

Hands-on tutorials

AWS Security Platform as a Service (PaaS) - Multi-Cloud Security Operations Console



AWS Security Platform as a Service (PaaS) - Multi-Cloud Security Operations Console: Hands-on tutorials

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon's trademarks and trade dress may not be used in connection with any product or service that is not Amazon's, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Amazon. All other trademarks not owned by Amazon are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Amazon.

Table of Contents

AWS Security Platform as a Service - Multi-cloud security operations console	i
Overview	1
What you will accomplish	1
Prerequisites	2
Architecture	3
AWS CDK and multi-cloud integration	4
Cloud Security Posture Management with multi-cloud integration	4
Built-in multi-cloud integration connectors	6
Unified CSPM console features	7
Security Information and Event Management with multi-cloud integration	7
Built-in multi-cloud log integration connectors	9
Unified SIEM console features	10
Advanced SIEM capabilities	10
Cloud Workload Protection Platform with multi-cloud integration	11
Multi-cloud workload protection components	13
Built-in multi-cloud workload connectors	14
Unified CWPP console features	15
Advanced CWPP capabilities	16
Implementation	18
Tasks	18
Supporting documentation URLs	20
AWS security platform documentation	20
Multi-cloud integration documentation	20
Implementation guides	20
Conclusion	21

AWS Security Platform as a Service - Multi-cloud security operations console

AWS experience	Intermediate
Time to complete	2 hours
Cost to complete	See services for specific pricing details.
Services used	Amazon OpenSearch Service , Amazon Security Lake , Amazon GuardDuty , Amazon Inspector , AWS Systems Manager , and AWS Security Hub CSPM
Last updated	January 12, 2026

Overview

This tutorial shows you how to implement a complete AWS Security Platform as a Service (PaaS) that provides a unified security operations console. You'll learn to integrate Cloud Security Posture Management (CSPM), Security Information and Event Management (SIEM), and Cloud Workload Protection Platform (CWPP) capabilities through a single interface with multi-cloud support.

This tutorial focuses on [Microsoft Azure](#) and [Google Cloud Platform](#) integration, but you can apply the same approach to any cloud provider or on-premises.

What you will accomplish

- Monitor security across multiple cloud providers from a single console
- Detect threats and vulnerabilities in real time
- Maintain compliance posture across your multi-cloud infrastructure
- Respond to security incidents efficiently with centralized analytics

Prerequisites

For this tutorial, you'll need:

- An AWS account with administrator-level access: If you don't already have one, follow the [Setting Up Your AWS Environment](#) getting started guide for a quick overview
- Active subscriptions to Microsoft Azure and Google Cloud Platform
- [AWS CLI](#) installed
 - See [Installing or updating the latest version of the AWS CLI](#)
- Node.js: Version 18.x or later
 - Download from [nodejs.org](#)
- AWS CDK: Installed globally
 - Installation command: `npm install -g aws-cdk`
- Security Lake: Preconfigured Amazon Security Lake instance with an Amazon S3 bucket
 - See [Getting started with Amazon Security Lake](#)
- AWS Lake Formation: Admin role configured for Security Lake operations
- AWS Identity and Access Management (IAM) permissions: Sufficient permissions to create Lambda functions, SQS queues, KMS keys, and IAM roles

Azure integration requirements:

- Azure Event Hub namespace and connection strings
- Microsoft Defender for Cloud continuous export configured
- Service principal with appropriate permissions

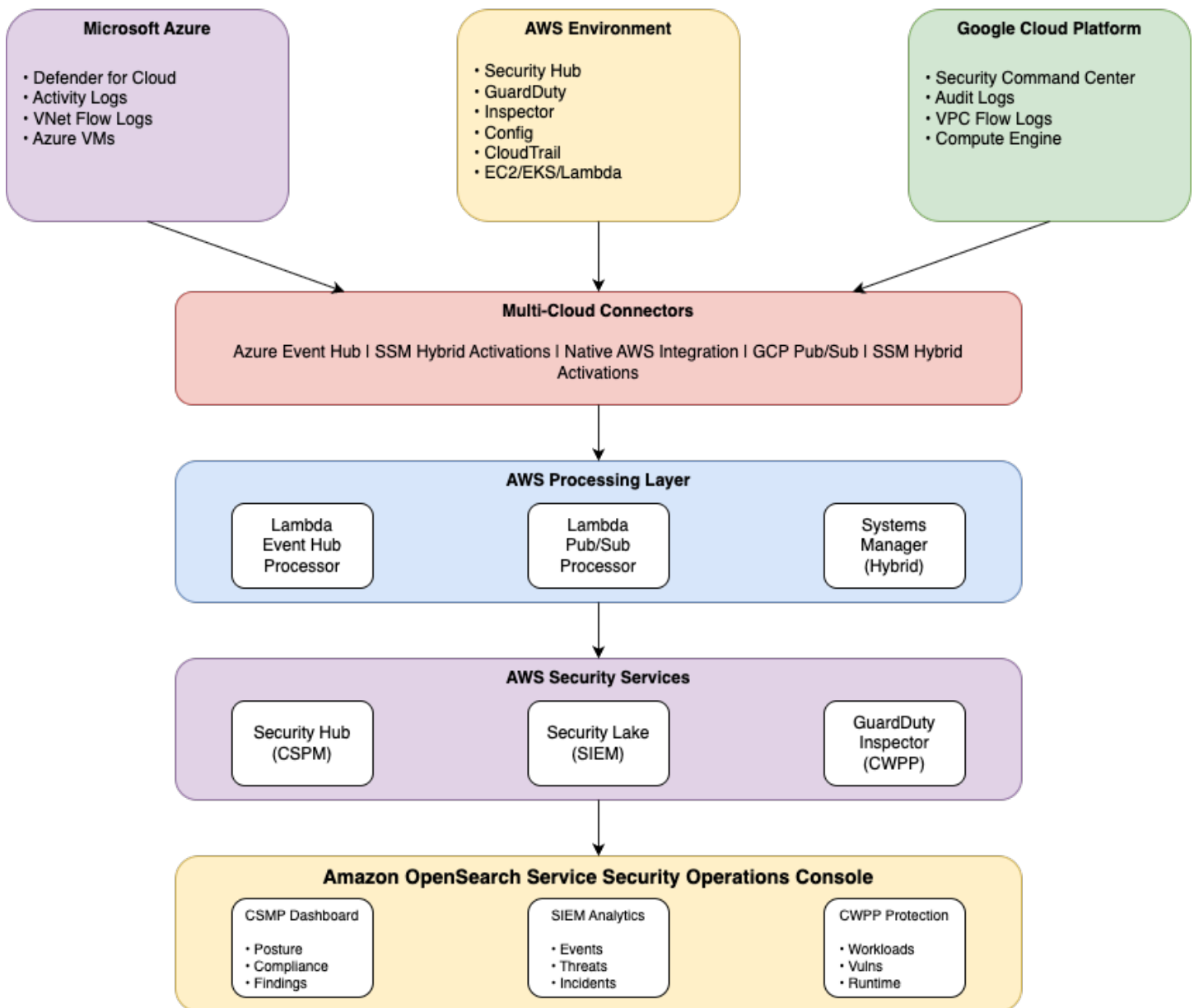
Google Cloud integration requirements:

