AWS re:Inforce

JUNE 10 - 12, 2024 | PHILADELPHIA, PA

TDR331

Unlock OCSF: Turn raw logs into insights with generative AI

Keith Gilbert
(he/him)
Senior Security Engineering Manager
Amazon Web Services

Pratima Singh
(she/her)
Senior APJ Security Specialist SA
Amazon Web Services

Chris Lamont-Smith
(he/him)
Senior Security Consultant
Amazon Web Services

Agenda

Challenges with security log analysis

Open Cybersecurity Schema Framework

Generative AI in the mix

A typical security investigation scenario

UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS

Challenges

Multiple log schemas

Additional data wrangling

Onboarding new log sources

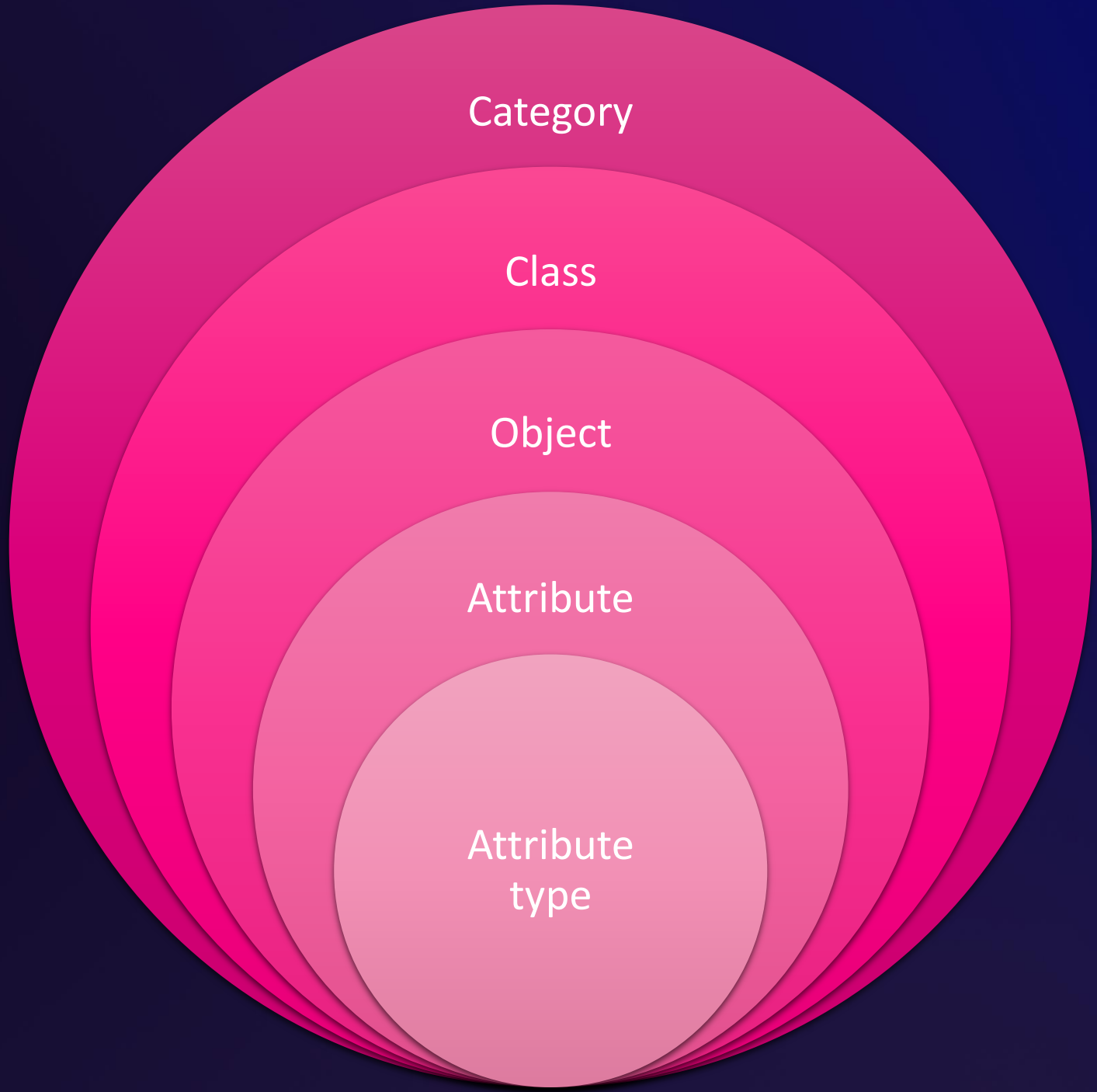
Schema evolution

Management overhead

Open Cybersecurity Schema Framework (OCSF)

- Framework to render schema
- Security-focused
- Designed for the cloud
- Customizable and extendable
- Self-describing and unambiguous
- Consistent query paths
- Source agnostic taxonomy

Fundamentals



Sample OCSF formatted log


```
"activity_id": 1,
"activity_name": "Create",
"category_name": "Findings",
"category_uid": 2,
"class_name": "Detection Finding",
"class_uid": 2004,
"cloud": {
    "account": {
        "uid": "111111111111"
    },
    "provider": "AWS",
    "region": "us-east-2"
},
```

```
"observables": [
    {
        "name": "evidences[].src_endpoint.ip",
        "type": "IP Address",
        "type_id": 2,
        "value": "52.94.133.131"
    },
    {
        "name": "resources[].uid",
        "type": "Resource UID",
        "type_id": 10,
        "value": "AWS::IAM::AccessKey:ASIATMJPC7EXAMPLE"
    }
],
```

```
"metadata": {
    "extensions": [
        {
            "name": "linux",
            "uid": "1",
            "version": "1.1.0"
        }
    ],
    "log_version": "2018-10-08",
    "product": {
        "feature": {
            "uid": "arn:aws:guardduty:us-east-2:111111111111:detector/1ac1bfceda6679698215d5d0EXAMPLE"
        },
        "name": "GuardDuty",
        "uid": "arn:aws:securityhub:us-east-2::product/aws/guardduty",
