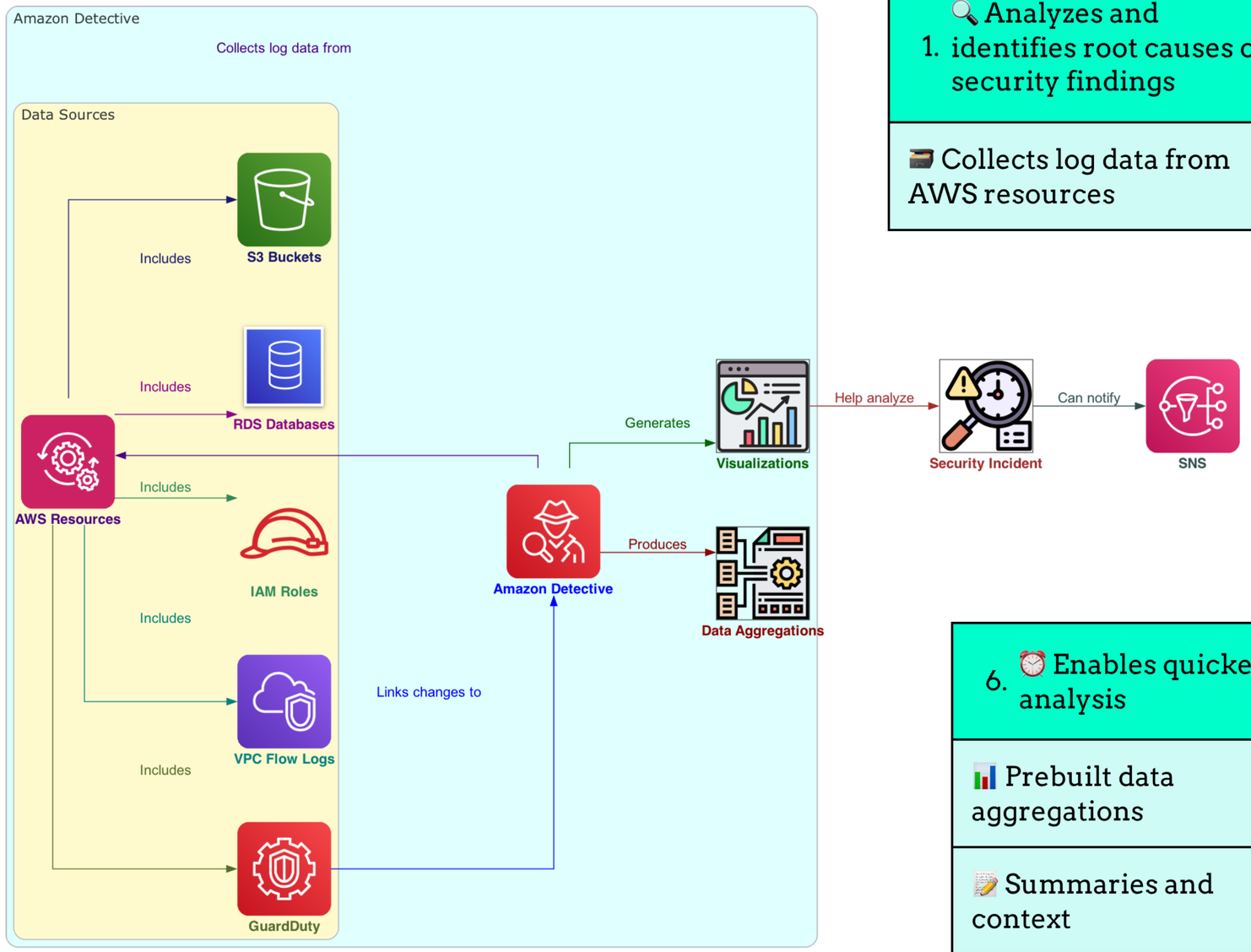
Amazon Detective

Table of Contents

What is Amazon Detective?



1. 🔍 Analyzes and identifies root causes of security findings

🗃️ Collects log data from AWS resources

2. 📊 Utilizes advanced techniques

🧠 Machine learning

📈 Statistical analysis

🕸️ Graph theory

💡 Generates meaningful insights

3. 📈 Generates visualizations

⏩ Faster investigations

🔎 Efficient security investigations

4. 📅 Accesses historical event data

⏳ Up to 1 year

🔍 Comprehensive view of security activities

5. 🔗 Links data changes to GuardDuty findings

🚨 Identifies potential security issues

6. ⏰ Enables quicker analysis

📊 Prebuilt data aggregations

📝 Summaries and context

🔍 Analyze nature and extent of issues

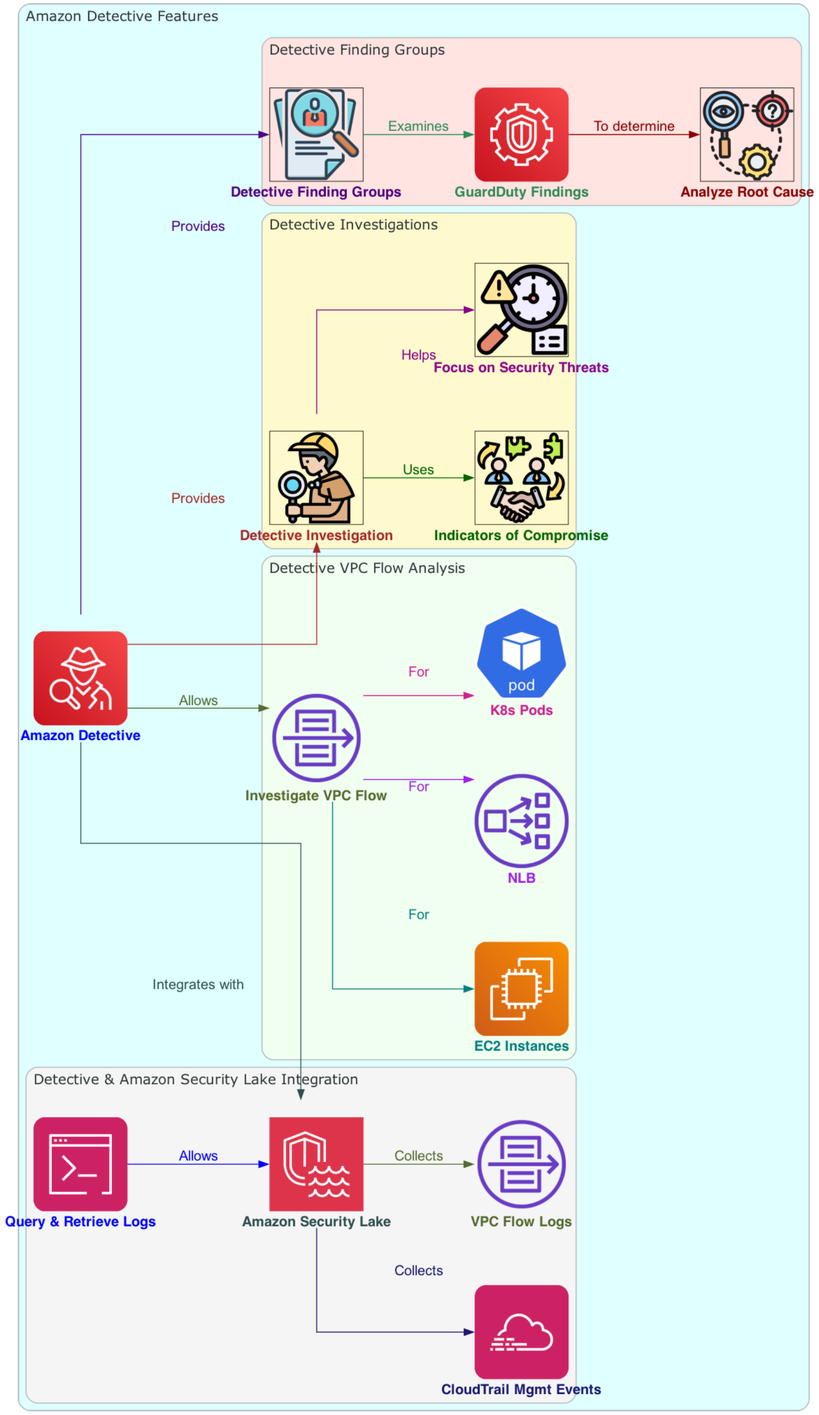
7. 🎯 Determines scope of security threats

