
AWS
re:Invent
NOV. 28 – DEC. 2, 2022 | LAS VEGAS, NV

ANT311

Building security operations with Amazon OpenSearch Service

Manish Arora (he/him)

Sr. WW OpenSearch GTM Specialist
AWS

Jimish Shah (he/him)

Sr. Product Manager
AWS

Aruna Govindaraju (she/her)

Analytics Specialist Solution Architect, WWSO Analytics,
AWS

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Agenda

- OpenSearch and Amazon OpenSearch Service
- Protecting your data with OpenSearch
- Customer use cases and stories
- Security analytics with OpenSearch
- Demo

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



OpenSearch is a **community-driven, open-source** search and analytics suite derived from Apache 2.0 licensed Elasticsearch 7.10.2

The OpenSearch project consists of a distributed search engine powered by Apache Lucene, **OpenSearch,** and a data visualization and user interface, **OpenSearch Dashboards**

40+ partners and service providers

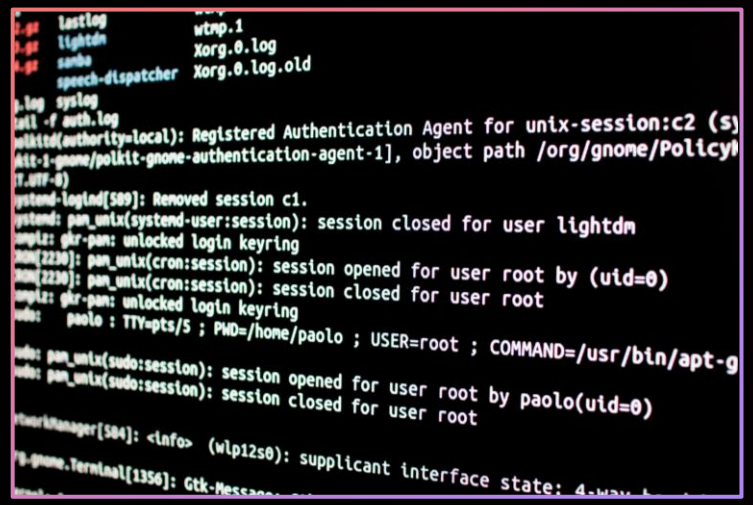
100s of contributors 1000s of pull requests

80+ repositories and clients

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Powerful analytics engine







Text search

Natural language

Boolean queries

Relevance

Streaming data

High-volume ingest

Near real time

Distributed storage

Analysis

Time-based visualizations

Nestable statistics

Time series tools

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Amazon OpenSearch Service

Amazon OpenSearch Service securely unlocks real-time search, monitoring, and analysis of operational data



Managed: Increase operational excellence by using a popular open source solution



Cost conscious: Optimize time and resources for strategic work



Observability: Systematically detect potential threats and react to a system's state through an open source solution for machine learning, alerting, and visualization



Secure: Audit and secure your data with a data center and network architecture and built-in certifications

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Security with Amazon OpenSearch Service

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What are your security requirements?



- Confidential business data
- Data access control
- Auditing user actions
- Data encryption
- Advanced security controls
- Integrate with SAML or other identity providers
- Compliance: HIPAA, FedRAMP, DoD CC SRG, SOC, PCI, ISO, etc.
- Backwards compatible security patches