        "vendor_name": "Amazon"
    },
    "profiles": [
        "cloud",
        "datetime",
        "linux"
    ],
    "version": "1.1.0"
},
"observables": [
    {
        "name": "evidences[].src_endpoint.ip",
        "type": "IP Address",
        "type_id": 2,
        "value": "52.94.133.131"
    },
    {
        "name": "resources[].uid",
        "type": "Resource UID",
        "type_id": 10,
        "value": "AWS::IAM::AccessKey:ASIATMJPC7EXAMPLE"
    }
],
```

Sample OCSF formatted log

```
"activity_id": 1,
"activity_name": "Create",
"category_name": "Findings",
"category_uid": 2,
"class_name": "Detection Finding",
"class_uid": 2004,
"cloud": {
    "account": {
        "uid": "111111111111"
    },
    "provider": "AWS",
    "region": "us-east-2"
},
```

Category

```
"observables": [
    {
        "name": "evidences[].src_endpoint.ip",
        "type": "IP Address",
        "type_id": 2,
        "value": "52.94.133.131"
    },
    {
        "name": "resources[].uid",
        "type": "Resource UID",
        "type_id": 10,
        "value": "AWS::IAM::AccessKey:ASIATMJPC7EXAMPLE"
    }
],
```

```
"metadata": {
    "extensions": [
        {
            "name": "linux",
            "uid": "1",
            "version": "1.1.0"
        }
    ],
    "log_version": "2018-10-08",
    "product": {
        "feature": {
            "uid": "arn:aws:guardduty:us-east-2:111111111111:detector/1ac1bfceda6679698215d5d0EXAMPLE"
        },
        "name": "GuardDuty",
        "uid": "arn:aws:securityhub:us-east-2::product/aws/guardduty",
        "vendor_name": "Amazon"
    },
    "profiles": [
        "cloud",
        "datetime",
        "linux"
    ],
    "version": "1.1.0"
},
"observables": [
    {
        "name": "evidences[].src_endpoint.ip",
        "type": "IP Address",
        "type_id": 2,
        "value": "52.94.133.131"
    },
    {
        "name": "resources[].uid",
        "type": "Resource UID",
        "type_id": 10,
        "value": "AWS::IAM::AccessKey:ASIATMJPC7EXAMPLE"
    }
],
```