🗃️ Automatic data aggregation

📊 Visual tools

⚡ Faster and efficient investigations

Features



1. 🔍 Detective finding groups

- 🕵️ Examine multiple activities
- 🔎 Analyze root cause of GuardDuty findings
- 🚨 Identify threat actor actions
- 🚩 Generate security findings, unusual behaviors

2. 🕵️ Detective Investigation to triage findings

- 🔍 Investigate IAM users and roles
- 🚨 Use indicators of compromise (IOC)
- 🎯 Determine resource involvement in incidents
- ⚡ Maximize efficiency
- 🔒 Focus on security threats
- 🛡️ Strengthen incident response capabilities

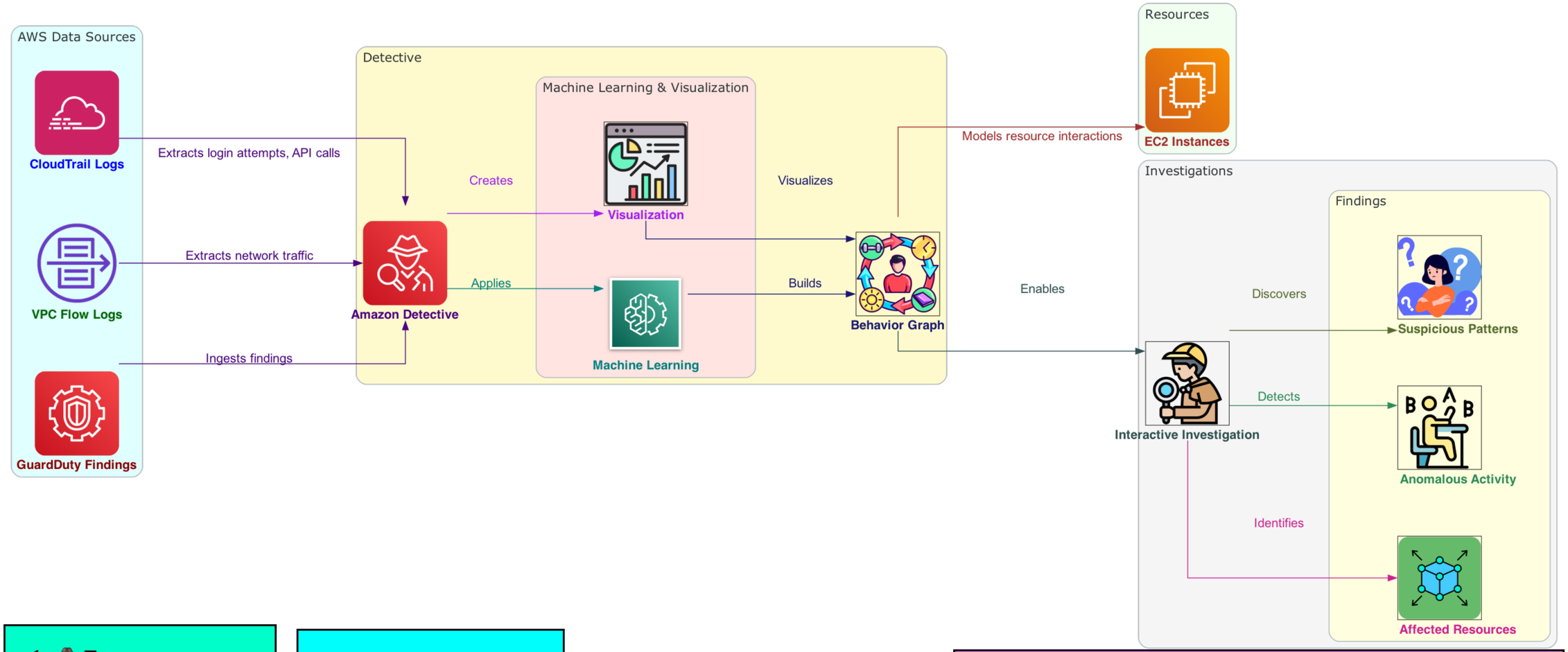
3. 🔗 Detective integration with Amazon Security Lake

- 🔍 Query and retrieve raw log data
- 📥 Collect logs and events from:
- ☁️ AWS CloudTrail management events
- Amazon VPC Flow Logs

4. 🔍 Investigate VPC flow volume

- 🕵️ Examine VPC network flow activity details
- 💻 For EC2 instances
- 📦 For Kubernetes pods
- 🗃️ Collects VPC flow logs from monitored accounts
- 📊 Aggregates by EC2 instance
- 📈 Presents visual summaries and analytics

