
AWS
re:Inforce
JUNE 13 - 14, 2023 | ANAHEIM, CA

TDR310

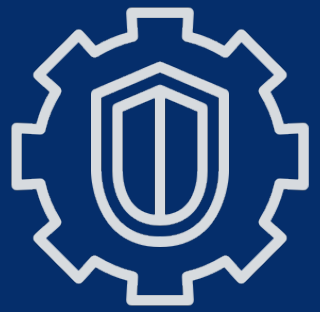
Developing new findings using machine learning in Amazon GuardDuty

Baris Coskun (he/him)
Sr. Principal Scientist
Amazon Web Services

Amit Megiddo (he/him)
Sr. Manager PMT Amazon GuardDuty
Amazon Web Services

© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What is Amazon GuardDuty?



Amazon GuardDuty is a threat detection service that uses machine learning, anomaly detection, and integrated threat intelligence to identify and prioritize potential threats to your AWS environment

Tens of thousands of customers across industries and geographies

Used by over 90% of the top 2,000 AWS customers

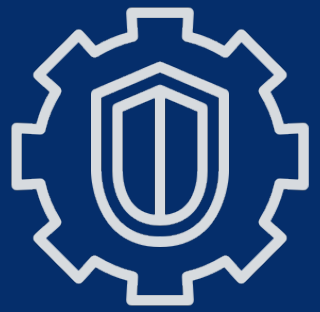
Helps protect millions of accounts, including over half a billion Amazon EC2 instances & millions of Amazon S3 buckets

Analyzes tens of billions of events per minute

aws

© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What is Amazon GuardDuty?



Amazon GuardDuty is a threat detection service that uses machine learning, anomaly detection, and integrated threat intelligence to identify and prioritize potential threats to your AWS environment

Tens of thousands of customers across industries and geographies

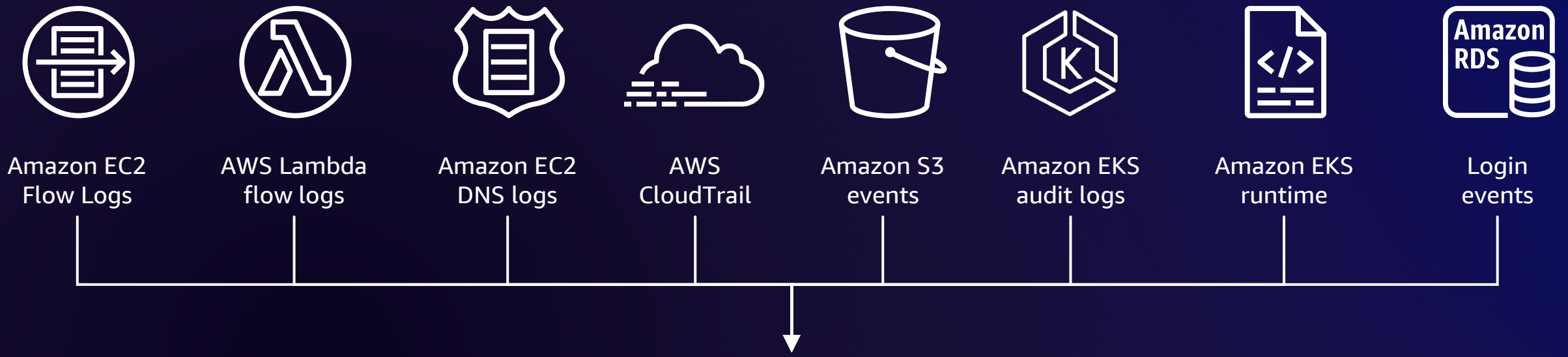
Used by over 90% of the top 2,000 AWS customers

Helps protect millions of accounts, including over half a billion Amazon EC2 instances & millions of Amazon S3 buckets

Analyzes tens of billions of events per minute

aws

© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.



© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.



© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.



How can we detect threats when there isn't a strong indicator of compromise?

© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

We need to look for unusual behavior such as

© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

We need to look for unusual behavior such as



Does this user normally access this Amazon S3 bucket from this location?

© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

We need to look for unusual behavior such as



Does this user normally access this Amazon S3 bucket from this location?



Does this IAM role normally list and describe Amazon DynamoDB tables?

© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

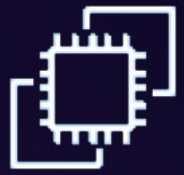
We need to look for unusual behavior such as



Does this user normally access this Amazon S3 bucket from this location?



Does this IAM role normally list and describe Amazon DynamoDB tables?



Does this Amazon EC2 instance normally egress this volume of traffic to this remote network?

aws

© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

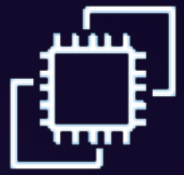
We need to look for unusual behavior such as



Does this user normally access this Amazon S3 bucket from this location?



Does this IAM role normally list and describe Amazon DynamoDB tables?



Does this Amazon EC2 instance normally egress this volume of traffic to this remote network?



Is this container image normally used in this Amazon EKS cluster?

aws

© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Easy! We'll profile what normally happens and then detect when something unusual happens



Unusual API for user



aws

© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Easy! We'll profile what normally happens and then detect when something unusual happens



Unusual API for user





Unusual ASN for bucket

aws

© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Easy! We'll profile what normally happens and then detect when something unusual happens



Unusual API for user





Unusual ASN for bucket



Unusual port for instance

aws

© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Easy! We'll profile what normally happens and then detect when something unusual happens



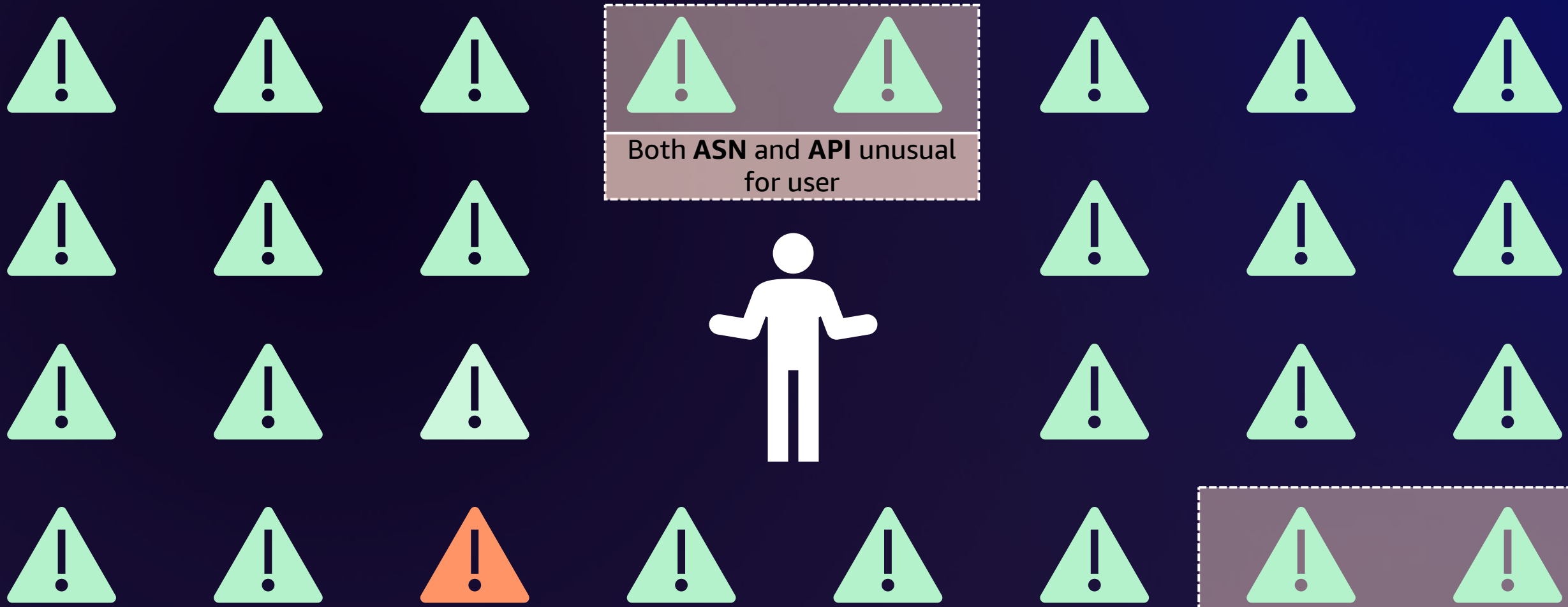
aws
© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Not a problem! We'll add rules to make sure we only detect really (really!) unusual activity



© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Not a problem! We'll add rules to make sure we only detect really (really!) unusual activity



aws
© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Not a problem! We'll add rules to make sure we only detect really (really!) unusual activity



© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Not a problem! We'll add rules to make sure we only detect really (really!) unusual activity



aws

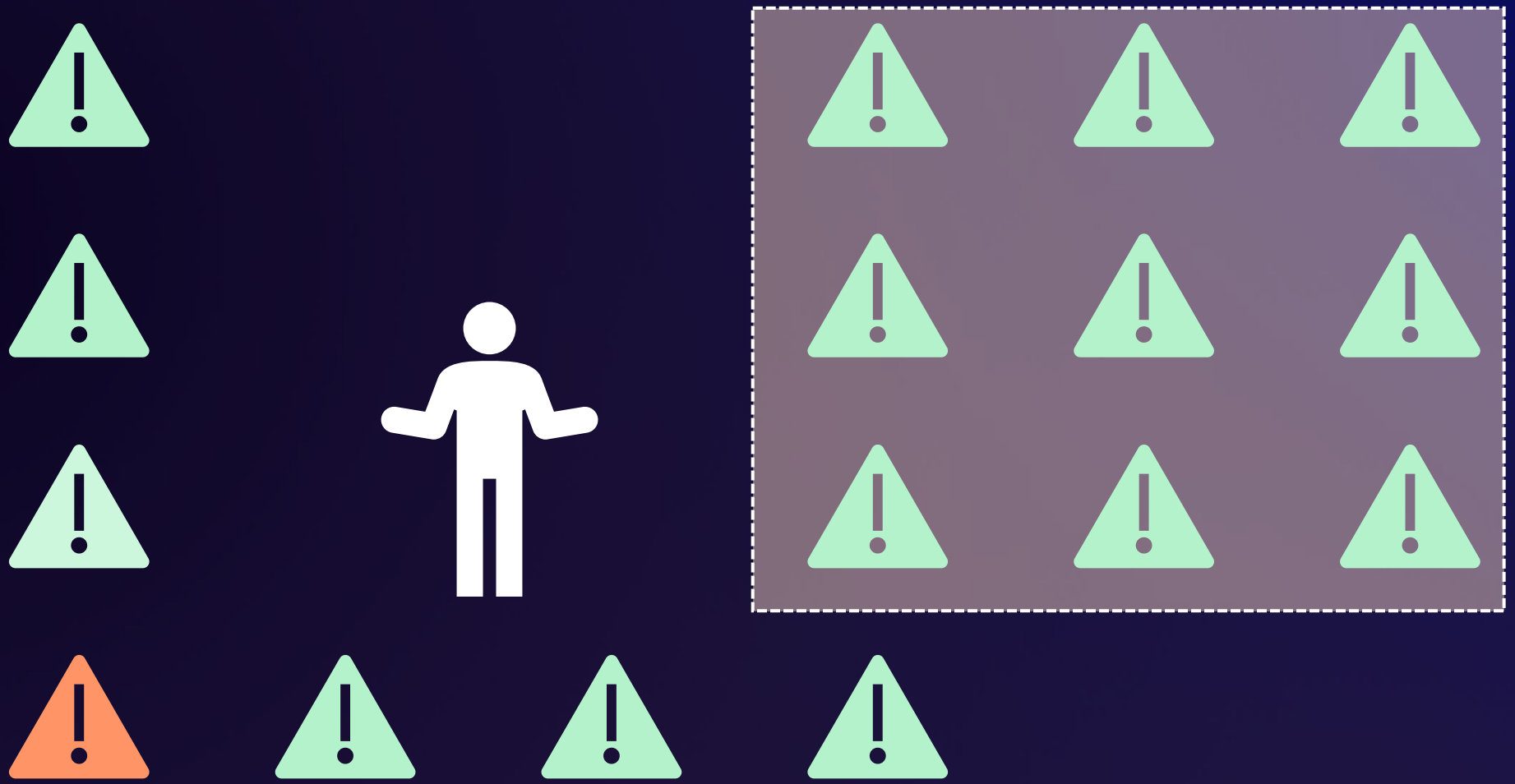
© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Not a problem! We'll add rules to make sure we only detect really (really!) unusual activity



© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Not a problem! We'll add rules to make sure we only detect really (really!) unusual activity



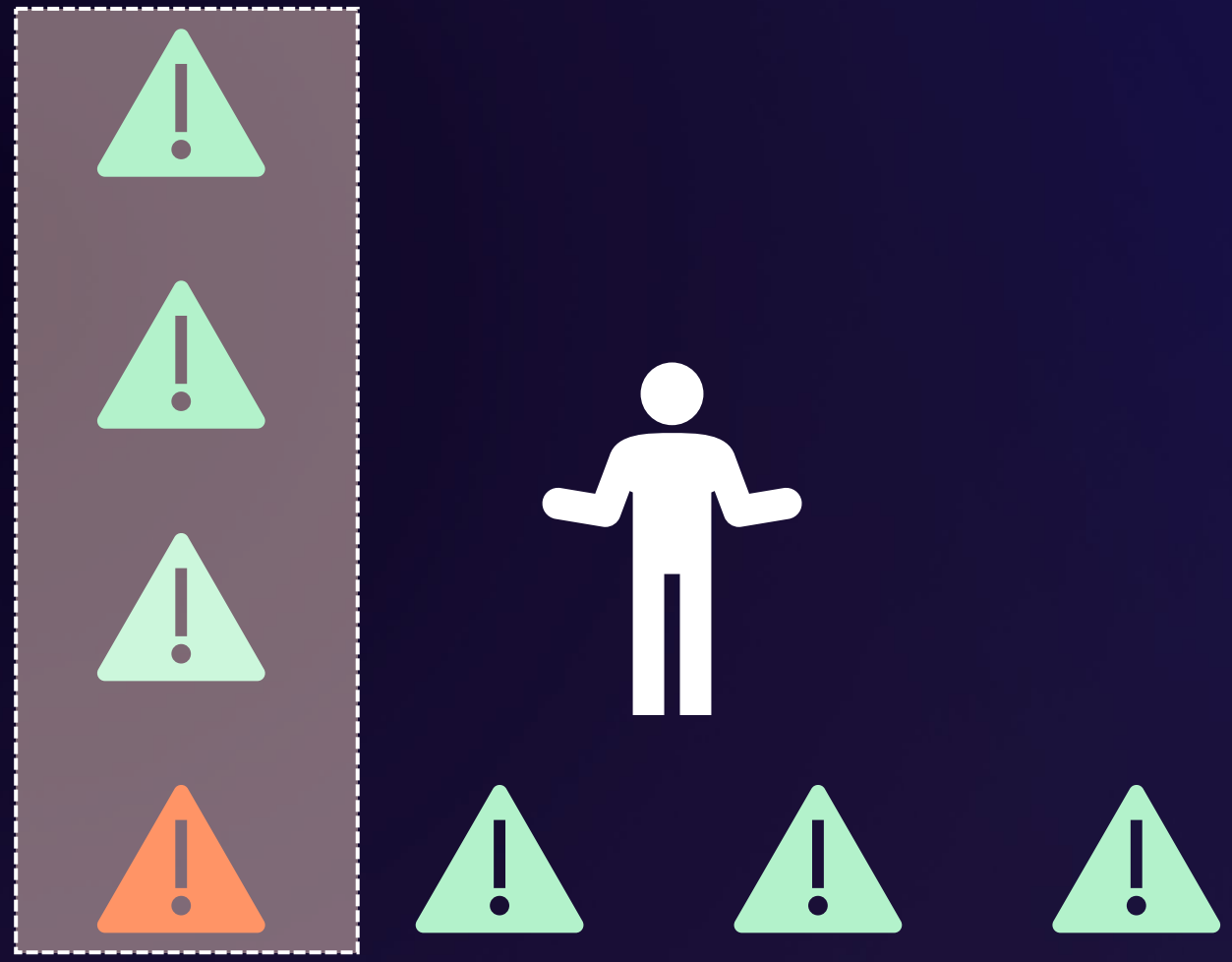
© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Not a problem! We'll add rules to make sure we only detect really (really!) unusual activity



© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Not a problem! We'll add rules to make sure we only detect really (really!) unusual activity



© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Not a problem! We'll add rules to make sure we only detect really (really!) unusual activity



© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Using anomaly detection to detect security incidents in complex AWS environments is challenging

© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Using anomaly detection to detect security incidents in complex AWS environments is challenging

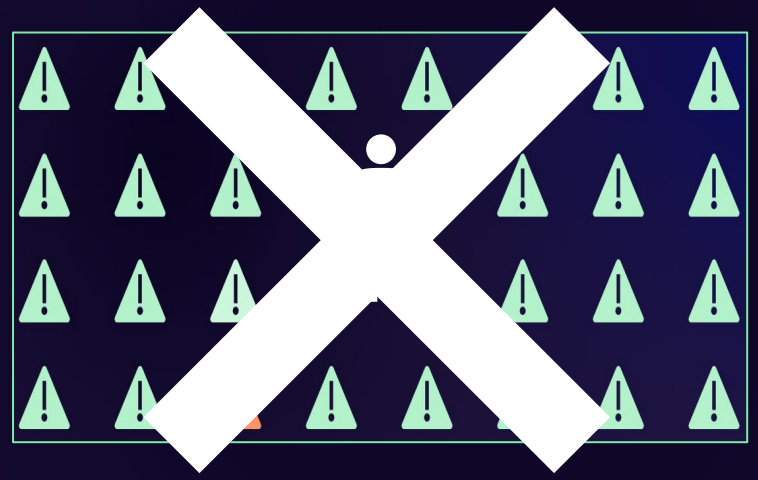


Looking for anything unusual will result in too much noise

aws

© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Using anomaly detection to detect security incidents in complex AWS environments is challenging

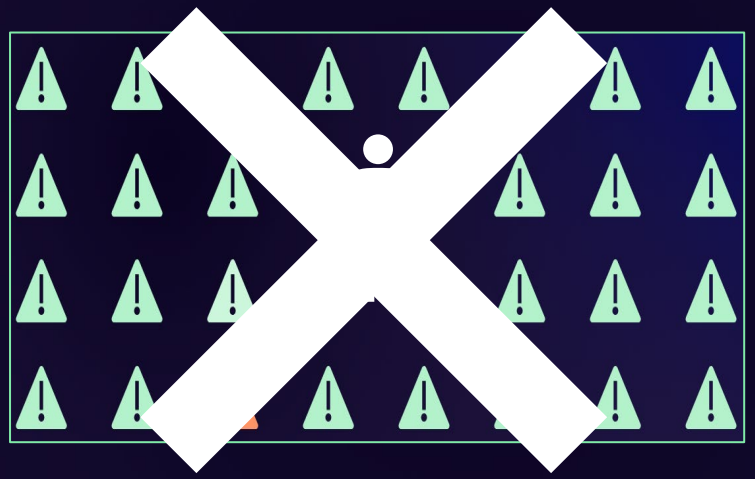


Looking for anything unusual will result in too much noise

aws

© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Using anomaly detection to detect security incidents in complex AWS environments is challenging



Looking for anything unusual will result in too much noise

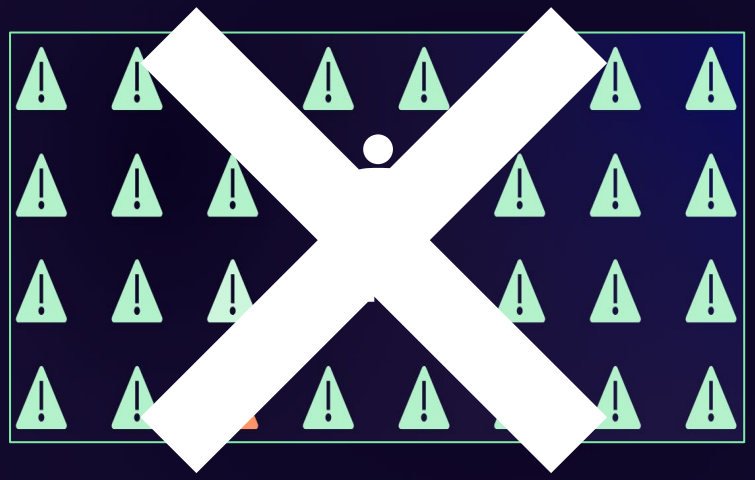


Applying rules to get rid of noise will result in missing the signal

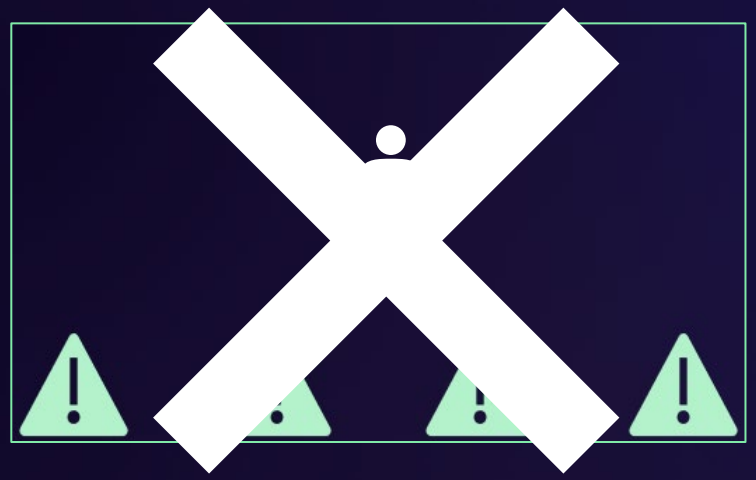
aws

© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Using anomaly detection to detect security incidents in complex AWS environments is challenging