- Google Cloud Pub/Sub subscription configured
- Service account credentials with Security Command Center permissions
- Organization-level or project-level access

Architecture

You get a unified security platform through Amazon OpenSearch Service as your central security operations console. This integrates with native AWS security services and extends to multi-cloud environments, as shown in the following diagram.

**AWS Security Platform as a Service (PaaS)
Single-Pane-of-Glass Architecture**



AWS CDK and multi-cloud integration

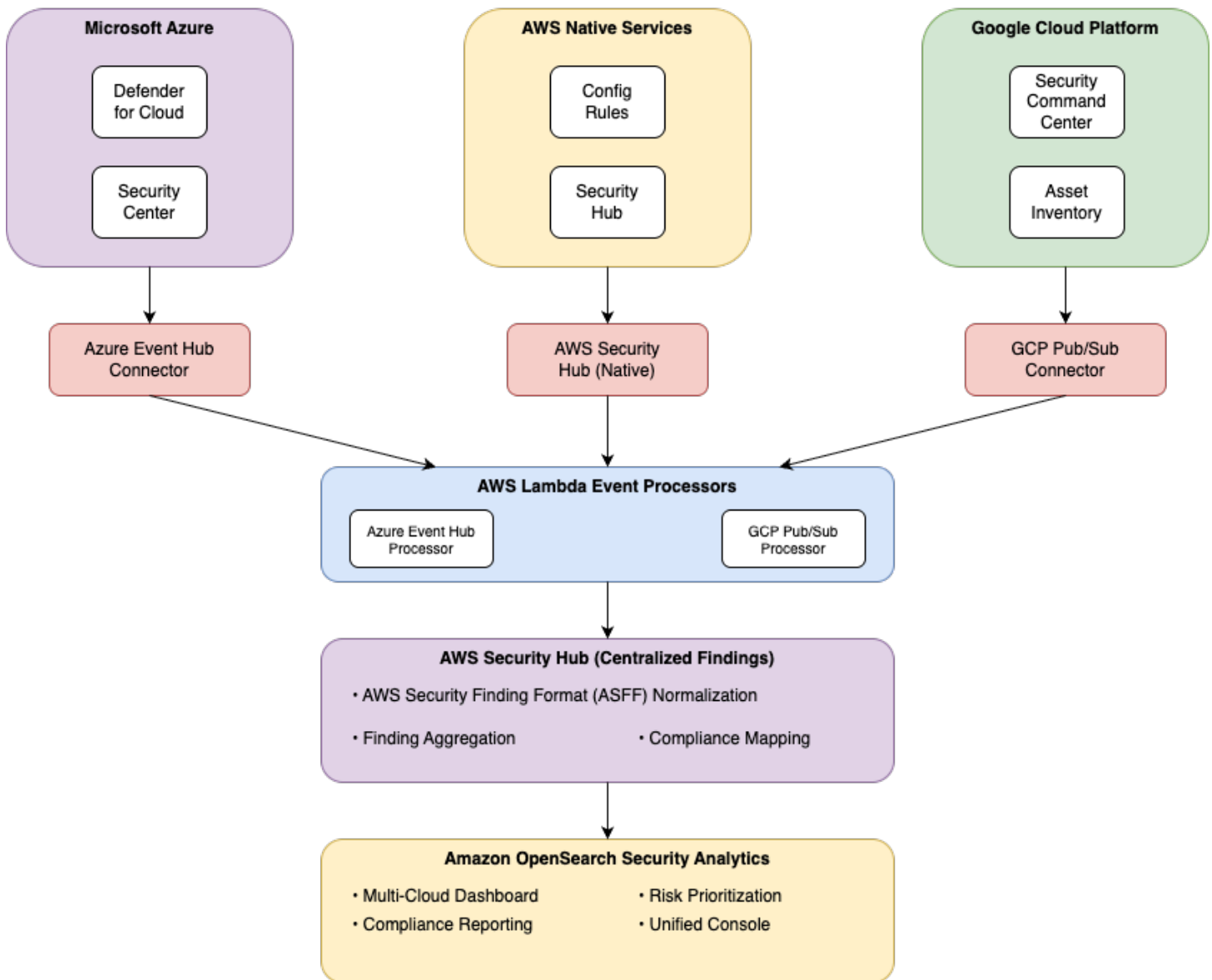
You use the AWS Cloud Development Kit (AWS CDK) to deploy pre-built connectors for the third-party cloud integration. The AWS CDK automatically provisions AWS Lambda functions, Amazon SQS queues, IAM roles, and other required services to establish secure connections with the Microsoft Azure and Google Cloud Platform (GCP).

