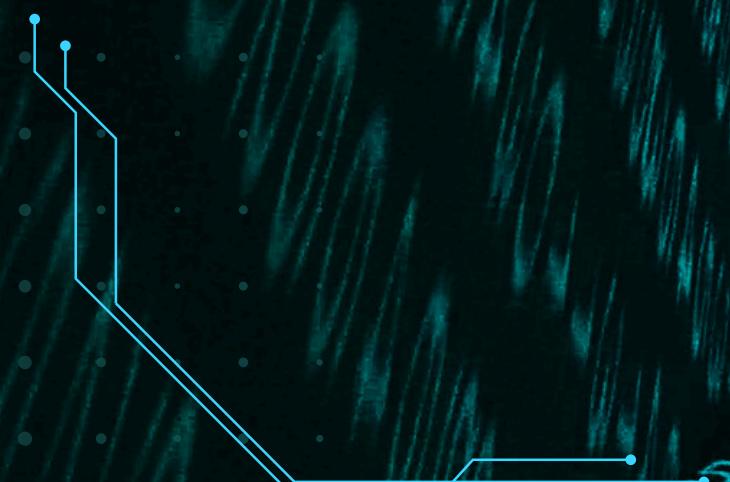




Chewy GDPR compliance and Data Loss Prevention Project

MID GROUP PROJECT:
401n2



Cyberia Security.

AGENDA

- 1. Team member Introductions**
- 2. Problem Domain & Project Solution**
- 3. Application Demonstration**
- 4. Documentation**
- 5. Q&A**

Team Members Introduction

OUR TEAM

Diogo Figueiredo