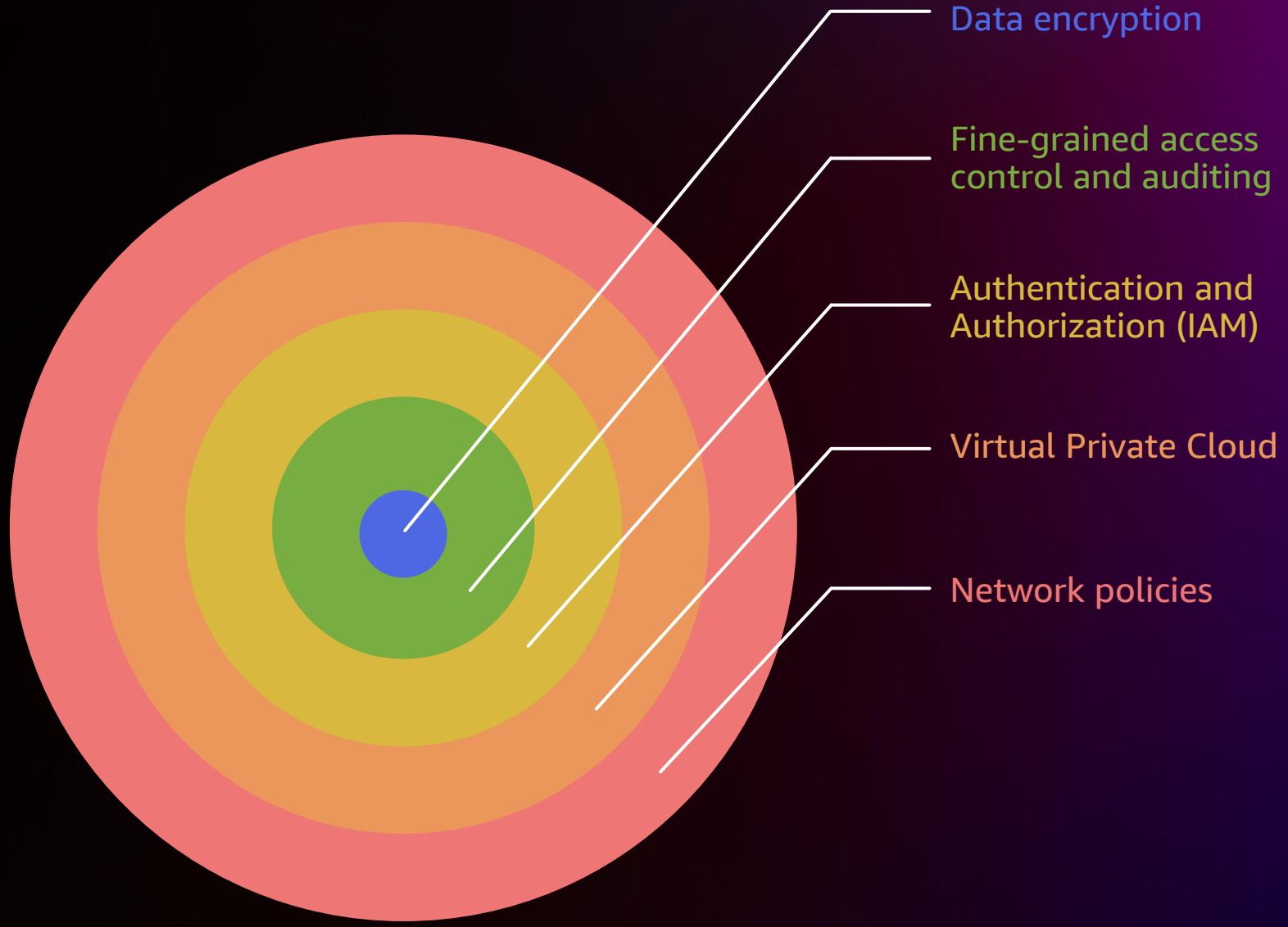
aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

10,000-foot view of security

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

OpenSearch security is defense in layers



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Four pillars of security

Encryption

Keep your data secure



AWS Key Management Service

Authentication

Leverage your existing authentication infrastructure



AWS Identity & Access Management

Authorization

Granular access control to control the user actions on your cluster



Fine-grained access control (SAML, IAM, Basic Authentication, OpenID Connect, Cognito)

Audit and compliance

Track and record all user actions to help meet compliance standards



Amazon CloudWatch



AWS CloudTrail

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS security controls

AWS IAM IP based policy (without VPC)

Virtual Private Cloud (VPC)

- Security groups
- NACL (Network Access Control List)
- VPC flow logs for auditing network traffic

