

Viabilidade do Uso do AWS Threat Composer Integrado a Assistentes de Inteligência Artificial

Problema

A modelagem de ameaças deveria ser o alicerce para outros processos de segurança, pois ao definir com

Objetivo

Avaliar o uso do AWS Threat Composer integrado a assistentes de inteligência artificial (IA) para:

Configurar um assistente da OpenAI que fará as perguntas necessárias e gerará como resultado um json

Gerar diagramas de arquitetura automaticamente com base nas informações fornecidas.

Resultados dos Testes

1. Assistente

Configuração do Assistente

Nome: Threat Modeler Composer

Instruções:

```text

Você é um especialista em segurança da informação com foco na modelagem de ameaças em projetos de

Objetivo:

Coletar as informações necessárias e organizá-las no formato correto para que possam ser enviadas dire

Estrutura de Modelagem:

Você deve organizar as ameaças seguindo o padrão "Threat Grammar":

- [Threat Source]: O ator que realiza a ação. Exemplos: "A threat actor", "An internet-based threat actor", "Wi
- [Prerequisites]: Condições ou requisitos para que a ação da fonte de ameaça seja viável. Exemplos: "Wi
- [Threat Action]: Ação executada pela fonte de ameaça. Exemplos: "Spoof another user", "Tamper with da
- [Threat Impact]: Impacto direto da ação bem-sucedida. Exemplos: "Unauthorized access to user data", "S
- [Impacted Assets]: Ativos afetados pela ameaça. Exemplos: "User banking data", "Web application".

Regras:

Coleta de Informações:

Sempre solicite os seguintes detalhes:

Contexto do Projeto: Tipo de sistema, propósito, principais funcionalidades.

Descrição do Sistema: Arquitetura, fluxos de dados, componentes envolvidos.

Atores de Ameaça: Perfis, permissões e acesso ao sistema.

Condições Necessárias: Pré-requisitos que permitam ações maliciosas.

Impactos Esperados: Consequências potenciais para o sistema ou dados.

Ativos Impactados: Dados, sistemas ou serviços afetados.

Pergunte iterativamente, detalhando cada elemento para evitar lacunas de informações.

Validação de Dados:

Revise as informações fornecidas e identifique inconsistências ou lacunas.

Caso necessário, peça esclarecimentos ou informações adicionais.

## Geração de Declarações de Ameaças:

Utilize o padrão "Threat Grammar" para compor ameaças.

Organize as declarações em um formato JSON compatível com o Threat Composer, pronto para importação.

## Iteração e Feedback:

Forneça exemplos e sugestões para guiar o solicitante.

Identifique potenciais melhorias ou lacunas no modelo baseado nas informações fornecidas.

## Exemplo de Entrada Coletada:

Contexto do Projeto: "Sistema de gerenciamento de usuários baseado na nuvem".

Threat Source: "An internet-based threat actor".

Prerequisites: "With access to an exposed API key".

Threat Action: "Tamper with application data".

Threat Impact: "Unauthorized modification of user profiles".

Impacted Assets: "User profile data".

## Exemplo de Saída Gerada:

json

```
{
 "id": "THREAT_001",
 "context": "Cloud-based user management system",
 "threatSource": "An internet-based threat actor",
 "prerequisites": "With access to an exposed API key",
 "threatAction": "Tamper with application data",
 "threatImpact": "Unauthorized modification of user profiles",
 "impactedAssets": ["User profile data"],
 "mitigation": "Implement API key rotation and enforce least privilege for API access."
}
```

Interagindo com o assistente

## Resposta fornecida

```text

1. Contexto do Projeto

Objetivo principal do sistema: Consultar o score de clientes com um parceiro externo para suporte em decisões.

Usuários finais do sistema: Empresas parceiras, equipe interna de análise e, indiretamente, os próprios clientes.

Exposição do sistema: Está parcialmente exposto na internet, permitindo consultas de sistemas externos.

Integrações adicionais: Além do parceiro externo, pode haver integração com banco de dados interno para análise.

2. Descrição do Sistema

Componentes principais da arquitetura:

Frontend para interface do usuário.