🔍 How Amazon Detective Works



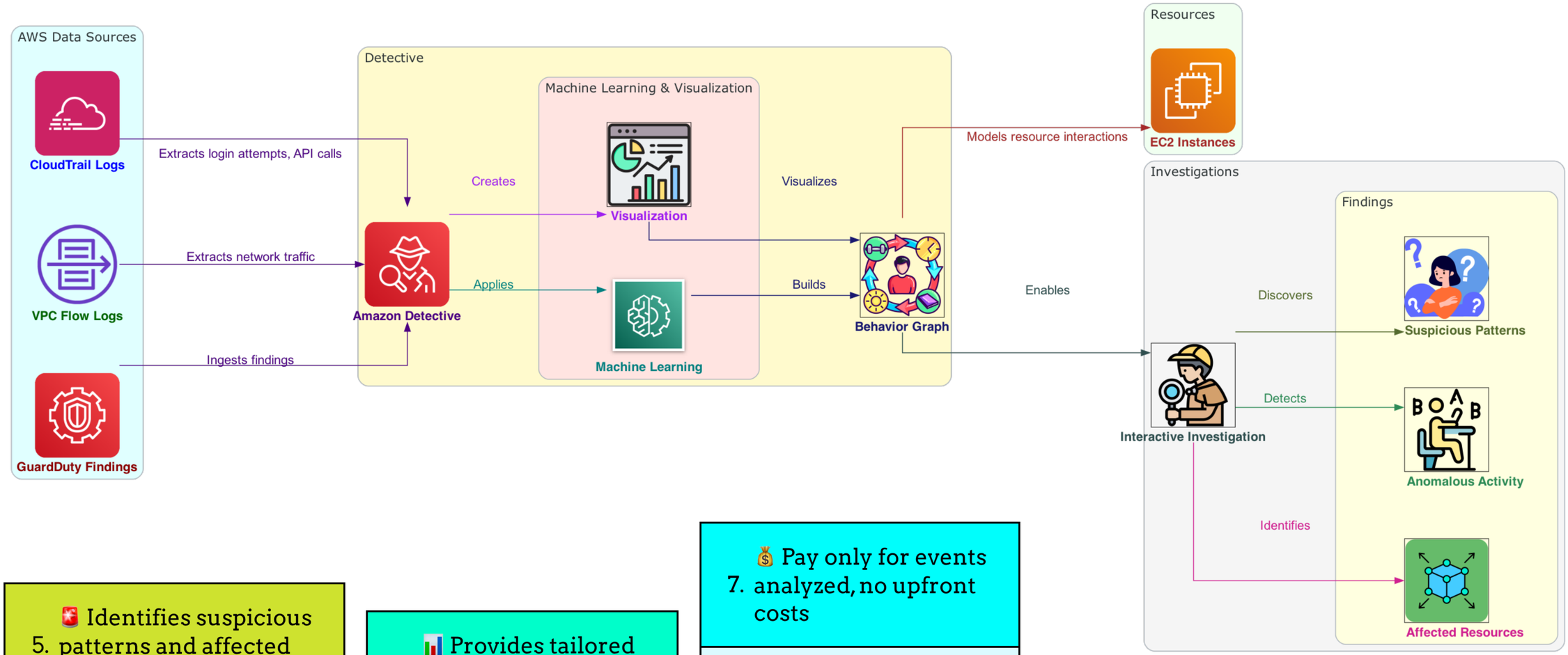
1. 🕵️ Extracts events
☁️ From CloudTrail
🖥️ From VPC flow logs
🚨 From GuardDuty findings

2. 🧠 Uses machine learning and visualization
📊 Analyzes data
🖼️ Presents data meaningfully

3. 🌐 Creates an interactive behavior graph
🔗 Shows resource behaviors and interactions
⏳ Over time

4. 🔎 Enables investigation of anomalous activities
🔍 Explore behavior graph
🚨 Examine suspicious actions
⚡ Rapidly investigate abnormal activities

🔍 How Amazon Detective Works

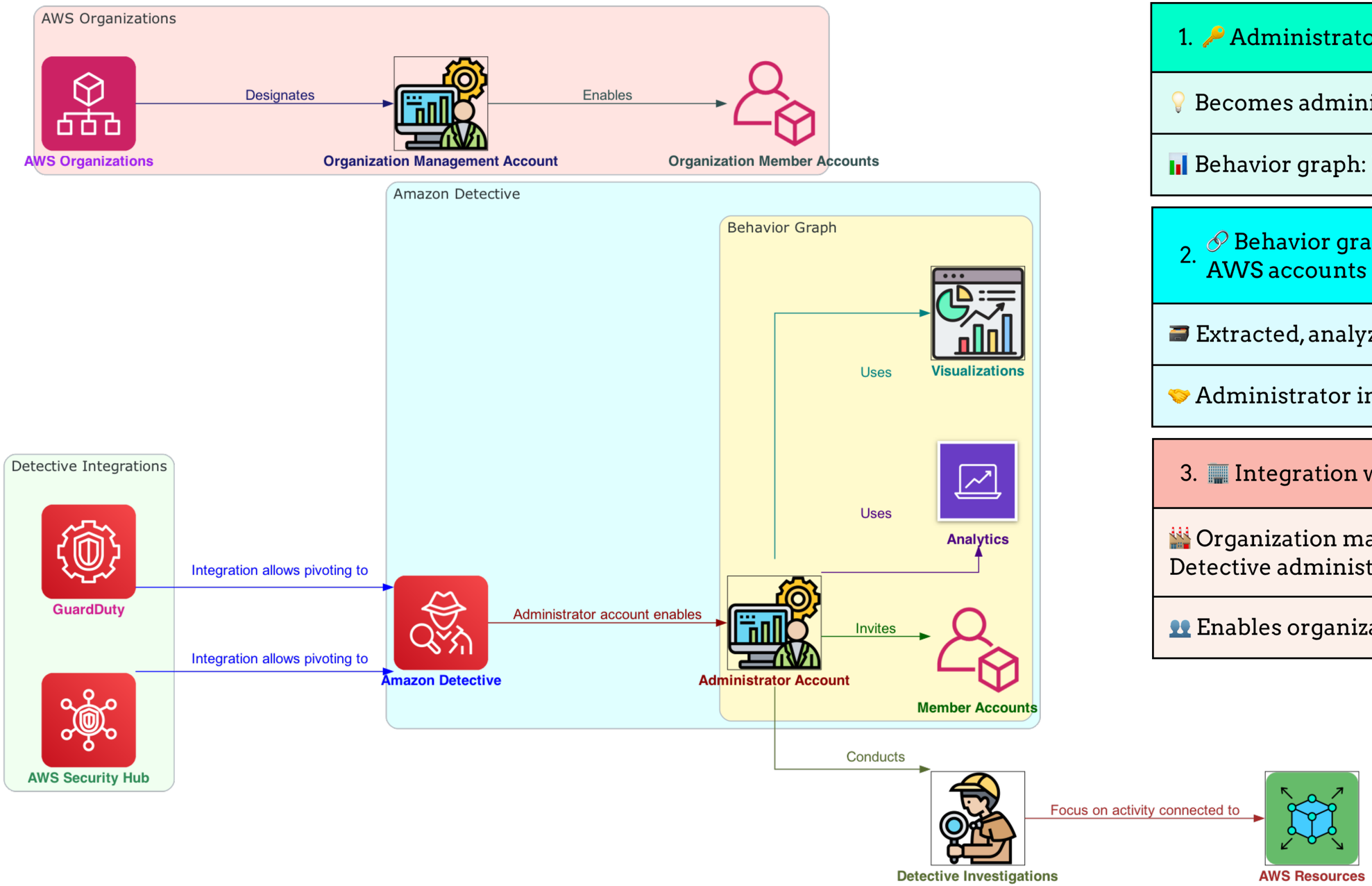


5. 🚨 Identifies suspicious patterns and affected resources
🔍 Detects security issues
💻 Understands impacted AWS accounts and EC2 instances

6. 📊 Provides tailored visualizations and baselines
📈 Summarizes account information
❓ Answers key questions

7. 💰 Pay only for events analyzed, no upfront costs
🚫 No data organization or algorithm tuning needed
💸 Pay per event analyzed
🔧 No additional software or feeds required

👥 Who Uses Amazon Detective?