Sample OCSF formatted log

```
"activity_id": 1,
"activity_name": "Create",
"category_name": "Findings",
"category_uid": 2,
"class_name": "Detection Finding",
"class_uid": 2004,
"cloud": {
    "account": {
        "uid": "111111111111"
    },
    "provider": "AWS",
    "region": "us-east-2"
},
```

Category

Class

```
"observables": [
    {
        "name": "evidences[].src_endpoint.ip",
        "type": "IP Address",
        "type_id": 2,
        "value": "52.94.133.131"
    },
    {
        "name": "resources[].uid",
        "type": "Resource UID",
        "type_id": 10,
        "value": "AWS::IAM::AccessKey:ASIATMJPC7EXAMPLE"
    }
],
```

```
"metadata": {
    "extensions": [
        {
            "name": "linux",
            "uid": "1",
            "version": "1.1.0"
        }
    ],
    "log_version": "2018-10-08",
    "product": {
        "feature": {
            "uid": "arn:aws:guardduty:us-east-2:111111111111:detector/1ac1bfceda6679698215d5d0EXAMPLE"
        },
        "name": "GuardDuty",
        "uid": "arn:aws:securityhub:us-east-2::product/aws/guardduty",
        "vendor_name": "Amazon"
    },
    "profiles": [
        "cloud",
        "datetime",
        "linux"
    ],
    "version": "1.1.0"
},
"observables": [
    {
        "name": "evidences[].src_endpoint.ip",
        "type": "IP Address",
        "type_id": 2,
        "value": "52.94.133.131"
    },
    {
        "name": "resources[].uid",
        "type": "Resource UID",
        "type_id": 10,
        "value": "AWS::IAM::AccessKey:ASIATMJPC7EXAMPLE"
    }
],
```

Sample OCSF formatted log

```
"activity_id": 1,
"activity_name": "Create",
"category_name": "Findings",
"category_uid": 2,
"class_name": "Detection Finding",
"class_uid": 2004,
"cloud": {
    "account": {
        "uid": "111111111111"
    },
    "provider": "AWS",
    "region": "us-east-2"
},
```

Category

Class

```
"observables": [
    {
        "name": "evidences[].src_endpoint.ip",
        "type": "IP Address",
        "type_id": 2,
        "value": "52.94.133.131"
    },
    {
        "name": "resources[].uid",
        "type": "Resource UID",
        "type_id": 10,
        "value": "AWS::IAM::AccessKey:ASIATMJPC7EXAMPLE"
    }
],
```

```
"metadata": {
    "extensions": [
        {
            "name": "linux",
            "uid": "1",
            "version": "1.1.0"
        }
    ],
    "log_version": "2018-10-08",
    "product": {
        "feature": {
            "uid": "arn:aws:guardduty:us-east-2:111111111111:detector/1ac1bfceda6679698215d5d0EXAMPLE"
        },
        "name": "GuardDuty",
        "uid": "arn:aws:securityhub:us-east-2::product/aws/guardduty",
        "vendor_name": "Amazon"
    },
    "profiles": [
        "cloud",
        "datetime",
        "linux"
    ],
    "version": "1.1.0"
},
"observables": [
    {
        "name": "evidences[].src_endpoint.ip",
        "type": "IP Address",
        "type_id": 2,
        "value": "52.94.133.131"
    },
    {
        "name": "resources[].uid",
        "type": "Resource UID",
        "type_id": 10,
        "value": "AWS::IAM::AccessKey:ASIATMJPC7EXAMPLE"
    }
],
```

