CLOUD SUMMIT +AI CERRADO

Cloud + IA
Summit Cerrado
2025

CLOUD SUMMIT +AI CERRADO

Quando a IA vira DevSecOps

Quem sou eu ?

Luiz Machado

Head de Eng. & IT Services - Cilia Tecnologia
AWS Community Builder - Security & Identity (3Y)
Líder de comunidade - @GYNSec
Criar, desenvolver e contribuir com ferramentas OpenSource

Agenda

- Atuando como Vetor de Ataque
- Prompt injection e LLM injection
- Contra Inteligência
  - Caso de uso de Pipeline segura com IA
- IA na Operação
- Cuidados, Futuro e Reflexões

IA como Vetor de Ataque

Modelos generativos sendo usados para:

- **Criar payloads automatizados**
- **Gerar eng. social mais convincente**
- **Escrever códigos maliciosos**

IA como Vetor de Ataque

Exemplo:

- **IA criando código com SQLi, XSS e etc..**

IA como Vetor de Ataque

OpenSource:

- **LOKI (Leverage Offensive Knowledge Intelligently)**

Tipo	Exemplo
Hardcoded Secrets	AWS keys, database credentials
Injection Flaws	SQL Injection, Command Injection in Flask/Express
Dependency Vulnerabilities	Use of outdated libraries with known CVEs
Dangerous Code Use	eval(), pickle.load() on user input
Access Control Bypass	Missing authorization checks

Prompt Injection & LLM Injection

Prompt Injection:

- **Inserir instruções maliciosos (caracteres invisíveis unicode)**

Prompt Injection & LLM Injection

Prompt Injection:

- **Inserir instruções maliciosos (caracteres invisíveis unicode)**

LLM Injection:

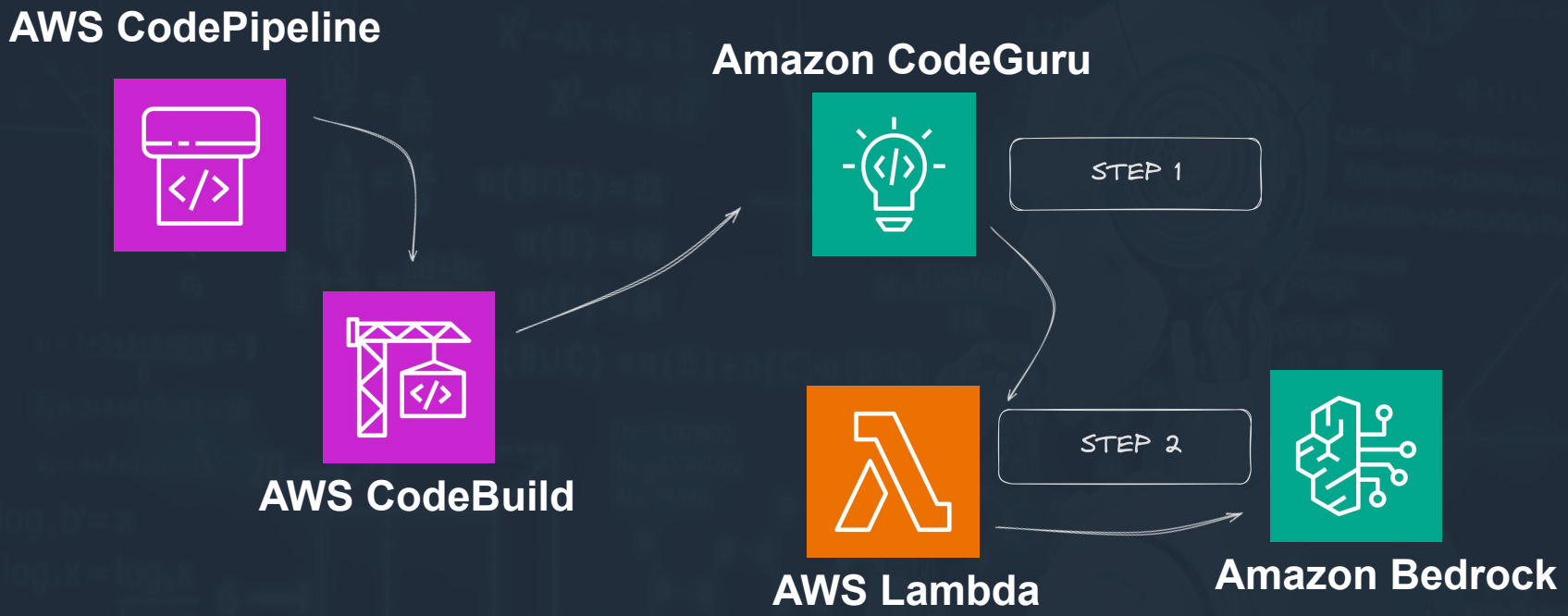
- **Explorar a lógica do modelo (obter ou manipular dados)**

Contra Inteligência: IA vs IA

A mesma IA pode ser usada para:

- Detectar falhas com SAST
- Reescrever código com segurança
- Automatizar PRs de correção

Caso de uso de Pipeline segura com IA


AWS CodePipeline
Amazon CodeGuru
STEP 1
AWS CodeBuild
STEP 2
AWS Lambda
Amazon Bedrock

Código vulnerável

```
query = f"SELECT * FROM users WHERE username = '{username}'"
```