AWS IAM identity policy

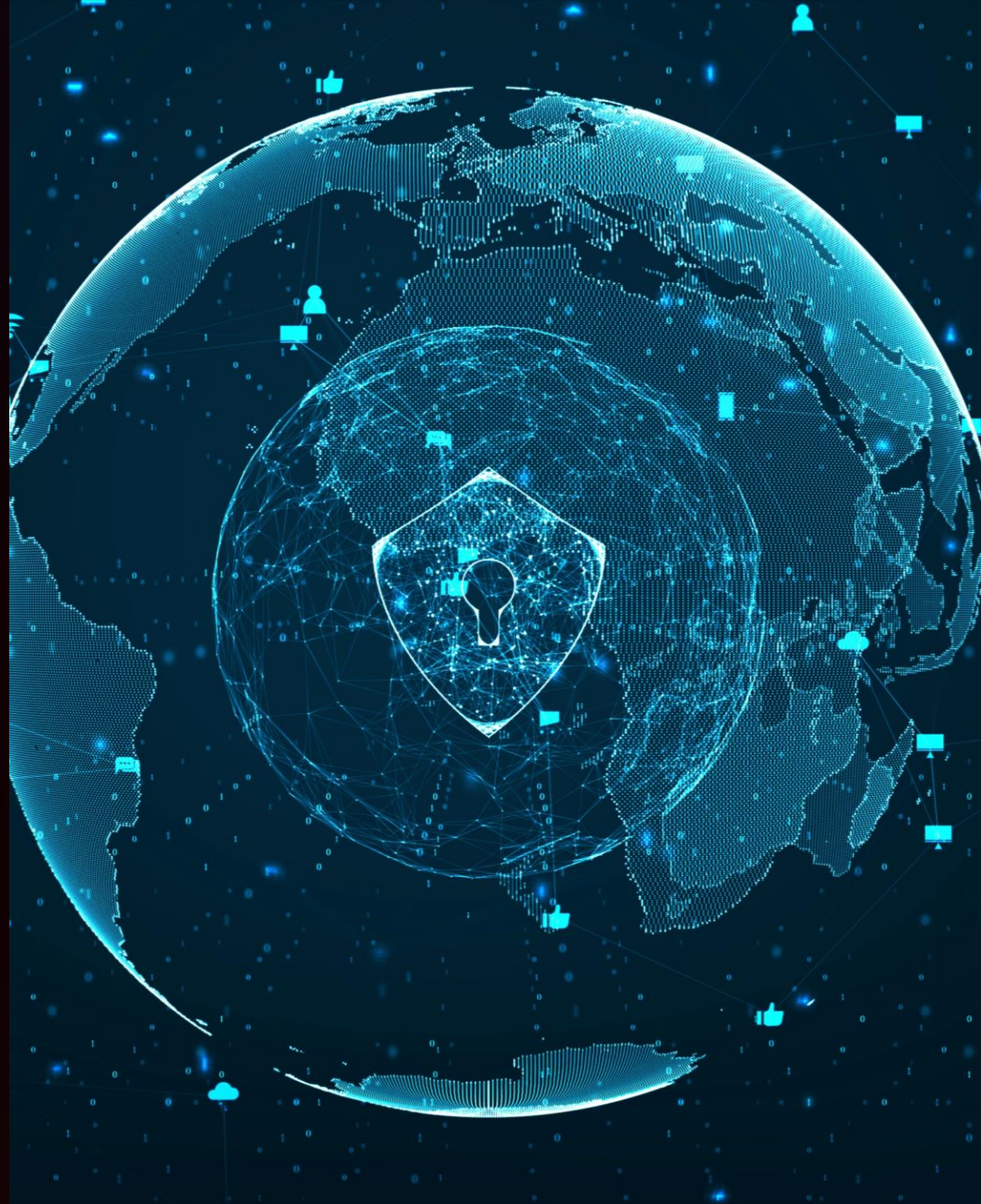
AWS IAM resource policy (or domain access policy)



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Fine-grained access control (FGAC)

- Identity management
  (basic auth, SAML, Amazon Cognito, IAM, ADFS/LDAP)
- Cluster and Index permissions
- Document and field level security
- Field masking
- Audit logging and compliance



aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon OpenSearch Service security core concepts



Users

Users are principals who make requests to OpenSearch clusters; a user has credentials



Permissions

Assign individual permissions or a group of permissions, such as creating an index



Roles

Security roles define the scope of a set of permissions: cluster, index, document, or field



Backend roles

External identities from an authorization backend (e.g., SAML, IAM, ADFS)



Role mappings

Users assume roles after they successfully authenticate; role mappings map roles to users (or backend roles)