1. 🔑 Administrator account for behavior graph

💡 Becomes administrator when enabling Detective

📊 Behavior graph: linked data from AWS accounts

2. 🔗 Behavior graph: linked data from multiple AWS accounts

🗃️ Extracted, analyzed data from AWS accounts

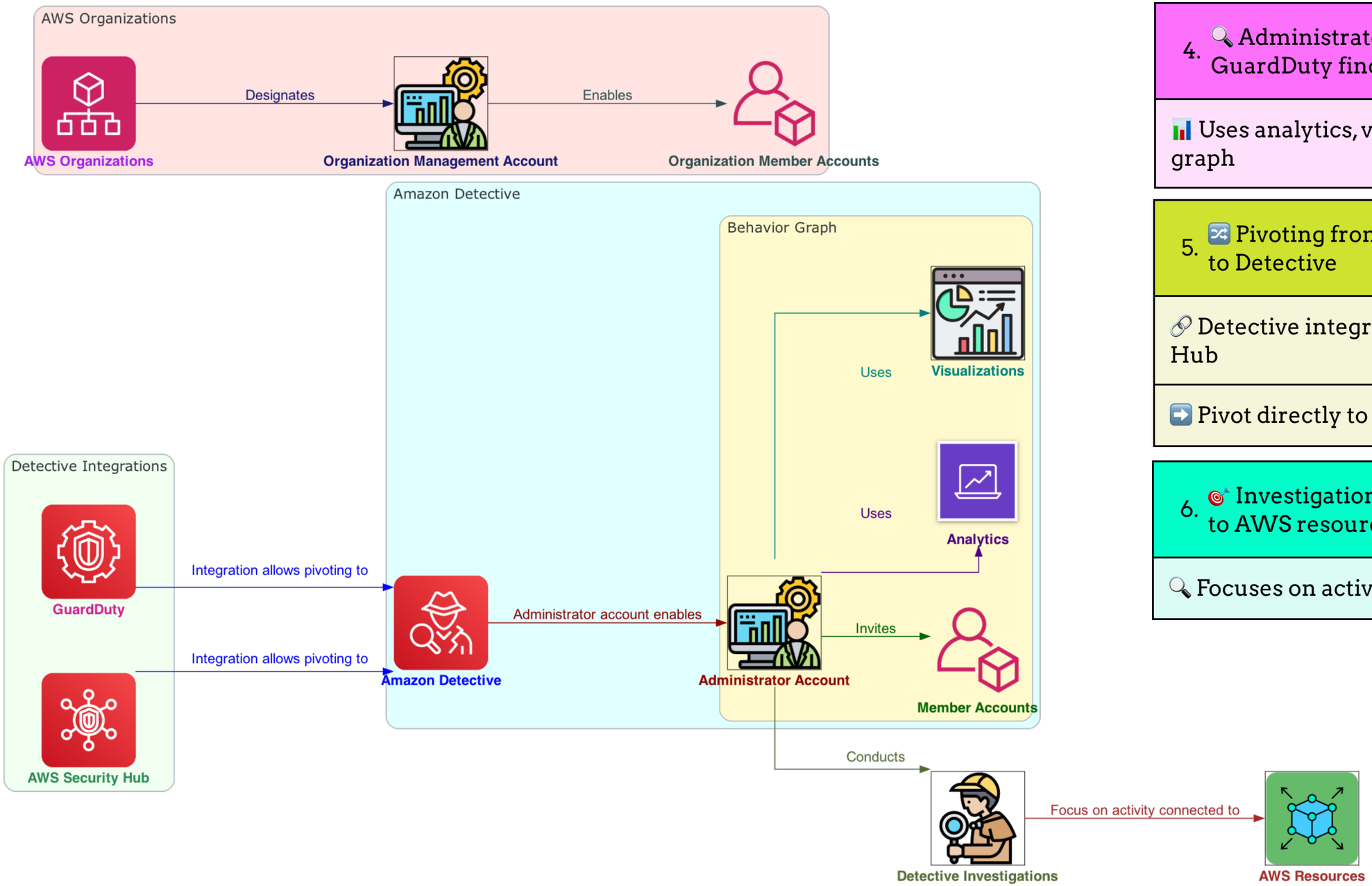
🤝 Administrator invites member accounts

3. 🏢 Integration with AWS Organizations

🏭 Organization management account designates Detective administrator

👥 Enables organization accounts as members

👥 Who Uses Amazon Detective?