The modular framework lets you deploy production-ready connectors for Azure Event Hub and Google Cloud Pub/Sub using configuration files. This removes the need for manual infrastructure setup and helps to ensure consistent, secure deployments with built-in monitoring and error handling.

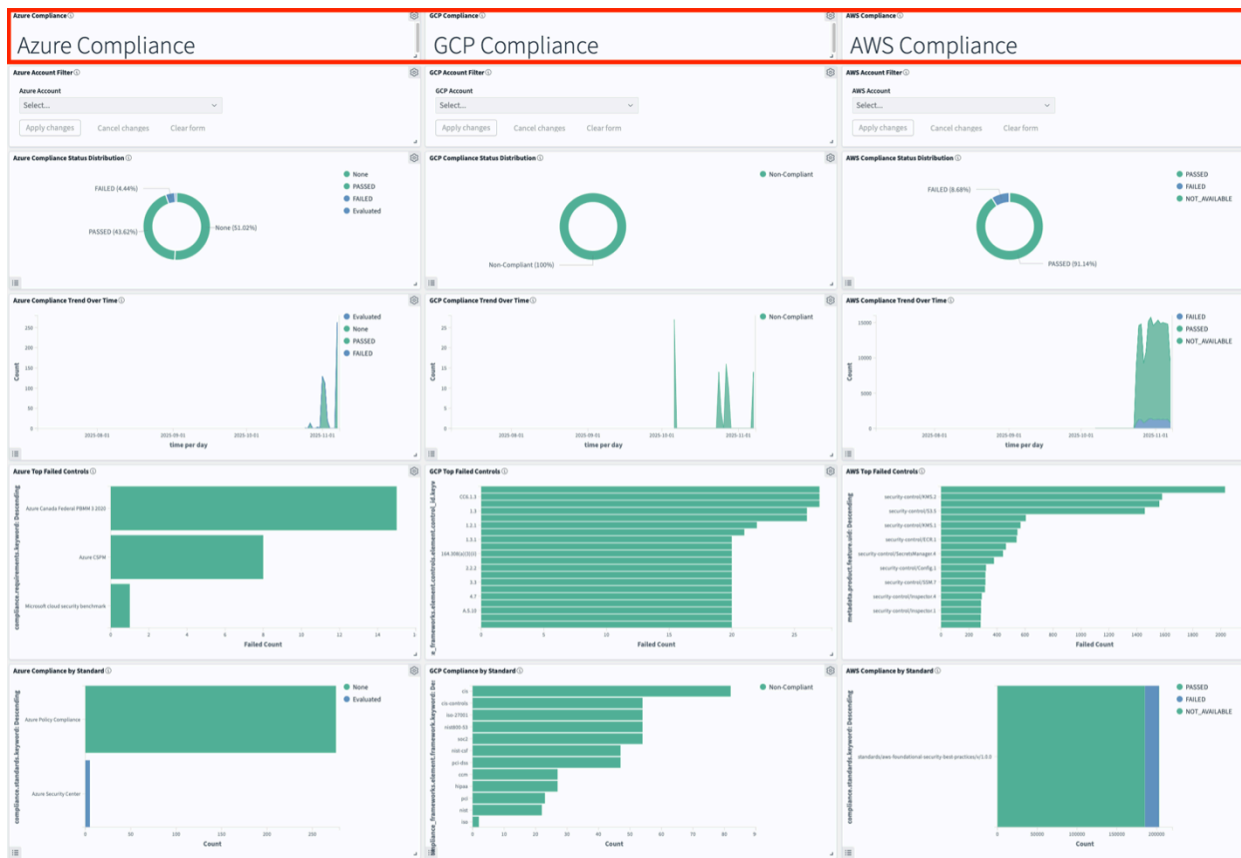
Cloud Security Posture Management with multi-cloud integration

You get comprehensive Cloud Security Posture Management (CSPM) through AWS Security Hub integrated with Amazon OpenSearch Service. This gives you unified security visibility across AWS, Microsoft Azure, and the Google Cloud Platform.

AWS Multi-Cloud CSPM Architecture



Your Amazon OpenSearch Security Analytics dashboard will display a multi-cloud security posture overview with compliance status across AWS, Azure, and GCP environments.



Built-in multi-cloud integration connectors

Microsoft Azure integration

Service: AWS Security Hub CSPM with Azure Security Center Integration

- **Built-in connector:** Native [Azure Event Hub](#) integration through [AWS Lambda](#)
- **Data sources:** [Microsoft Defender for Cloud](#) security findings, compliance assessments, secure score data
- **Implementation:** Automated Azure Event Hub, AWS Lambda, Security Hub CSPM, OpenSearch pipeline
- **Configuration:** Zero-code connector setup through [AWS CDK](#) deployment templates

Configuration reference: See the [Azure CSPM integration settings](#) in the [sample-aws-security-lake-integrations](#) repository on GitHub.