"I try every day to become a better version of myself. I believe that my diverse background in biology and hospitality will make a huge contribution to my aspiring cybersecurity career."

Hélio Ferreira



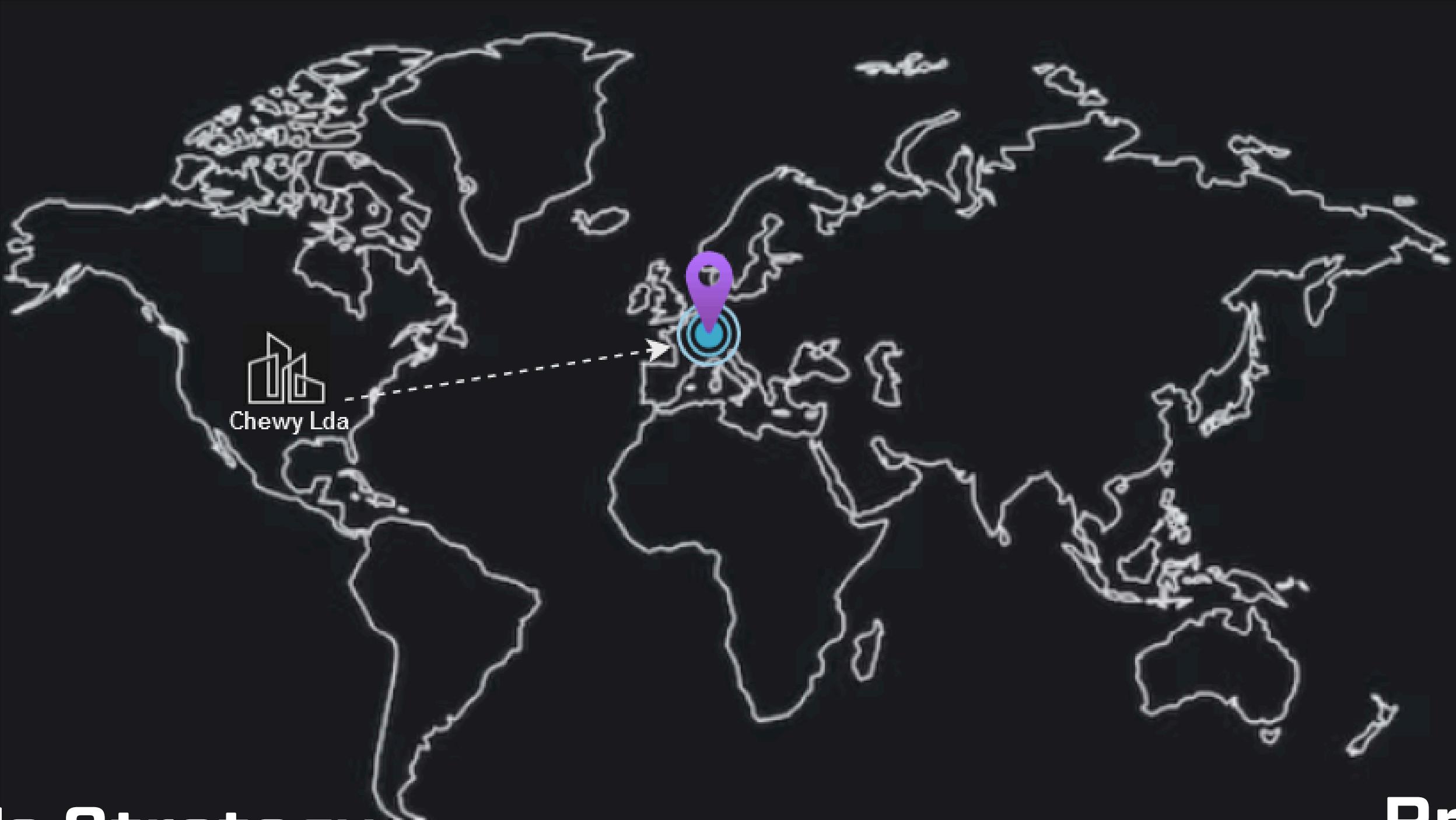
"I am a cybersecurity enthusiast who's guided by the values of professionalism and good faith. With a background in accounting and insurance, I hope in the future I can use that knowledge in multiple Cybersecurity areas."