Looking for anything unusual will result in too much noise

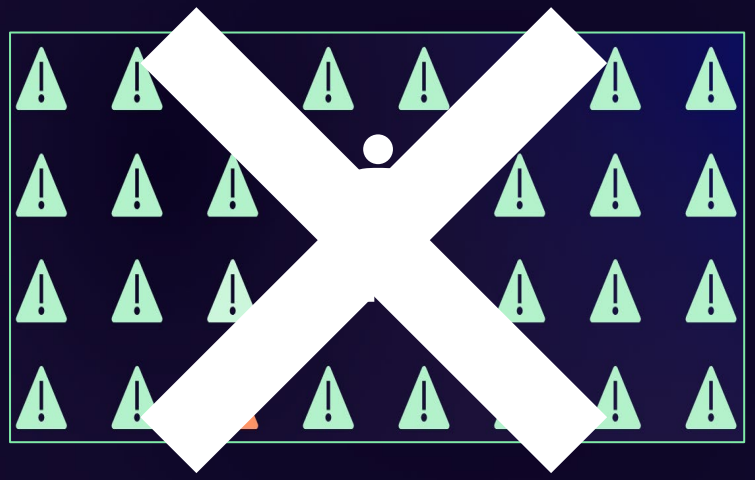


Applying rules to get rid of noise will result in missing the signal

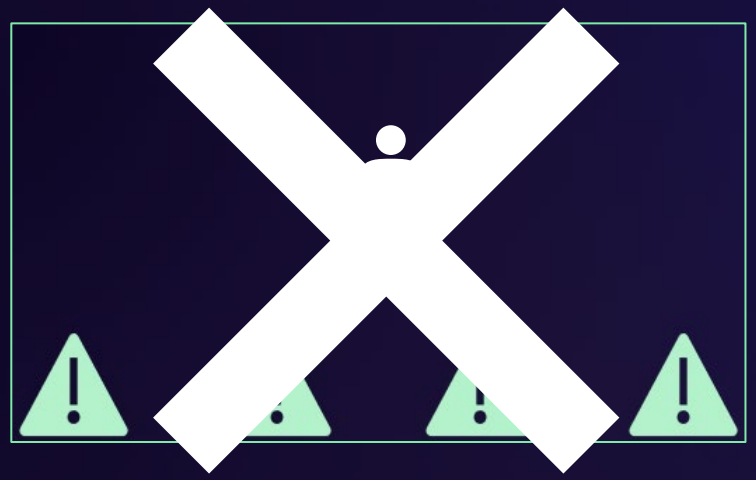
aws

© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

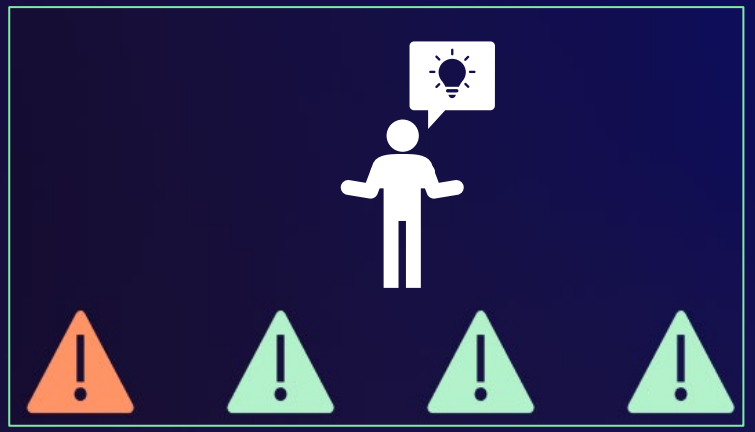
Using anomaly detection to detect security incidents in complex AWS environments is challenging



Looking for anything unusual will result in too much noise



Applying rules to get rid of noise will result in missing the signal



So how do we get rid of the noise without missing the signal?

aws

© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

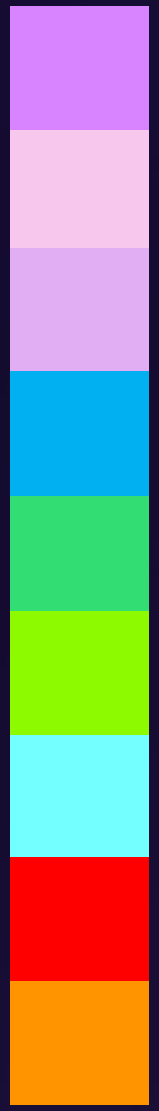
Activity logs

- API activity
- Network activity
- Database access activity
- Compute runtime activity
- Container cluster activity
- And so on

© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Activity logs

- API activity
- Network activity
- Database access activity
- Compute runtime activity
- Container cluster activity
- And so on



© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Activity logs

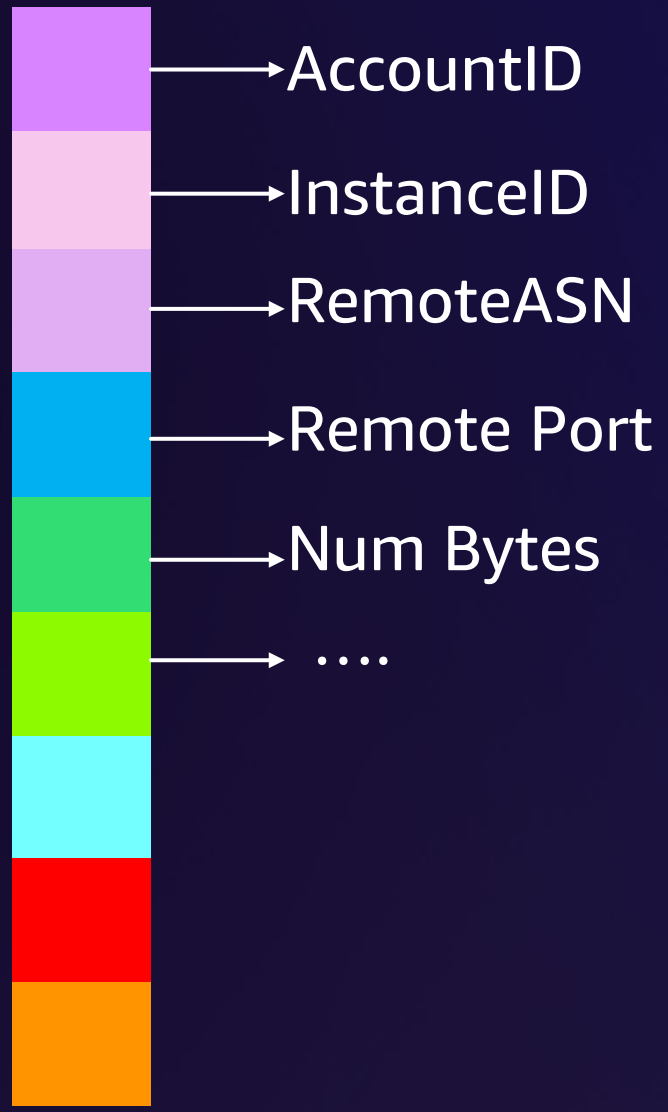
- API activity
- Network activity
- Database access activity
- Compute runtime activity
- Container cluster activity
- And so on



aws
© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

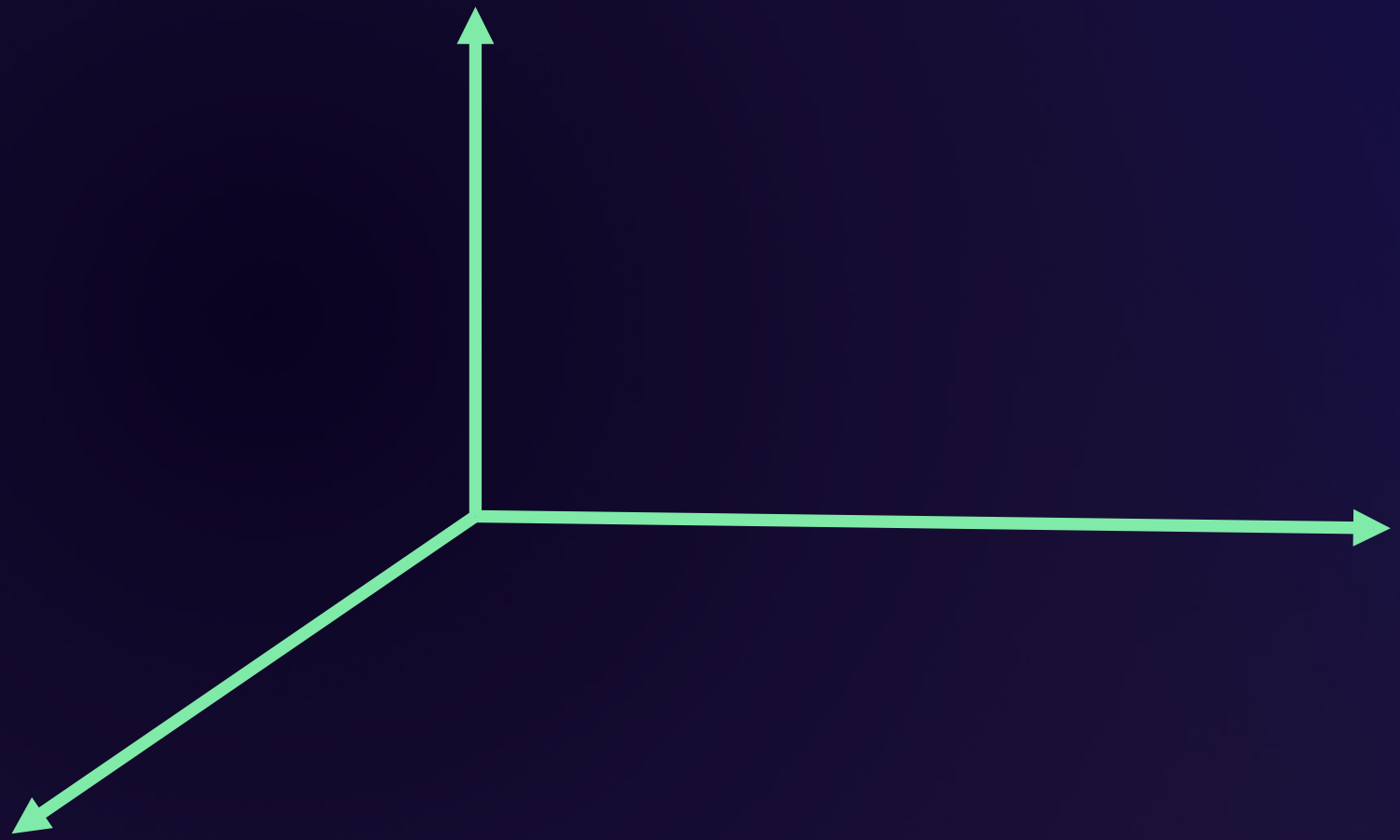
Activity logs

- API activity
- Network activity
- Database access activity
- Compute runtime activity
- Container cluster activity
- And so on



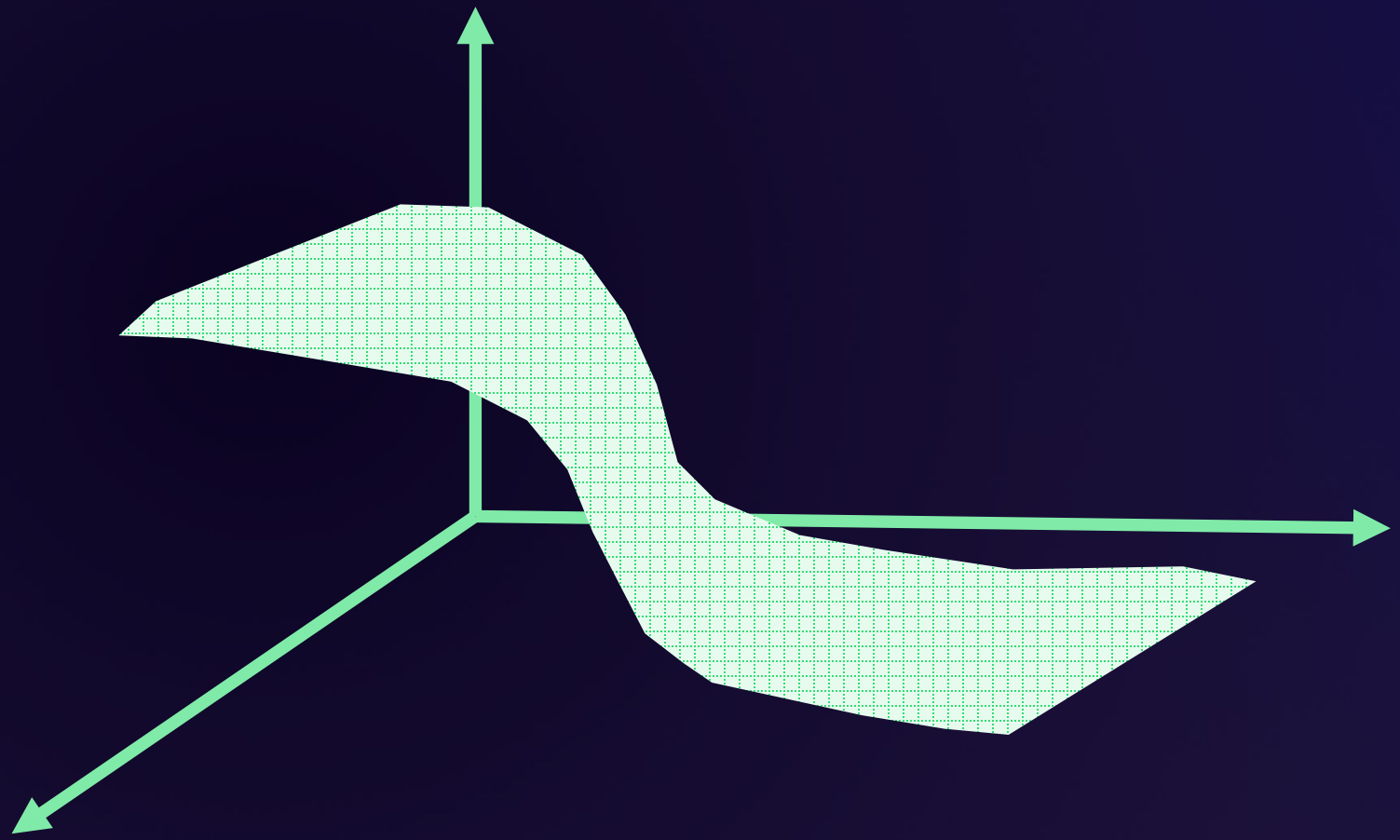
aws
© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Region of normality



© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Region of normality

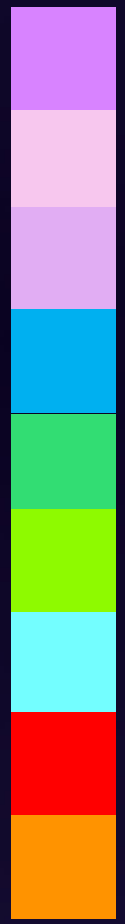


© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

The model

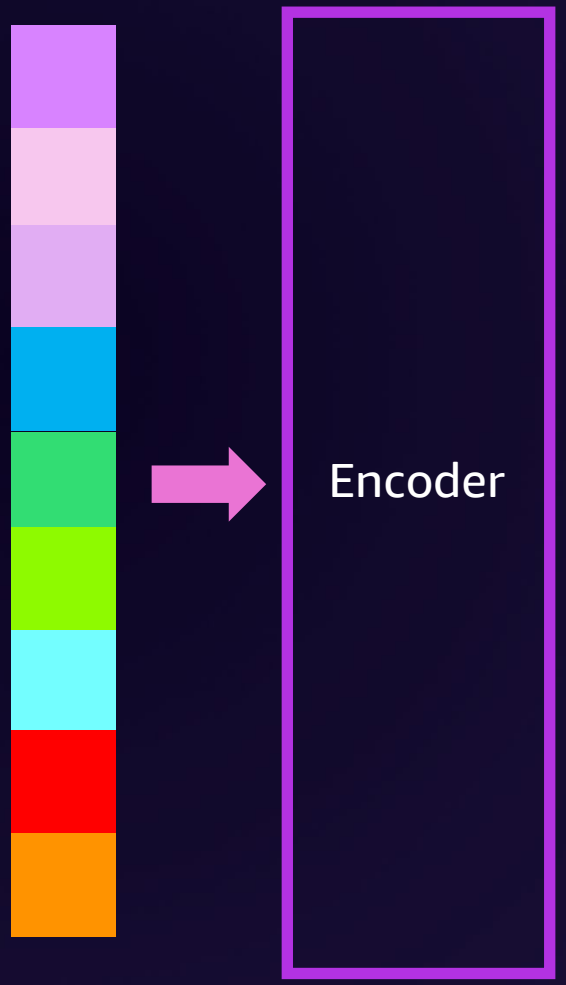
© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

The model



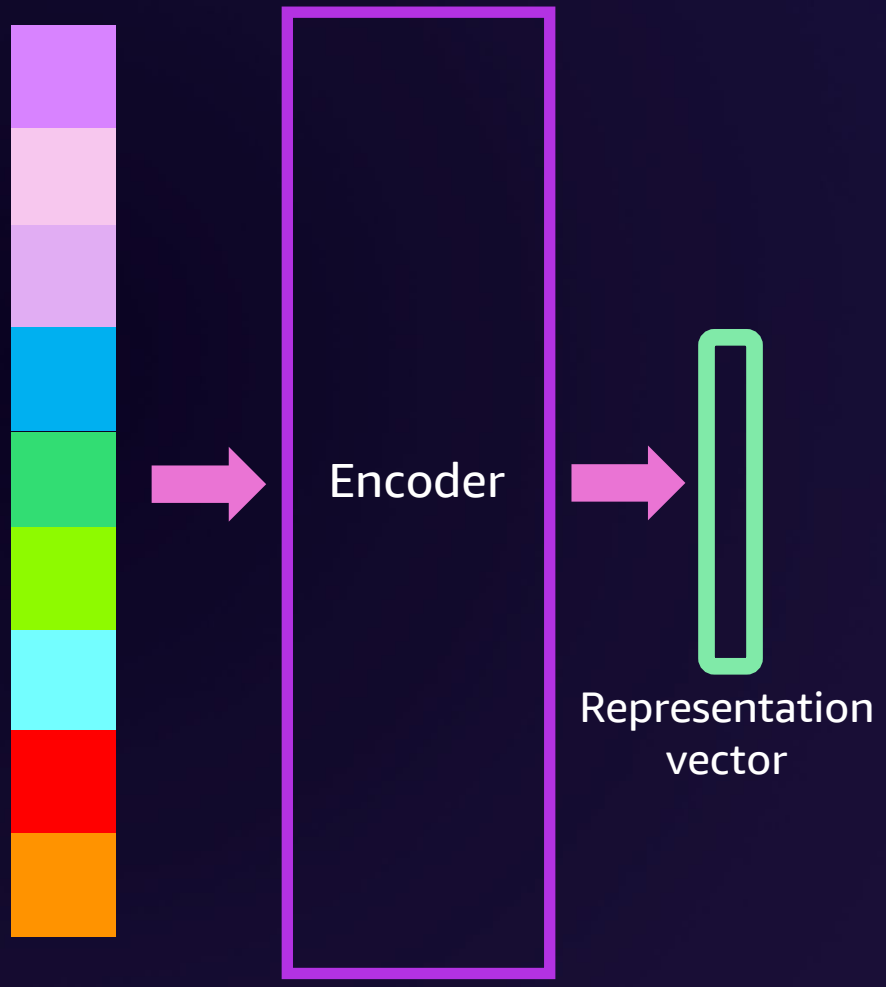
© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

The model



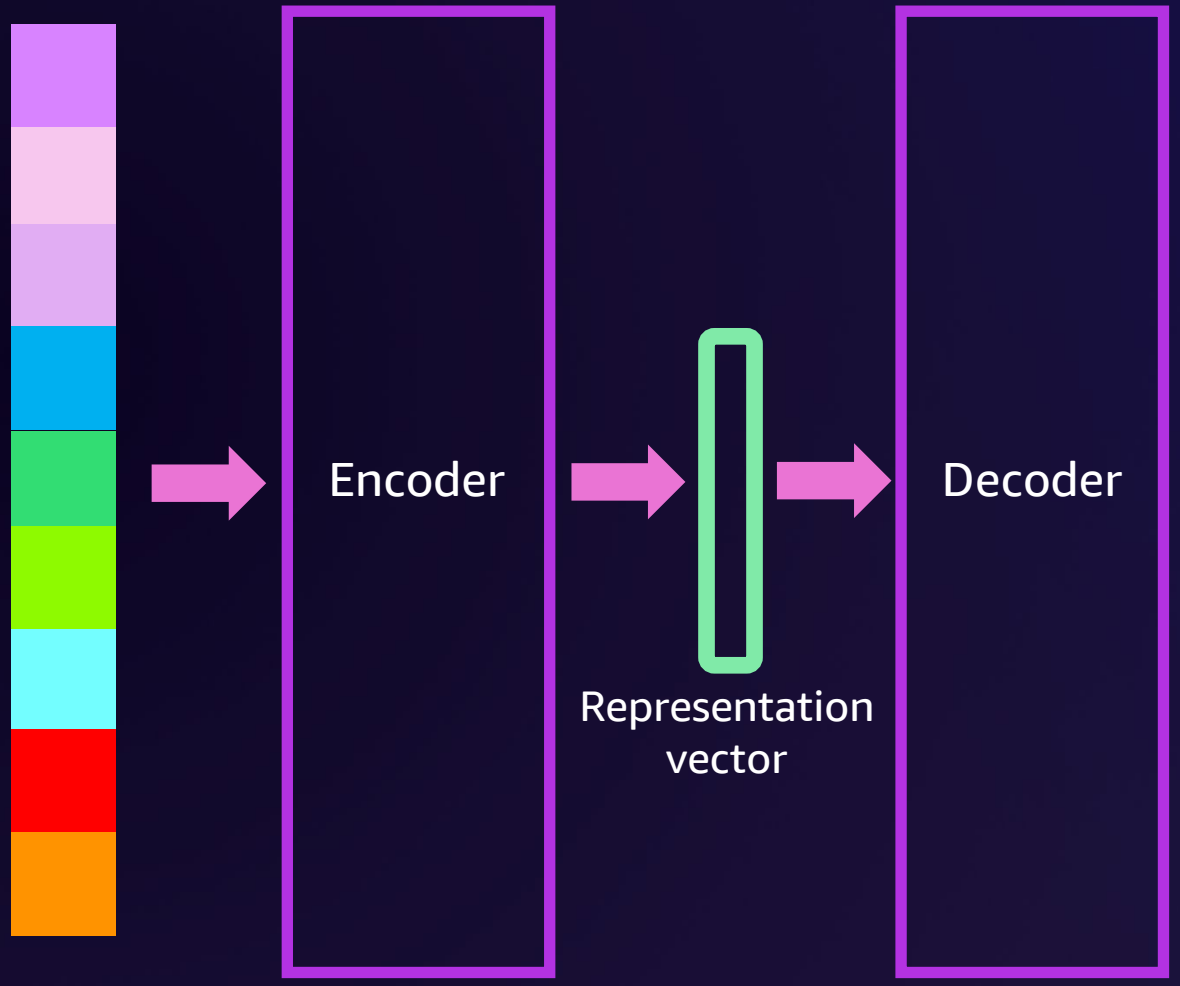
© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