Google Cloud Platform integration

Service: AWS Security Hub CSPM with [Google Security Command Center](#) Integration

- **Built-in connector:** Native [GCP Pub/Sub](#) integration through AWS Lambda
- **Data sources:** Google SCC security findings, vulnerability assessments, compliance findings
- **Implementation:** Automated GCP Pub/Sub, AWS Lambda, Security Hub CSPM, OpenSearch pipeline
- **Configuration:** Zero-code connector setup through AWS CDK deployment templates

Configuration reference: See the [GCP CSPM integration settings](#) in the sample-aws-security-lake-integrations repository on GitHub.

Unified CSPM console features

Amazon OpenSearch Service Security Analytics dashboard provides:

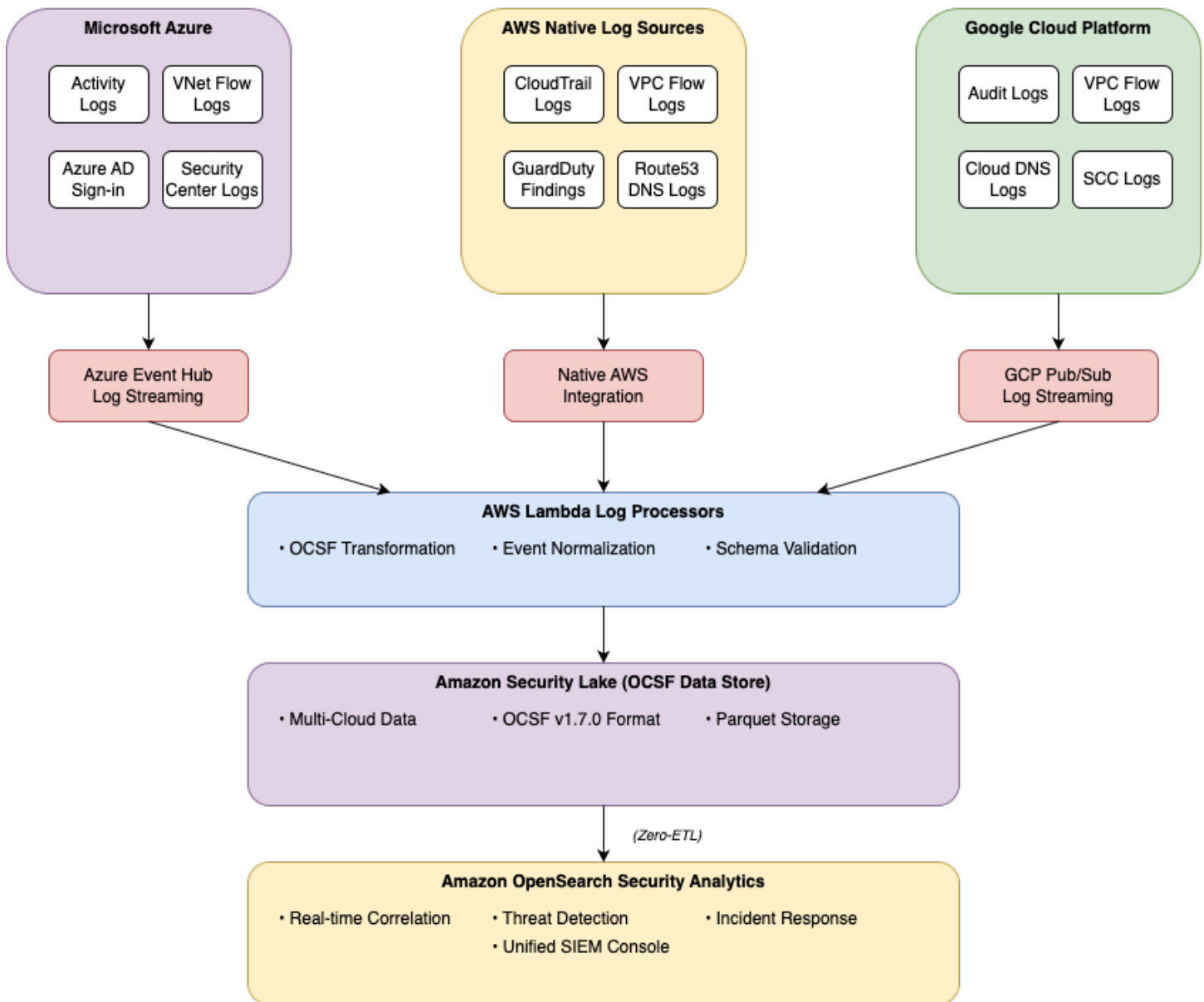
- **Multi-cloud asset inventory:** Unified view of security posture across AWS, Azure, and GCP
- **Compliance dashboards:** Real-time compliance status across multiple frameworks (CIS, NIST, ISO 27001)
- **Security score trending:** Comparative security posture metrics across all cloud environments
- **Risk prioritization:** AI-powered risk scoring based on exploitability and business impact
- **Automated remediation:** Integration with AWS Systems Manager for cross-cloud remediation workflows