4. 🔍 Administrator investigates resources and GuardDuty findings

📊 Uses analytics, visualizations from behavior graph

5. 🔀 Pivoting from GuardDuty and Security Hub to Detective

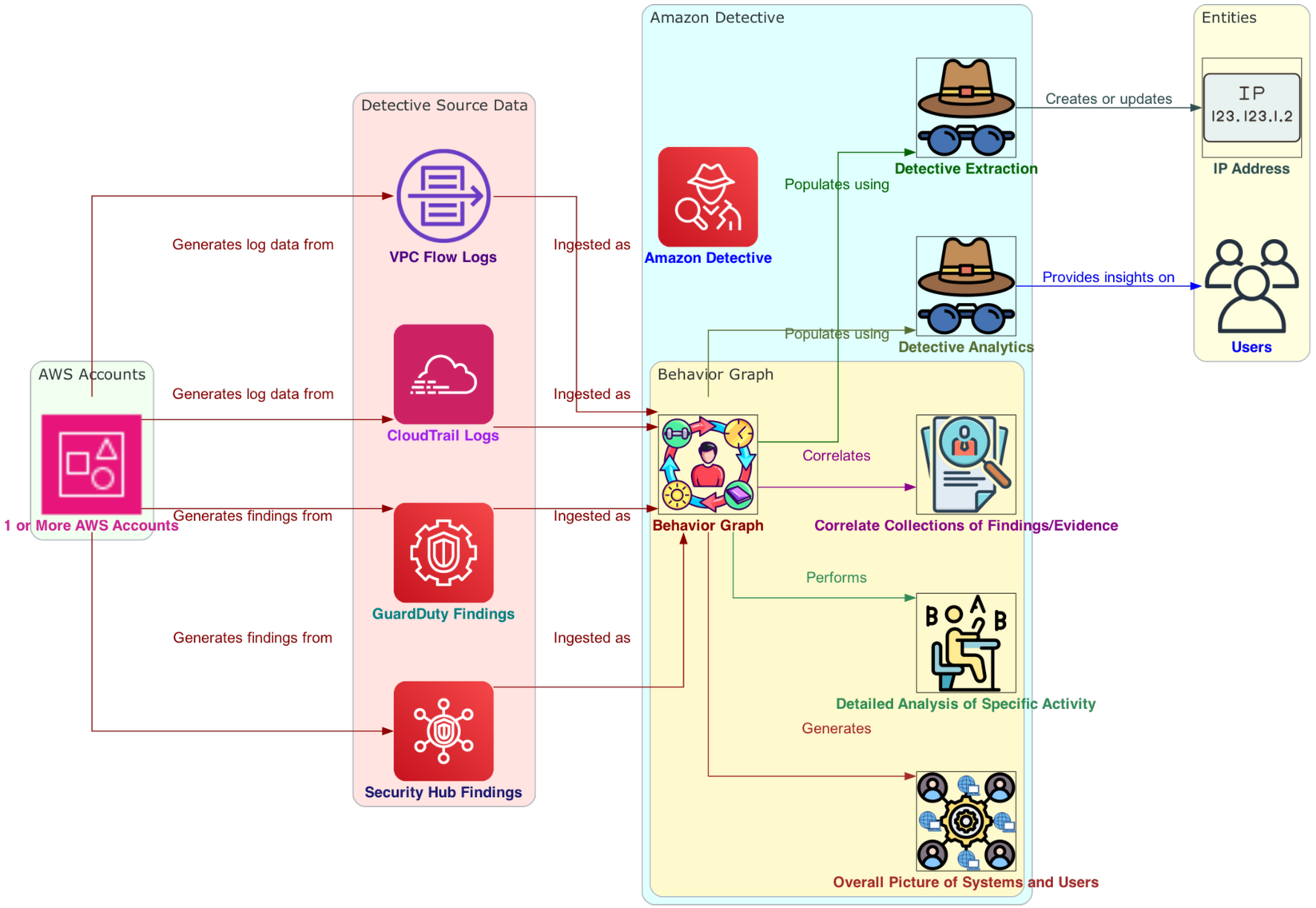
🔗 Detective integrations with GuardDuty, Security Hub

➡️ Pivot directly to Detective console

6. 🎯 Investigations focus on activity connected to AWS resources

🔍 Focuses on activity related to involved resources

Typical Workflow



1. 🕵️ Investigations use data from Detective behavior graph

🔍 Conduct investigations using behavior graph data

2. 🕸️ Behavior graph: linked data from 1+ AWS accounts

🔗 Generated from ingested Detective source data

3. 📩 Source data: VPC & CloudTrail logs, GuardDuty & Security Hub findings

☁️ Amazon VPC and AWS CloudTrail logs

🚨 Amazon GuardDuty and AWS Security Hub findings

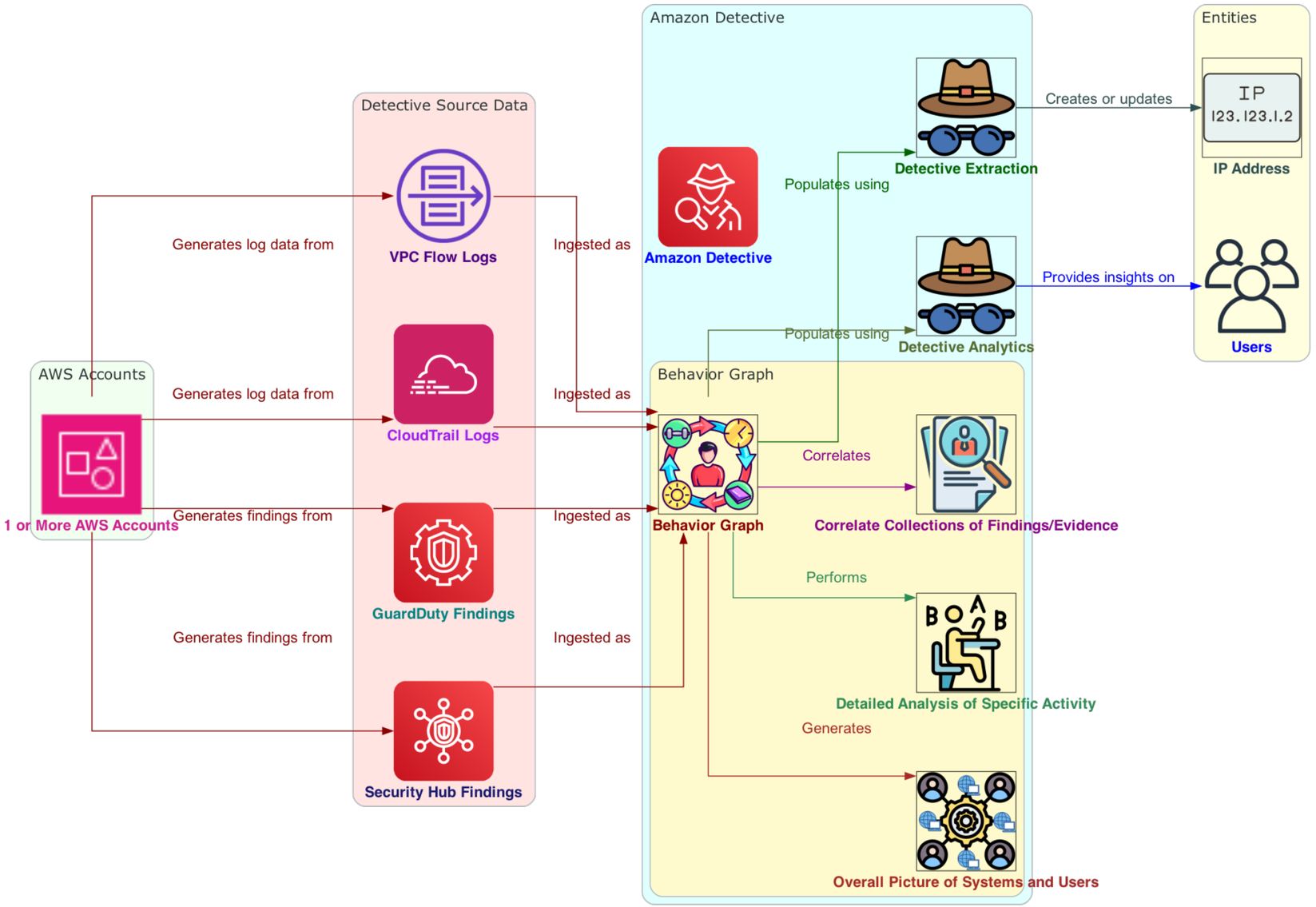
4. 🌐 Generates overall picture of systems, users, interactions

