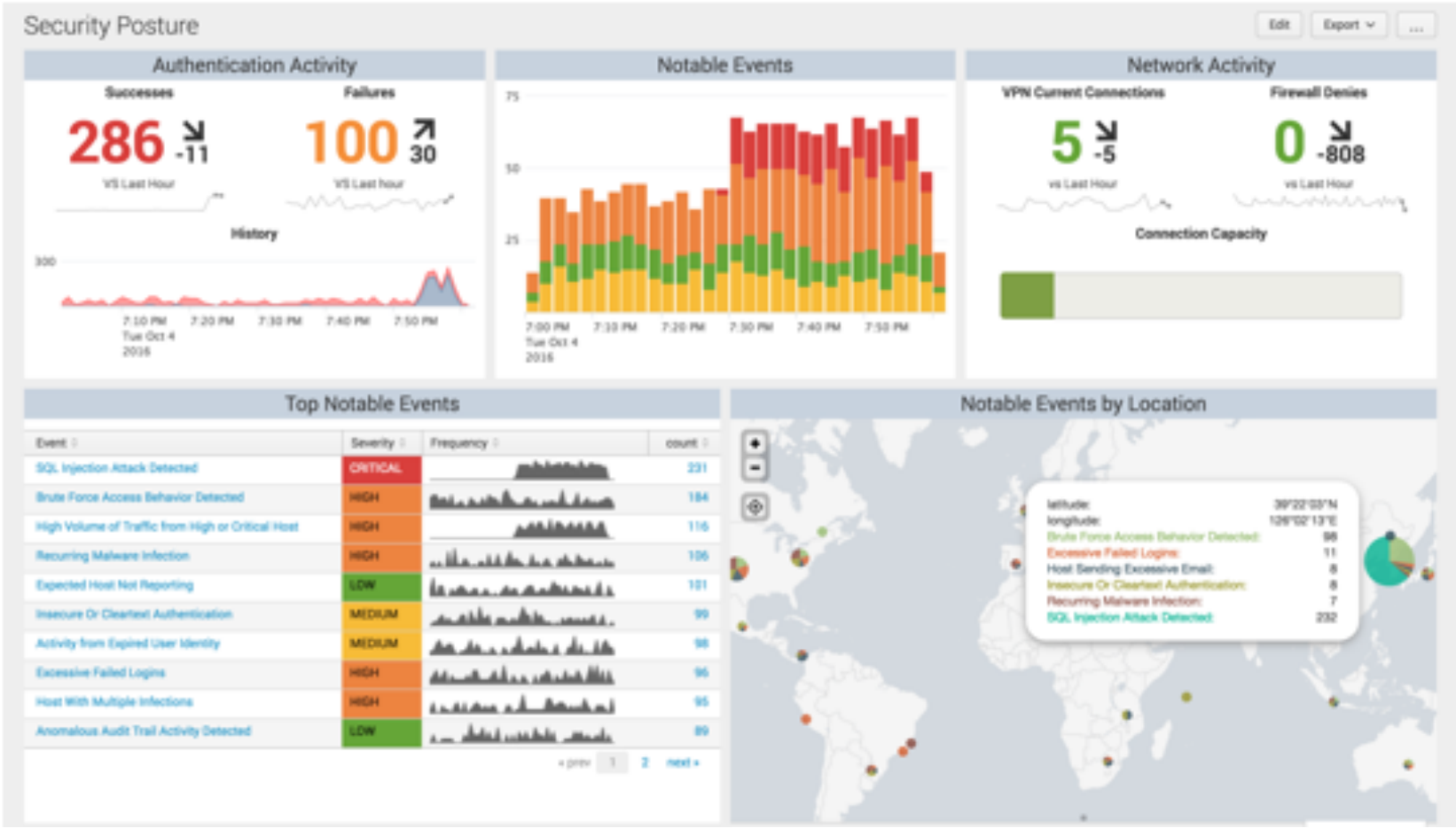
Sistema de Gerenciamento de Eventos e Informações de Segurança (SIEM)

- Análise centralizada de segurança
  - Coleta logs, relatórios, dados etc. de diversos pontos da rede e de diversos sistemas e equipamentos
  - Correlaciona para identificar ameaças
- Gerenciamento de informações de segurança (SIM)
  - Armazenamento de longo prazo, visualização
- Gerenciamento de eventos de segurança (SEM)
  - Monitoramento em tempo real, correlação, alertas
- Componentes típicos do SIEM
  - Coletores de dados
  - Inteligência (correlação)
  - Reporte (visualização, alertas etc.)

SIEM – Coleta de Dados



SIEM – Inteligência e Visualização



Gerenciamento Unificado de Ameaças (UTM)

- Oferece múltiplas funções de defesa
- Minimamente: FW/IDS/IPS
- Outras funções
  - Anti-virus de gateway
  - Firewall de aplicação (camada 7)
  - Inspeção profunda de pacotes
  - Proxy web e filtro de conteúdo
  - Prevenção de perda de dados (DLP)
  - Gerenciamento de informações e eventos de segurança (SIEM)
  - ...