Security Information and Event Management with multi-cloud integration

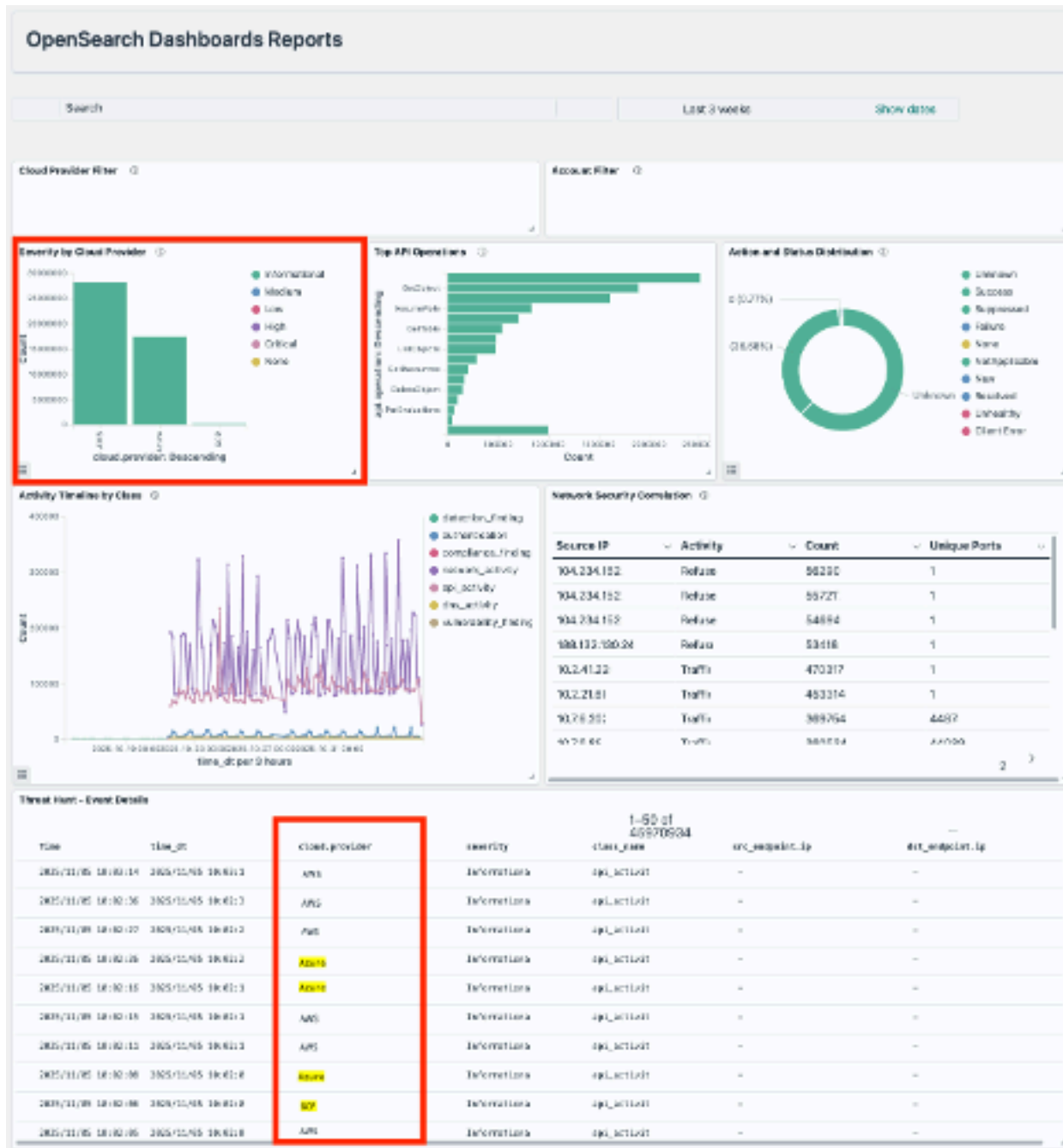
AWS provides enterprise-grade SIEM capabilities through **Amazon OpenSearch Service** with **Security Analytics plugin**, integrated with **Amazon Security Lake** for multi-cloud log ingestion and analysis.

The architecture diagram shows how Amazon Security Lake ingests logs from Azure Event Hub and GCP Pub/Sub through native connectors. AWS Lambda processors transform data to OCSF v1.7.0 format and zero-ETL integration to OpenSearch Security Analytics for unified SIEM capabilities.

AWS Multi-Cloud SIEM Architecture



The Amazon OpenSearch Service Security Analytics timeline view shows correlated security events from AWS, Azure, and GCP with unified event correlation and threat detection.



Built-in multi-cloud log integration connectors

Microsoft Azure log integration

Service: Amazon Security Lake with [Azure Log Analytics](#) Integration

- **Built-in connector:** Native Azure Event Hub log streaming connector

- **Log sources:** [Azure Activity Logs](#), [Azure AD Sign-in Logs](#), Azure Security Center Logs, [VNet Flow Logs](#)
- **Implementation:** Azure Event Hub, AWS Lambda, Amazon Security Lake, OpenSearch zero-ETL integration
- **OCSF compliance:** Automatic normalization to Open Cybersecurity Schema Framework v1.7.0

Configuration reference: See the [Azure SIEM log integration configuration file](#) in the sample-aws-security-lake-integrations repository on GitHub.

Google Cloud Platform log integration

Service: Amazon Security Lake with [GCP Cloud Logging](#) Integration

- **Built-in connector:** Native GCP Pub/Sub log streaming connector
- **Log sources:** [GCP Audit Logs](#), [VPC Flow Logs](#), [Cloud DNS](#) Logs, Security Command Center Logs
- **Implementation:** GCP Pub/Sub, AWS Lambda, Security Lake, OpenSearch zero-ETL integration
- **OCSF compliance:** Automatic normalization to Open Cybersecurity Schema Framework v1.7.0

Configuration reference: See the [GCP SIEM log integration configuration file](#) in the sample-aws-security-lake-integrations repository on GitHub.