The model



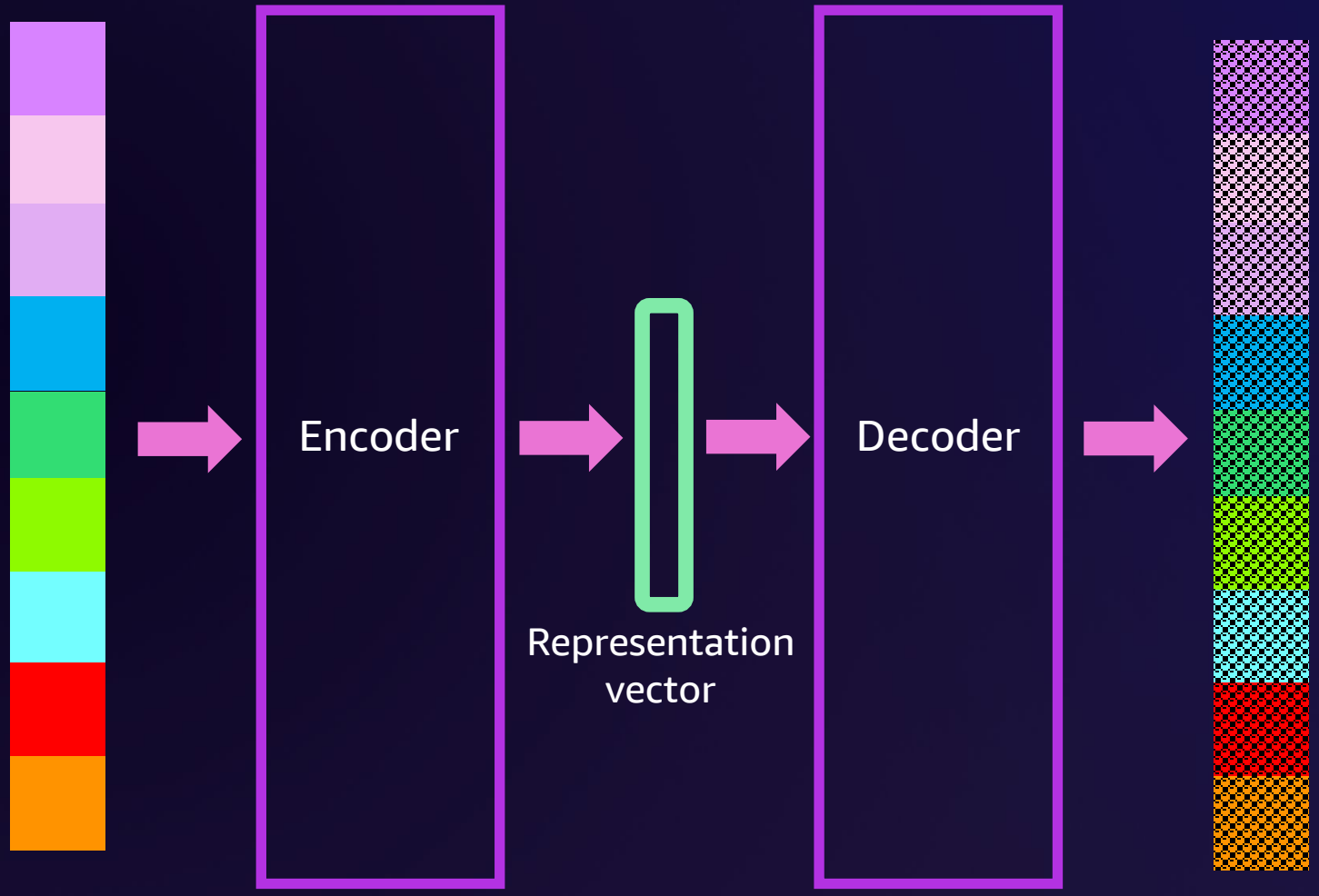
aws
© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

The model



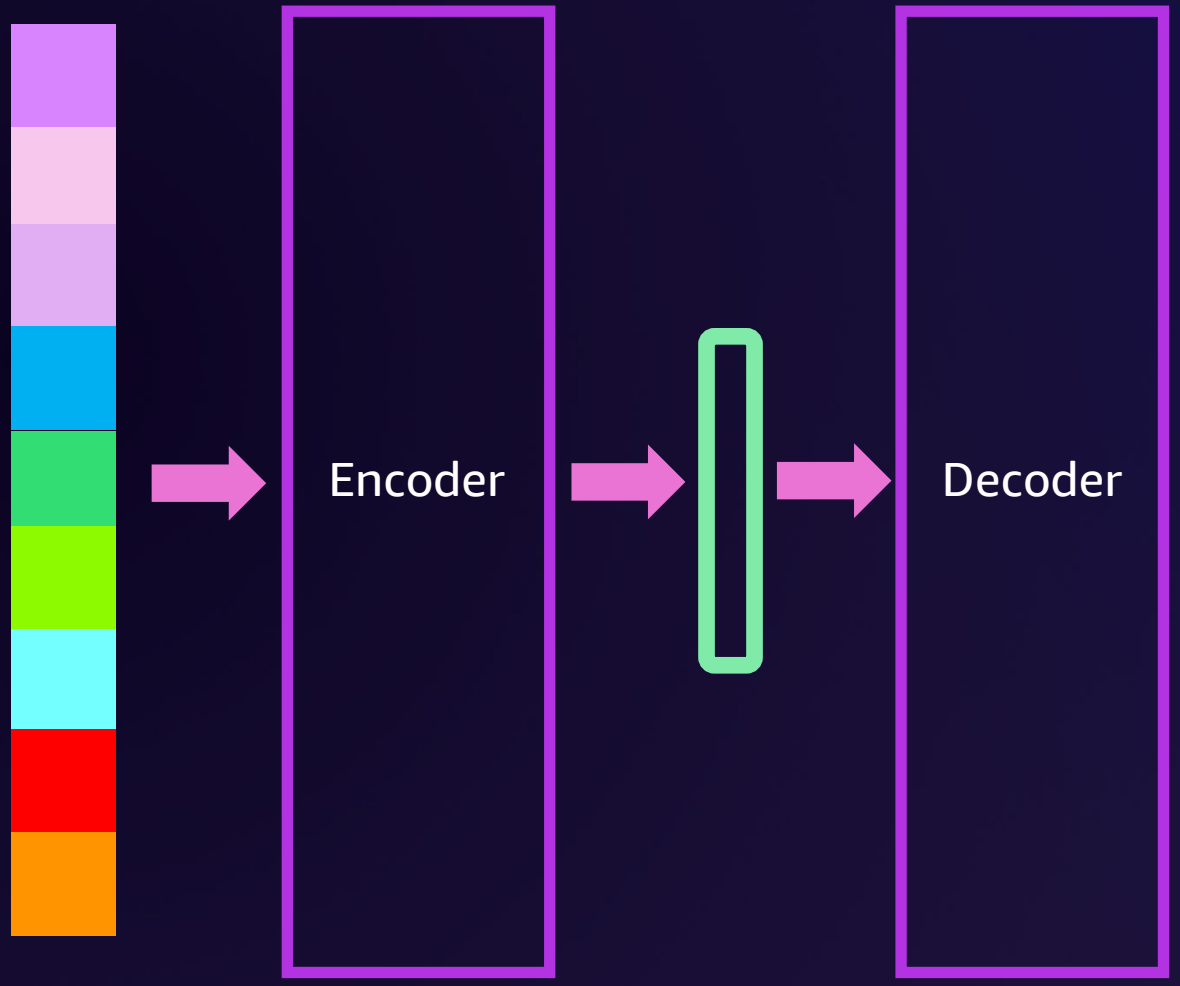
aws
© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

The model



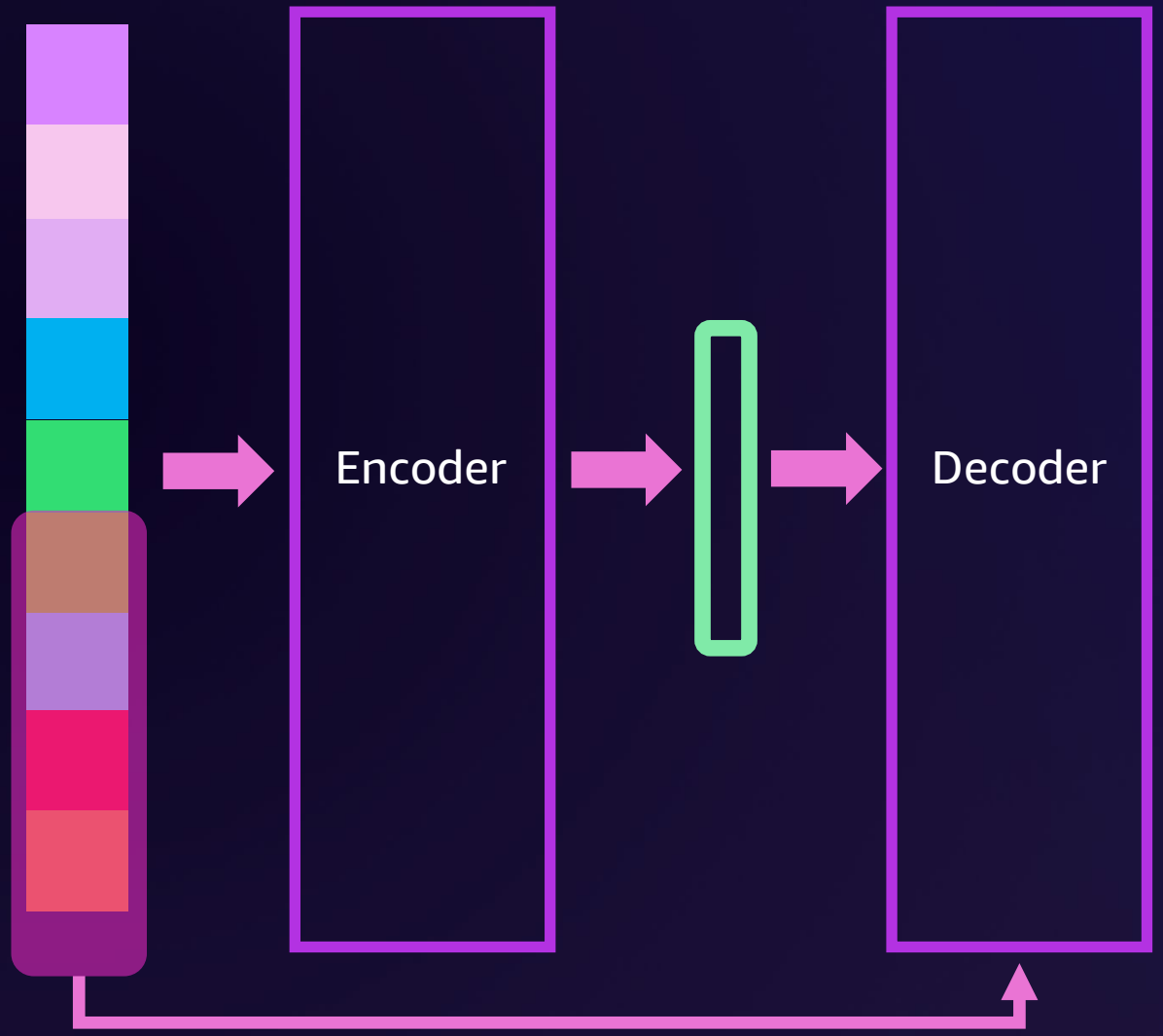
aws
© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

The conditional model



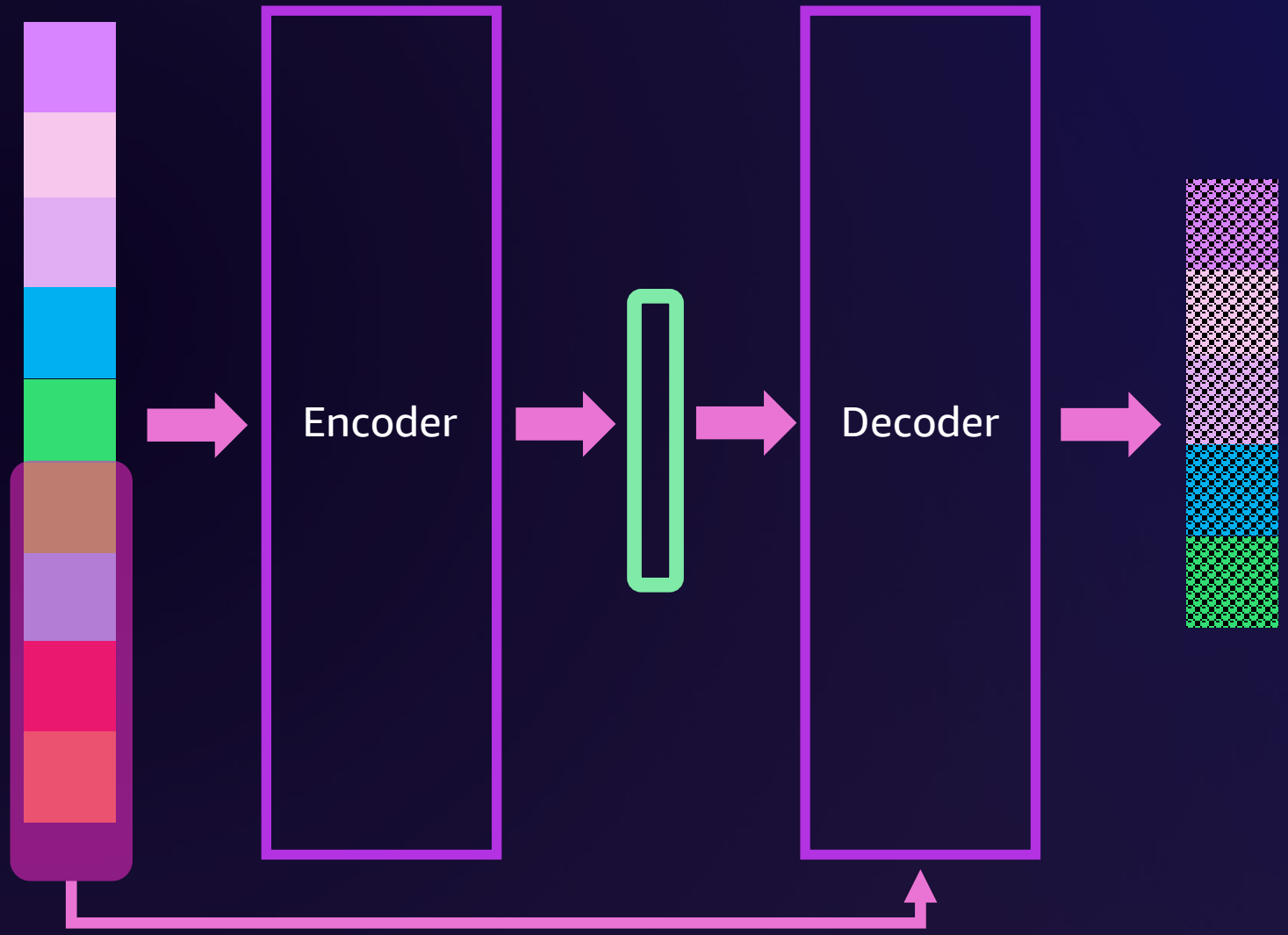
© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

The conditional model



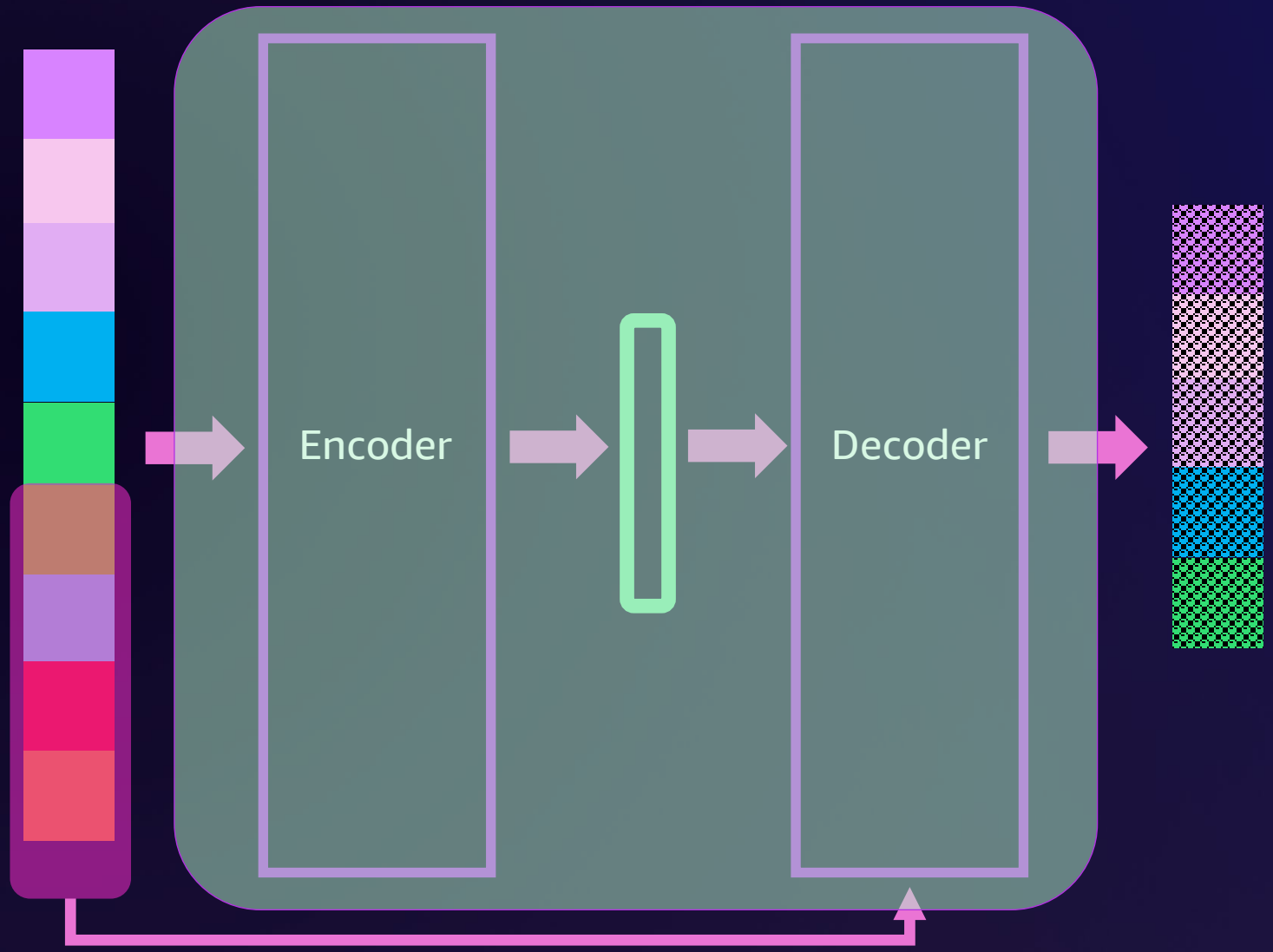
© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

The conditional model



© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

The conditional model



© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Training



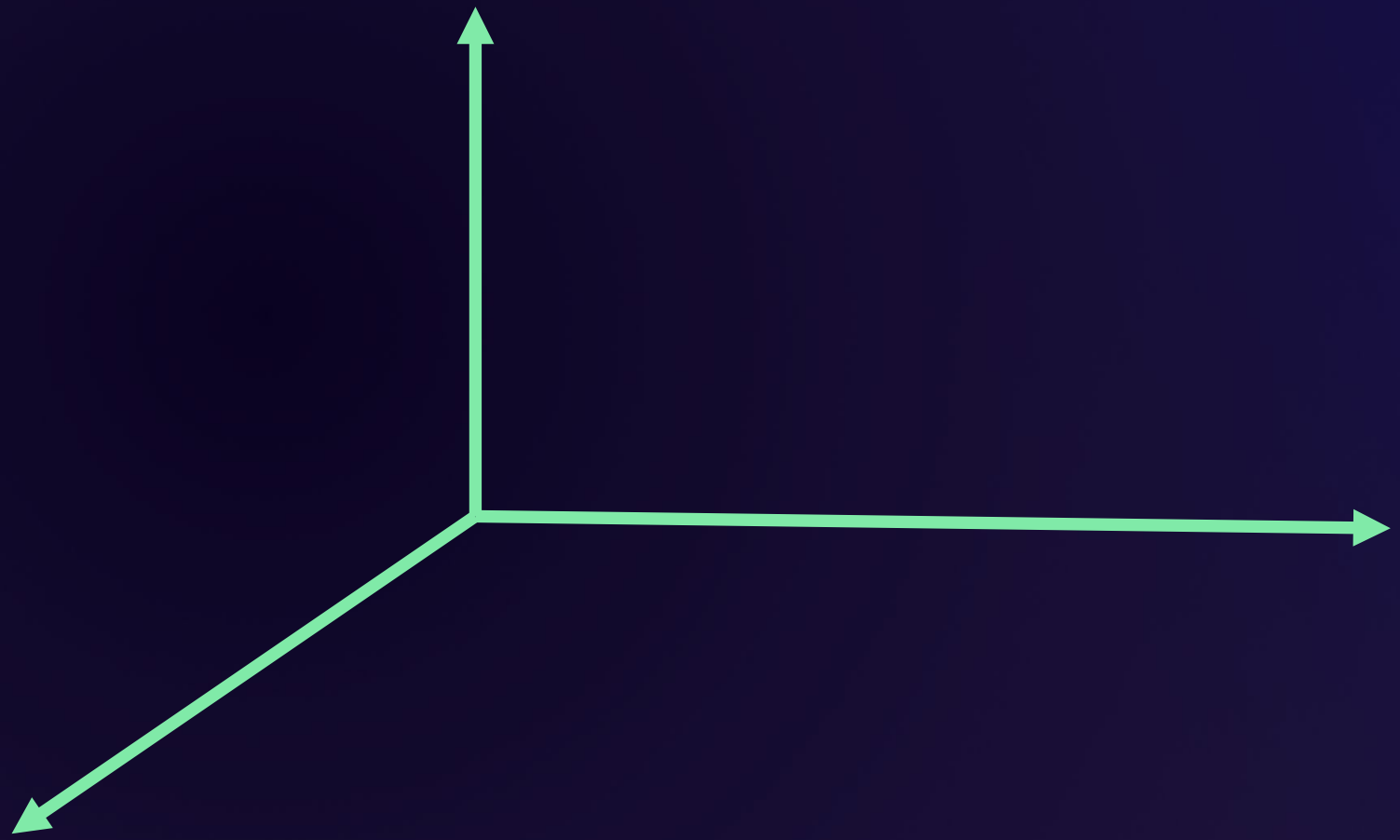
© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Training



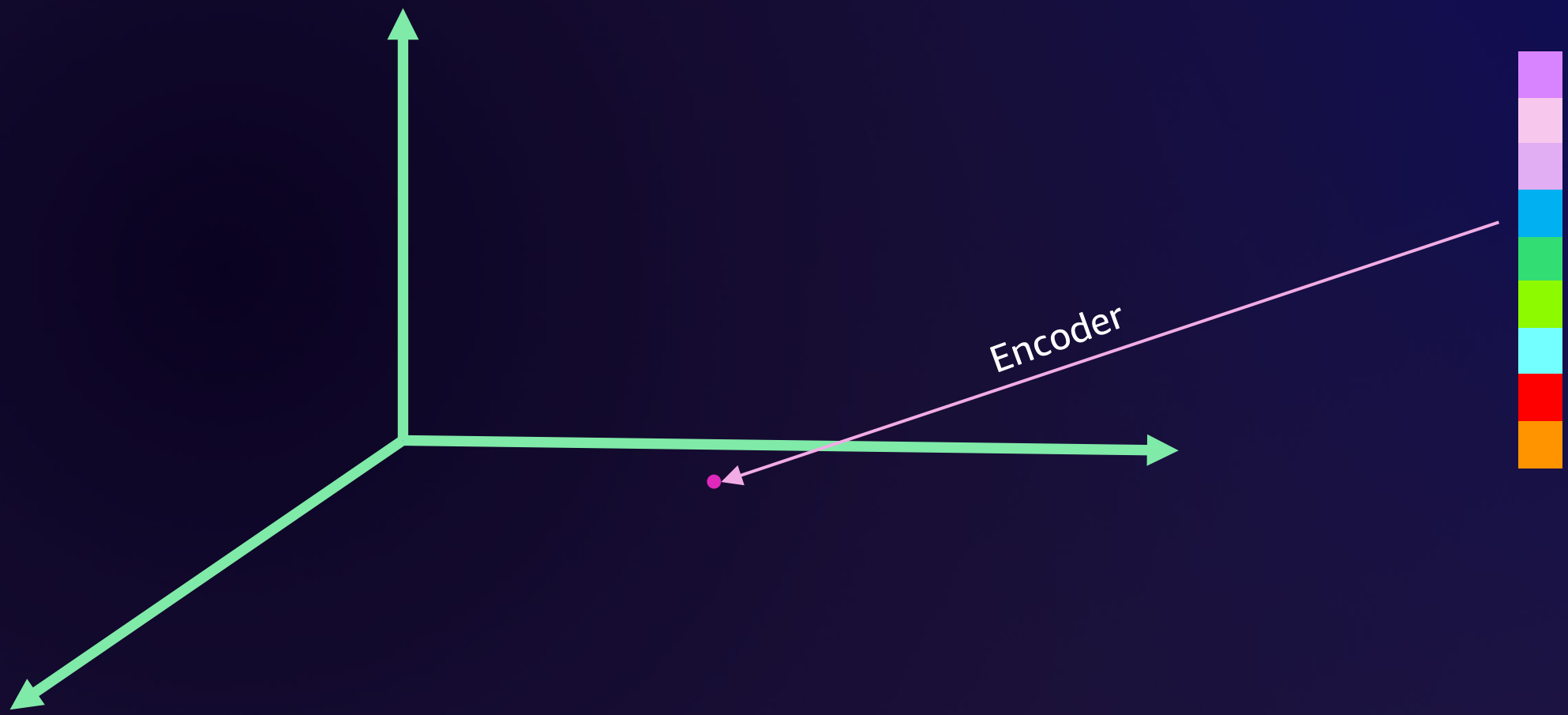
© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Learning normal activity