Dashboards tenants

Allow sharing of data, visualizations and dashboards between users/roles belonging to same tenant

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Large e-commerce customer use case

- 100s of TBs of customer order transactions data ingested daily
- PII data
- Application team – fraud detection from order transactions
- Compliance and audit team
- SAML identity provider (Okta)

Goal

Create data access boundaries

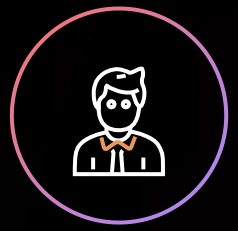
Restrict permissions to specific documents

Auto mapping of users by organizational workgroup

Audit usage patterns

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

User personas and needs



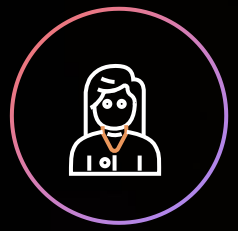
DevOps Administrators

Access and validate entire order transactions data set



Application users

Securely query specific order transactions – access to restricted data sets (US only orders)



Auditors

Read only user who views compliance reports. PII data will be masked

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Goal accomplished

Customized data access permissions

Personalized views for different user personas

Restrict permissions to specific indices, documents or fields

Mask sensitive data

Predefined permissions assignment by user attribute

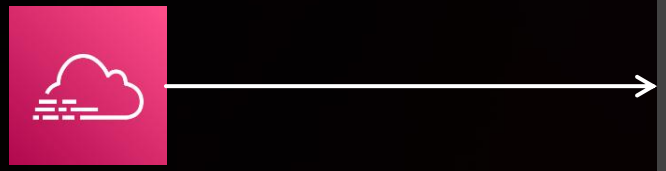
Analyzing audit logs with Amazon CloudWatch Logs



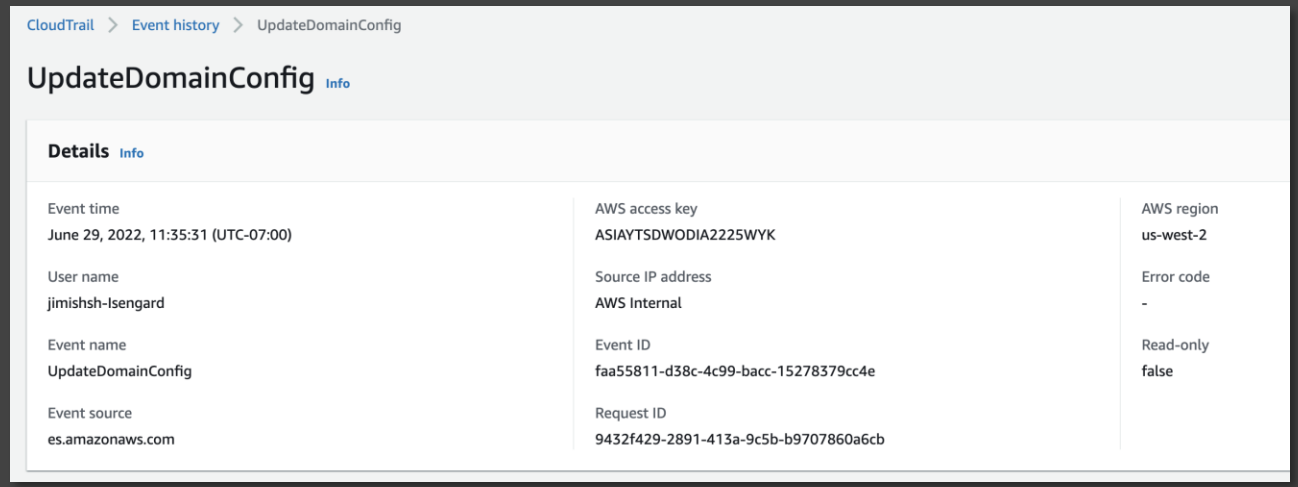
aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Auditing domain configuration management