Unified SIEM console features

Amazon OpenSearch Service Security Analytics provides:

- **Multi-cloud log correlation:** Unified timeline view of security events across AWS, Azure, and GCP
- **Threat detection rules:** Pre-built detection rules for multi-cloud attack patterns
- **Security incident response:** Automated playbooks triggered by cross-cloud security events
- **Threat hunting:** Interactive queries across normalized multi-cloud security data
- **Real-time alerting:** Integrated notifications for critical security events across all environments

Advanced SIEM capabilities

Amazon GuardDuty integration:

- **Extended threat detection:** AI/ML-powered attack sequence identification across cloud boundaries
- **Malware protection:** Cross-cloud malware detection and response
- **Runtime monitoring:** Container and serverless threat detection across multi-cloud workloads

Cloud Workload Protection Platform with multi-cloud integration

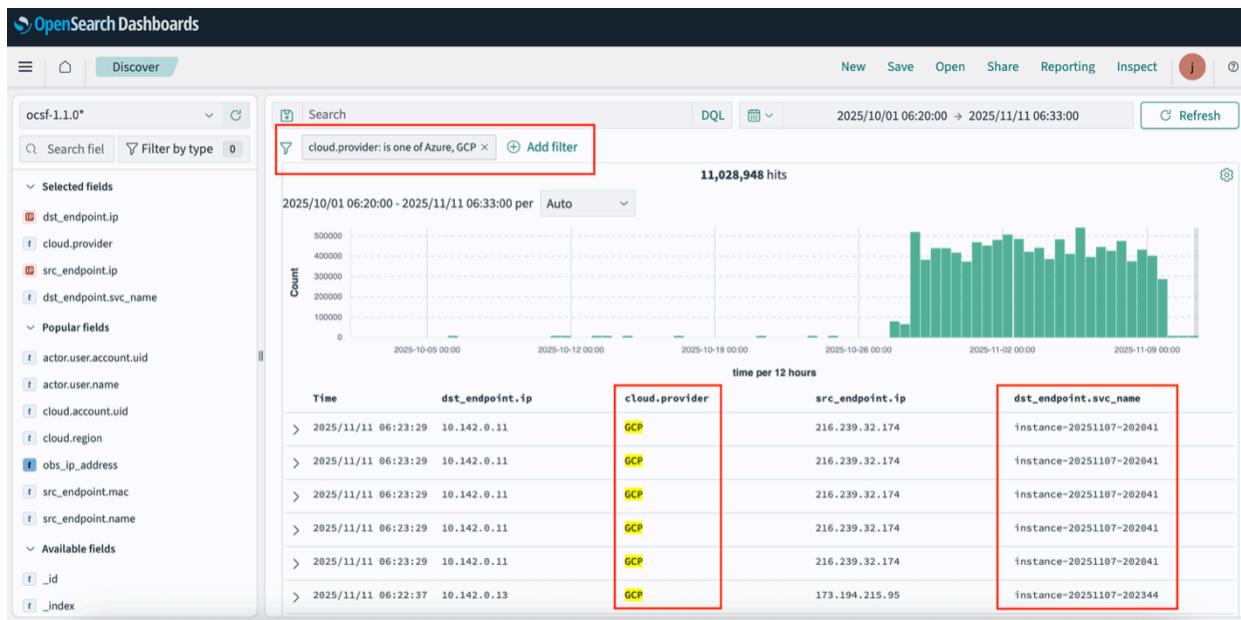
AWS provides comprehensive Cloud Workload Protection Platform (CWPP) capabilities through **Amazon OpenSearch Service** as the central console, integrated with **Amazon GuardDuty**, **Amazon Inspector**, and **AWS Systems Manager** for multi-cloud workload protection.

The architecture diagram shows how AWS Systems Manager hybrid activations enable virtual machine workload protection across Azure virtual machines (VMs) and GCP Compute Engine instances. Systems Manager is integrated with Amazon GuardDuty, Amazon Inspector, and Security Hub for unified threat detection, vulnerability management, and runtime protection in the OpenSearch Security Operations console.

AWS Multi-Cloud CWPP Architecture



AWS multi-cloud virtual machine inventory dashboard shows the real-time protection status of VMs across Amazon EC2, Azure VMs, and GCP Compute Engine instances through Systems Manager.



Multi-cloud workload protection components

Threat detection across multi-cloud workloads

Amazon GuardDuty provides:

- **Cross-cloud threat correlation:** AI/ML analysis of security signals across AWS, Azure, and GCP workloads
- **Container security:** Runtime threat detection for containers across all cloud environments
- **Serverless protection:** Lambda and Azure Functions security monitoring
- **Network threat detection:** [VPC Flow Log](#) analysis extended to [Azure VNet](#) and [GCP VPC](#) networks

Vulnerability management across multi-cloud workloads

Amazon Inspector integrated with AWS Systems Manager provides:

- **Multi-cloud VM scanning:** Vulnerability assessment of [Amazon EC2](#), [Azure VMs](#), and [GCP Compute instances](#) through Systems Manager Agent (SSM Agent)
- **Container image scanning:** [ECR](#) vulnerability detection (native AWS capability)
- **AWS serverless vulnerability management:** Lambda function security assessment (native AWS capability)

- **Risk-based prioritization:** Contextualized vulnerability scoring across managed workloads
- **Multi-cloud scope:** Direct vulnerability scanning limited to virtual machines with SSM Agent (container and serverless scanning requires cloud-native tools)

Runtime protection across multi-cloud workloads

AWS Systems Manager provides:

- **Hybrid activations:** Direct management of Azure VMs and GCP Compute Engine instances
- **Cross-cloud patch management:** Unified patching across Amazon EC2, Azure VMs, and GCP Compute instances
- **Compliance monitoring:** Security baseline enforcement across virtual machine workloads in all cloud environments
- **Automated response:** Remediation workflows triggered by security events across managed instances
- **Scope:** Limited to virtual machines and compute instances (containers and serverless functions require complementary security approaches)

Built-in multi-cloud workload connectors

Microsoft Azure workload integration

Service: AWS Systems Manager hybrid activations and Amazon Inspector

- **Built-in connector:** Native SSM Agent deployment on Azure virtual machines
- **Workload types:** Azure virtual machines (Windows and Linux)
- **Protection capabilities:**
 - Vulnerability scanning through Inspector (for VMs with SSM Agent)
 - Runtime protection through Systems Manager (patch management, compliance monitoring)
 - Threat detection through GuardDuty correlation (network-level analysis)
- **Implementation:** Automated SSM Agent installation and registration on Azure VMs
- **Limitations:** SSM Agent supports virtual machines only (containers and serverless functions require alternative monitoring approaches)

Implementation reference: See the [Azure workload integration setup](#) in the sample-aws-security-lake-integrations repository on GitHub.

