Service Name

Amazon Detective

Service Overview

Amazon Detective is a security investigation service that helps users analyze and identify the root cause of security findings or suspicious activities in their AWS environment. It automatically collects log data from various AWS resources including Amazon VPC Flow Logs, AWS CloudTrail logs, and Amazon EKS audit logs, then uses machine learning, statistical analysis, and graph theory to generate visualizations for faster and more efficient security investigations. Detective constructs a behavior graph that creates a unified view of resource behaviors and entity relationships, enabling security analysts to conduct thorough investigations with contextual insights and interactive visualizations powered by generative AI.

Key Use Cases

- Security incident investigation: Analyzing GuardDuty findings and Security Hub alerts to determine root cause and scope of security events
- Threat hunting: Proactively searching for indicators of compromise and suspicious activities across AWS environments
- Malware analysis: Investigating EC2 instances for potential malware compromises and understanding attack chains
- Compliance reporting: Supporting security compliance requirements through detailed investigation capabilities and audit trails
- Multi-account security monitoring: Centralizing security investigations across multiple AWS accounts through behavior graphs

Features

- **Behavior Graph Construction**: Creates linked datasets from log data using machine learning and graph theory to visualize entity relationships and behaviors
- **Detective Investigations**: Automated investigations using machine learning models and threat intelligence to analyze IAM users and roles for indicators of compromise
- **Finding Groups**: Consolidates related security findings and events into single navigable timelines for holistic incident analysis
- **Interactive Visualizations**: Provides guided visualizations and generative AI insights to help analysts understand attack patterns and investigate security events
- **Multi-Account Management**: Supports administrator and member account structures with AWS Organizations integration for centralized security monitoring

- **Security Lake Integration**: Enables querying and retrieval of raw log data through Amazon Security Lake integration

Value Proposition

Amazon Detective provides unique value through its automated behavior graph construction that creates a unified view of security events across AWS environments, eliminating the need for manual log correlation. The service significantly reduces investigation time by using machine learning to surface critical insights and providing guided visualizations that help analysts quickly understand attack chains:

- Detective's integration with GuardDuty, Security Hub, and Security Lake creates a seamless security workflow, while its automated investigations capability performs initial security analysis automatically
- The service requires no upfront data source integration or complex configurations, making it simple to deploy while providing enterprise-scale multi-account support through AWS Organizations integration

Service Integration

Amazon Detective deeply integrates with core AWS security services to provide comprehensive investigation capabilities. It automatically ingests findings from Amazon GuardDuty and AWS Security Hub, creating seamless investigation workflows from detection to analysis:

- Detective integrates with Amazon Security Lake for advanced querying and raw log data retrieval, while supporting AWS Organizations for multi-account security management
- The service collects data from AWS CloudTrail, Amazon VPC Flow Logs, and Amazon EKS audit logs automatically
- Additional integrations include AWS Identity and Access Management for access control, Amazon EventBridge for automation workflows, and AWS Lambda for custom investigation logic
- Detective also supports integration with third-party security tools through its APIs

Onboarding and Offboarding

Customers can get started with Amazon Detective through the AWS Management Console, AWS CLI, or Detective API by simply enabling the service in their desired AWS Region. Upon enabling, Detective automatically creates a Region-specific behavior graph with the account as administrator and begins a 30-day free trial:

- Data ingestion starts immediately from CloudTrail and VPC Flow Logs, with visualizations typically available within 2 hours

- Administrator accounts can invite member accounts to contribute data to the behavior graph for multi-account investigations
- The service requires minimal configuration as it automatically discovers and ingests relevant log data sources
- Detective works best when integrated with GuardDuty and Security Hub for comprehensive security coverage

Getting Started Guide:
https://docs.aws.amazon.com/detective/latest/userguide/detective-setup.html

Data Removal

When disabling Amazon Detective, the behavior graph and all associated data are permanently and irreversibly deleted. Customers can disable Detective through the console, Detective API, or AWS CLI. For administrator accounts, disabling Detective removes the entire behavior graph including all member account data. Member accounts can be individually removed using the DeleteMembers operation, which stops data ingestion from those accounts while preserving existing data in the behavior graph. AWS provides Python scripts for bulk account management across multiple regions during offboarding.

Backup/Restore and Disaster Recovery

Amazon Detective does not provide traditional backup and disaster recovery capabilities as it is an analytical service that processes and visualizes log data rather than storing critical business data. Detective maintains up to one year of aggregated data for analysis purposes, but this data cannot be backed up or restored by customers. The service operates as a managed service where AWS handles the underlying infrastructure resilience and data durability within each region.

Backup Capabilities

Amazon Detective does not have backup capabilities and does not integrate with AWS Backup service. The service is designed as an analytical tool that processes log data to create behavior graphs and investigations, rather than storing data that requires backup protection. Detective automatically maintains historical data for analysis purposes but does not provide customer-controlled backup or restore functionality.

Disaster Recovery

Amazon Detective does not support disaster recovery in the traditional sense and does not integrate with AWS Elastic Disaster Recovery. As a regional service, Detective operates independently in each AWS Region where it is enabled:

- Customers must enable Detective separately in each region where they require security investigation capabilities

- The service itself does not require disaster recovery planning as it is an analytical service

Recovery Objectives

Amazon Detective does not directly help customers meet RPO and RTO objectives as it is not a data protection or disaster recovery service. Detective serves as a security investigation tool that analyzes existing log data to help understand security incidents. The service can assist in post-incident analysis and forensics to understand the timeline and impact of security events, but does not provide backup or recovery capabilities.

Service Constraints

Service Quotas: https://docs.aws.amazon.com/detective/latest/userguide/regions-limitations.html

FAQ: https://aws.amazon.com/detective/faqs/

Technical Requirements

Service Documentation: https://docs.aws.amazon.com/detective/latest/userguide/index.html

User Guide: https://docs.aws.amazon.com/detective/latest/userguide/index.html

API Reference: https://docs.aws.amazon.com/detective/latest/APIReference/Welcome.html

Pricing Overview

Please see the AWS UK G Cloud 15 Pricing Document accompanying this service in the Digital Marketplace.

Public Pricing: https://aws.amazon.com/detective/pricing/

Cost Optimization

Amazon Detective offers several cost optimization options including a 30-day free trial for new behavior graphs and tiered pricing that reduces costs as data volume increases. The first 1,000 GB costs $2.00 per GB, decreasing to $0.25 per GB for volumes over 10,000 GB monthly:

- Customers can optimize costs by carefully selecting which accounts contribute to behavior graphs and monitoring data volume through the Usage page
- The service automatically aggregates and processes data to reduce storage requirements compared to raw log retention
- Customers can also disable Detective in regions where it’s not needed and use selective member account management to control data ingestion volumes

Savings Considerations

Main cost savings with Amazon Detective come from eliminating the need for separate log analysis infrastructure and reducing investigation time through automated analysis. The service's tiered pricing model provides significant per-GB cost reductions for high-volume customers, with costs dropping by 87.5% from the lowest to highest tier:

- Detective's automated investigations and finding groups reduce the time security analysts spend on manual investigation tasks, leading to operational cost savings
- The service's integration with existing AWS security services eliminates the need for additional third-party security tools
- Organizations can achieve savings through centralized multi-account management, avoiding duplicate investigation infrastructure across business units while maintaining comprehensive security visibility