* Ameaças Persistentes Avançadas (APT)

› Ataques direcionados e especializados
  - Ataque direcionado - alvo muito bem escolhido
  - Realizados por humanos – baixo grau de automação
  - Técnicas avançadas usadas de forma não-trivial
  - Alta furtividade – atacante permanece muito tempo nas redes e sistemas atacados

› Exemplos
  - Infiltração nas redes e sistemas de uma empresa de alta tecnologia para roubar segredos industriais
  - Infiltração em sistemas críticos de um país para realizar atos de sabotagem

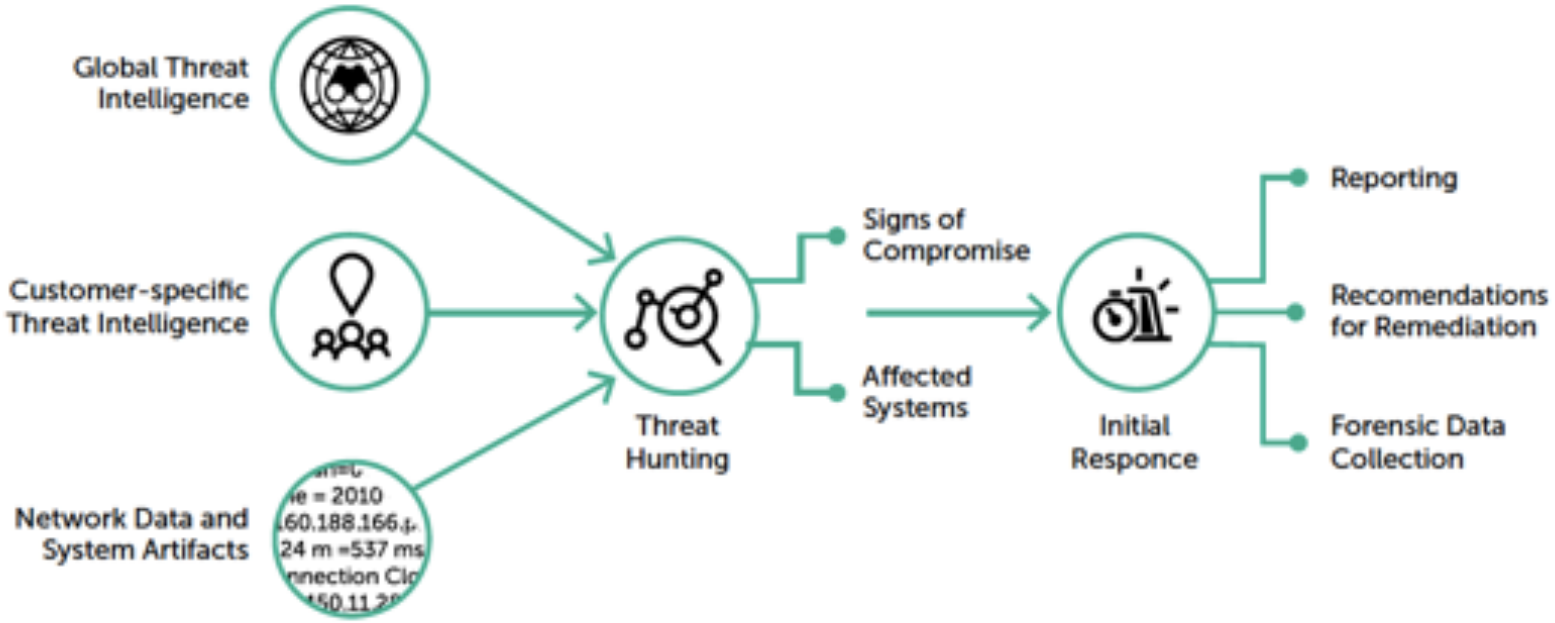
Métodos e ferramentas para deteção de intrusão e ameaças

- Diversas estratégias podem ser usadas
  - Locais de coleta de dados: hosts, equipamentos, segmentos de rede
  - Tipo de dados analisado: nível de agregação (pacotes, fluxos, logs), protocolos/camadas
  - Algoritmos: baseados em assinatura, baseados em comportamento
  - Tipo de intrusão (ameaça) procurado
    - intrusão no sentido amplo de ameaça – qualquer não-conformidade à Política de Segurança
- Exemplos de ferramentas:
  - Detecção passiva: IDS, SIEM, anti-vírus, anti-spam, proxy web
  - Detecção ativa: threat hunting

Threat Hunting

- Estratégia "ativa" de defesa
  - Busca proativa e iterativa de ameaças presentes numa organização
- Baixo grau de automatização – serviço realizado por especialistas
- Combina análise de dados de redes e sistemas com inteligência sobre ameaças cibernéticas
- Dá como retorno não apenas a indicação de ameaças, mas sugestões de eliminação e dados com finalidades forenser

Threat Hunting



Pentesting versus threat hunting

- Ambos envolvem abordagens "ativas" para avaliação de segurança – mas há diferença quanto aos objetivos
- Testes de penetração busca identificar caminhos para possíveis ataques
  - Lista de vulnerabilidades e possíveis cenários de ataque
  - Dificilmente identificará intrusões já realizadas
- Threat Hunting busca identificar intrusões realizadas e ataques em andamento
  - Lista de intrusões realizadas e ataques em andamento
  - Não é exaustivo ou analítico quando a vulnerabilidades ou estratégias de ataque
- A questão da prevenção versus detecção/resposta