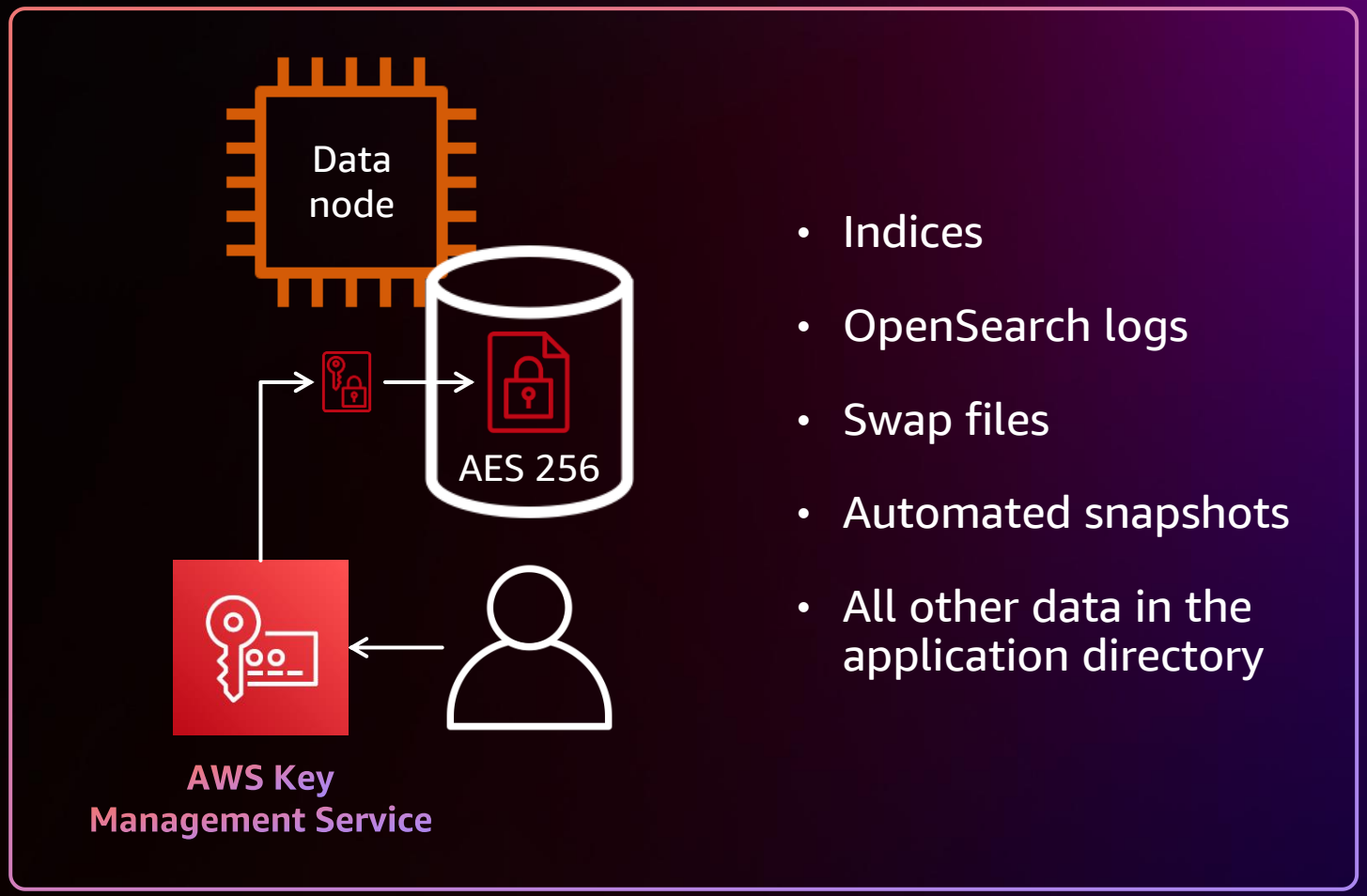
AWS CloudTrail



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Data encryption

- Uses AWS Key Management Service (KMS) to store and manage keys
- AWS managed or customer managed



- Indices
- OpenSearch logs
- Swap files
- Automated snapshots
- All other data in the application directory

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Modular security framework

Minimal

- IAM IP policy
- Domain endpoint security (HTTPS)
- Encryption at rest
- AWS managed key
- Sigv4 signed requests
- AWS CloudTrail logging

Basic

- *Everything in Minimal*
- Virtual Private Cloud and security groups
- Encryption in transit
- IAM Identity Policy
- IAM Resource policy
- AWS/customer managed key