Tomás Ferreira



“I specialize in cloud cybersecurity. I am fascinated about understanding how hackers think and operate. I believe that by studying their techniques, we can develop more effective defenses.”

Problem Domain



Chewy's Strategy

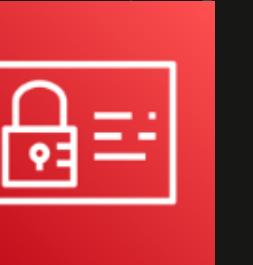
Sales growth in International markets

Problem

Europe GDPR compliance
Protect PCI/PII Data

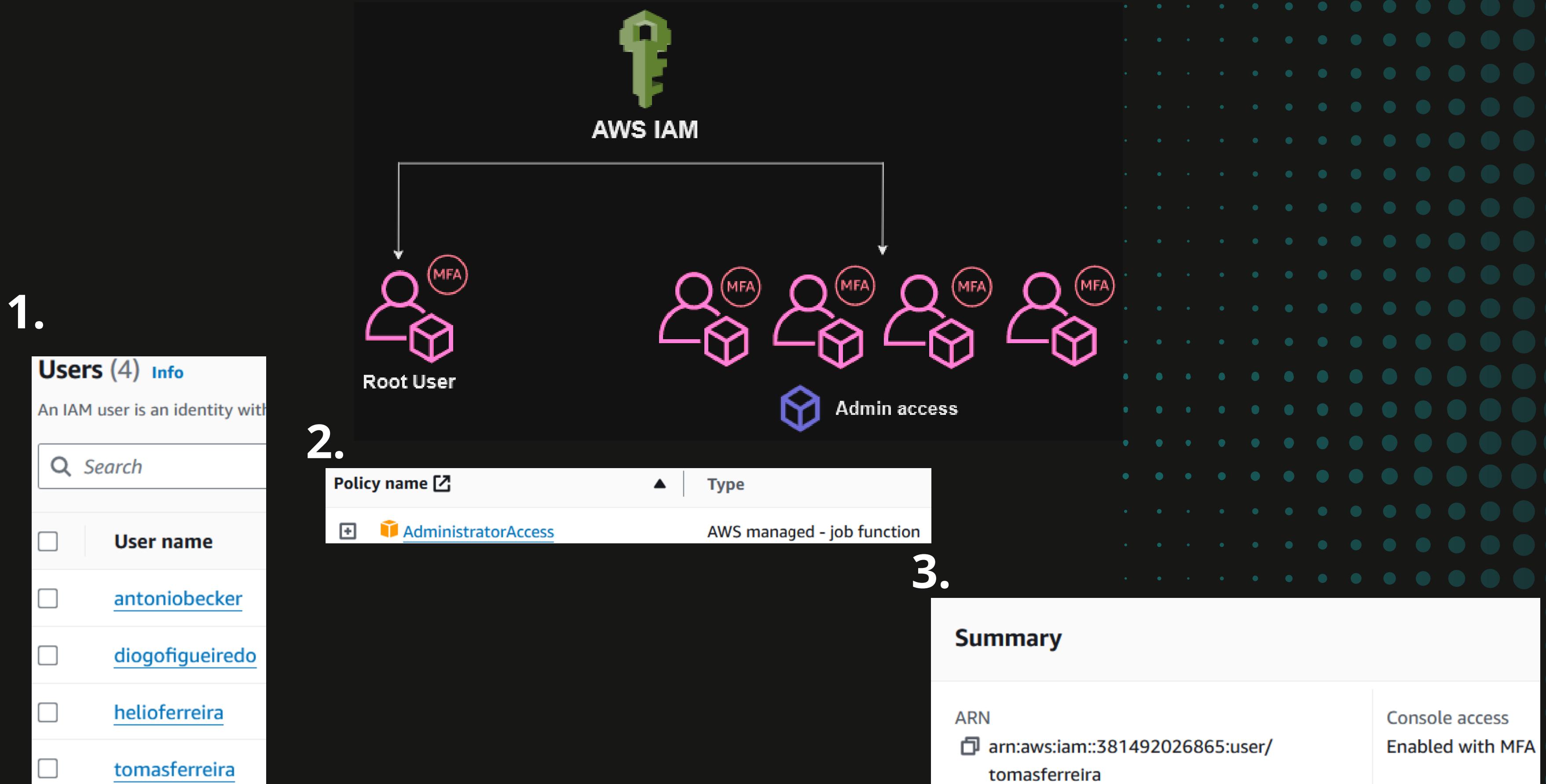
PROJECT SOLUTION

Proper IAM Implementation



- Create individual IAM users for each team member.
- Assign least-privilege permissions to users based on their roles.
- Enable MFA for all users with high-level access.

