Prisma AIRS- Zero to Hero Part 02

Brown Bag Sessions

paloalto NETWORKS | PRISMA® AIRS

Part 02 - Agenda

- API Intercept Implementation
- Hands-On
- AI Model Security Implementation
- Hands-On
- Wrap up to Part 03

paloalto NETWORKS | PRISMA AIRS

API Intercept - Onboarding and Activation

- Quick Recap
- Onboarding and Activation
- Configuration
- Installing/Initializing API Python SDK
- Simulating Prompt flow to verify triggers
- Flow Scenarios to verify triggers

API Intercept - Onboarding and Activation

- Quick Recap
- **Onboarding and Activation**
- Configuration
- Installing/Initializing API Python SDK
- Simulating Prompt flow to verify triggers
- Flow Scenarios to verify triggers

API Intercept Onboarding

API Intercept - Onboarding and Activation

- Quick Recap
- Onboarding and Activation
- **Configuration**
- Installing/Initializing API Python SDK
- Simulating Prompt flow to verify triggers
- Flow Scenarios to verify triggers

API Intercept Onboarding

API Intercept - Onboarding and Activation

- Quick Recap
- Onboarding and Activation
- **Configuration**
- Installing/Initializing API Python SDK
- Simulating Prompt flow to verify triggers
- Flow Scenarios to verify triggers

API Intercept Onboarding

API Intercept - Onboarding and Activation

- Quick Recap
- Onboarding and Activation
- Configuration
- **Installing/Initializing API Python SDK**
- Simulating Prompt flow to verify triggers
- Flow Scenarios to verify triggers

API Intercept Onboarding

API Intercept - Onboarding and Activation

- Quick Recap
- Onboarding and Activation
- Configuration
- Installing/Initializing API Python SDK
- **Simulating Prompt flow to verify triggers**
- Flow Scenarios to verify triggers

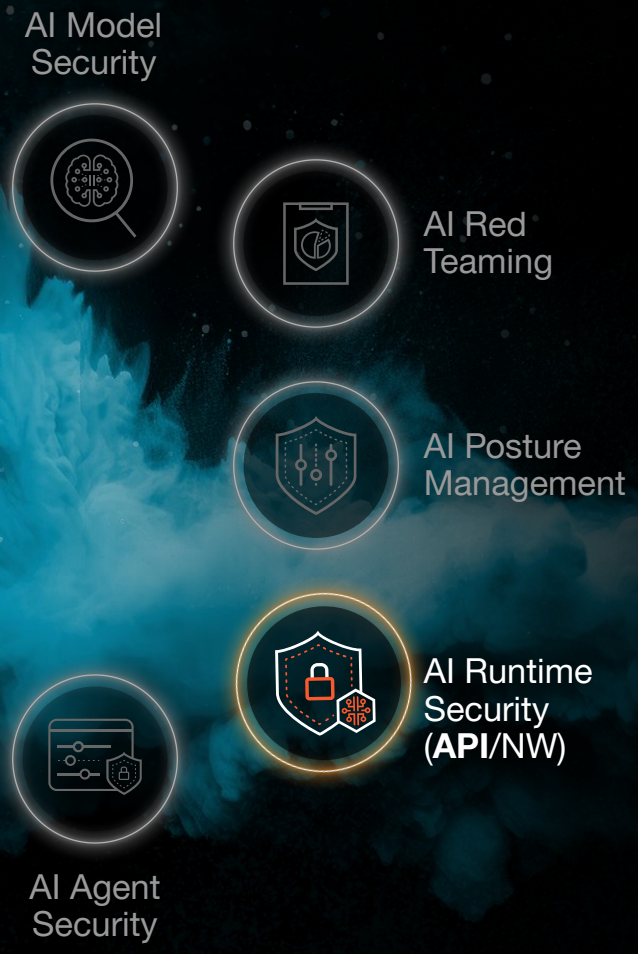
API Intercept - Onboarding and Activation

- Quick Recap
- Onboarding and Activation
- Configuration
- Installing/Initializing API Python SDK
- Simulating Prompt flow to verify triggers
- **Flow Scenarios to verify triggers**