Sugestão da IA (Prepared Statements)

```
query = "SELECT * FROM users WHERE username = ?"
cursor.execute(query, (username,))
```

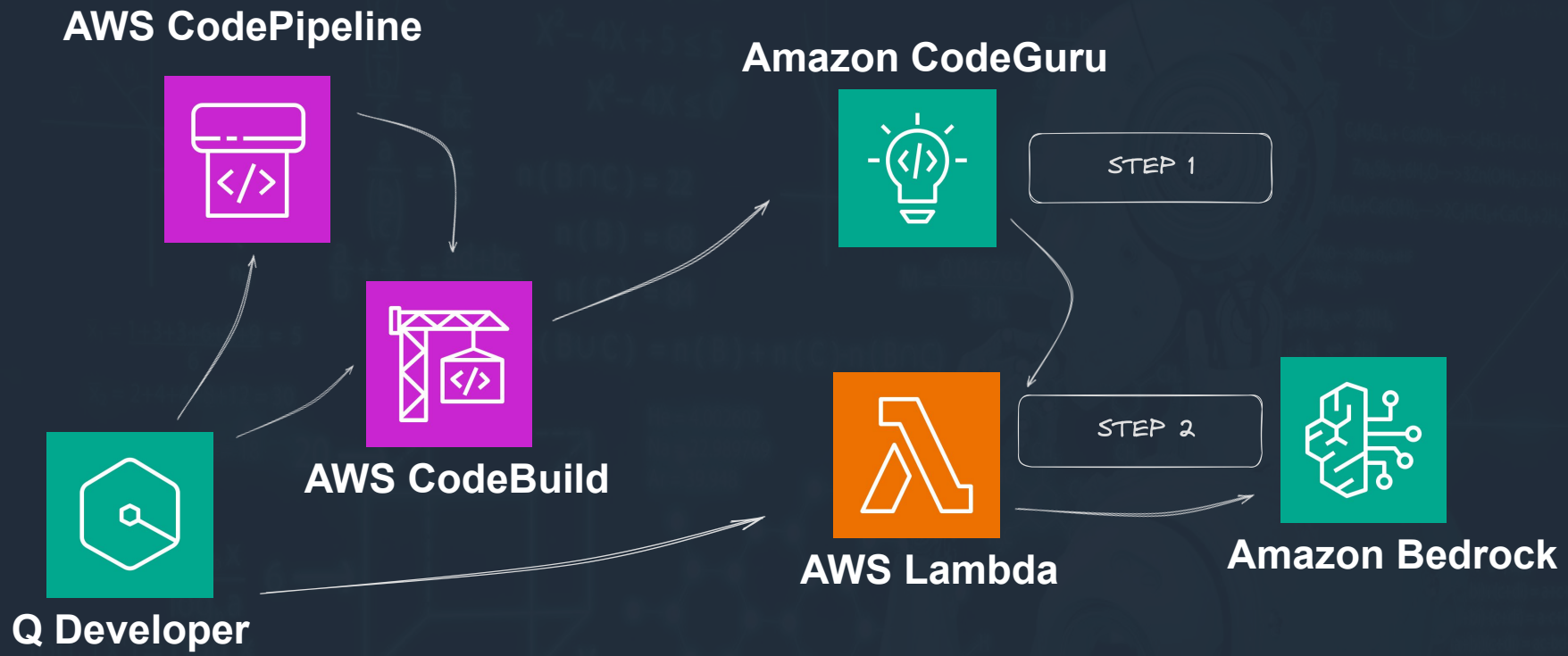
Contra Inteligência: IA vs IA

Principais vantagens:

- **Correção imediata ao detectar falha**
- **Aplicar padrões seguros**
- **Redução do tempo de exposição**
- **Aceleração do ciclo de DevSecOps**

IA na Operação

- Correções automáticas evitam incidentes em produção
- Geração de playbooks dinâmicos com IA
- Detecção de anomalias operacionais com IA
- Reações automatizadas baseadas em logs/eventos
- Operações mais proativas e resilientes

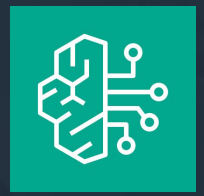

AWS CodePipeline
Amazon CodeGuru
STEP 1
AWS CodeBuild
STEP 2
Q Developer
AWS Lambda
Amazon Bedrock

Amazon CodeGuru

STEP 1

Q Developer

STEP 2



AWS Lambda

Amazon Bedrock

CLOUD SUMMIT +AI· CERRADO

cilia

Cuidados ⚠️

- Validação humana ainda é essencial
- IA não entende o negócio como um todo
- Log e auditoria das ações da IA são obrigatórios
- Automação sem contexto pode gerar riscos
- Atenção especial a ataques de prompt injection e jailbreaks em LLMs

Futuro da IA no DevSecOps

- Modelos ajustados com o código interno da empresa
- Correções nativas na IDE, PRs automáticos no Git
- Resposta a incidentes com orquestração baseada em IA
- Um ciclo contínuo onde IA identifica, corrige e opera
- Detecção automática de prompt injection nas interfaces e APIs

Reflexões

- A IA ofensiva já existe. Devemos nos preparar com IA defensiva.
- DevSecOps com IA não é uma tendência: é necessidade.
- E você pode começar agora.

CLOUD SUMMIT +AI+ CERRADO

Obrigado

cilia