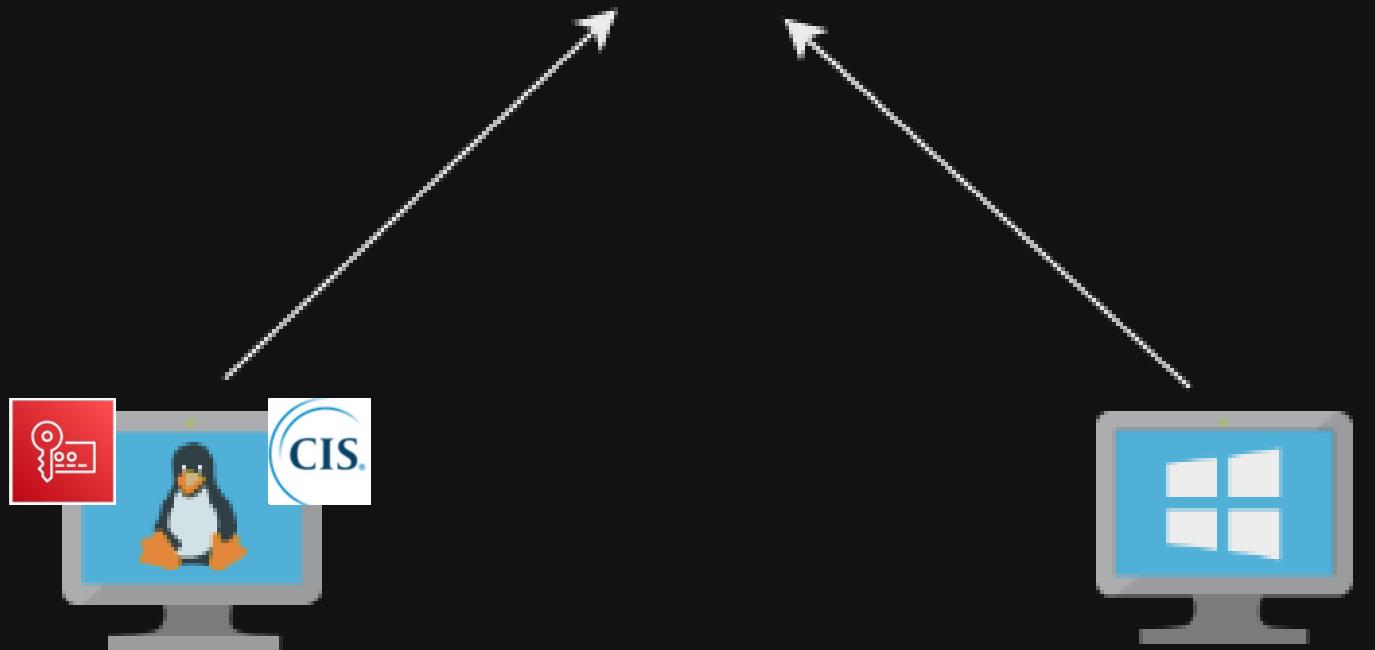
IAM Implementation



CIS Compliant Data Server



OpenVPN Server