Object

Sample OCSF formatted log

```
"activity_id": 1,
"activity_name": "Create",
"category_name": "Findings",
"category_uid": 2,
"class_name": "Detection Finding",
"class_uid": 2004,
"cloud": {
    "account": {
        "uid": "111111111111"
    },
    "provider": "AWS",
    "region": "us-east-2"
},
```

Category

Class

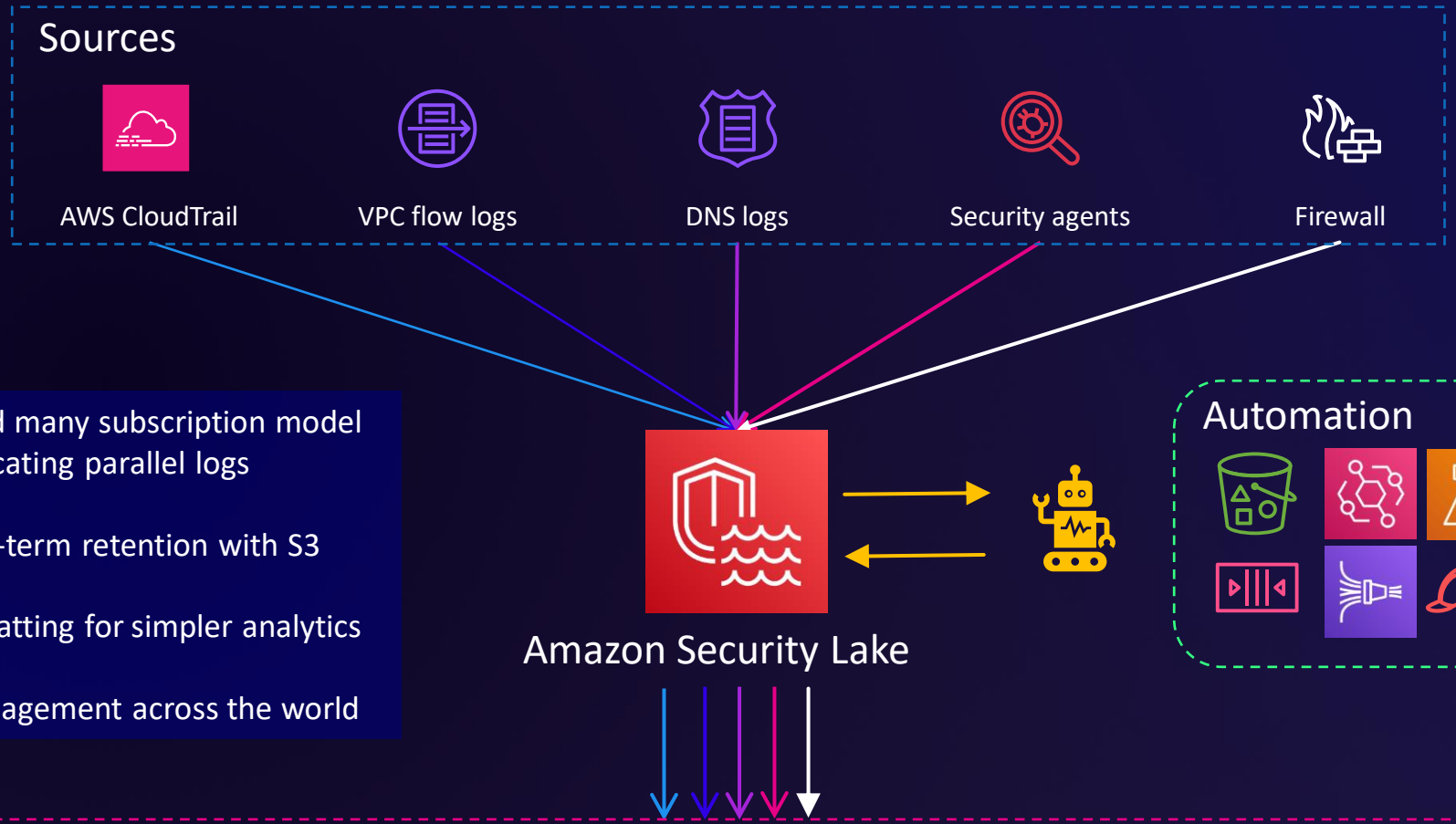
```
"observables": [
    {
        "name": "evidences[].src_endpoint.ip",
        "type": "IP Address",
        "type_id": 2,
        "value": "52.94.133.131"
    },
    {
        "name": "resources[].uid",
        "type": "Resource UID",
        "type_id": 10,
        "value": "AWS::IAM::AccessKey:ASIATMJPC7EXAMPLE"
    }
],
```