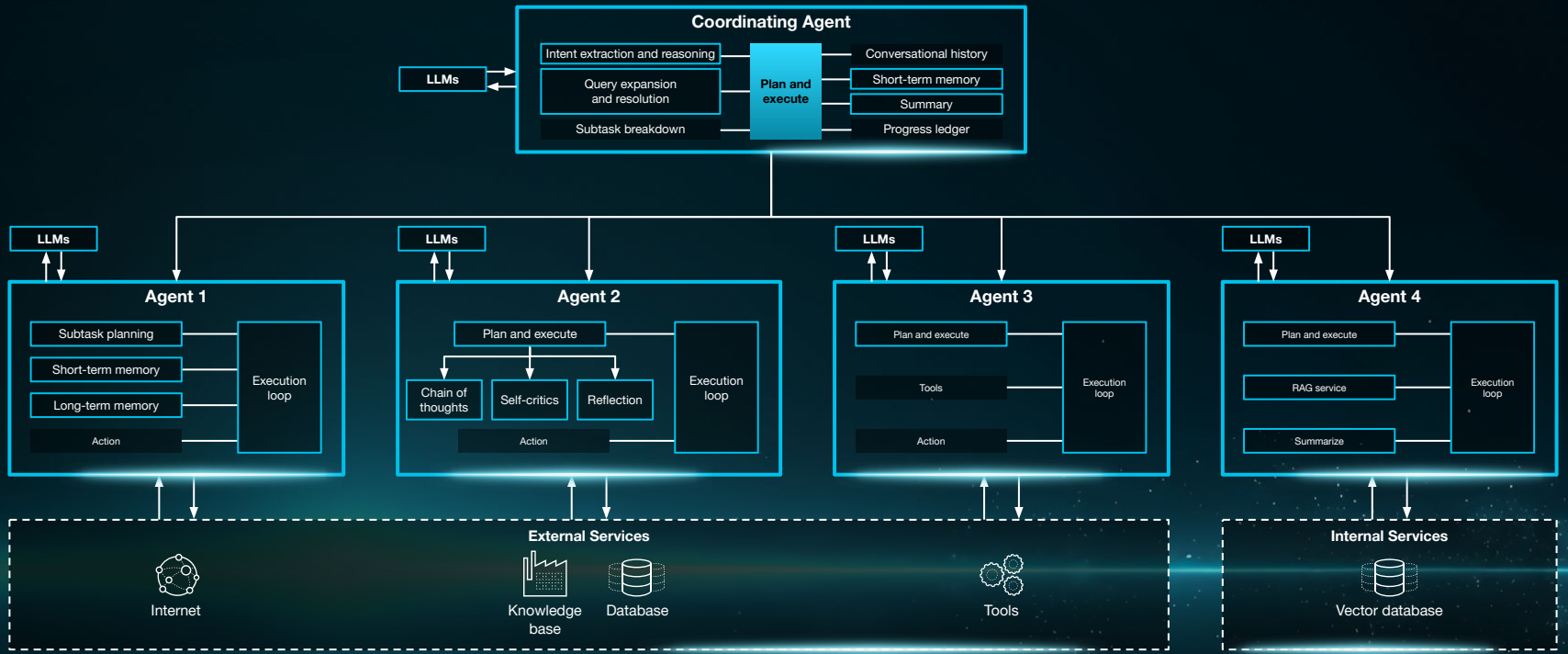
API Intercept Onboarding

AI Runtime API Security Additional Information

- **Limitations**
  - **One API key per deployment profile**
  - **Cross-region use of API keys isn't supported**
  - **Payload size per Synchronous Scan Request**
  - **Payload size per Asynchronous Scan Request**
  - **Async Scan Request Batch Limits**



Appendix


Coordinating Agent
LLMs
Intent extraction and reasoning
Query expansion and resolution
Subtask breakdown
Plan and execute
Conversational history
Short-term memory
Summary
Progress ledger
LLMs
Agent 1
Subtask planning
Short-term memory
Long-term memory
Action
Execution loop
LLMs
Agent 2
Plan and execute
Chain of thoughts
Self-critics
Reflection
Action
Execution loop
LLMs
Agent 3
Plan and execute
Tools
Action
Execution loop
LLMs
Agent 4
Plan and execute
RAG service
Summarize
Execution loop
External Services
Internet
Knowledge base
Database
Tools
Internal Services
Vector database