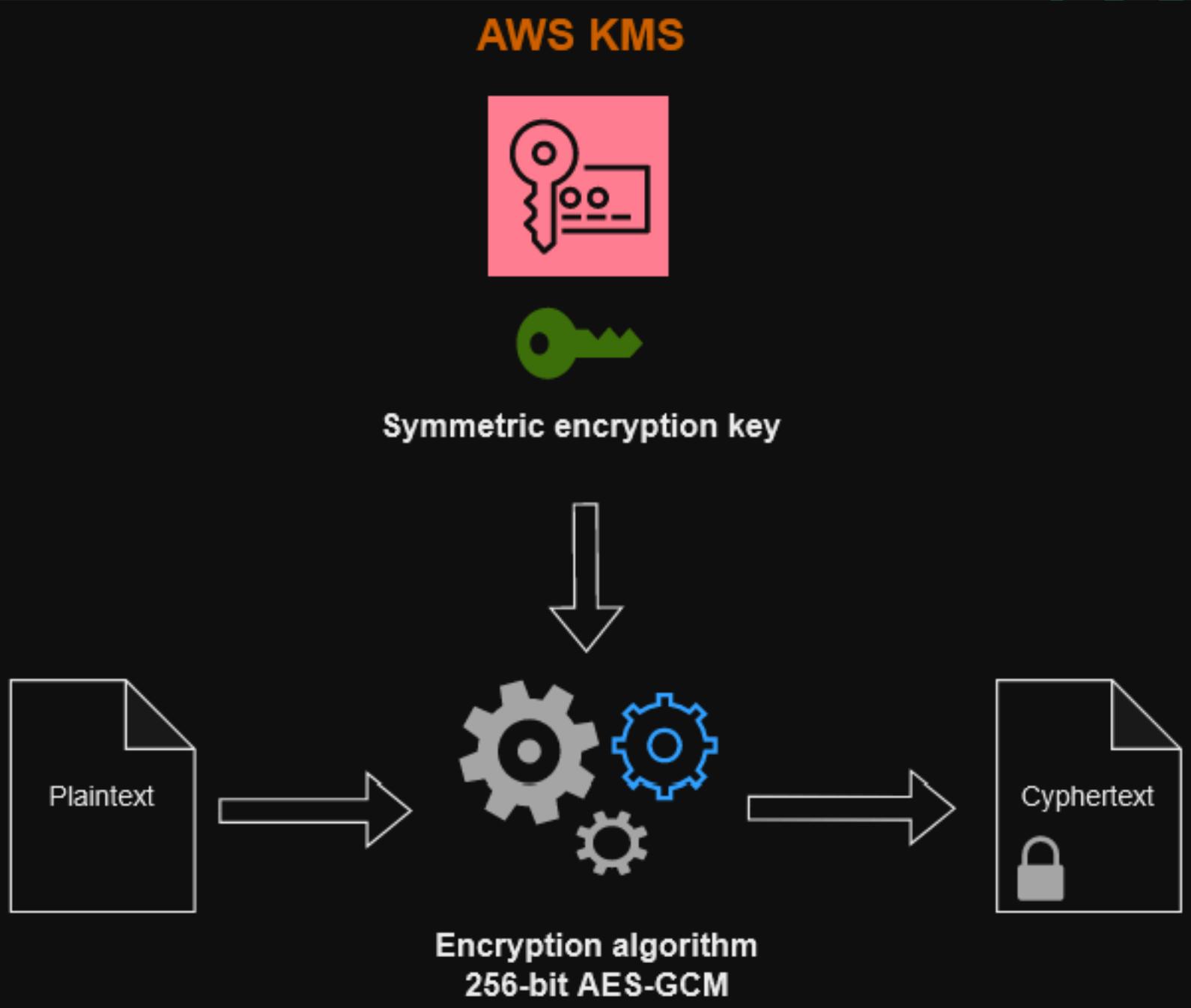


-Launch a Linux EC2 instance and configure it according to CIS benchmarks.