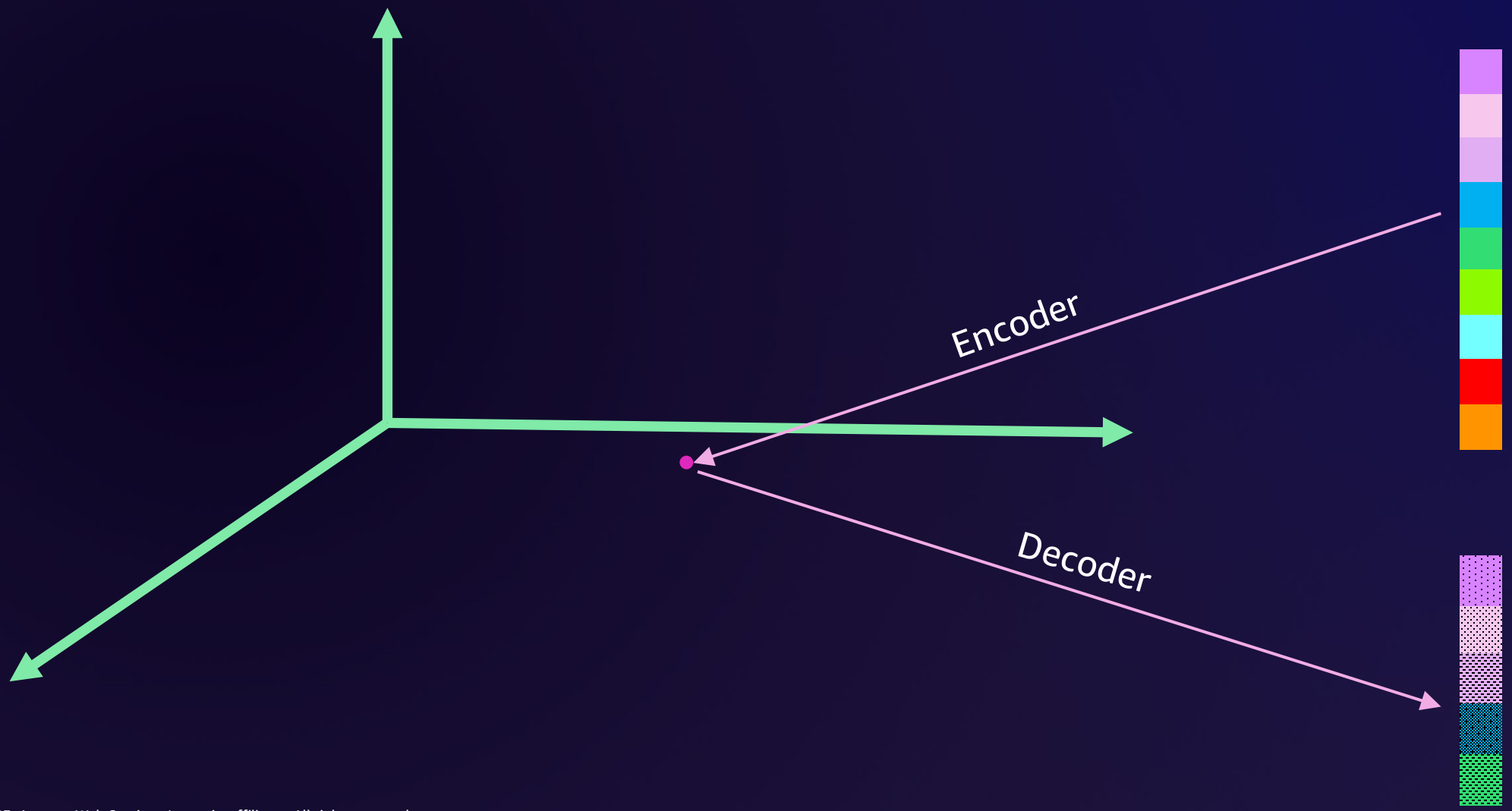
© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Learning normal activity



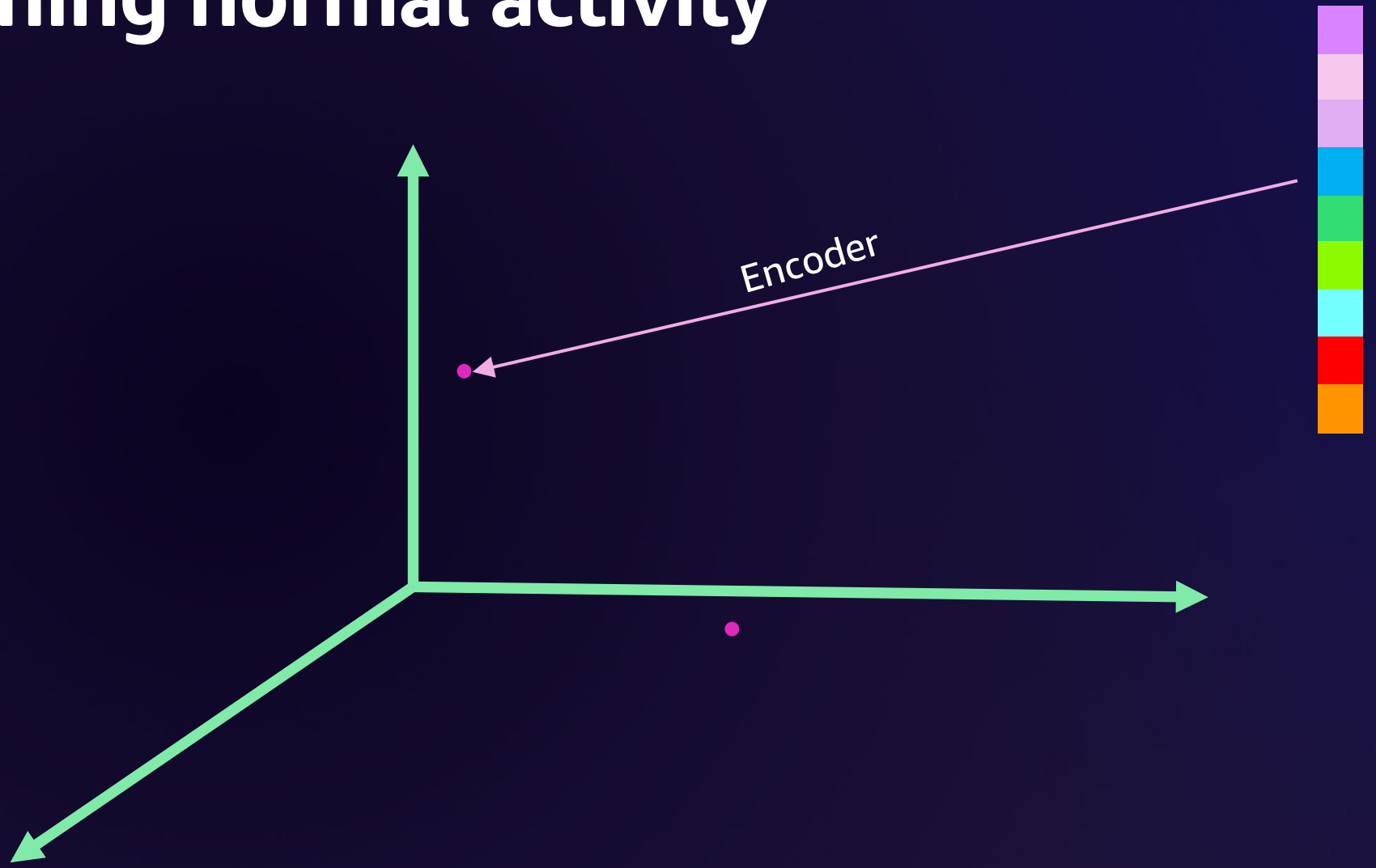
© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Learning normal activity



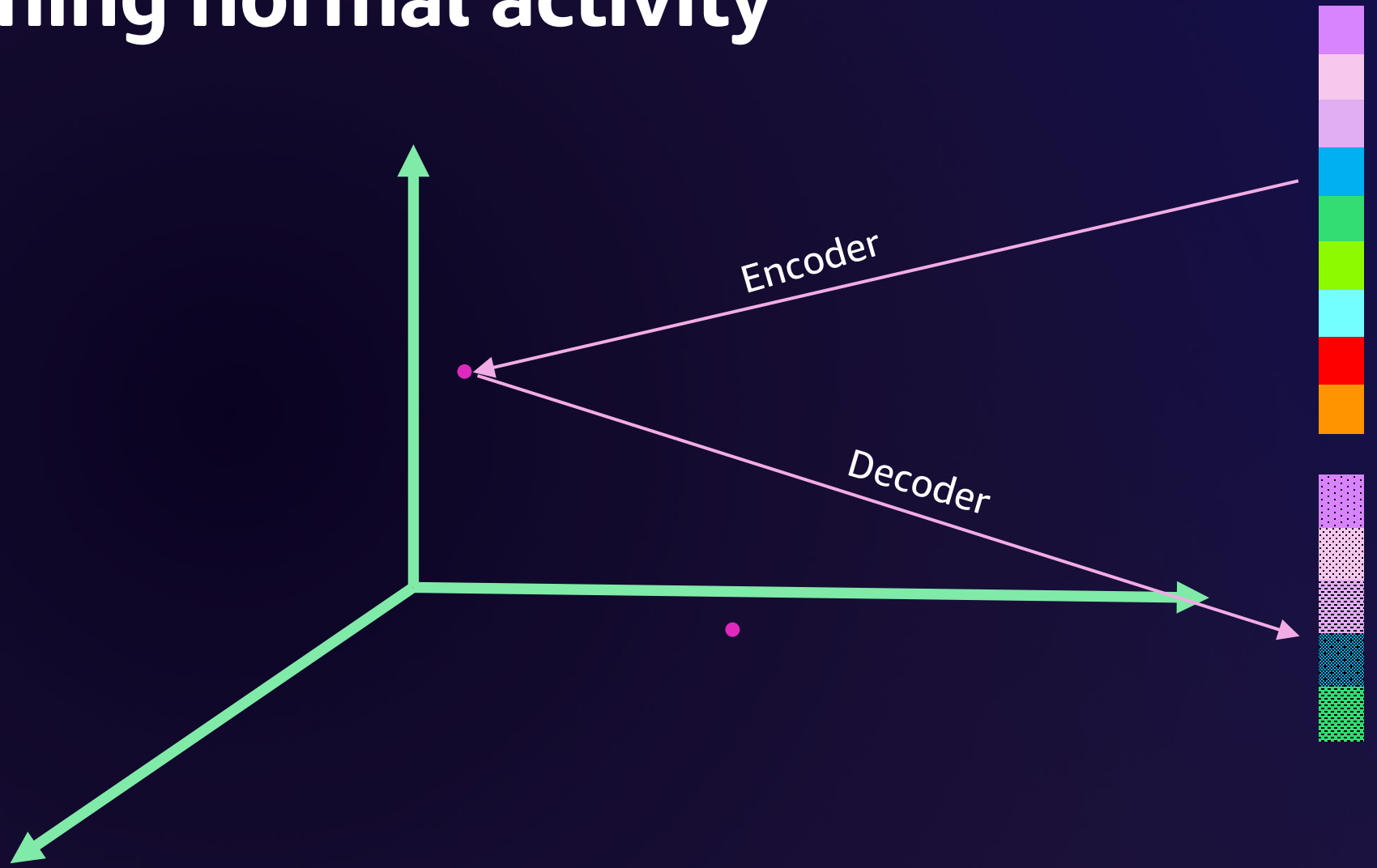
© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Learning normal activity



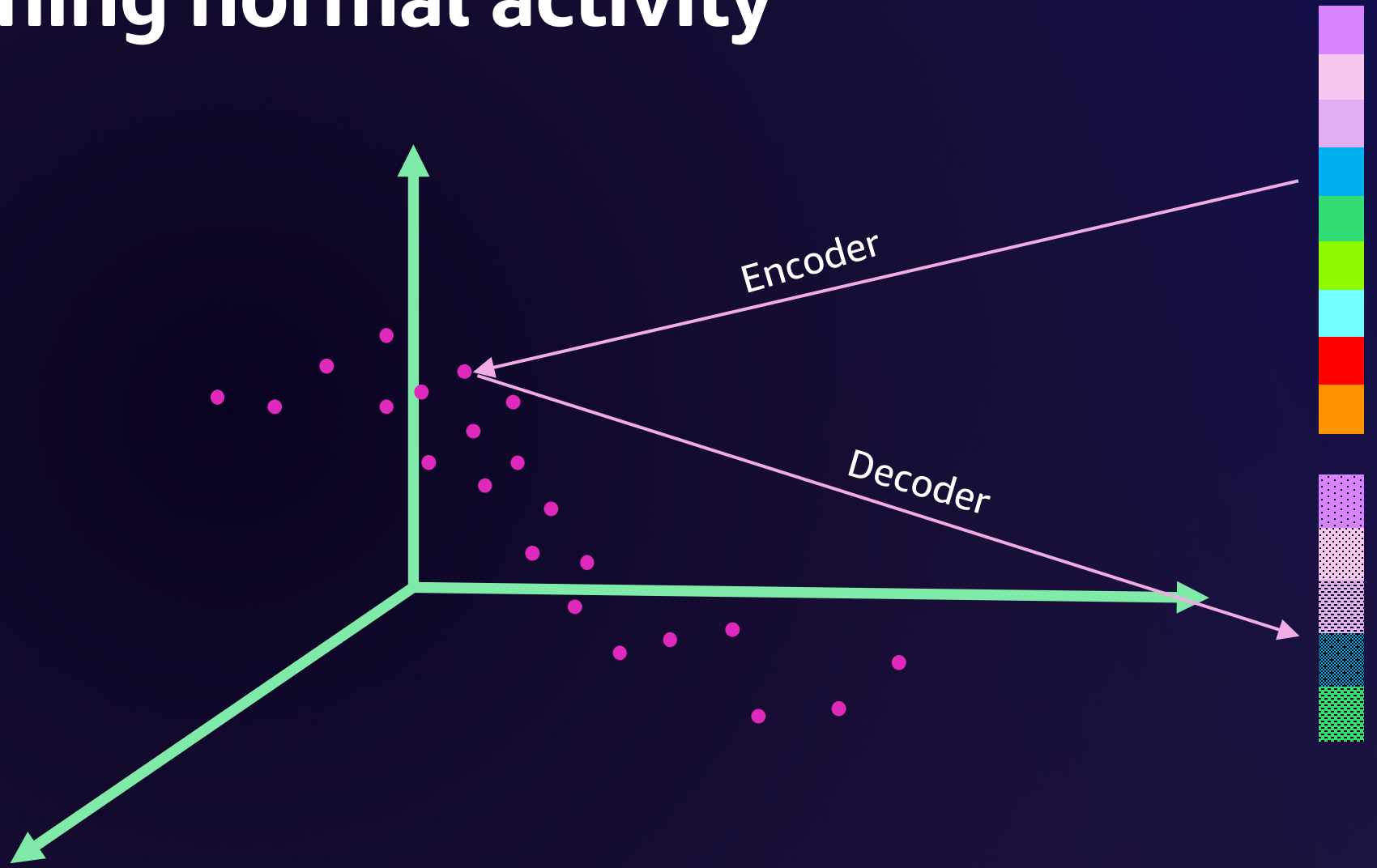
© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Learning normal activity



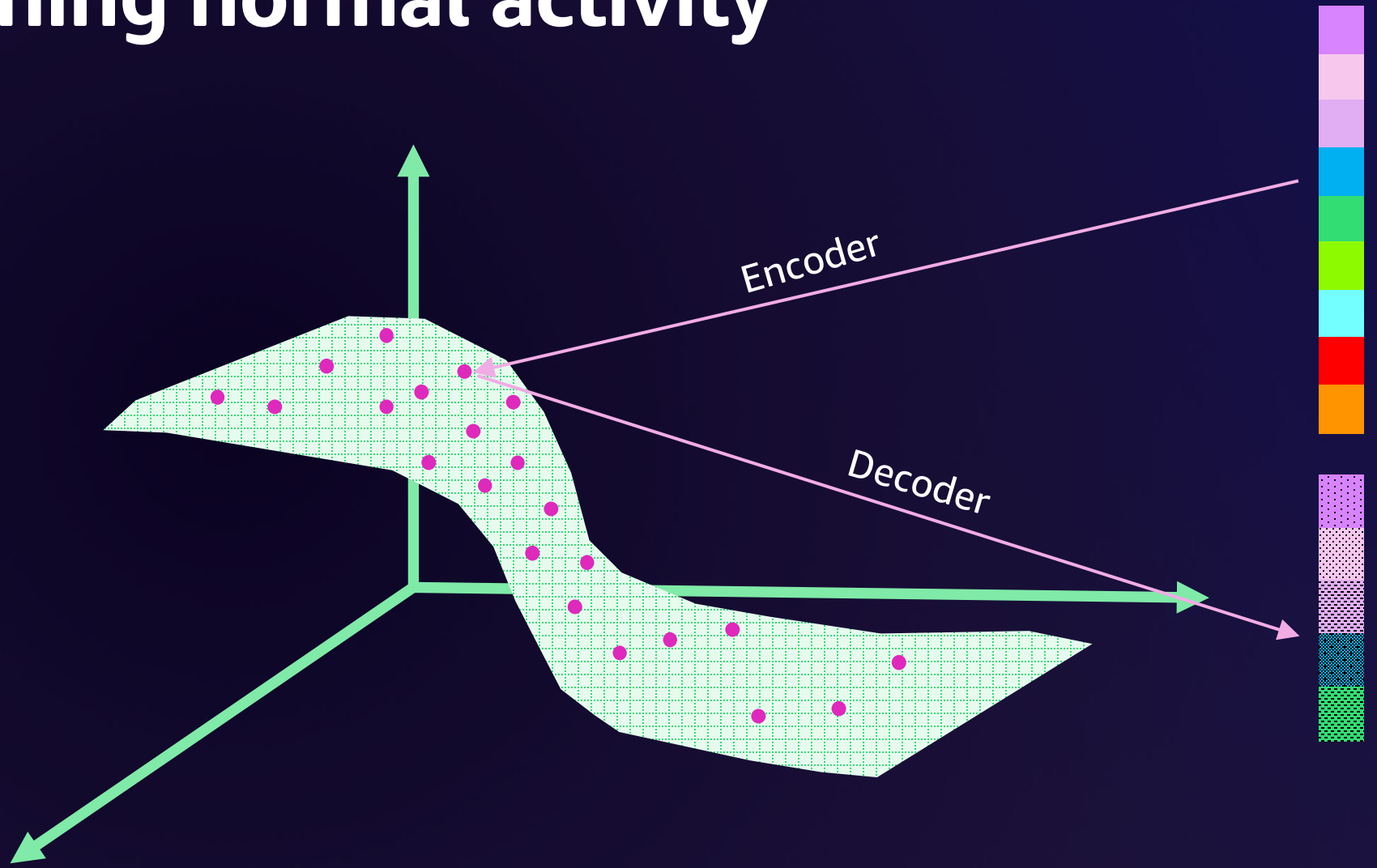
© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Learning normal activity



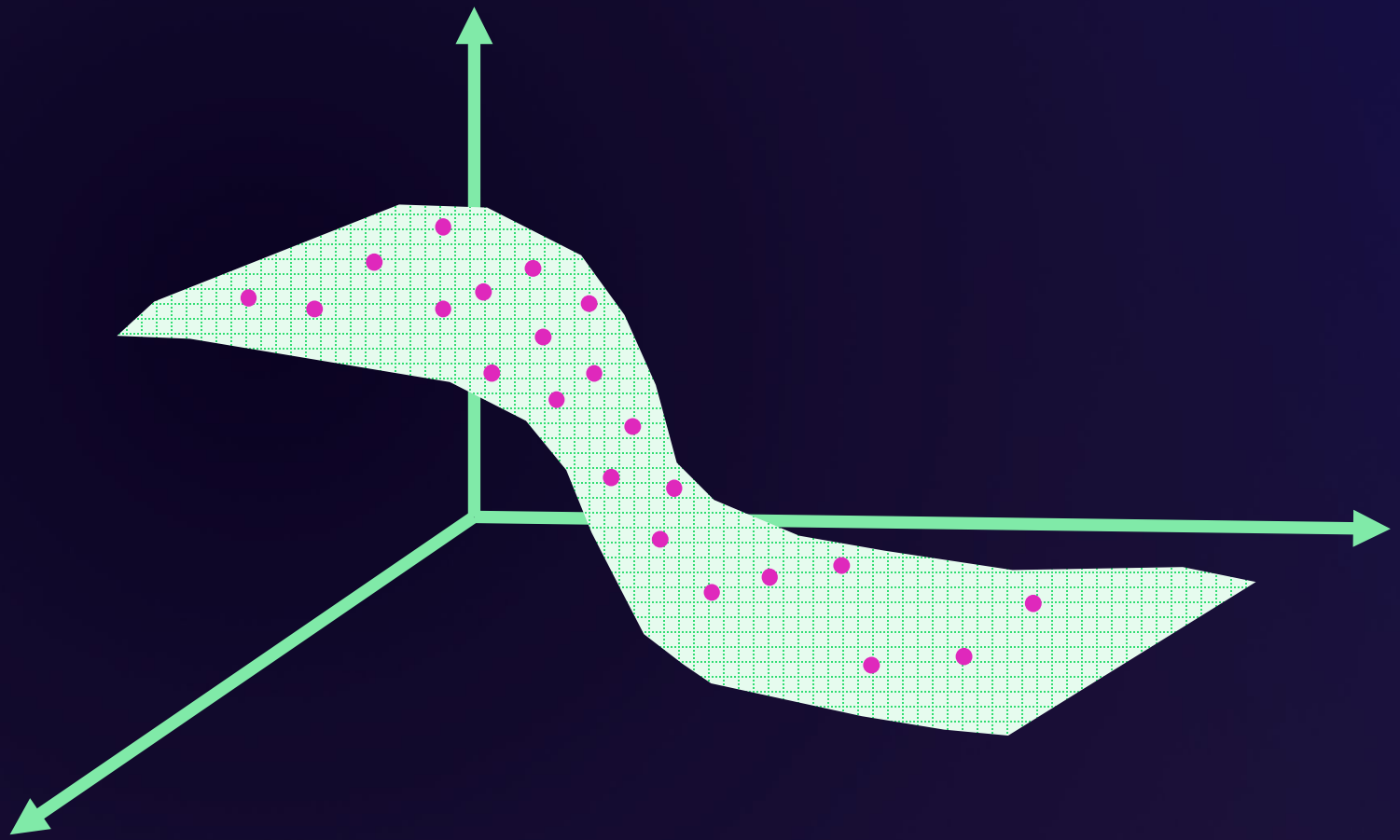
© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Learning normal activity