🕰️ Shows interactions over time

5. 🔎 Performs detailed analysis of specific activity

❓ Helps answer investigation questions

Typical Workflow



6. 🔗 Correlates findings, entities, evidence related to events/issues

🧩 Within context of each individual behavior graph

7. 🧩 Extraction and analytics populate behavior graph with new data

🆕 As new data comes in

8. 🗺️ Extraction based on mapping rules to update graph data

🔪 "Whenever you see this data, use it this way"

💻 Example: IP address in source data record

9. 🧠 Analytics provide insights into entity-associated activity

🔢 Complex algorithms analyze data

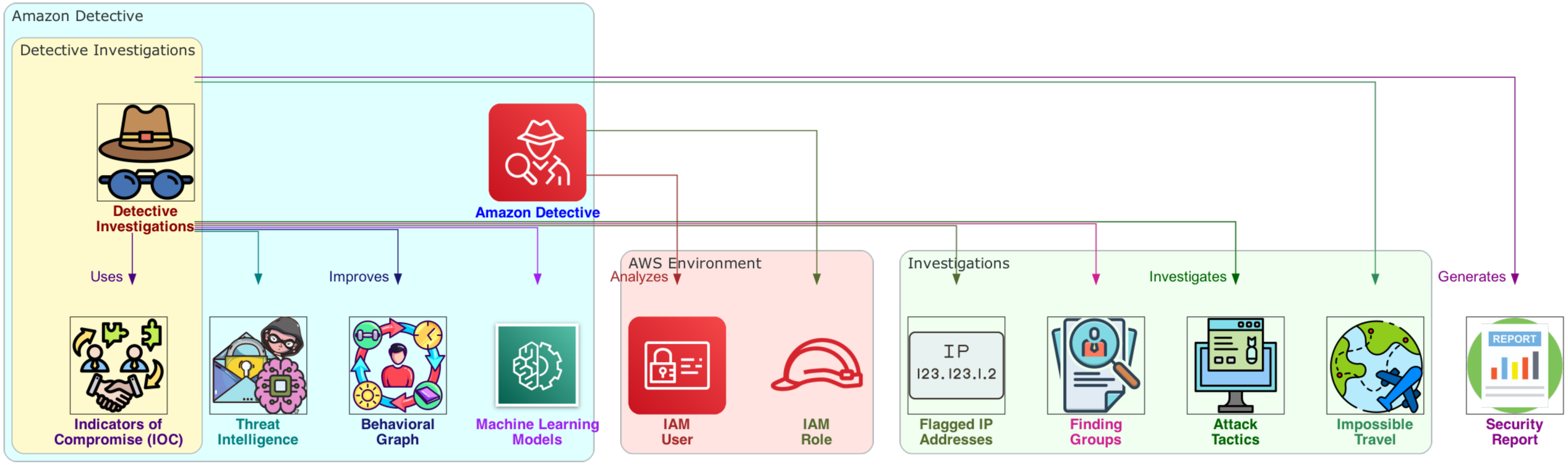
🔍 Example: Analyzes frequency of activity

📞 Looks for unusual API calls, spikes in call volume

❓ Provides answers to key analyst questions

📊 Populates finding and entity profile panels

🕵️‍♀️ Amazon Detective Investigations



1. 🔍 Investigates IAM users and roles using indicators of compromise (IOC)

🔎 Determines resource involvement in security incidents

2. 🚨 IOC: artifact identifying malicious activity or security incidents

🕵️ Observed in network, system, environment

🔍 High confidence identification

3. ⚡ Maximizes efficiency, focuses on threats, strengthens incident response

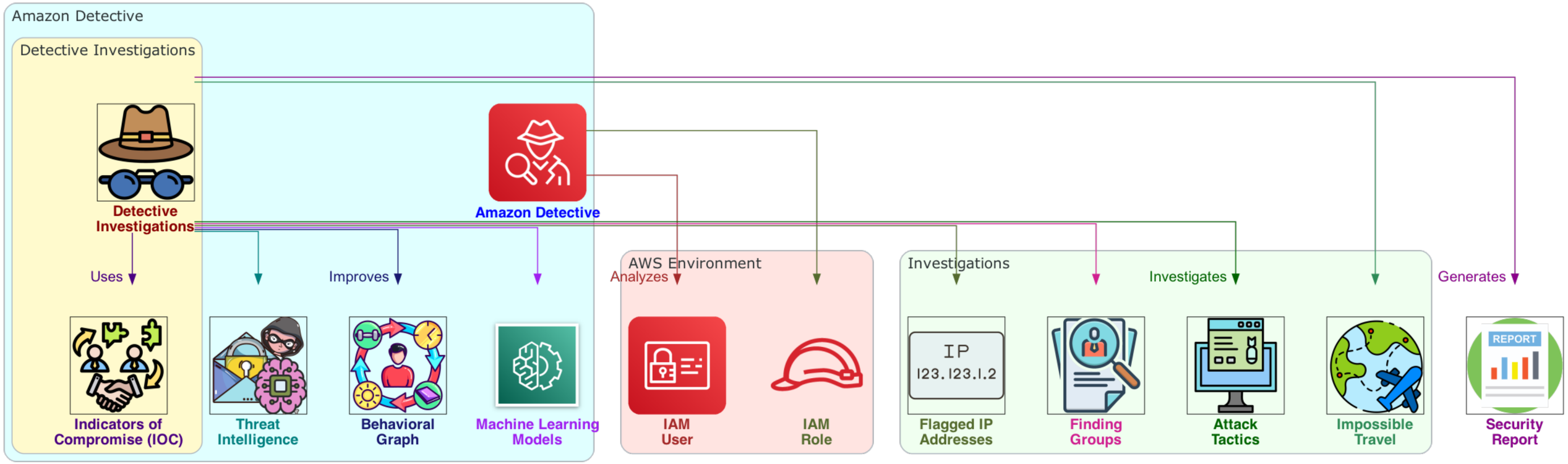
🎯 Improves incident response capabilities