Advanced

- *Everything in basic*
- Fine-grained access control
- SAML/Cognito-OIDC
- Audit logging and compliance
- Document and field level security
- Field masking
- Dashboards tenants
- Custom endpoint

Note: you can pick and choose any mix of above features as needed—above categorization is meant as a guidance

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

How to enable security controls



AWS
Console/SDK

- Virtual Private Cloud
- AWS IAM policies
- HTTPS
- Data encryption
- Fine-grained access control
- Audit logs
- SAML/Cognito configuration
- AWS KMS keys



OpenSearch
API/Dashboards

- Role mapping
- Document and field level security
- Data masking
- Audit and compliance logs
- Dashboards tenants

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon OpenSearch Service customers

Software and Internet

Adobe · IAC · AUTODESK

Education Technology

McGraw Hill Education · INSTRUCTURE · Blackboard

BioTech and Pharma

MONSANTO · Bristol-Myers Squibb

Financial Services

THOMSON REUTERS · stripe · KICKSTARTER

Media and Entertainment

NETFLIX · FOX

Social Media

cookpad · ancestry · Nextdoor

Telecommunications

COMCAST · T-Mobile

Travel and Transportation

lyft · Expedia · UBER

Real Estate

Zillow · move

Logistics and Operations

here · elementum · infor

Publishing

FT FINANCIAL TIMES · ELSEVIER · The Washington Post

Other

Canon · SAMSUNG · British Gas

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Security breaches happen

A major airline confirms data breach that allowed an unauthorized actor to gain access to personal information of a small number of customers and employees

A major oil pipeline was shut down as a result of a malware/ransomware attack (compromised password)

A major rideshare company was impacted as a result of a social engineering attack



aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Security analytics with



(Experimental feature)

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Key requirements for security analytics

Built for the cloud—agility, scale, and flexibility

Identify latest adversarial techniques/tactics (MITRE ATT&CK framework)

Easy to add and update security content

Integrate with external threat intelligence feeds

Enrich with contextual information

Detect and hunt threats

Respond to incidents



aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Security analytics with OpenSearch

SECURE YOUR BUSINESS DATA AND RAPIDLY DETECT POTENTIAL THREATS

- **Pre-packaged rules:** 2200+ Sigma security rules supported out of the box
- **Supported log types:** including Windows, Netflow, AWS CloudTrail, DNS, System logs, Amazon S3 access, Apache access, AD/LDAP
- **Threat detection:** customize threat detectors for your logs using pre-packaged rule sets
- **Security findings:** automatically detect potential security threats
- **Security alerts:** create customized alerts from detector generated findings
- **Rules builder:** to copy, create and modify rules
- **Dashboards:** faster time to insights using custom dashboards



aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What are you waiting for?



Investigate, detect, and respond to potential threats rapidly with security analytics



Data encryption and fine grained access control for your data



Audit and compliance needs



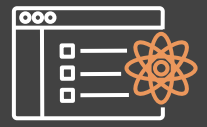
Comprehensive suite of security features to meet your business requirements

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Getting started

1



Launch an Amazon OpenSearch Service cluster in minutes

2



Follow the Getting Started Tutorial to build a log analytics solution

3

Learn how to use OpenSearch security features

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Resources



Stay up to date!
www.aws.amazon.com/opensearch-service



Contribute to OpenSearch project
opensearch.org



Amazon OpenSearch Service Immersion Days
Deep dive through online training and hands-on labs
searchservices-ww-gtm@amazon.com



Public Roadmap
OpenSearch



Documentation
Developer Guide



Partners
Get help from AWS Partner Network

Stay connected



Twitter: @OpenSearchProj
https://twitter.com/OpenSearchProj



LinkedIn:
https://www.linkedin.com/company/opensearch-project



Facebook:
https://www.facebook.com/OpenSearchProject



Twitch:
https://www.twitch.tv/OpenSearchProject



Meetup:
https://www.meetup.com/OpenSearch/

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!

Manish Arora (he/him)

LinkedIn: maurora

Jimish Shah (he/him)

LinkedIn: jimishrshah

Aruna Govindaraju (she/her)

LinkedIn: arunavaidyanathan



Please complete the session survey in the **mobile app**

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.