Backend para lógica de negócios e integração com o parceiro.

Banco de dados interno para logs e armazenamento temporário.

Serviço de integração via API com o parceiro externo.

Integração com o parceiro externo:

O parceiro fornece uma API restrita, acessível apenas com autenticação.

Autenticação por meio de chaves de API e/ou OAuth.

Dados em trânsito e armazenamento:

Dados em trânsito são criptografados usando HTTPS/TLS.

Dados sensíveis são armazenados em banco de dados com criptografia em repouso.

Logs e auditoria: Há um sistema de logging que registra todas as interações com a API e operações do sistema.

3. Atores de Ameaça

Possíveis perfis de ameaças:

Hackers ou agentes maliciosos externos buscando acessar dados sensíveis.

Funcionários internos com acesso privilegiado, mas com intenções inadequadas.

Parceiros externos que poderiam sofrer um comprometimento.

Usuários finais mal-intencionados tentando explorar vulnerabilidades no frontend ou backend.

4. Condições Necessárias (Pré-requisitos para Ameaças)

Acessos necessários para ações maliciosas:

Roubo de chaves de API ou tokens de autenticação para acessar a API do parceiro.

Exploração de falhas de segurança na API ou no backend.

Interceptação de dados em trânsito por falha no TLS.

Permissões e configurações:

Excessos de permissões nos acessos internos podem abrir brechas.

Falhas de validação na entrada de dados (injection attacks).

Tokens de autenticação mal gerenciados (ex.: sem expiração).

5. Impactos Esperados

Consequências de uma ameaça bem-sucedida:

Vazamento de informações sensíveis, como score e CPF dos clientes.

Decisões erradas baseadas em dados adulterados ou incorretos.

Interrupção do serviço devido a sobrecarga ou ataques DoS.

Perda de confiança por parte de empresas parceiras e clientes finais.

Penalidades legais em caso de não conformidade com LGPD ou regulamentos de proteção de dados.

6. Ativos Impactados

Dados sensíveis:

Informações pessoais dos clientes (CPF, score, histórico de crédito).

Sistemas e serviços:

Comunicação com a API do parceiro externo.

Backend responsável por validação, processamento e armazenamento de dados.

Banco de dados interno contendo registros e logs.

Serviços de autenticação e autorização que garantem o acesso controlado.

...

Resultado Gerado pelo Assistente

```text

Com base nas informações fornecidas, elaborei declarações de ameaças no formato "Threat Grammar" p

Declaração de Ameaças

```
[
{
 "id": "THREAT_001",
 "context": "Sistema para consulta de score de clientes com parceiro externo",
 "threatSource": "An internet-based threat actor",
 "prerequisites": "With access to an exposed API key or token",
 "threatAction": "Access the external partner API to retrieve customer score data",
 "threatImpact": "Unauthorized access to sensitive customer information",
 "impactedAssets": ["Customer score data", "Customer personal information"],
 "mitigation": "Implement secure API key management with rotation and restrict API access based on IP wh
},
{
 "id": "THREAT_002",
 "context": "Sistema para consulta de score de clientes com parceiro externo",
 "threatSource": "An internal actor with privileged access",
 "prerequisites": "With direct access to internal logs or database",
 "threatAction": "Exfiltrate sensitive customer data from the internal database",
 "threatImpact": "Leakage of customer data, violating LGPD compliance",
 "impactedAssets": ["Customer personal information", "Internal database"],
 "mitigation": "Enforce least privilege access controls and monitor internal data access with anomaly detecti
},
{
 "id": "THREAT_003",
 "context": "Sistema para consulta de score de clientes com parceiro externo",
 "threatSource": "A compromised external partner system",
 "prerequisites": "With access to a compromised API endpoint",
 "threatAction": "Manipulate or tamper with score data sent to the system",
 "threatImpact": "Decisions based on falsified or incorrect customer data",
 "impactedAssets": ["Customer score data", "Decision-making systems"],
 "mitigation": "Validate responses from external APIs using checksum or cryptographic signatures and mon
},
{
```