4. 🧠 Uses machine learning models and threat intelligence

🔍 Automatically analyzes AWS resources

🚨 Identifies potential security incidents

🕵️ Amazon Detective Investigations



5. 🔎 Automatically analyzes AWS resources for potential incidents

⚡ Proactive, effective, efficient automation

🔒 Improves security operations

6. 🕸️ Built on Detective's behavioral graph for proactive automation

⚡ Enables proactive and efficient automation

7. 🎯 Investigates attack tactics, impossible travel, flagged IPs, finding groups

🔍 Multiple investigation areas

8. 📊 Generates report highlighting risks identified by Detective

🔍 Performs initial security investigation steps

🚨 Helps understand and respond to security events

Analyzing Findings in Amazon Detective

1. 🚨 Finding: instance of potentially malicious activity or risk

🔎 Detected malicious activity or risk

2. 🕵️ Finding groups: examine multiple related activities

🔍 Examines activities related to potential security event

3. 🔍 Analyze root cause for high severity GuardDuty findings

🕵️ Using finding groups

4. 🦹 Threat actors perform sequence of actions across time and entities

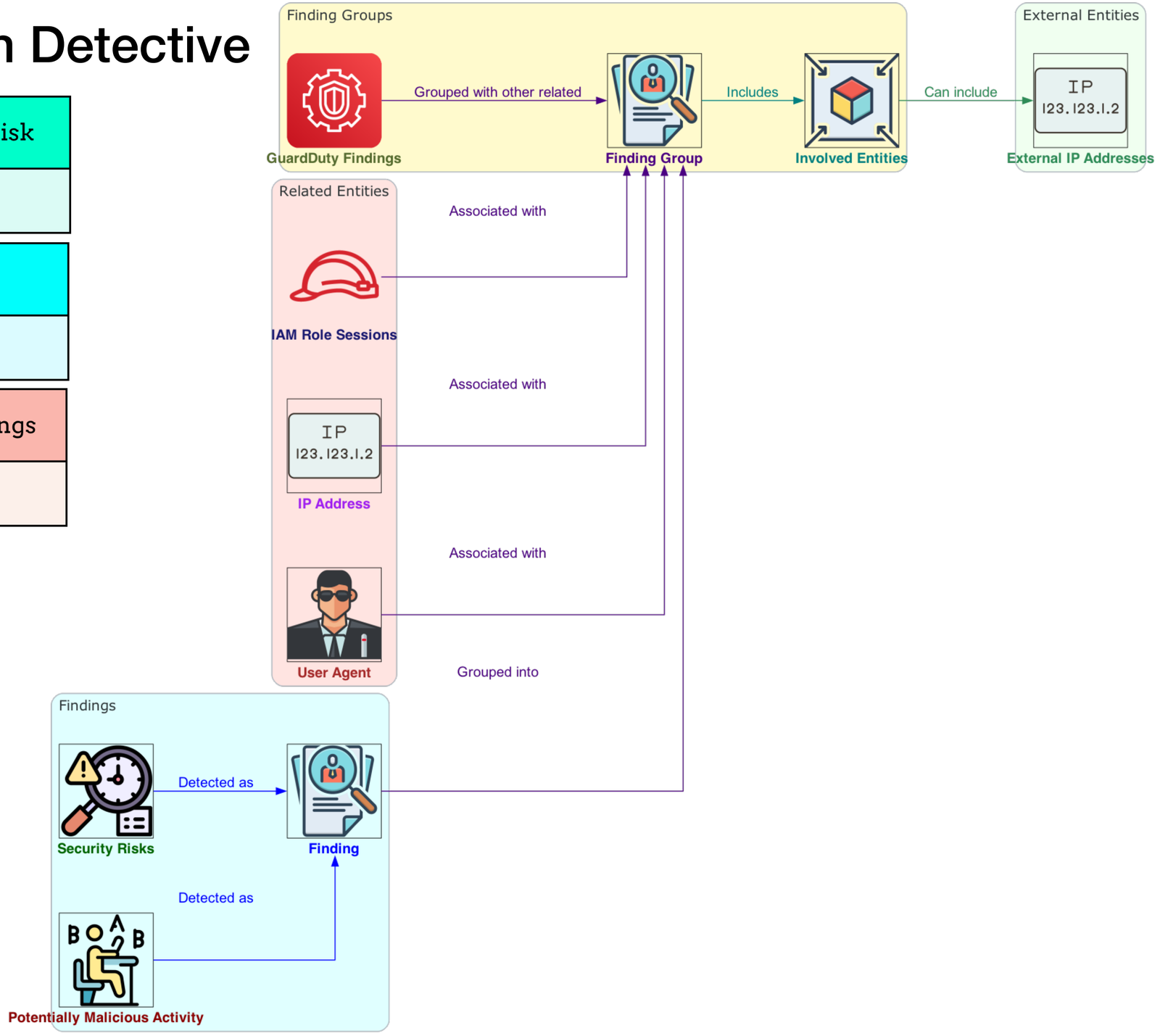
🚨 Leads to multiple security findings, unusual behaviors