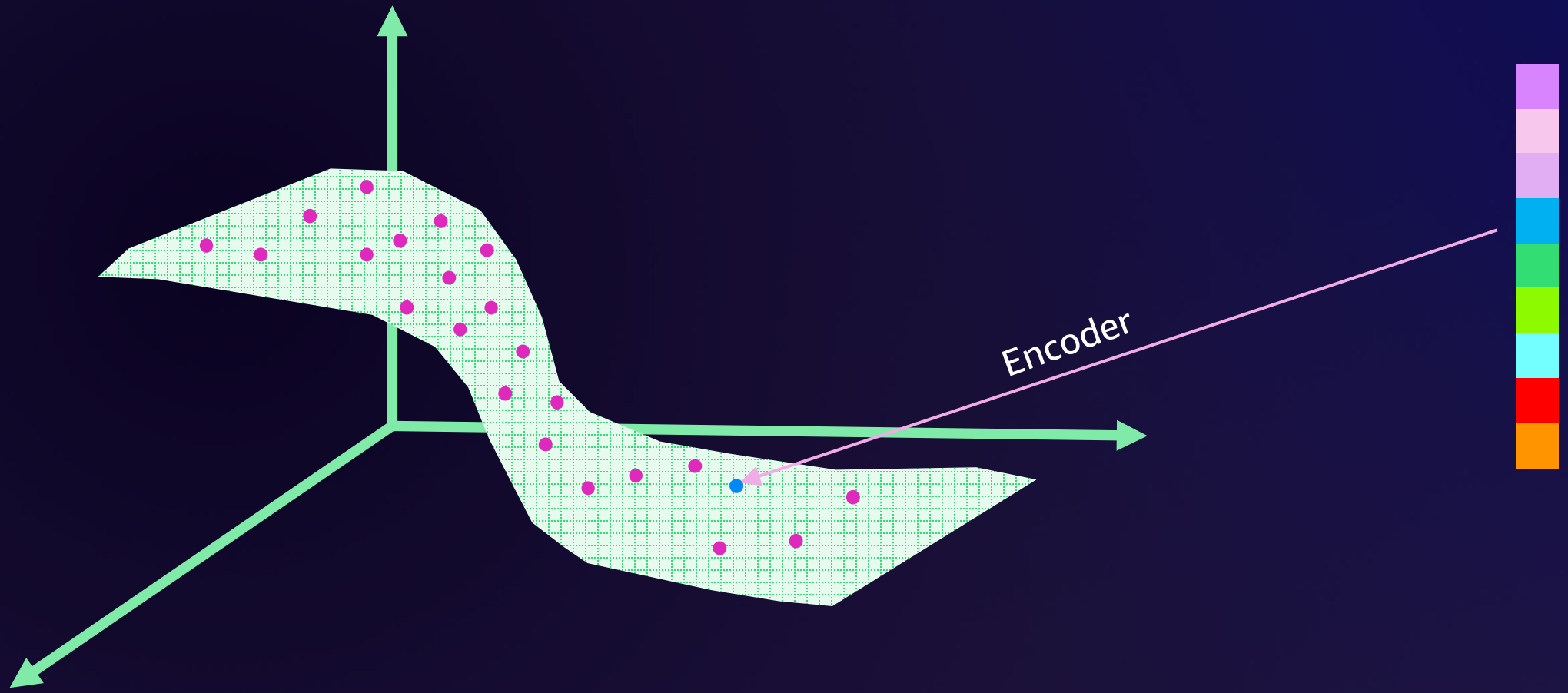
aws
© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Normal activity



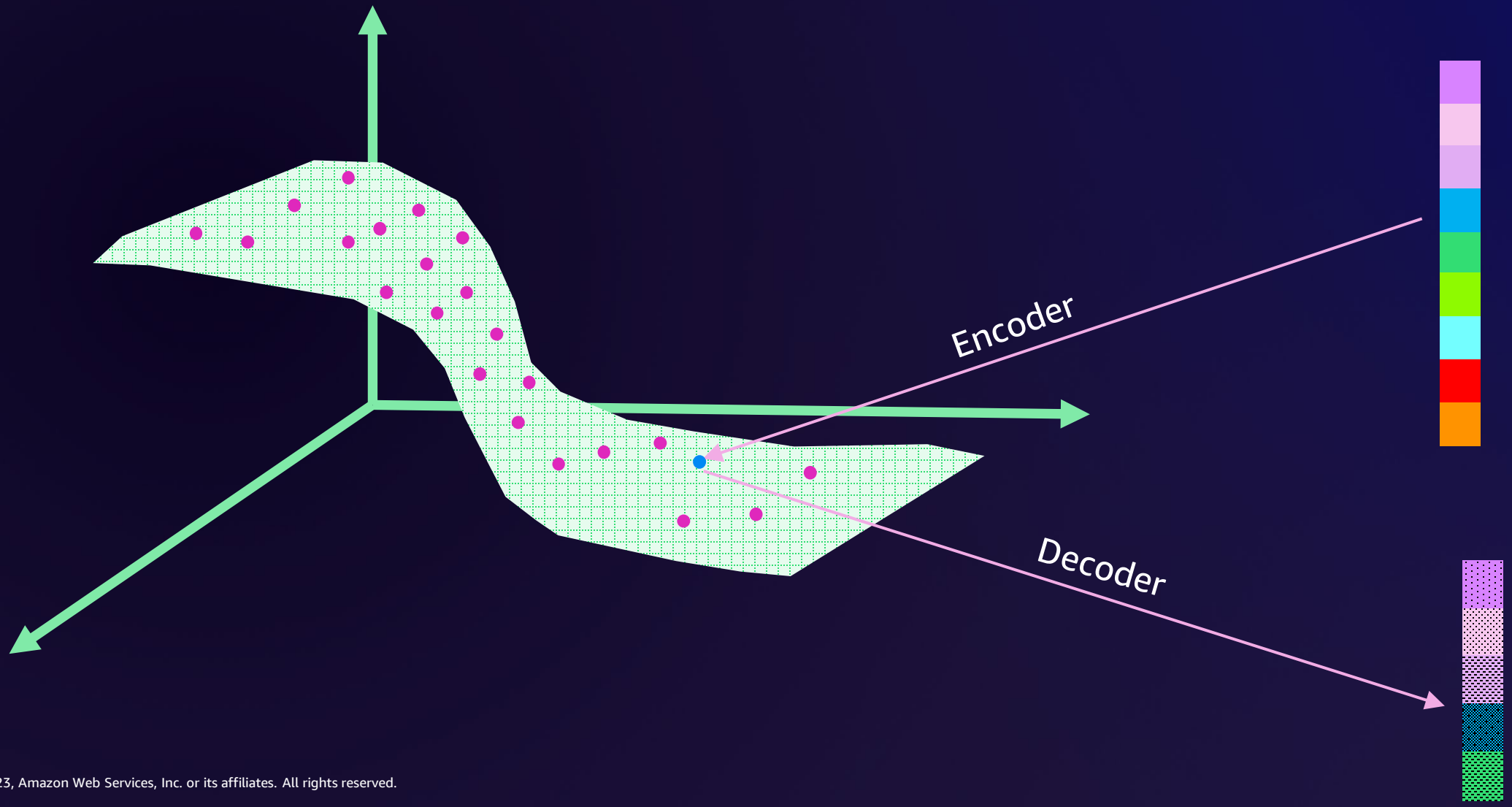
© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Normal activity



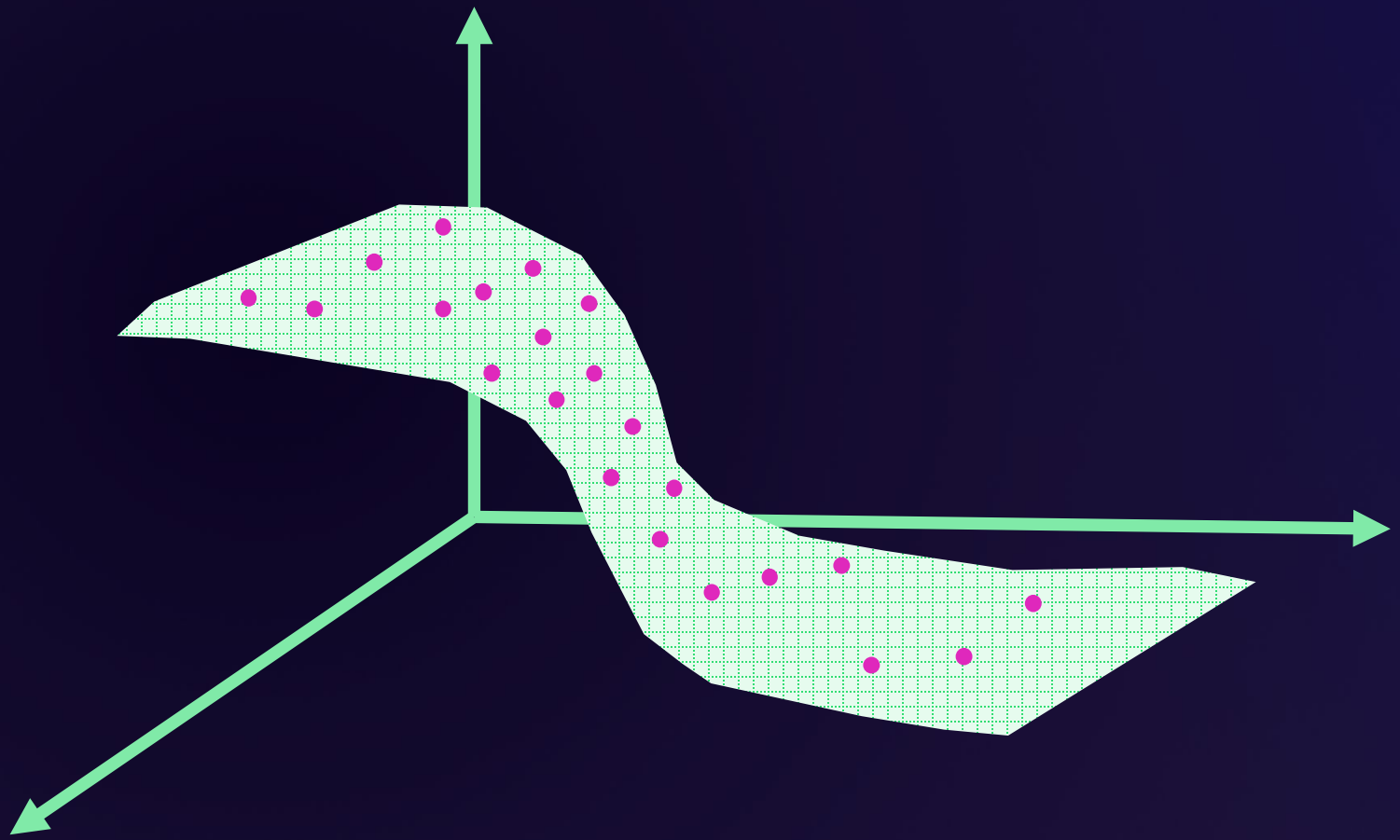
© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Normal activity



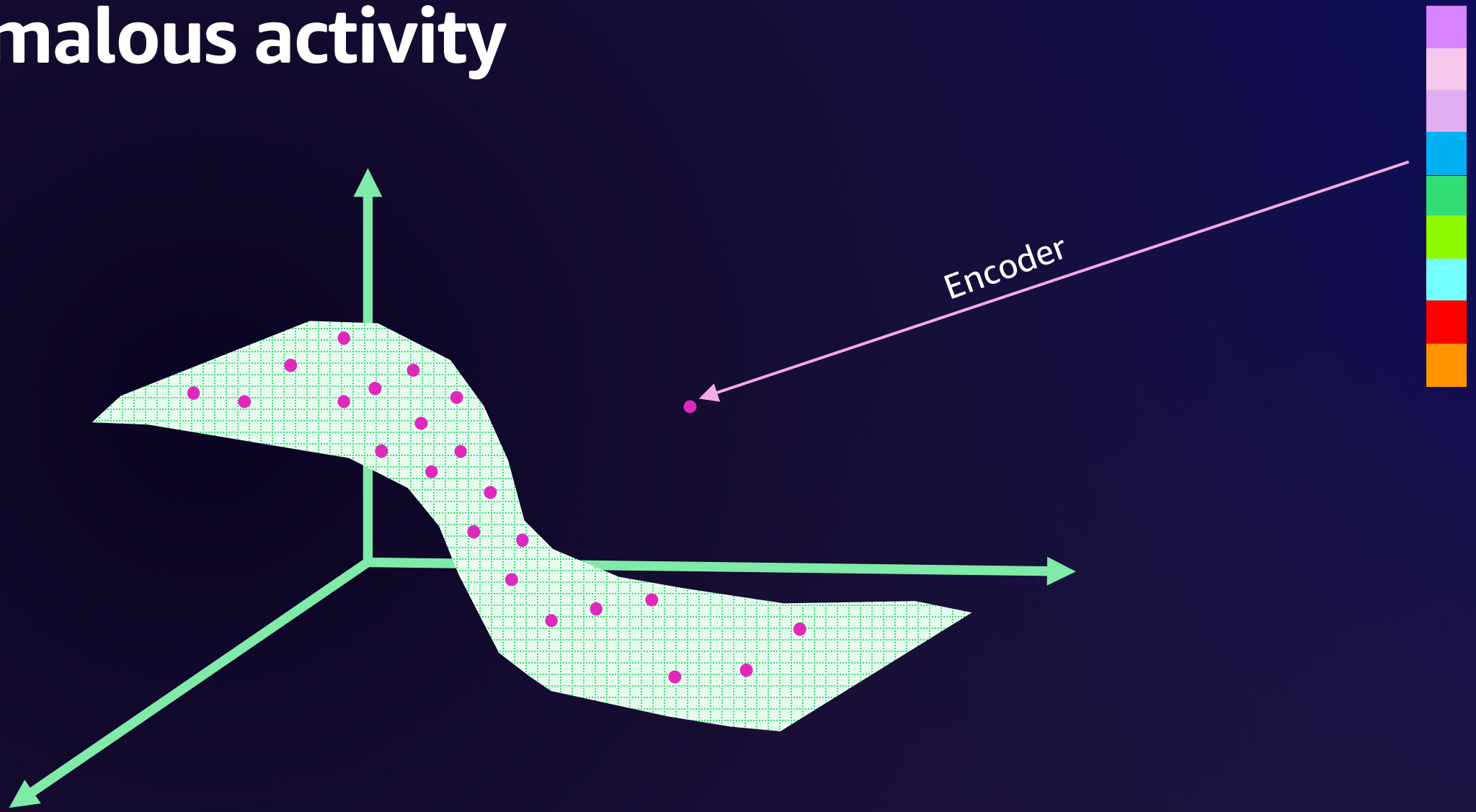
© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Anomalous activity



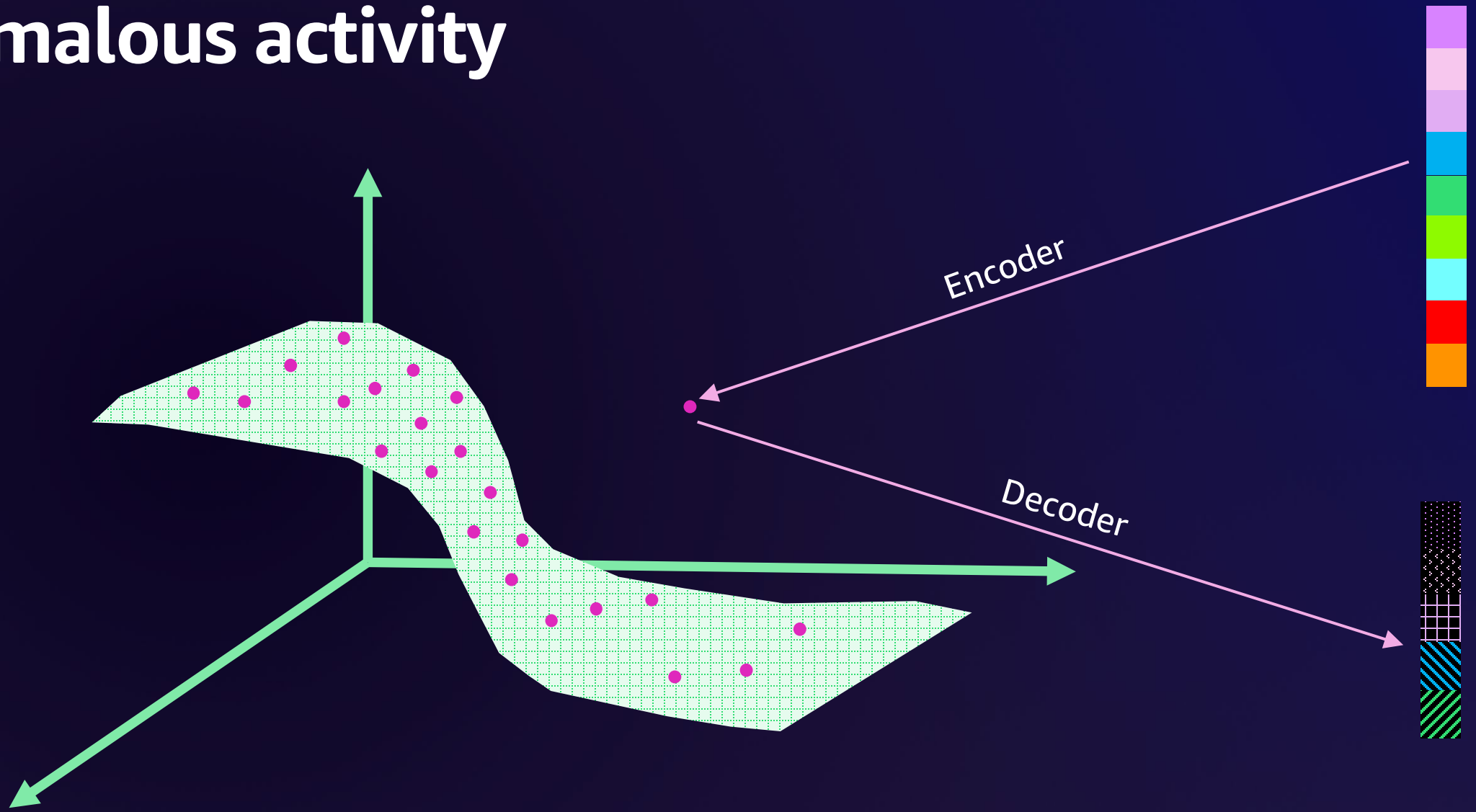
© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Anomalous activity



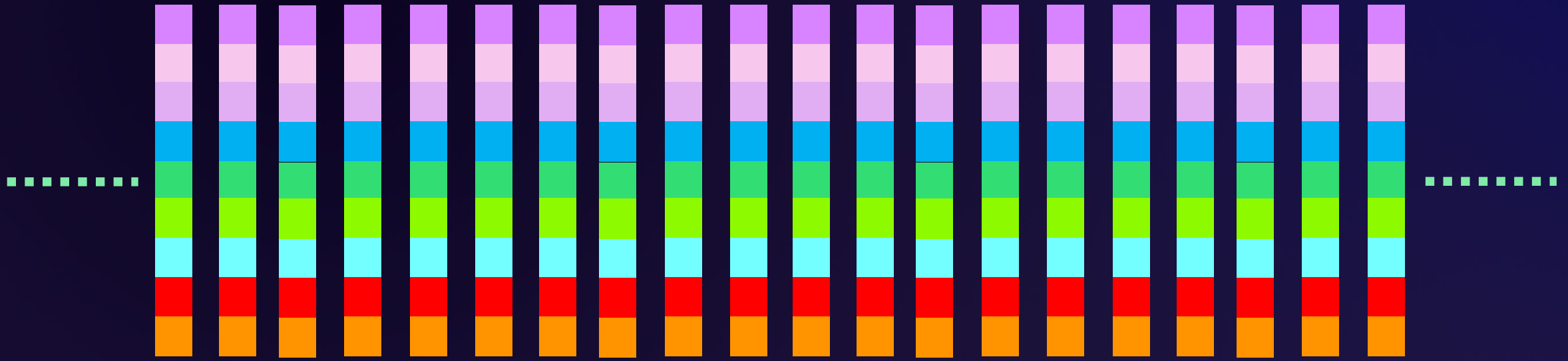
© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Anomalous activity



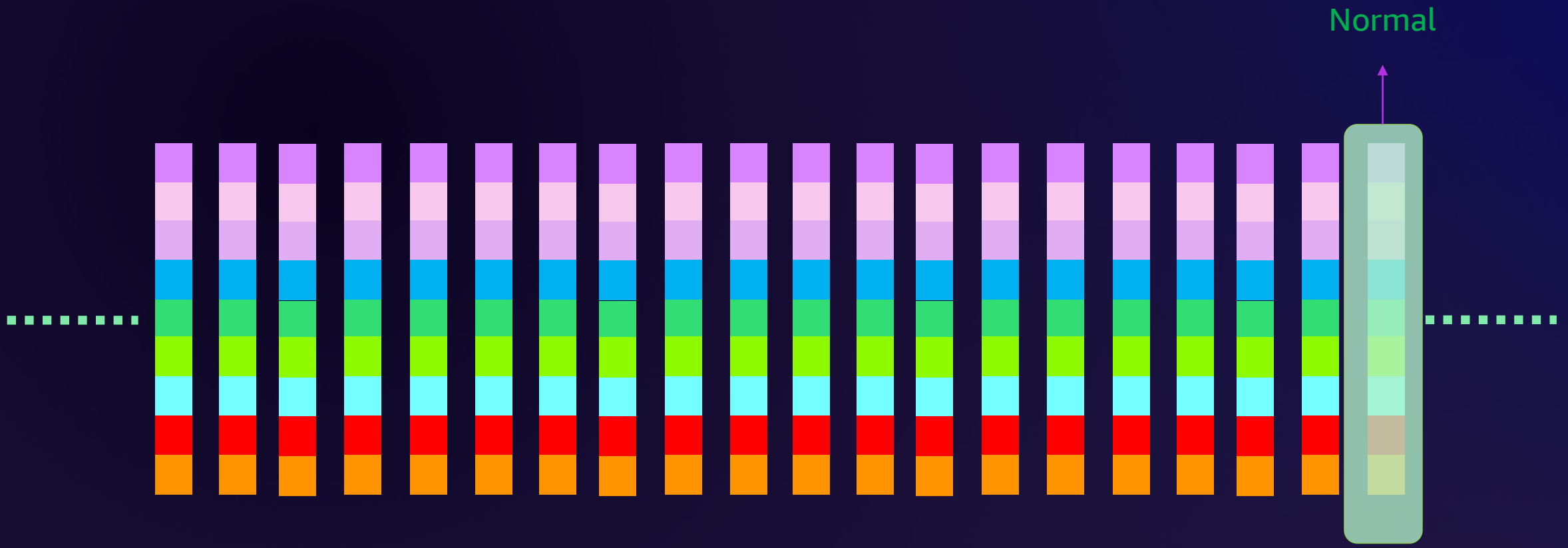
aws
© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Inference



© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

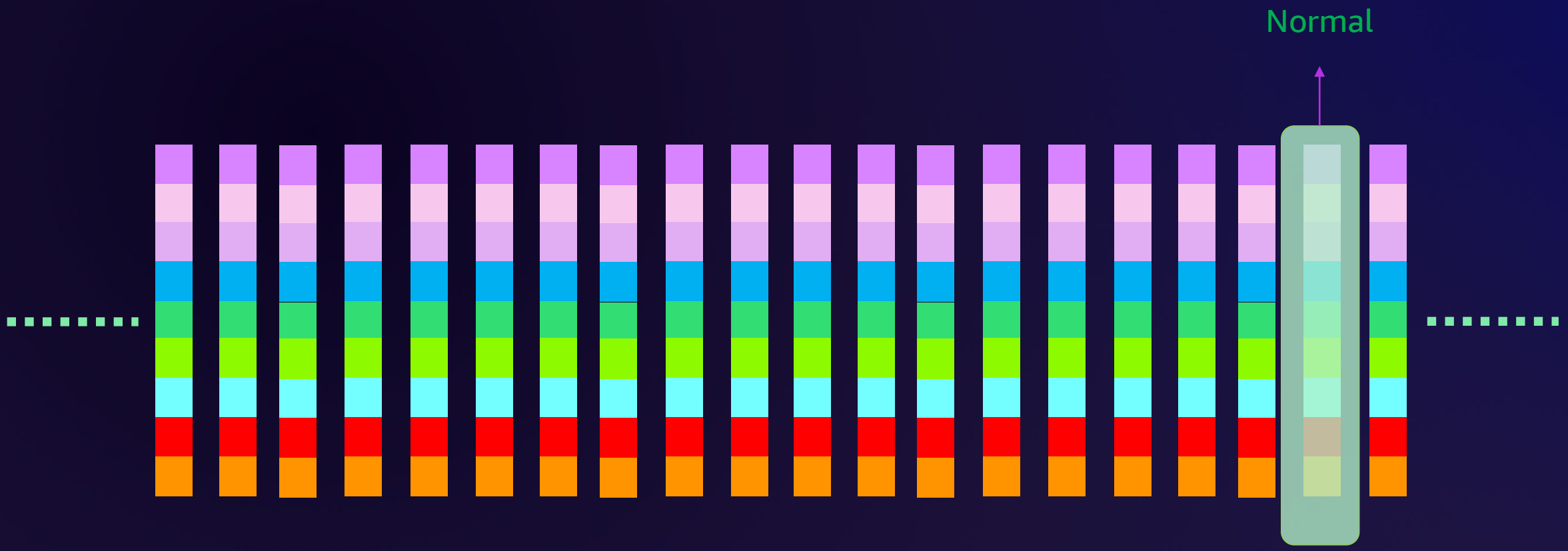
Inference



aws

© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

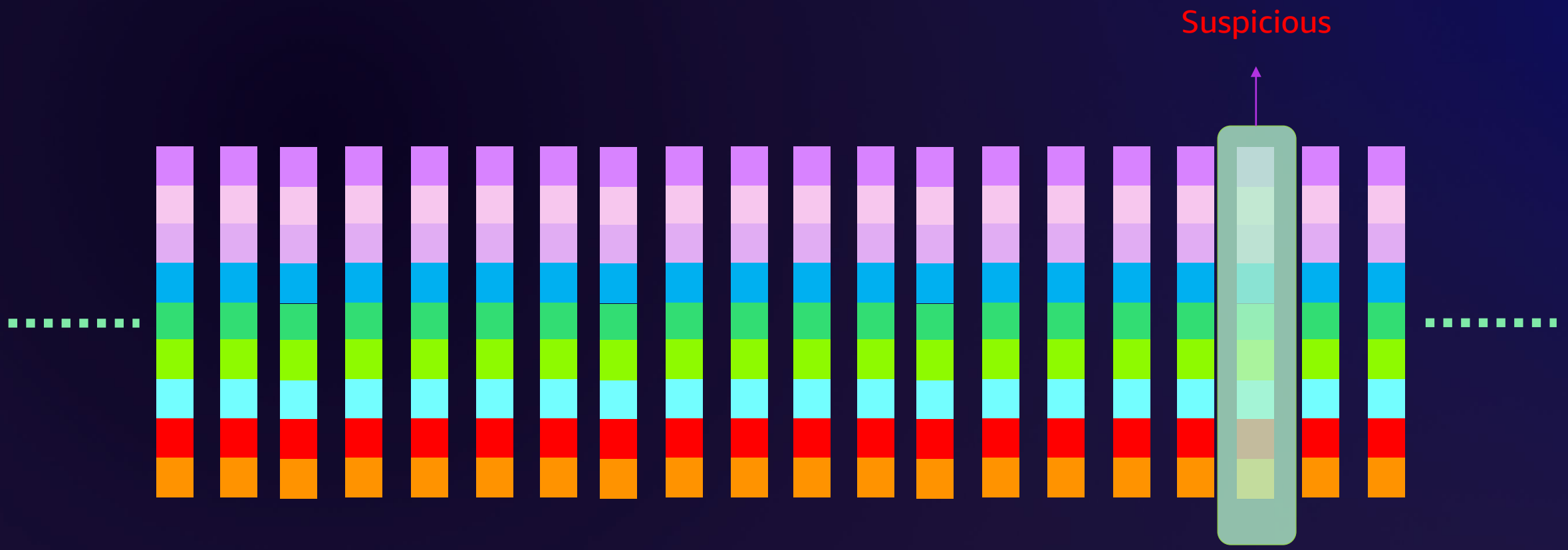
Inference



aws

© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

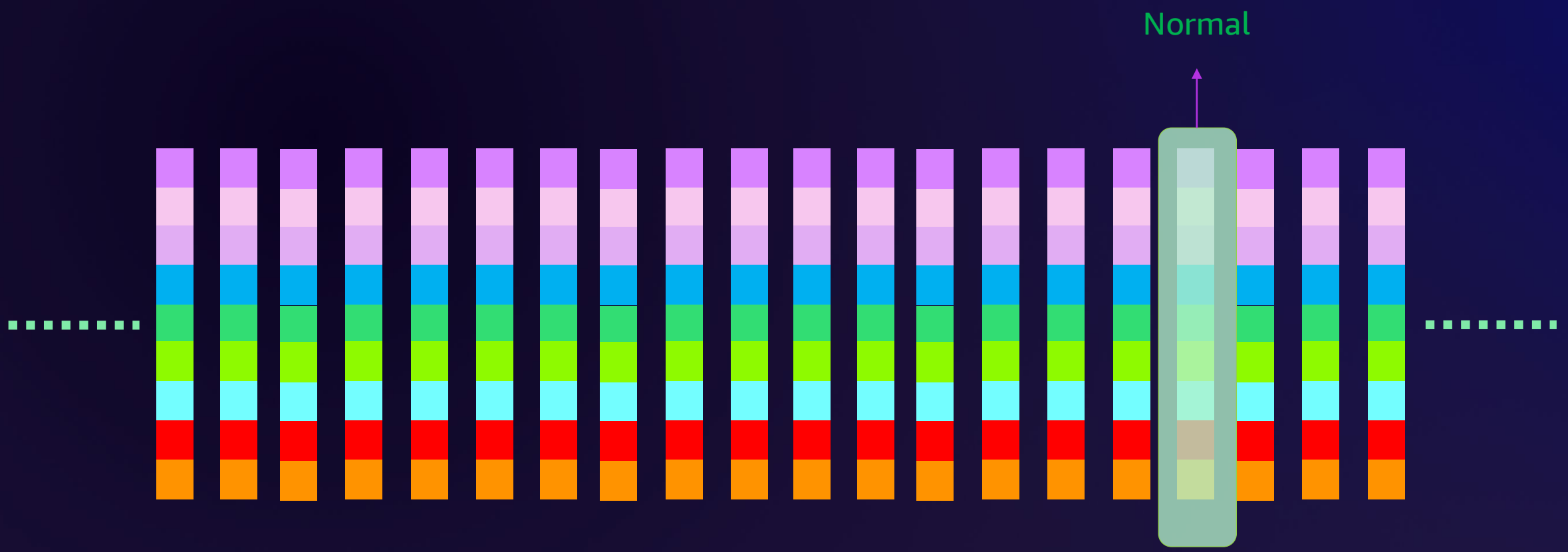
Inference



aws

© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Inference

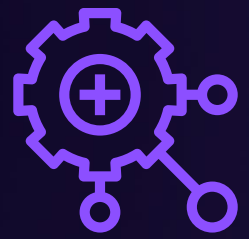


© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Post-processing



Security value filtering



Aggregation



Gathering context



Finding generation

aws

© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Tuning and evaluation



Low alert rate



Detect known attack patterns



Signs of true positives

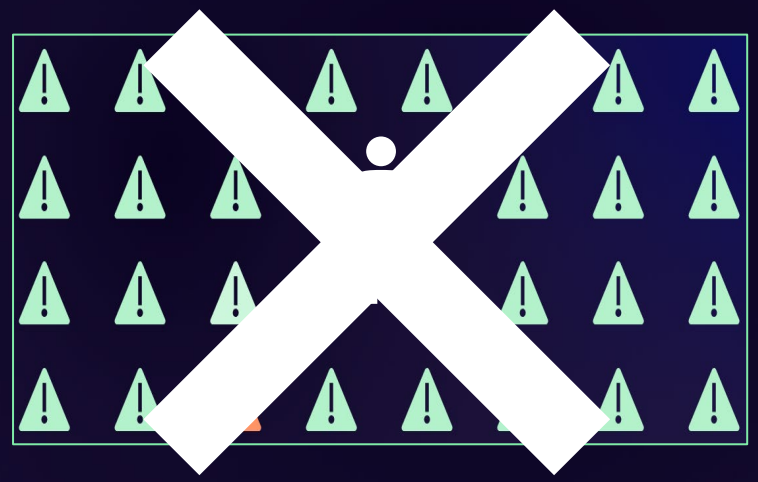


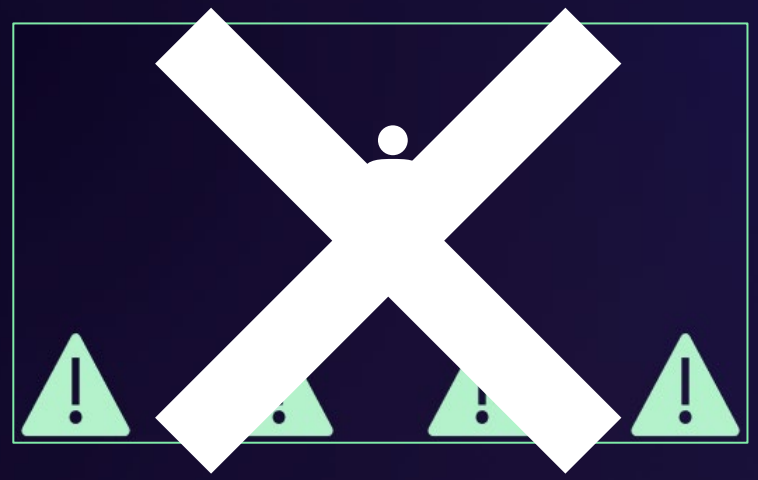
No glaring false positives

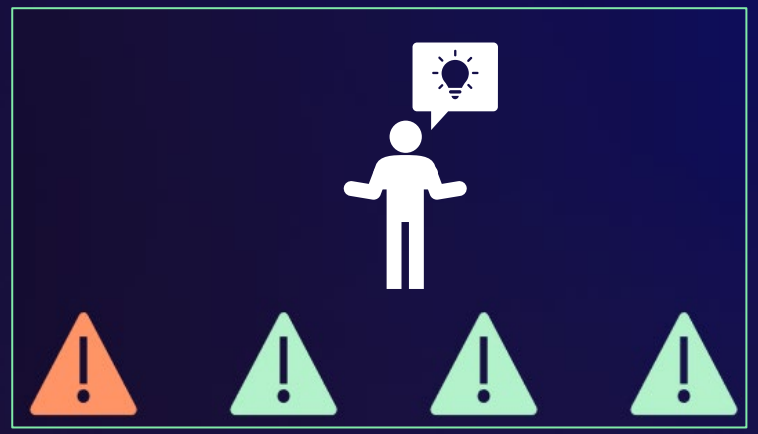
aws

© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Where we left off – How do we get rid of noise without missing the event?







aws

© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Improved accuracy

88% reduction in
likely benign findings



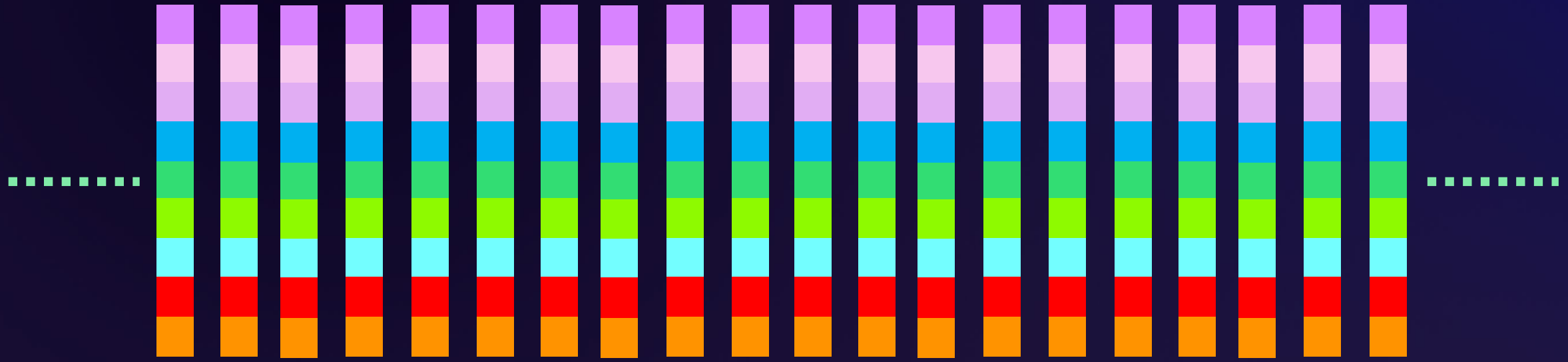
1,200% increase in
highly suspicious findings



aws

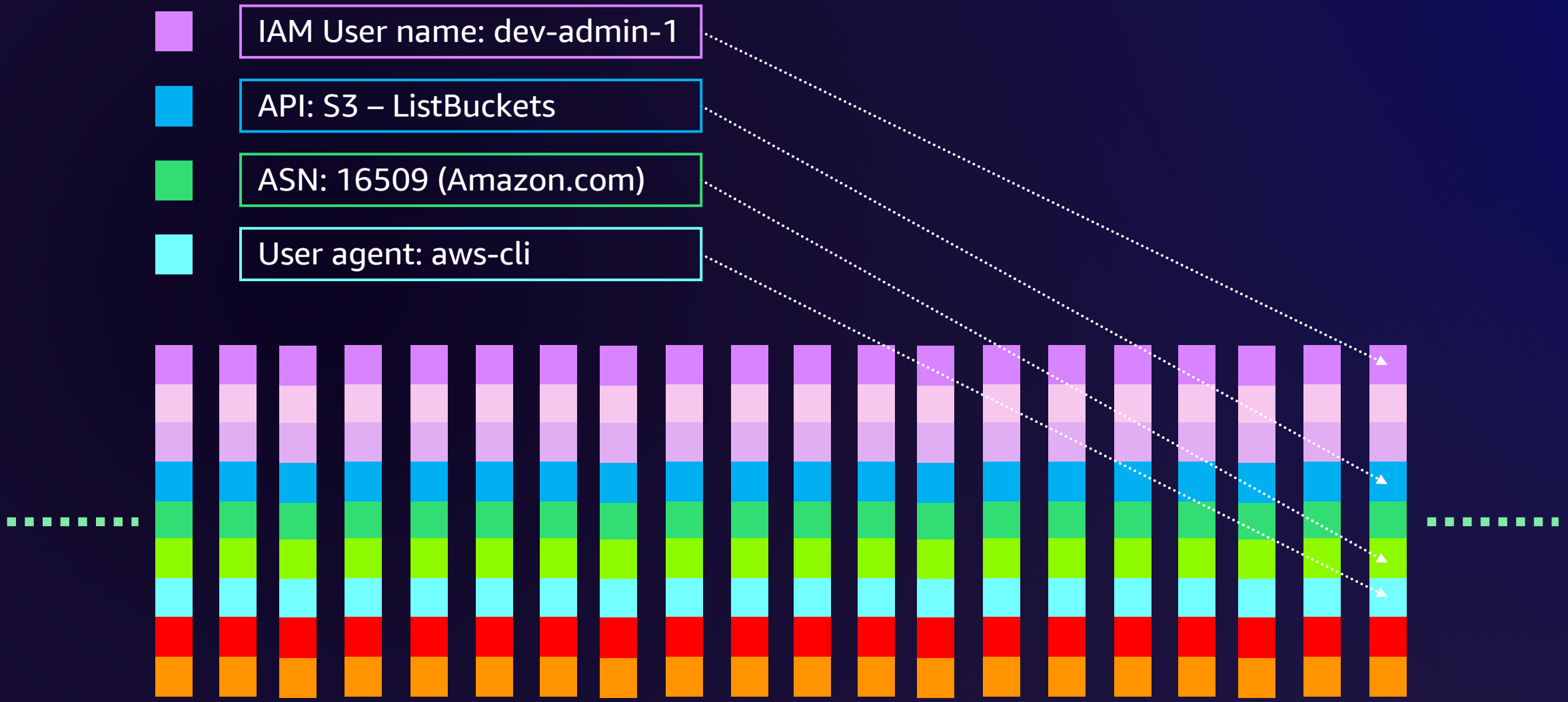
© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

From an ML model to a GuardDuty finding – Detection



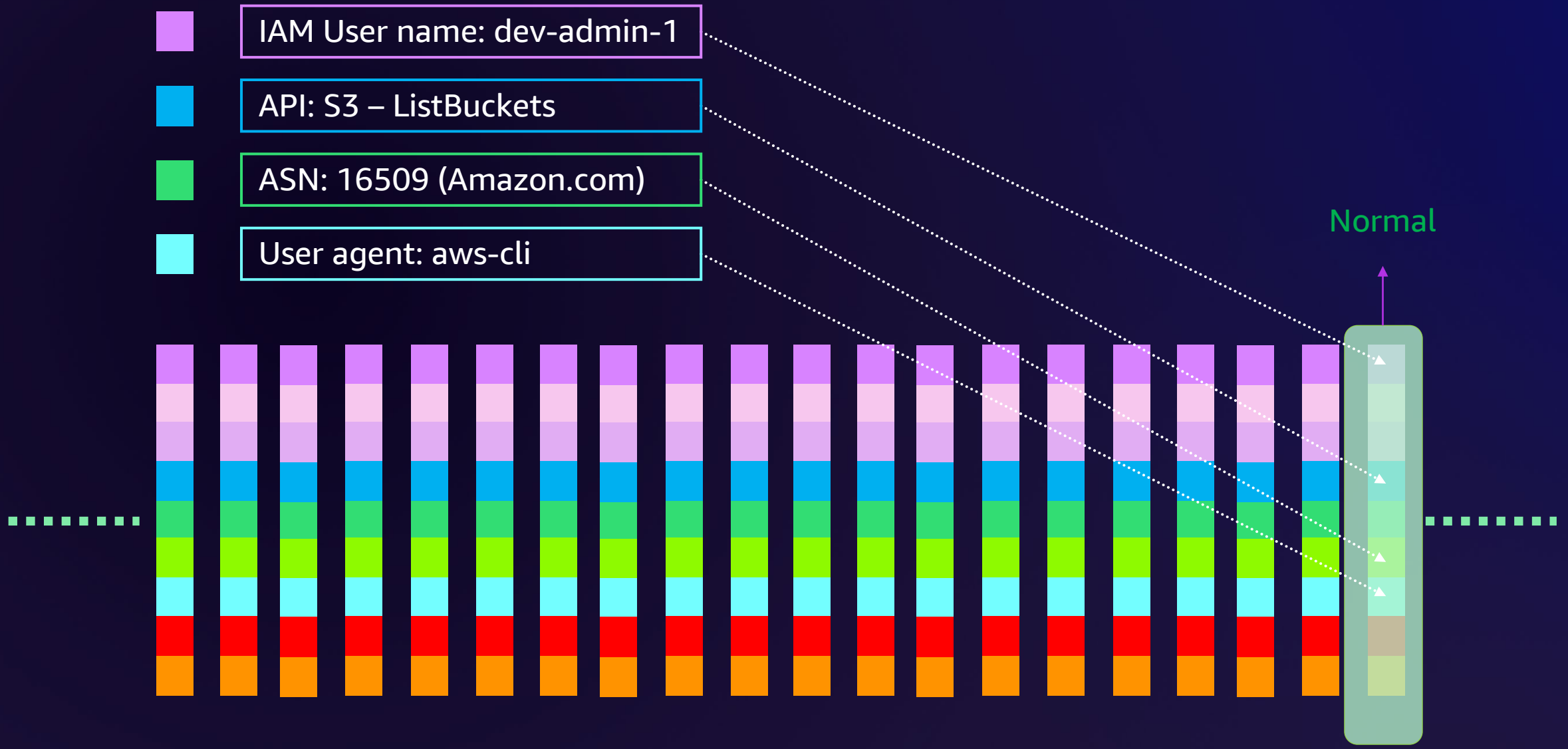
© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

From an ML model to a GuardDuty finding – Detection



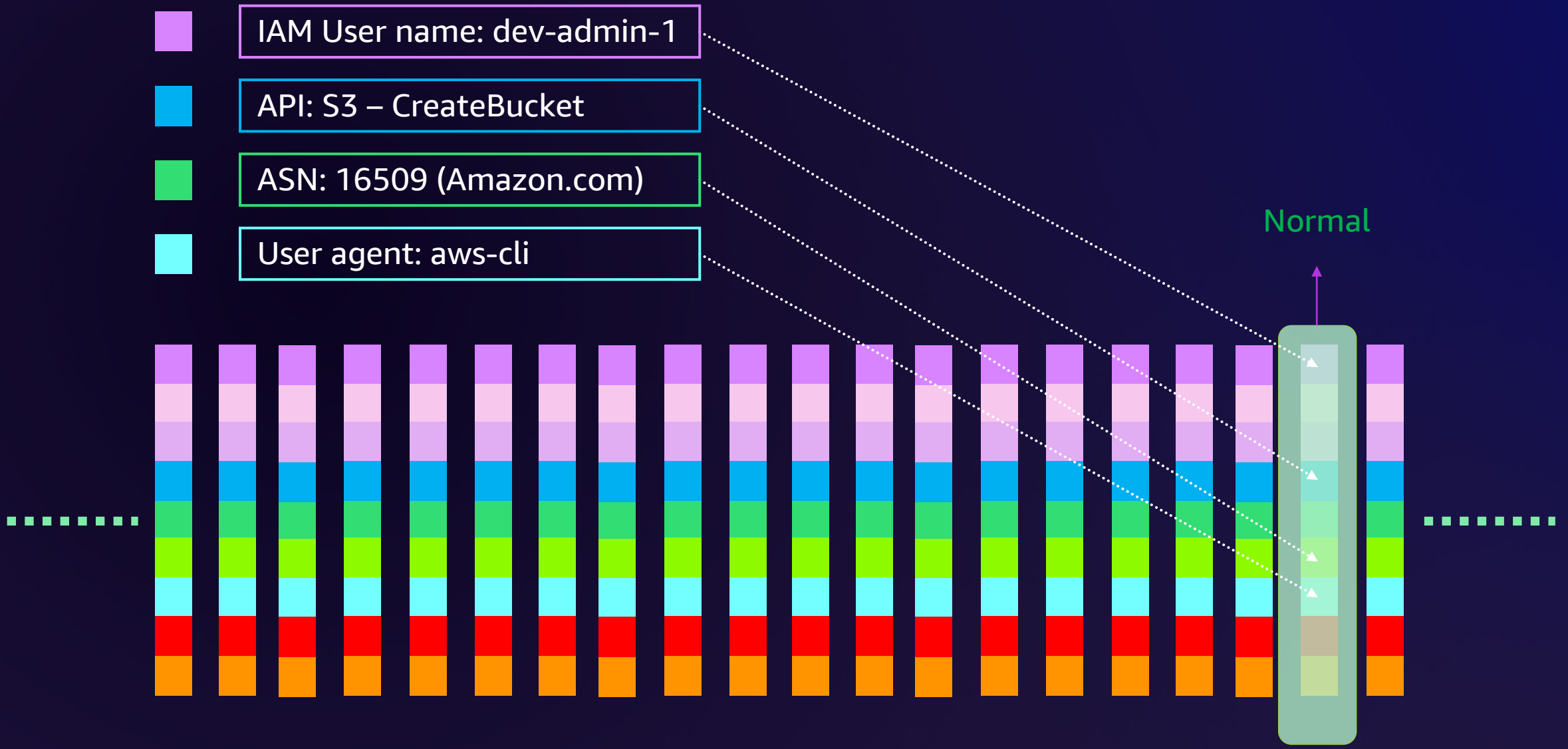
© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