Chewy Linux Server

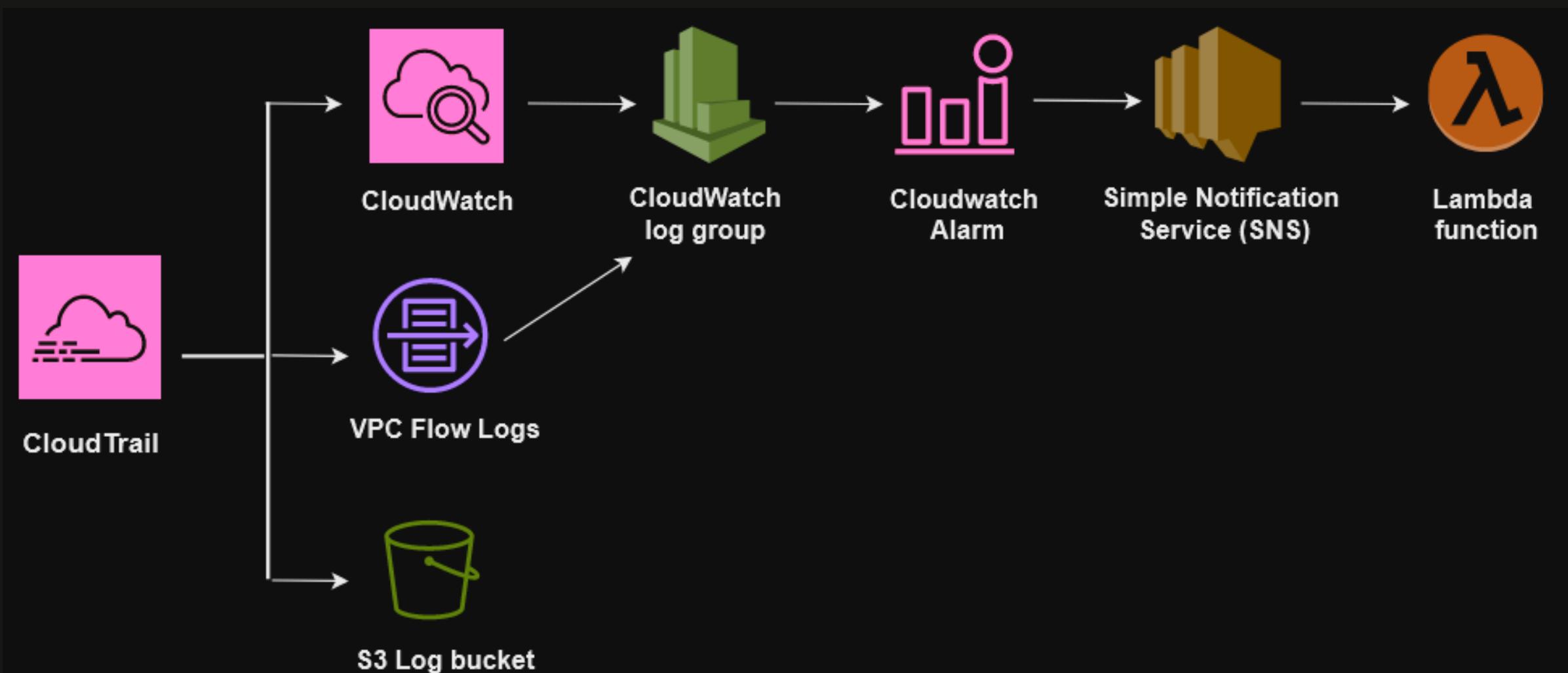
Windows Endpoint

-Use AWS KMS to manage encryption keys and encrypt EBS volumes attached to the instance.



SIEM/Log Aggregation System

- Set up the chosen SIEM tool and integrate it with AWS services.
- Configure CloudTrail, CloudWatch Logs, and VPC Flow Logs.
- Set up notification channels (email) to alert administrators.



SIEM/Log aggregation system

1. Configure CloudTrail



CloudWatch Logs - optional

Configure CloudWatch Logs to monitor your trail logs and notify you when specific activity occurs. Standard CloudWatch and CloudWatch Logs charges apply. [Learn more](#)

CloudWatch Logs [Info](#)

Enabled

Log group [Info](#)

New

Existing

Log group name

chewy_cloudwatch_logs

1-512 characters. Only letters, numbers, dashes, underscores, forward slashes, and periods are allowed.

IAM Role [Info](#)

AWS CloudTrail assumes this role to send CloudTrail events to your CloudWatch Logs log group.

New

Existing

Role name

chewy_watch_role

Trail name
Enter a display name for your trail.

3-128 characters. Only letters, numbers, periods, underscores, and dashes are allowed.

Enable for all accounts in my organization
To review accounts in your organization, open AWS Organizations. See all accounts [\[?\]](#)

Storage location [Info](#)

Create new S3 bucket
Create a bucket to store logs for the trail.

Use existing S3 bucket
Choose an existing bucket to store logs for this trail.

Trail log bucket and folder
Enter a new S3 bucket name and folder (prefix) to store your logs. Bucket names must be globally unique.

Logs will be stored in chewy_log_s3bucket/AWSLogs/381492026865

Log file SSE-KMS encryption [Info](#)