⏳ Actions spread across time and entities

5. 🧩 Investigating findings in isolation can lead to misinterpretation

❓ Misinterpretation of significance

🔍 Difficulty finding root cause



Analyzing Findings in Amazon Detective

1. 🔗 Infers relationships between findings and entities

👥 Groups them together

2. 👥 Groups related findings and entities together

🕸️ Using graph analysis technique

3. 🏁 Recommended starting point for investigations

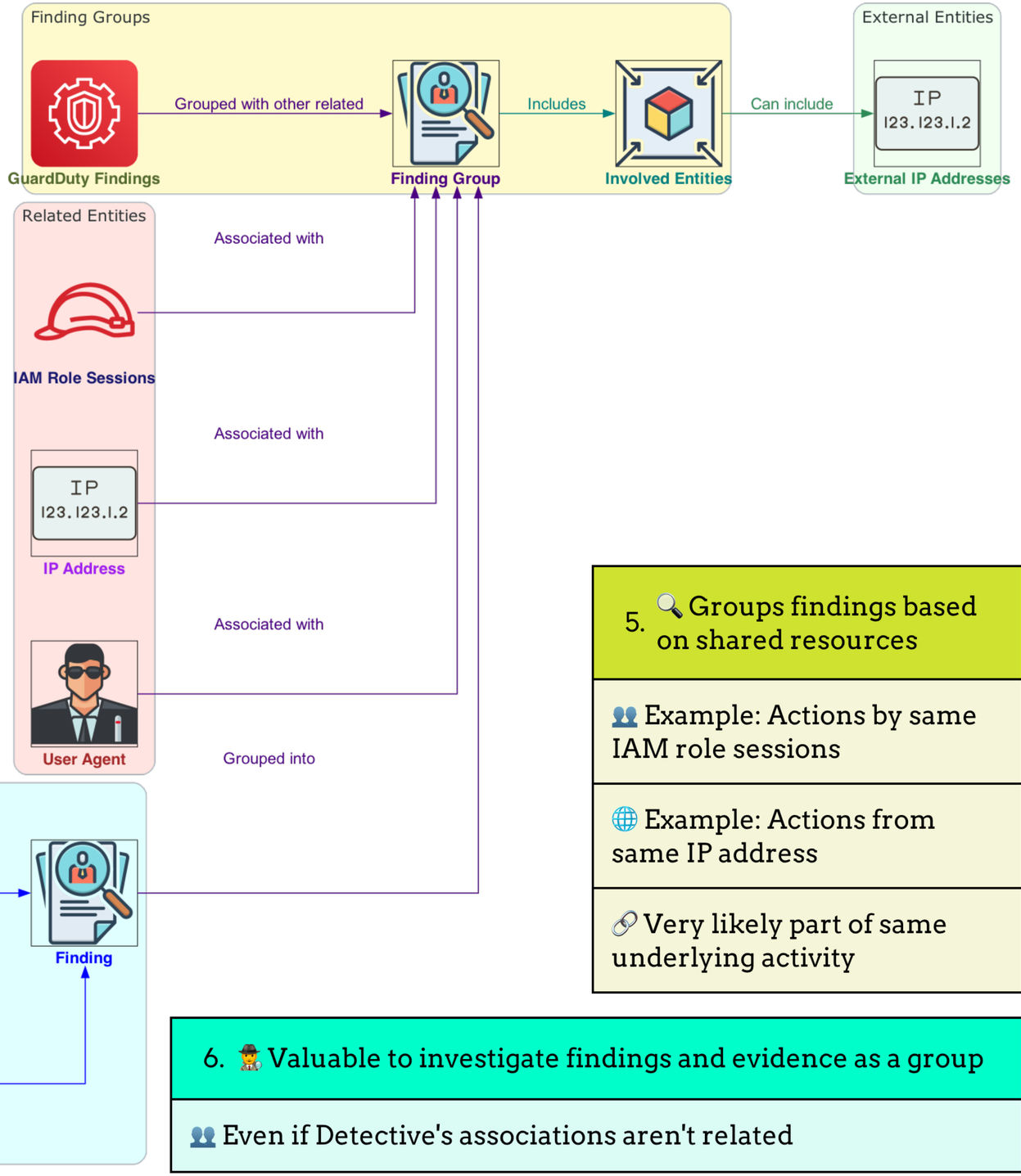
🕵️ Treat finding groups as starting point

🔍 For investigating entities and findings

4. 🗃️ Analyzes data from findings

🔗 Groups related findings

🔍 Based on shared resources



5. 🔍 Groups findings based on shared resources

👥 Example: Actions by same IAM role sessions

🌐 Example: Actions from same IP address

🔗 Very likely part of same underlying activity

6. 🕵️ Valuable to investigate findings and evidence as a group

👥 Even if Detective's associations aren't related

Finding Group Components

1. 🔍 Each group includes entities involved in the findings

➕ In addition to findings

2. 💻 Entities can include AWS resources

🔍 Involved in the findings

3. 🌐 Entities can include resources outside of AWS

🌍 Example: IP Addresses

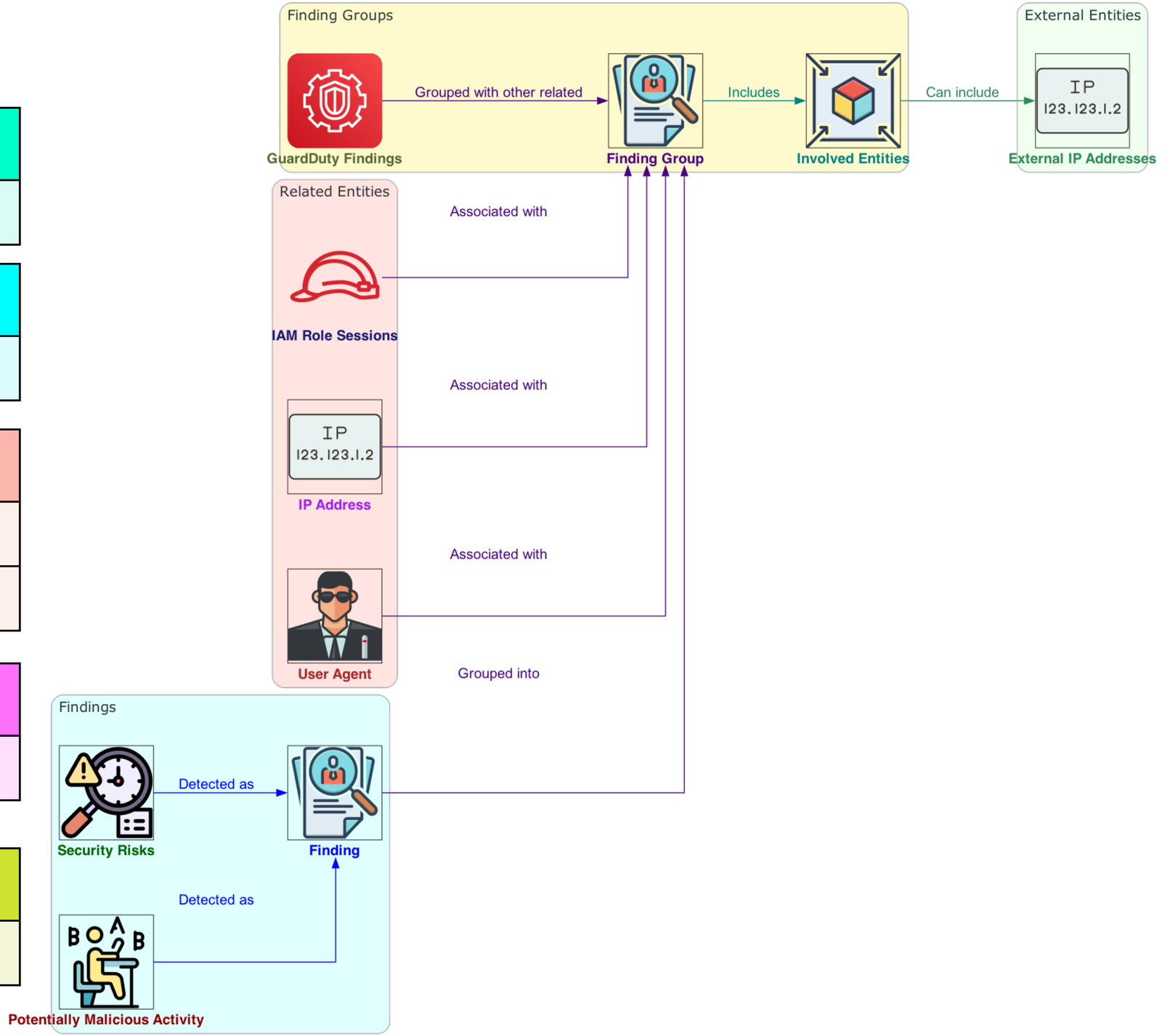
👤 Example: User Agents

4. 🌍 Examples: IP Addresses

🌐 May be outside of AWS

5. 👤 Examples: User Agents

🌐 May also be outside of AWS



Thanks for Watching