From an ML model to a GuardDuty finding – Detection



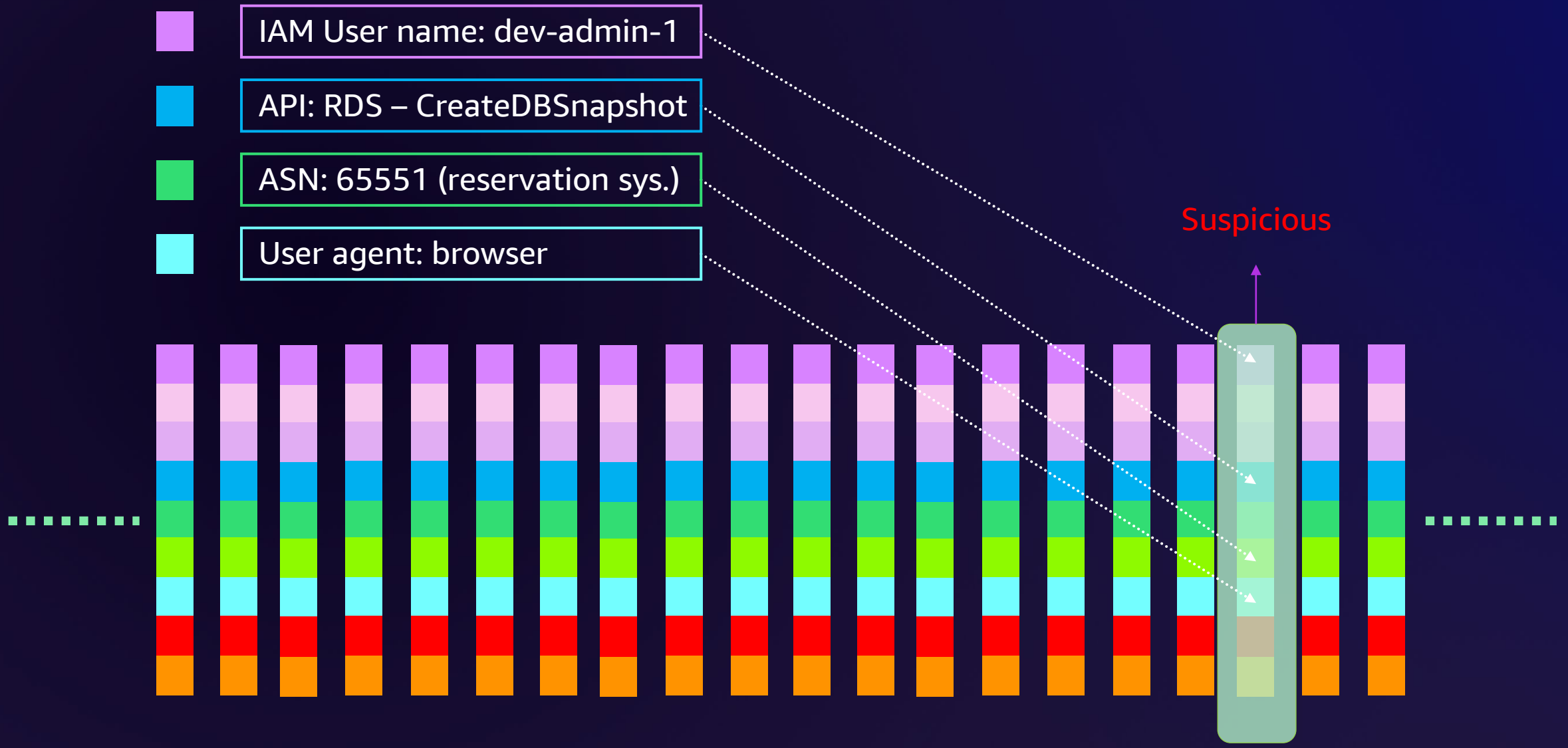
© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

From an ML model to a GuardDuty finding – Detection



© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

From an ML model to a GuardDuty finding – Detection



aws
© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

From an ML model to a GuardDuty finding – Post-processing



Security value filtering



Amazon RDS – **CreateDBSnapshot** associated with observed **unauthorized user techniques**

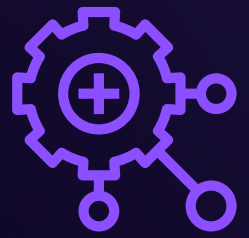
aws

© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

From an ML model to a GuardDuty finding – Post-processing



Security value filtering



Aggregation



Amazon RDS – **CreateDBSnapshot** associated with observed **unauthorized user techniques**



Additional APIs in the session: [IAM] – ListRolePolicies, ListPolicies, ListUsers, ListUserPolicies | [Amazon RDS] – CopyDBSnapshot | [Amazon Redshift] – DescribeClusters (FAILED), DescribeClusterSecurityGroups (FAILED), DescribeClusterSnapshots (FAILED) |

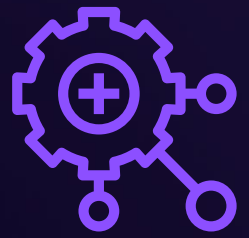
aws

© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

From an ML model to a GuardDuty finding – Post-processing



Security value filtering



Aggregation



Gathering context



Amazon RDS – **CreateDBSnapshot** associated with observed **unauthorized user techniques**



Additional APIs in the session: [IAM] – ListRolePolicies, ListPolicies, ListUsers, ListUserPolicies | [Amazon RDS] – CopyDBSnapshot | [Amazon Redshift] – DescribeClusters (FAILED), DescribeClusterSecurityGroups (FAILED), DescribeClusterSnapshots (FAILED) |



Profiled ASNs: 16509 (Amazon.com), 64496 (phone services)
Unusual ASNs: 65551 (restaurant reservation system)

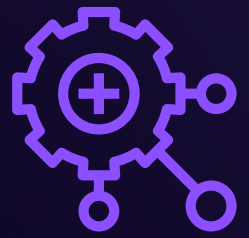
aws

© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

From an ML model to a GuardDuty finding – Post-processing



Security value filtering



Aggregation



Gathering context



Amazon RDS – **CreateDBSnapshot** associated with observed **unauthorized user techniques**



Additional APIs in the session: [IAM] – ListRolePolicies, ListPolicies, ListUsers, ListUserPolicies | [Amazon RDS] – CopyDBSnapshot | [Amazon Redshift] – DescribeClusters (FAILED), DescribeClusterSecurityGroups (FAILED), DescribeClusterSnapshots (FAILED) |



Profiled ASNs: 16509 (Amazon.com), 64496 (phone services)
Unusual ASNs: 65551 (restaurant reservation system)



Profiled APIs: [Amazon S3] ListBuckets, CreateBucket, GetBucketAcl, [IAM] ListUserPolicies
Unusual APIs: [Amazon RDS] CreateDBSnapshot, [Amazon Redshift] DescribeClusters, DescribeClusterSecurityGroups, DescribeClusterSnapshots

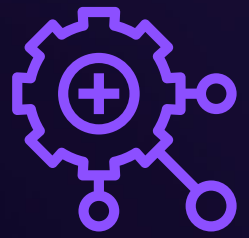
aws

© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

From an ML model to a GuardDuty finding – Post-processing



Security value filtering



Aggregation



Gathering context



Finding generation



Amazon RDS – **CreateDBSnapshot** associated with observed **unauthorized user techniques**



Additional APIs in the session: [IAM] – ListRolePolicies, ListPolicies, ListUsers, ListUserPolicies | [Amazon RDS] – CopyDBSnapshot | [Amazon Redshift] – DescribeClusters (FAILED), DescribeClusterSecurityGroups (FAILED), DescribeClusterSnapshots (FAILED) |



Profiled ASNs: 16509 (Amazon.com), 64496 (phone services)
Unusual ASNs: 65551 (restaurant reservation system)



Profiled APIs: [Amazon S3] ListBuckets, CreateBucket, GetBucketAcl, [IAM] ListUserPolicies
Unusual APIs: [Amazon RDS] CreateDBSnapshot, [Amazon Redshift] DescribeClusters, DescribeClusterSecurityGroups, DescribeClusterSnapshots

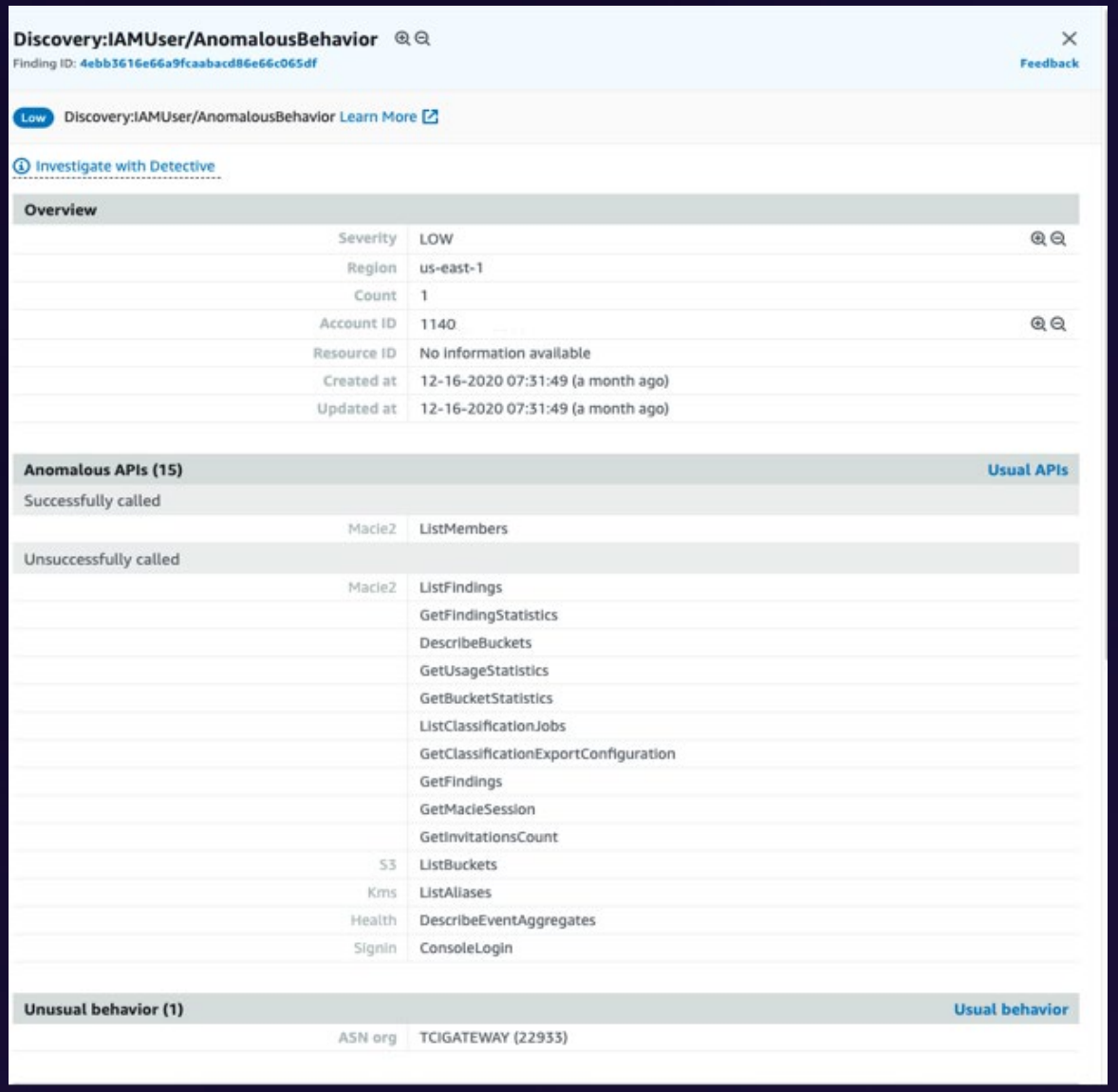


API mapped to exfiltration tactic → Exfiltration:IAM/AnomalousBehavior, severity is HIGH

aws

© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

From an ML model to a GuardDuty finding – Putting it all together



Discovery:IAMUser/AnomalousBehavior

Finding ID: 4ebb3616e66a9fcaabacd86e66c065df

Feedback

Low Discovery:IAMUser/AnomalousBehavior Learn More

Investigate with Detective

Overview

Severity	LOW
Region	us-east-1
Count	1
Account ID	1140
Resource ID	No information available
Created at	12-16-2020 07:31:49 (a month ago)
Updated at	12-16-2020 07:31:49 (a month ago)

Anomalous APIs (15) Usual APIs

Successfully called

Macie2	ListMembers

Unsuccessfully called

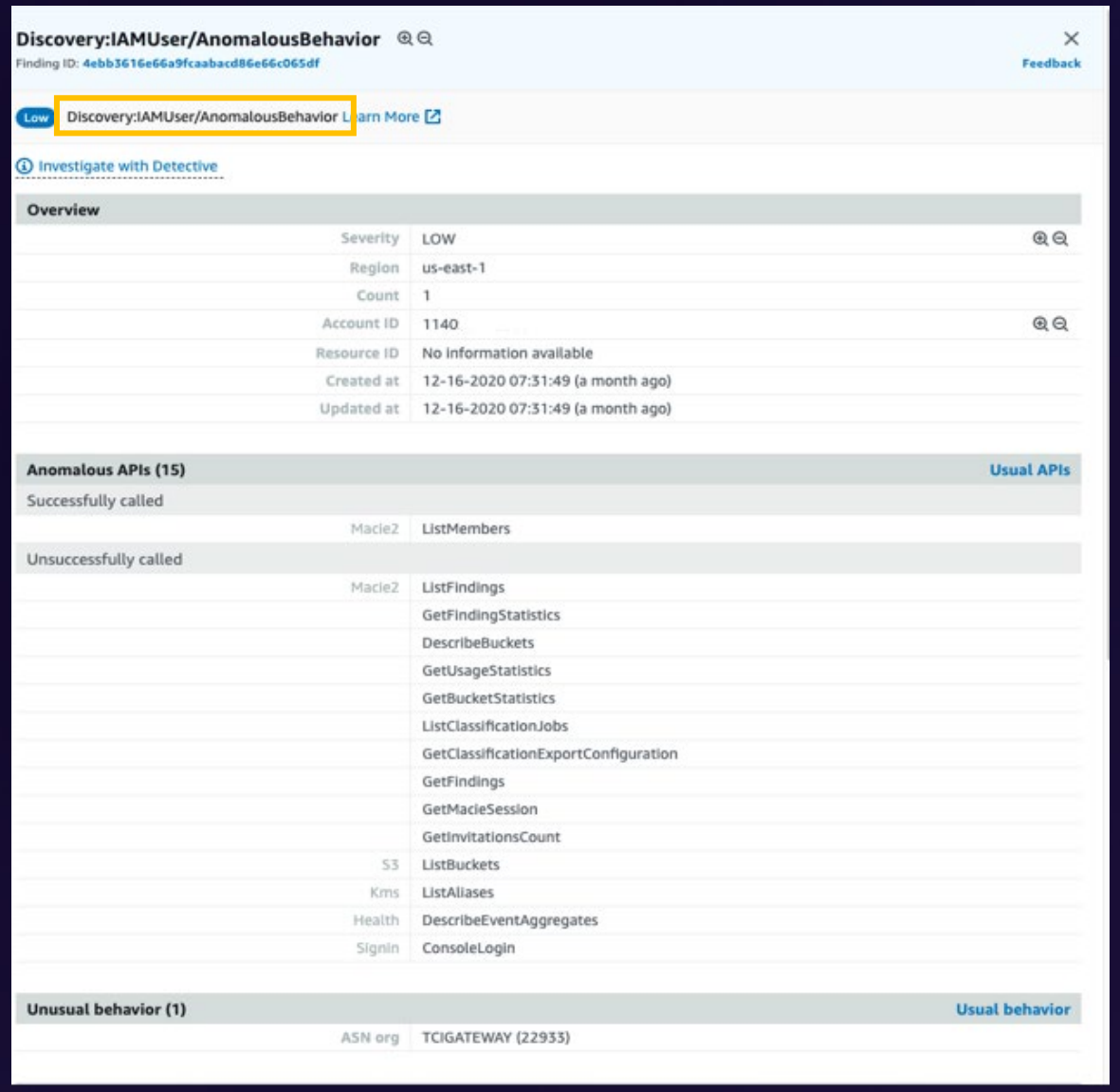
Macie2	ListFindings
	GetFindingStatistics
	DescribeBuckets
	GetUsageStatistics
	GetBucketStatistics
	ListClassificationJobs
	GetClassificationExportConfiguration
	GetFindings
	GetMacieSession
	GetInvitationsCount
S3	ListBuckets
Kms	ListAliases
Health	DescribeEventAggregates
Signin	ConsoleLogin

Unusual behavior (1) Usual behavior

ASN org	TCIGATEWAY (22933)

© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

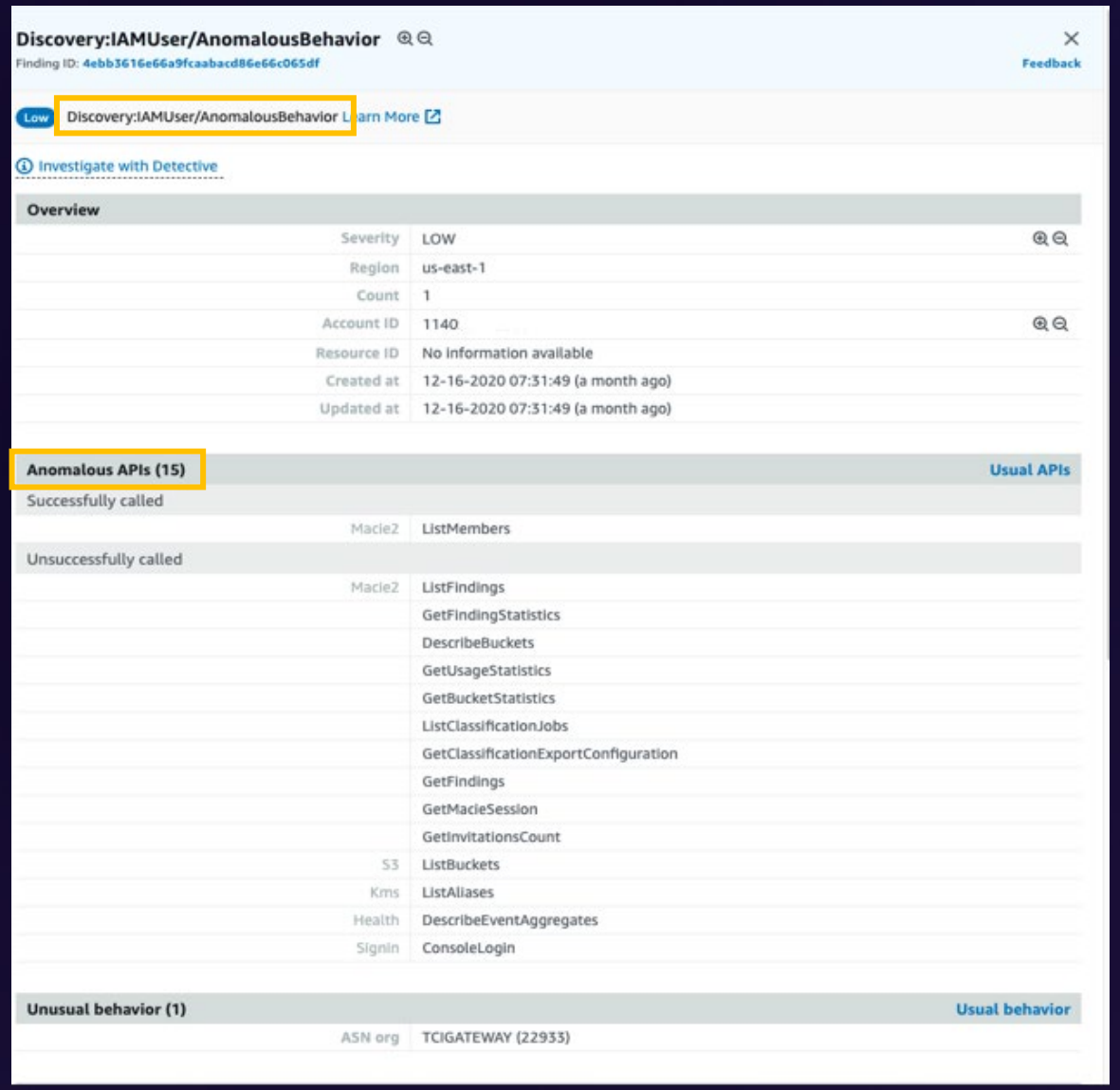
From an ML model to a GuardDuty finding – Putting it all together