Google Cloud Platform workload integration

Service: AWS Systems Manager hybrid activations and Amazon Inspector

- **Built-in connector:** Native SSM Agent deployment on GCP Compute Engine instances
- **Workload types:** GCP Compute Engine (Windows and Linux virtual machines)
- **Protection capabilities:**
 - Vulnerability scanning through Inspector (for VMs with SSM Agent)
 - Runtime protection through Systems Manager (patch management, compliance monitoring)
 - Threat detection through GuardDuty correlation (network-level analysis)
- **Implementation:** Automated SSM Agent installation and registration on GCP Compute instances
- **Limitations:** SSM Agent supports virtual machines only (GKE containers and Cloud Functions require alternative monitoring approaches)

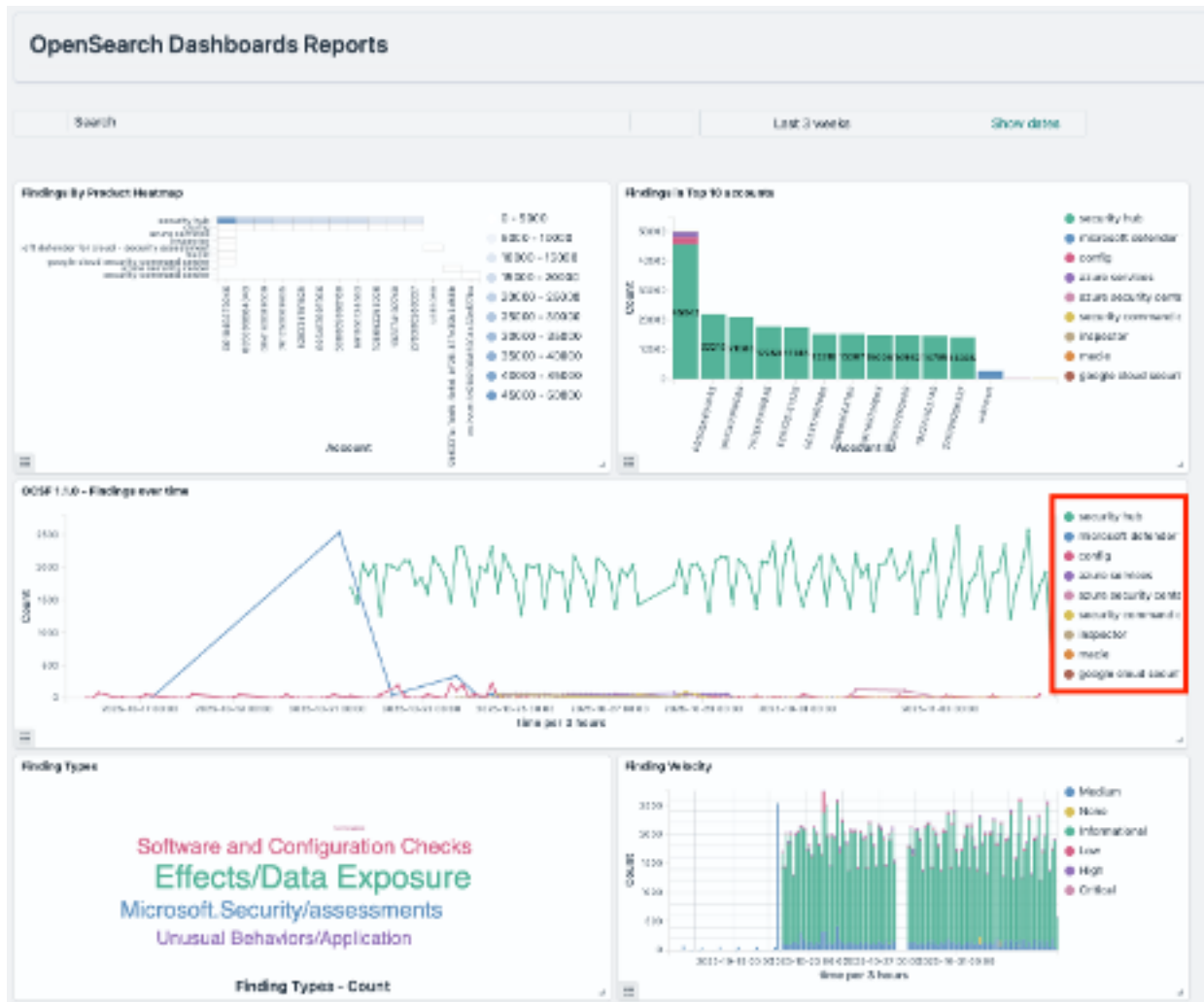
Implementation reference: See the [GCP workload integration setup](#) in the sample-aws-security-lake-integrations repository on GitHub.