Attributes
Attribute types

```
"metadata": {
    "extensions": [
        {
            "name": "linux",
            "uid": "1",
            "version": "1.1.0"
        }
    ],
    "log_version": "2018-10-08",
    "product": {
        "feature": {
            "uid": "arn:aws:guardduty:us-east-2:111111111111:detector/1ac1bfceda6679698215d5d0EXAMPLE"
        },
        "name": "GuardDuty",
        "uid": "arn:aws:securityhub:us-east-2::product/aws/guardduty",
        "vendor_name": "Amazon"
    },
    "profiles": [
        "cloud",
        "datetime",
        "linux"
    ],
    "version": "1.1.0"
},
"observables": [
    {
        "name": "evidences[].src_endpoint.ip",
        "type": "IP Address",
        "type_id": 2,
        "value": "52.94.133.131"
    },
    {
        "name": "resources[].uid",
        "type": "Resource UID",
        "type_id": 10,
        "value": "AWS::IAM::AccessKey:ASIATMJPC7EXAMPLE"
    }
],
```

Object

Amazon Security Lake



Amazon OpenSearch Service

Advanced analytical capabilities to query and analyze OCSF data with powerful visualization and monitoring capabilities

Search: Query at scale to find relevant security events within seconds

Security analytics: Securely and easily visualize and analyze your security data or send alerts using automated workflows

Detection rules: Customize or use prepackaged threat detection rules for your OCSF data

OpenSearch ingestion: Simplify data ingestion, filtering, and transformation with pre-built pipelines

Analytics tools and service partners

aws

Amazon Athena

Amazon OpenSearch Service

Amazon SageMaker

Partner analytics

CHAOSSEARCH, DATADOG, DEVO, IBM, new relic., RAPID7, RIPJAR, securonix, SentinelOne, SNC PRIME, splunk>, STELLAR CYBER, sumo logic, SWIMLANE, tines, torq, Trellix, wazuh.

Service partners

accenture, Booz Allen, CMD, Deloitte., DXC TECHNOLOGY, insbuild. Growing with the cloud, kyndryl, EVIDEN, HCOOP, IBM, Infosys, leidos, MEGAZONE CLOUD, pwc, SNC PRIME, tcs TATA CONSULTANCY SERVICES, wipro

This is not a complete list. To view all AWS Partners for this category, visit AWS Partner Solutions Finder. This list of partners is current as of May 13, 2024.

Generative AI in the mix

Features and use cases

Capabilities

Contextualizing

Reasoning

Responding

Summarizing

Features and use cases

Capabilities	Use cases
Contextualizing	Generating SQL
Reasoning	Chatbots
Responding	Automating incident response
Summarizing	Building business insights

What’s next

Roadmap

Non-OCSF vs. OCSF

Non-OCSF

Multiple schemas

Attributes per schema

Manual ETL

Data normalizing

Manual partitioning

Schema evolution

Permissions management

Non-OCSF vs. OCSF

Non-OCSF	OCSF & Security Lake
Multiple schemas	Single framework to render schema
Attributes per schema	Consistent attributes
Manual ETL	Managed ETL with Security Lake
Data normalizing	Managed data lake with Security Lake
Manual partitioning	One-click schema upgrades
Schema evolution	Seamless connectivity with subscribers
Permissions management	Managed fine-grained permissions