Findings are categorized by attack stage based on MITRE ATT&CK Matrix

© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

From an ML model to a GuardDuty finding – Putting it all together

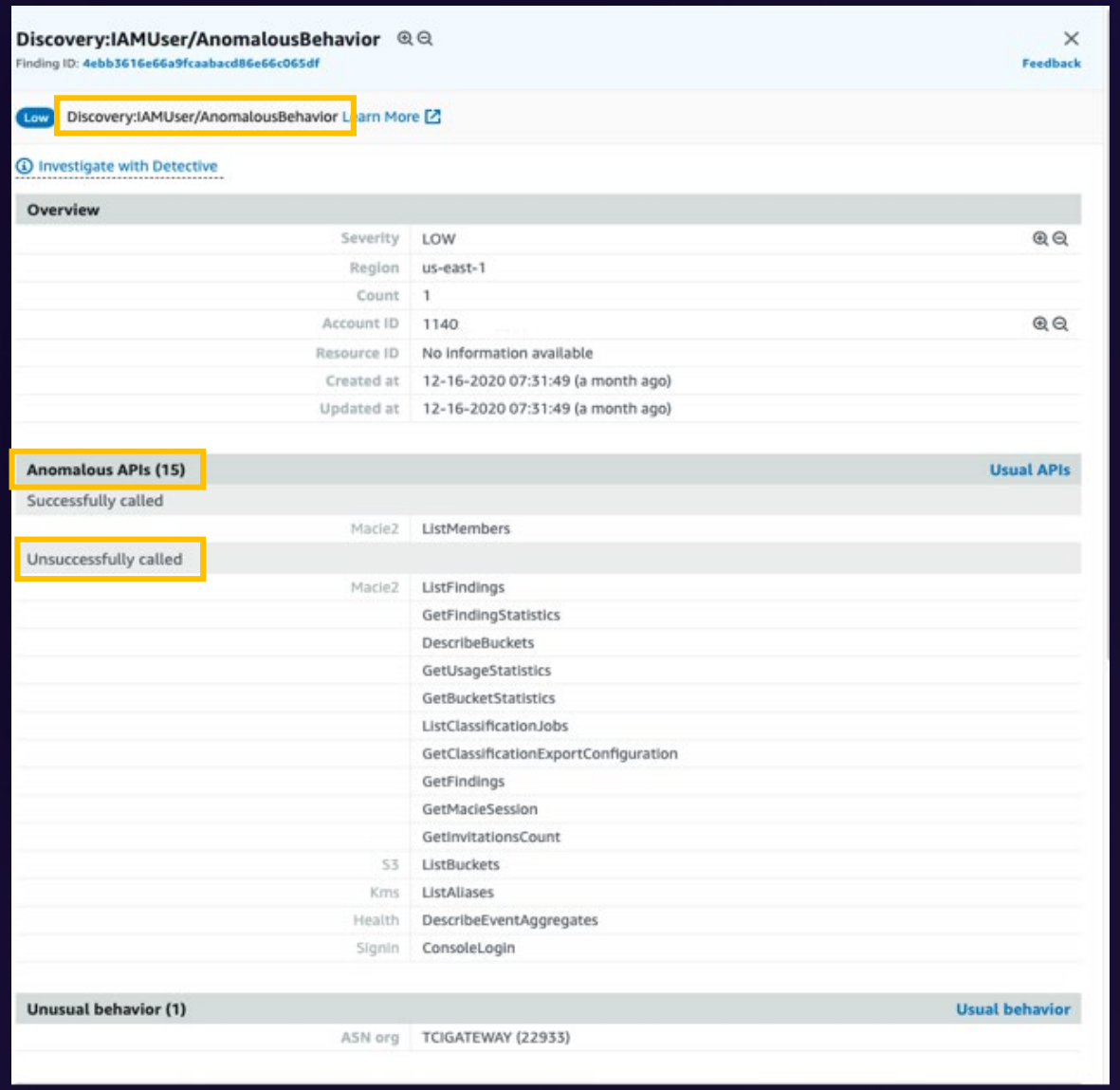


Findings are categorized by attack stage based on MITRE ATT&CK Matrix

Full list of all anomalously called APIs that were part of the session

© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

From an ML model to a GuardDuty finding – Putting it all together



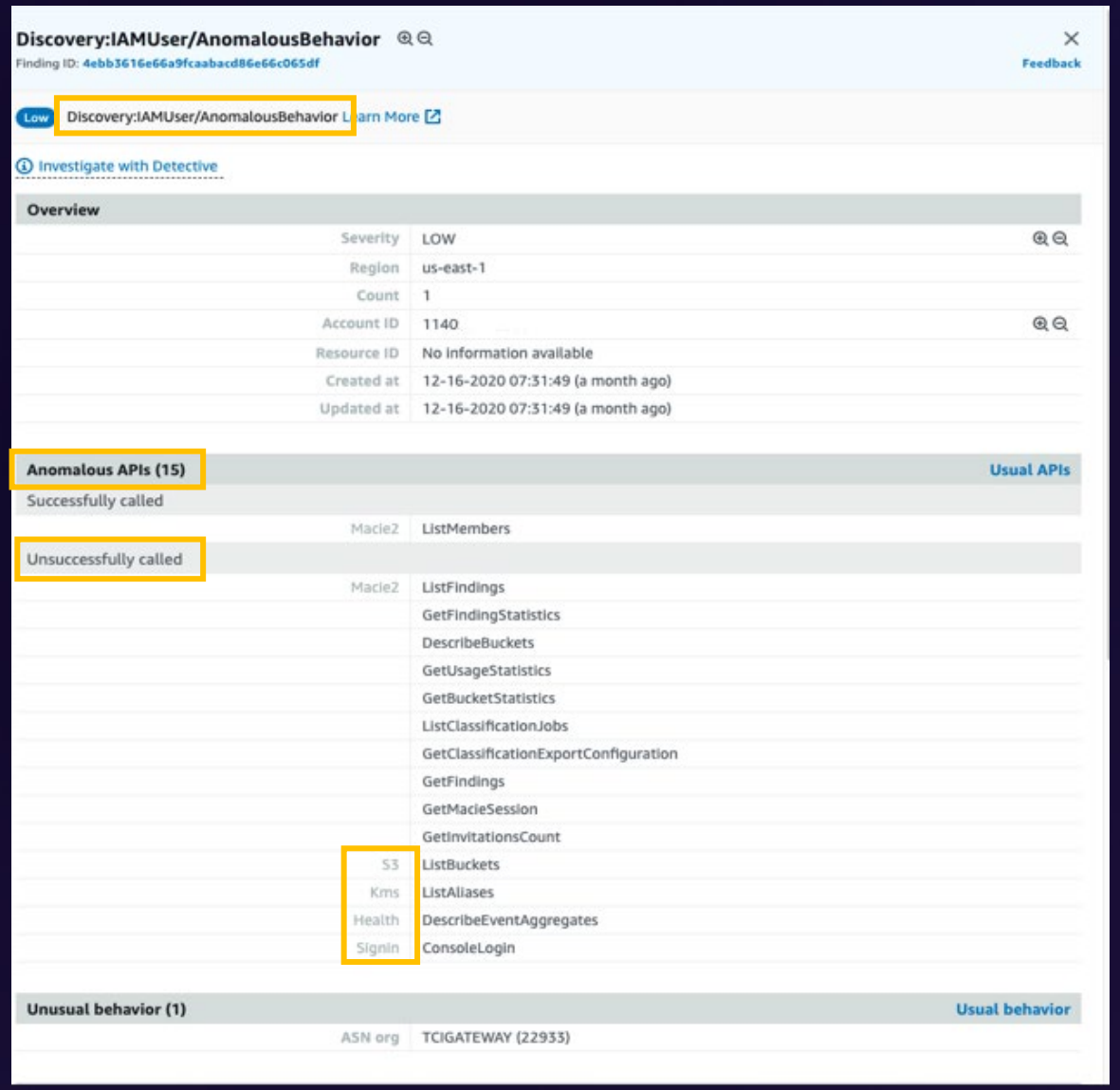
Findings are categorized by attack stage based on MITRE ATT&CK Matrix

Full list of all anomalously called APIs that were part of the session

API calls are broken down into successful/unsuccessful

© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

From an ML model to a GuardDuty finding – Putting it all together



Findings are categorized by attack stage based on MITRE ATT&CK Matrix

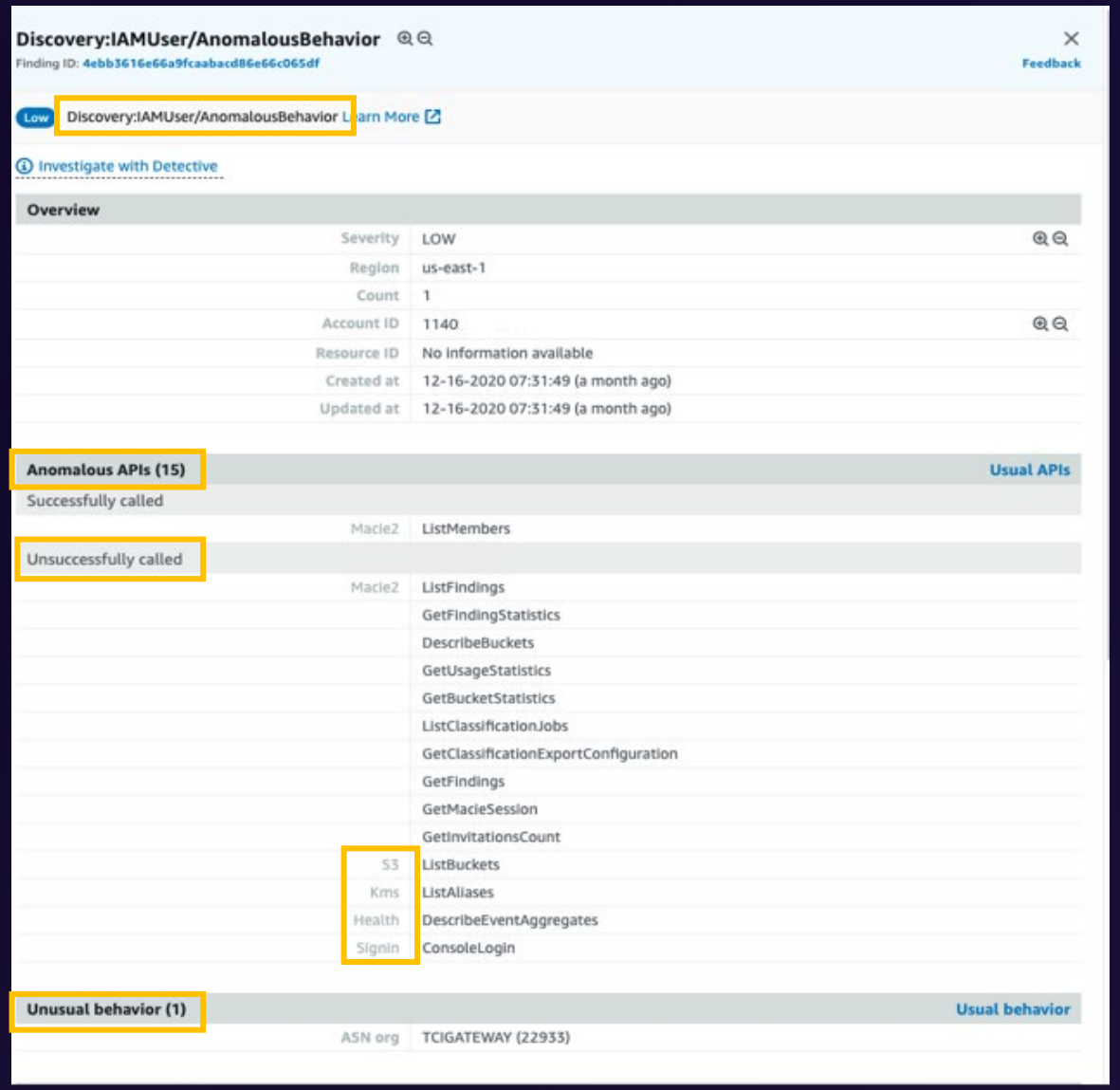
Full list of all anomalously called APIs that were part of the session

API calls are broken down into successful/unsuccessful

API calls are broken down by associated AWS Service

© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

From an ML model to a GuardDuty finding – Putting it all together



Findings are categorized by attack stage based on MITRE ATT&CK Matrix

Full list of all anomalously called APIs that were part of the session

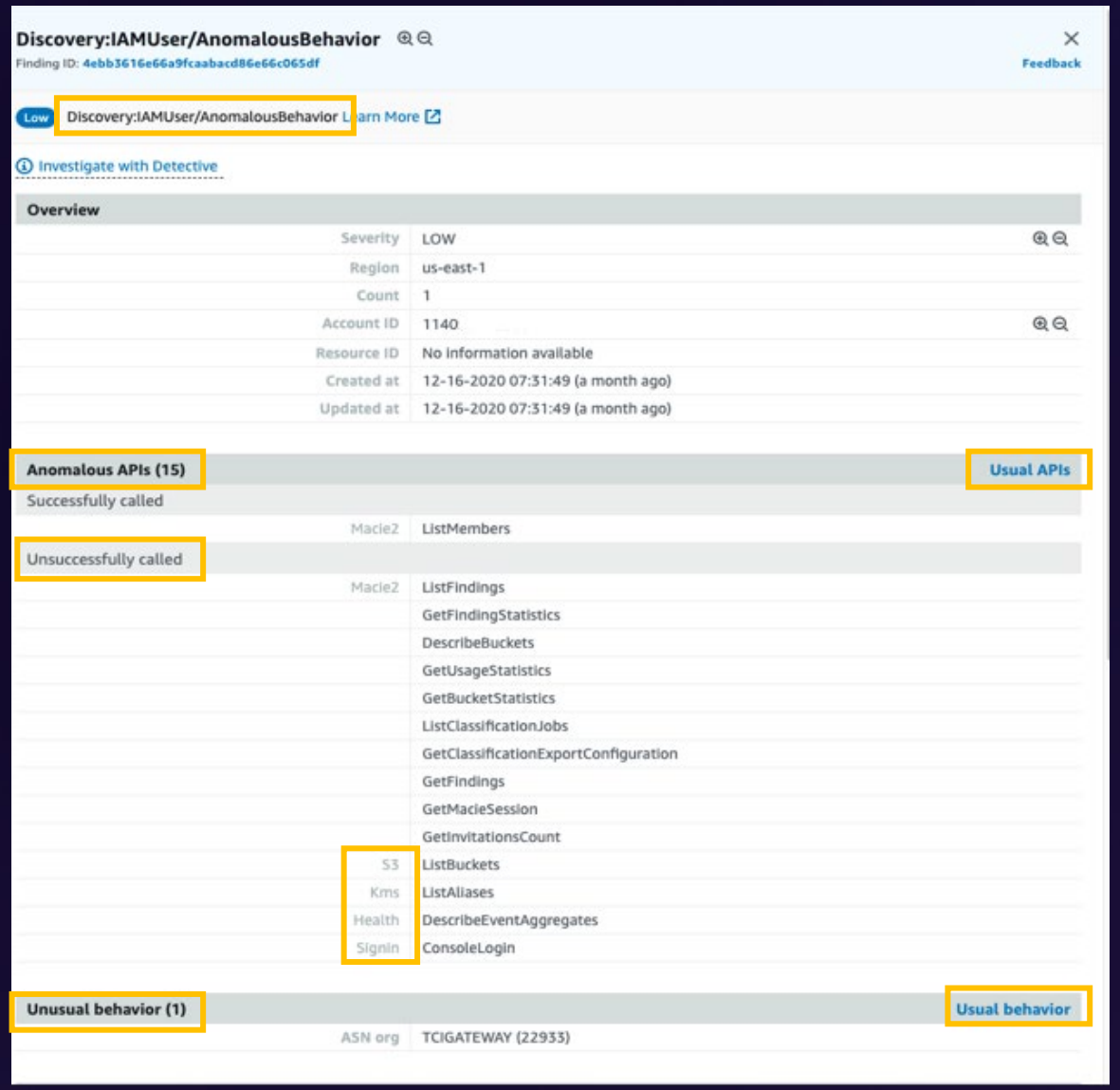
API calls are broken down into successful/unsuccessful

API calls are broken down by associated AWS Service

At a glance, we can see what was unusual about this activity

© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

From an ML model to a GuardDuty finding – Putting it all together



Findings are categorized by attack stage based on MITRE ATT&CK Matrix

Full list of all anomalously called APIs that were part of the session

API calls are broken down into successful/unsuccessful

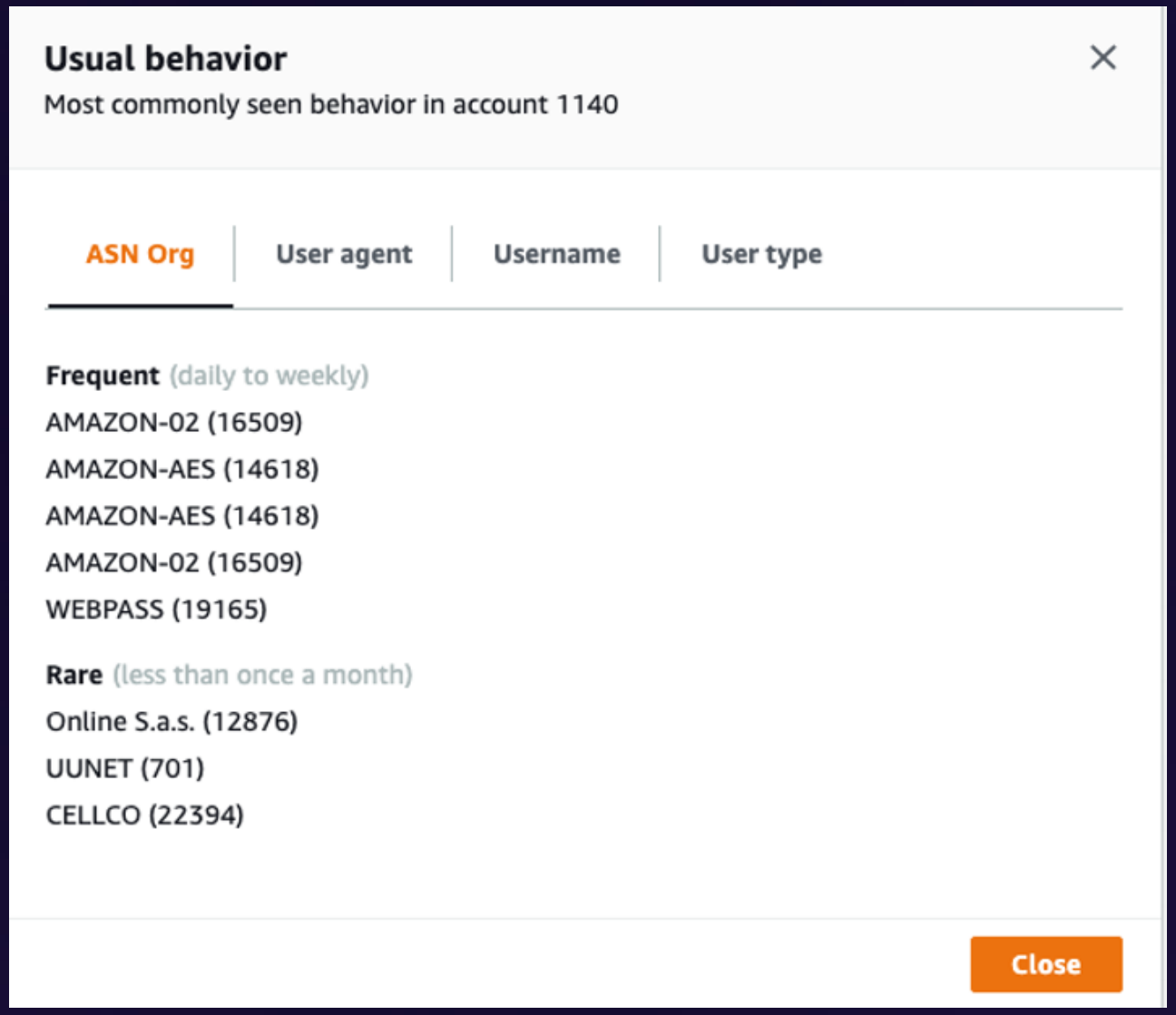
API calls are broken down by associated AWS Service

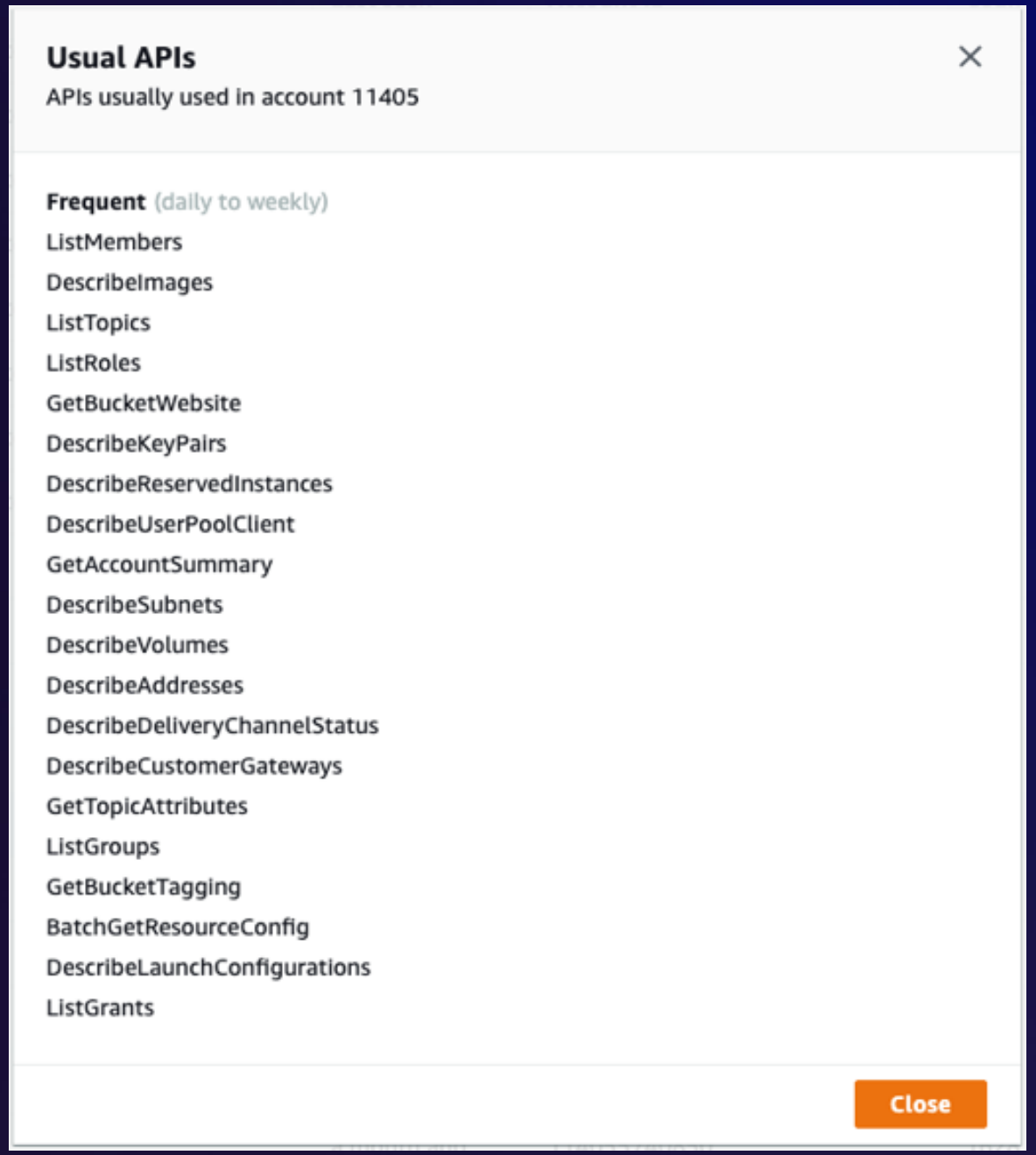
At a glance, we can see what was unusual about this activity

Click to view profiled behavior for user and all users in the account

© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Context helps us understand what the expected behavior is for the user that performed the action as well as for all users in the account





aws
© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

13 New GuardDuty findings – *AnomalousBehavior

- Discovery
- Initial Access
- Credential Access
- Defense Evasion
- Privilege Escalation
- Persistence
- Exfiltration
- Impact







aws

© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

"GuardDuty helped us to quickly scale anomaly detection across all our infrastructure and expand advanced threat detection capabilities quickly and efficiently."

Mrunal Shah

Head of container security at Warner Bros. Discovery

© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Takeaways

1. GuardDuty is continually evolving
2. Machine learning anomaly detection has proven to detect high-risk credential compromise (*AnomalousBehavior)
3. Feedback

© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!



Please complete the session survey in the mobile app

Baris Coskun
linkedin.com/in/coskubar

Amit Megiddo
linkedin.com/in/amit-megiddo

aws
© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.