Unified CWPP console features

Amazon OpenSearch Service Security Operations Console provides:

- **Multi-cloud workload inventory:** Real-time visibility of all workloads across AWS, Azure, and GCP
- **Threat detection dashboard:** Unified view of security threats across all cloud workloads
- **Vulnerability management console:** Centralized vulnerability assessment and remediation tracking
- **Runtime protection status:** Real-time monitoring of security controls across all environments
- **Automated response workflows:** Cross-cloud incident response and remediation automation

This AWS unified threat detection dashboard displays active security alerts and incidents across all connected cloud environments.



Advanced CWPP capabilities

Container and serverless protection:

- **Amazon GuardDuty with Amazon EKS runtime monitoring:** Kubernetes security for [Amazon EKS](#) (native AWS capability)

Lambda runtime protection: Serverless security monitoring for AWS Lambda functions (native AWS capability)

- **Container image vulnerability scanning:** Amazon ECR container image scanning (native AWS capability)
- **Multi-cloud container security:** Azure AKS, GCP GKE, Azure Functions, and GCP Cloud Functions require cloud-native security tools and integration through SIEM data ingestion

Compliance and governance:

- **Multi-cloud compliance monitoring:** Unified compliance dashboard across all cloud environments
- **Security baseline enforcement:** Automated security configuration management across clouds
- **Audit and reporting:** Comprehensive security reporting across all connected workloads

Implementation

To implement an AWS Security Platform as a Service (PaaS) that provides a unified security operations console, complete the following tasks.

Tasks

Task 1: Deploy the core AWS security platform

Deploy the Security Lake integration framework:

- **Primary configuration:** See the [config.example.yaml](#) file in the sample-aws-security-lake-integrations repository on GitHub.
- **Deployment scripts:** See the [deployment scripts](#) in the sample-aws-security-lake-integrations repository on GitHub.

Task 2: Configure multi-cloud integrations

Configure Azure Integration using deployment templates:

- **Azure infrastructure:** See the [deployment templates](#) in the sample-aws-security-lake-integrations repository on GitHub.
- **Azure configuration:** See the [terraform.tfvars](#) file in the sample-aws-security-lake-integrations repository on GitHub.

Configure GCP Integration using deployment templates located at:

- **GCP infrastructure:** See the [deployment templates](#) in the sample-aws-security-lake-integrations repository on GitHub.
- **GCP configuration:** See the [terraform.tfvars](#) in the sample-aws-security-lake-integrations repository on GitHub.

Task 3: Establish cross-cloud connectivity

Configure cross-cloud credentials using automation scripts:

- **Azure credential configuration:** See the [configure-secrets-manager.sh](#) file in the sample-aws-security-lake-integrations repository on GitHub.
- **GCP credential configuration:** See the [configure-secrets-manager.sh](#) file in the sample-aws-security-lake-integrations repository on GitHub.

Task 4: Validate Unified Console

Access the Amazon OpenSearch Service Security Analytics Dashboard to verify multi-cloud data ingestion and unified console functionality.

- **Validation procedures:** See the [validation queries and procedures](#) in the sample-aws-security-lake-integrations repository on GitHub.

Task 5: Clean up resources

To remove all deployed resources, run the following:

```
cd integrations/security-lake/cdk
cdk destroy -c "configFile=config.example.yaml"
```

Azure resource clean up: Navigate to your Azure Terraform configuration and run the following:

```
cd integrations/azure/microsoft_defender_cloud/terraform
# Preview what will be destroyed
terraform plan -destroy
```

After confirming what will be destroyed, run the following:

```
# Destroy all resources
terraform destroy
```

GCP resource clean up: Navigate to your GCP Terraform configuration and run the following:

```
cd integrations/google_security_command_center/terraform
# Preview what will be destroyed
terraform plan -destroy
```

After confirming what will be destroyed, run the following:

```
# Destroy all resources
terraform destroy
```

Supporting documentation URLs

AWS security platform documentation

- **Amazon OpenSearch Service:** <https://docs.aws.amazon.com/opensearch-service/>
- **Amazon Security Lake:** <https://docs.aws.amazon.com/security-lake/>
- **Amazon GuardDuty:** <https://docs.aws.amazon.com/guardduty/>
- **Amazon Inspector:** <https://docs.aws.amazon.com/inspector/>
- **AWS Systems Manager:** <https://docs.aws.amazon.com/systems-manager/>

Multi-cloud integration documentation

- **Security Lake multi-cloud integration:** <https://docs.aws.amazon.com/security-lake/latest/userguide/custom-sources.html>
- **Systems Manager hybrid activations:** <https://docs.aws.amazon.com/systems-manager/latest/userguide/activations.html>
- **OpenSearch Security Analytics plug-in:** <https://docs.aws.amazon.com/opensearch-service/latest/developerguide/security-analytics.html>

Implementation guides

- **Azure integration guide:** Available in the project repository at https://github.com/aws-samples/sample-aws-security-lake-integrations/blob/main/integrations/azure/microsoft_defender_cloud/README.md
- **GCP integration guide:** Available in the project repository at https://github.com/aws-samples/sample-aws-security-lake-integrations/blob/main/integrations/google_security_command_center/README.md
- **Security Lake framework:** Available in the project repository at <https://github.com/aws-samples/sample-aws-security-lake-integrations/blob/main/integrations/security-lake/cdk/README.md>

Conclusion

In this tutorial, we created and showed a comprehensive Security Platform as a Service (PaaS) that delivers the required native, multifunction security operations console:

1. **Native multi-cloud CSPM:** Provides built-in connectors for Azure Security Center and GCP Security Command Center with unified OpenSearch dashboard.
2. **Native multi-cloud SIEM:** Provides built-in connectors for Azure and GCP log sources with unified Security Analytics console
3. **Native multi-cloud CWPP:** Provides built-in connectors for Azure and GCP workload protection with unified threat detection, vulnerability management, and runtime protection

