🩹 Paddi

AI-Powered Multi-Agent Cloud Audit System

Google Cloud AI Hackathon: Multi-Agent Edition

Susumu Tomita

2025-06-21

📋 Agenda

1. **Problem Statement** - クラウドセキュリティの課題
2. **Solution Overview** - Paddiの提案
3. **Architecture** - マルチエージェントシステム
4. **Demo** - 実際の動作
5. **Technical Details** - 実装の詳細
6. **Future Vision** - 今後の展望

🔥 Problem Statement

クラウドセキュリティ監査の現状

😫 手動プロセスの課題

- **時間がかかる**: 数百のIAMポリシーを手動でレビュー
- **エラーが発生しやすい**: 人的ミスによる見落とし
- **専門知識が必要**: セキュリティベストプラクティスの深い理解
- **スケールしない**: マルチクラウド環境での複雑性

💰 ビジネスインパクト

- セキュリティインシデントのリスク増大

💡 Solution: Paddi

Paddiとは？

🤖 AIエージェントによる自動化

3つの専門エージェントが協調して動作：

1. **Collector Agent** 📊
   - GCP設定を自動収集
2. **Explainer Agent** 🧠
   - Gemini LLMでリスクを分析
3. **Reporter Agent** 📝
   - 人間が読みやすいレポートを生成

なぜマルチエージェント？

🎯 Single Responsibility Principle

各エージェントが**専門的なタスク**に集中

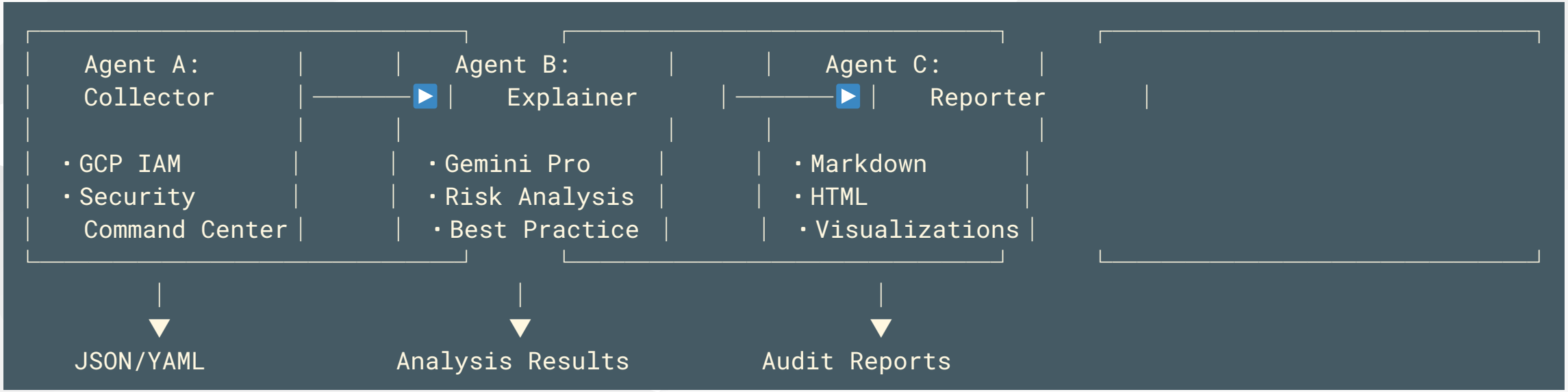
🔄 Modularity & Scalability

- エージェントの**独立した開発・テスト**が可能
- 新しいクラウドプロバイダーの**追加が容易**

🚀 Performance

Architecture

システムアーキテクチャ



技術スタック

Python Agents

- `google-cloud-iam`
- `google-cloud-securitycenter`
- `google-cloud-aiplatform` (Vertex AI)

Rust CLI

- 高速な実行
- クロスプラットフォーム対応

Demo

デモシナリオ

1 Configuration Collection

```
$ paddi collect --project my-gcp-project
✓ IAM policies collected: 47
✓ SCC findings retrieved: 12
```

2 AI Analysis

```
$ paddi analyze
✓ Analyzing with Gemini Pro...
✓ Risk score calculated: 7.3/10
```

生成されるレポート例

📊 Executive Summary

- Overall Risk Score: **7.3/10**
- Critical Findings: **3**
- Recommendations: **15**

🔍 Key Findings

1. **過剰な権限**: 5つのサービスアカウントにOwner権限
2. **未使用のIAMメンバー**: 90日以上アクセスなし

Technical Details

Geminiプロンプトエンジニアリング

📝 構造化プロンプト

```
prompt = f"""
As a cloud security expert, analyze the following
GCP IAM configuration:

{iam_config}

Identify:
1. Security risks and severity
2. Best practice violations
3. Specific remediation steps

Format: JSON with risk_score, findings, recommendations
"""
```

エージェント間通信

📨 データフロー

```yaml
# Agent A Output
collector_output:
  timestamp: "2025-06-21T10:00:00Z"
  project_id: "my-project"
  iam_policies:
    - member: "user:admin@example.com"
      role: "roles/owner"
  scc_findings:
    - severity: "HIGH"
      category: "PUBLIC_BUCKET"
```

Future Vision

ロードマップ

🌐 Multi-Cloud Support

- AWS (IAM, Security Hub)
- Azure (AD, Security Center)
- クロスクラウド比較レポート

🤖 Advanced AI Features

- 予測的リスク分析
- 自動修復提案

ビジネスインパクト

💰 コスト削減

- 監査時間を**80%削減**
- 手動エラーを**ゼロに**

🛡️ セキュリティ向上

- **24/7継続的監査**
- **プロアクティブなリスク検出**

📈 スケーラビリティ

🙏 Thank You!

Questions?

🔗 Links

- GitHub: github.com/susumutomita/Paddi
- Website: susumutomita.netlify.app

📧 Contact

- Email: (your-email@example.com)

Appendix: 実装の詳細

🔐 セキュリティ考慮事項

- Application Default Credentialsの使用
- 最小権限の原則
- 監査ログの暗号化

🧪 テスト戦略

- 単体テスト: 各エージェント
- 統合テスト: エンドツーエンド