Resources

OCSF schema definition

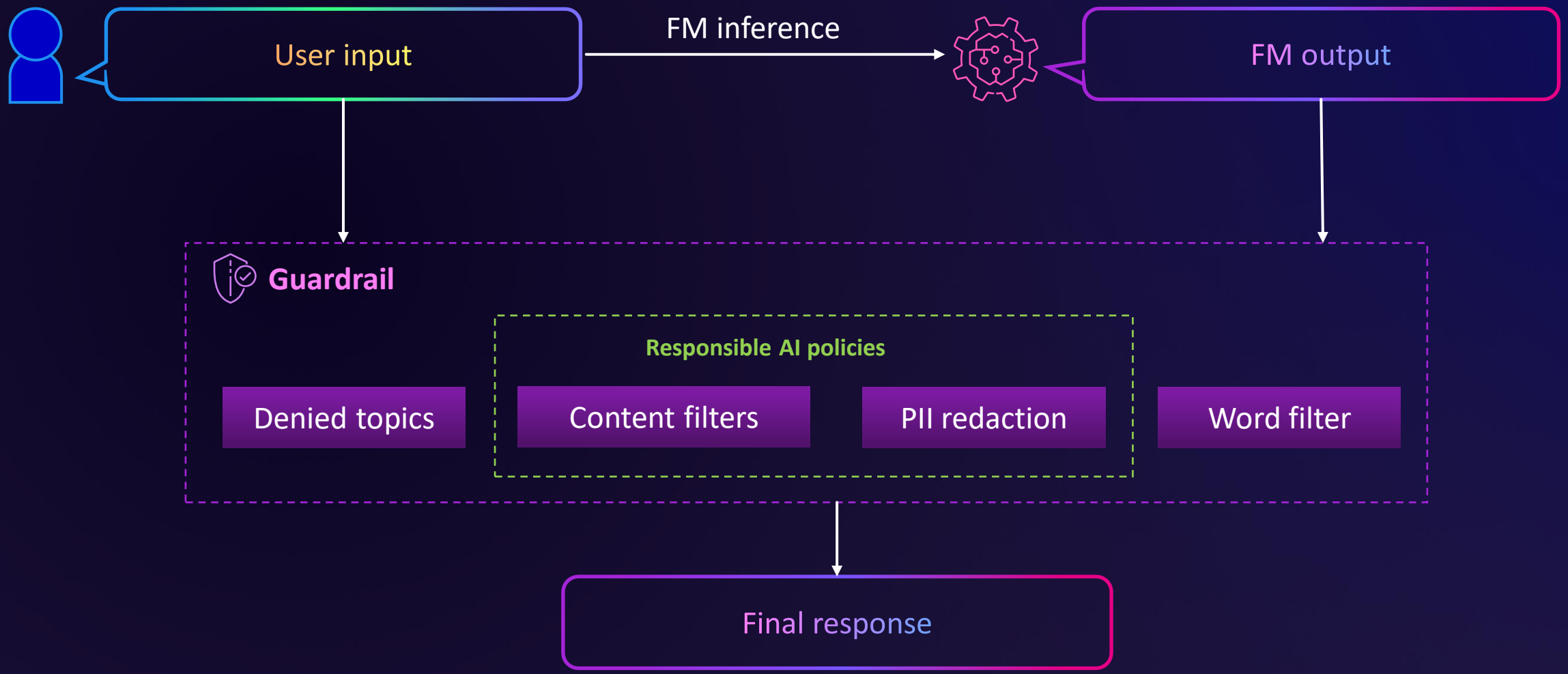
OCSF Slack channel

OCSF source code

How to develop an Amazon Security Lake POC

Open floor – Q&A

How it works



I can just forward all raw logs into a single S3 bucket and use Amazon Bedrock to generate insights. Why OCSF?

My organization has a fully operational SIEM solution. How do I justify changing approaches to OCSF and generative AI?

Security logs contain sensitive data. I have concerns about inadvertent sensitive data exposure using generative AI solutions across security logs.