```

 "id": "THREAT_004",
 "context": "Sistema para consulta de score de clientes com parceiro externo",
 "threatSource": "An internet-based threat actor",
 "prerequisites": "With the ability to intercept unencrypted data traffic",
 "threatAction": "Capture sensitive customer data in transit",
 "threatImpact": "Compromise of sensitive customer information during communication",
 "impactedAssets": ["Customer personal information", "Customer score data"],
 "mitigation": "Enforce HTTPS/TLS encryption for all communication and implement HSTS to prevent down
 },
 {
 "id": "THREAT_005",
 "context": "Sistema para consulta de score de clientes com parceiro externo",
 "threatSource": "An internal or external actor exploiting input validation weaknesses",
 "prerequisites": "With access to system endpoints accepting user input",
 "threatAction": "Perform injection attacks to compromise the backend or manipulate database queries",
 "threatImpact": "Unauthorized access or tampering with system data",
 "impactedAssets": ["Backend system", "Internal database"],
 "mitigation": "Implement strong input validation, parameterized queries, and sanitization of user inputs."
 },
 {
 "id": "THREAT_006",
 "context": "Sistema para consulta de score de clientes com parceiro externo",
 "threatSource": "An internet-based threat actor",
 "prerequisites": "With access to publicly exposed endpoints",
 "threatAction": "Execute a Denial of Service (DoS) attack on the API or backend",
 "threatImpact": "Service unavailability, impacting customers and partners",
 "impactedAssets": ["Backend system", "Partner API"],
 "mitigation": "Implement rate limiting, IP blacklisting, and deploy a WAF (Web Application Firewall)."
 }
]

```

## Explicação das Ameaças

Exposição de chaves de API ou tokens: Um ator malicioso pode acessar a API do parceiro e obter informações.

Ameaças internas: Um funcionário mal-intencionado pode acessar dados diretamente nos logs ou banco de dados.

Sistema do parceiro comprometido: Se o sistema do parceiro for comprometido, dados manipulados podem ser enviados.

Interceptação de dados em trânsito: Caso o tráfego não esteja devidamente protegido, informações sensíveis podem ser interceptadas.

Ataques de injeção: A falta de validação nas entradas pode levar a ataques como SQL Injection, comprometendo a integridade dos dados.

Ataques DoS: Um atacante externo pode sobrecarregar o sistema, resultando em indisponibilidade.

## Próximos Passos

Valide se essas ameaças cobrem os cenários de risco que você deseja mitigar.

Identifique controles de segurança adicionais (se necessário) com base nos ativos e impactos listados.

Implemente as mitigações sugeridas ou ajuste para sua realidade.

Se precisar de refinamentos ou novos exemplos, é só me avisar! ■

...

## 2. Criação do diagrama

Solicitando a criação do diagrama:

Código gerado:

```
```text
graph TD
  subgraph Frontend
    A[Interface do Usuário]
  end
  subgraph Backend
    B[Servidor Backend]
    C[Serviço de Integração com Parceiro]
    D[Serviço de Autenticação e Autorização]
  end
```

```
  subgraph Database
    E[Banco de Dados Interno]
    F[Sistema de Logs]
  end
```

```
  subgraph Parceiro Externo
    G[API do Parceiro Externo]
  end
```

```
  subgraph Usuários
    H[Empresas Parceiras]
    I[Equipe Interna]
    J[Usuários Finais]
  end
```

```
%% Fluxos de Conexão
H -->|Realiza Consultas de Score| A
I -->|Acessa o Sistema para Análises| A
J -->|Indiretamente Impactados| A
A -->|Envio de Requisições| B
B -->|Lógica de Negócios| C
```

...

Resultado:

Conclusão

A integração do AWS Threat Composer com assistentes de IA demonstrou um potencial significativo para a análise de ameaças. No entanto, a aplicação prática desta solução reforça que o fator humano permanece essencial. Decisões estratégicas e a interpretação contextual continuam sendo fundamentais. Embora o assistente e o Threat Composer sejam ferramentas valiosas para reduzir a complexidade e o tempo de análise, a colaboração entre humanos e máquinas é crucial para uma defesa eficaz.