Enabled

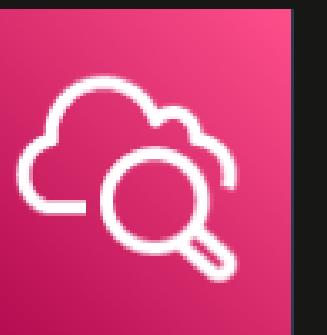
Customer managed AWS KMS key

New

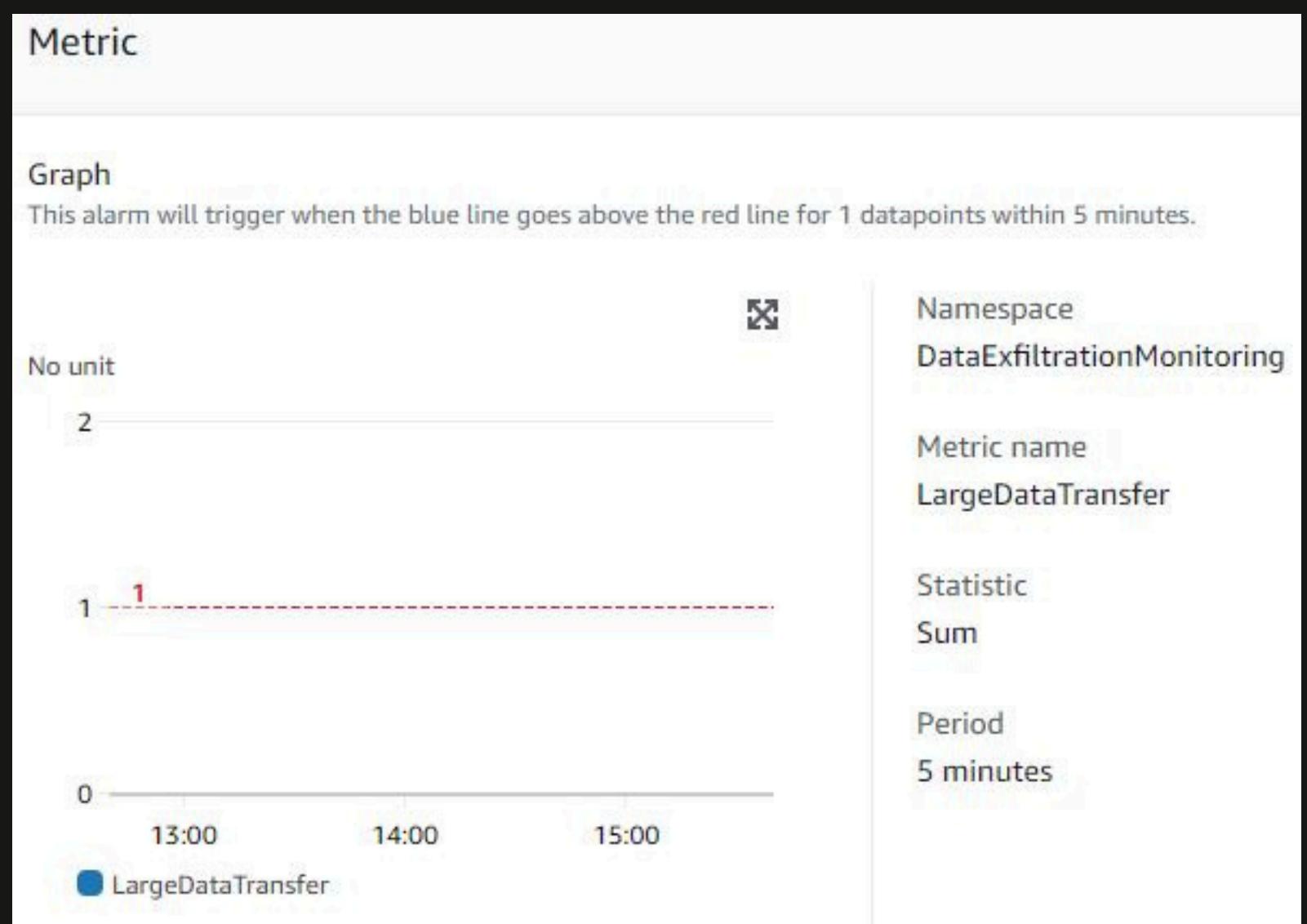
Existing

AWS KMS alias

2. Configure CloudWatch



3. Create VPC Flow logs



Name - optional
chewy_vpc_flowlogs

Filter
The type of traffic to capture (accepted traffic only, rejected traffic only, or all traffic).
 All
 Accept
 Reject

Maximum aggregation interval [Info](#)
The maximum interval of time during which a flow of packets is captured and aggregated into a flow log record.
 10 minutes
 1 minute

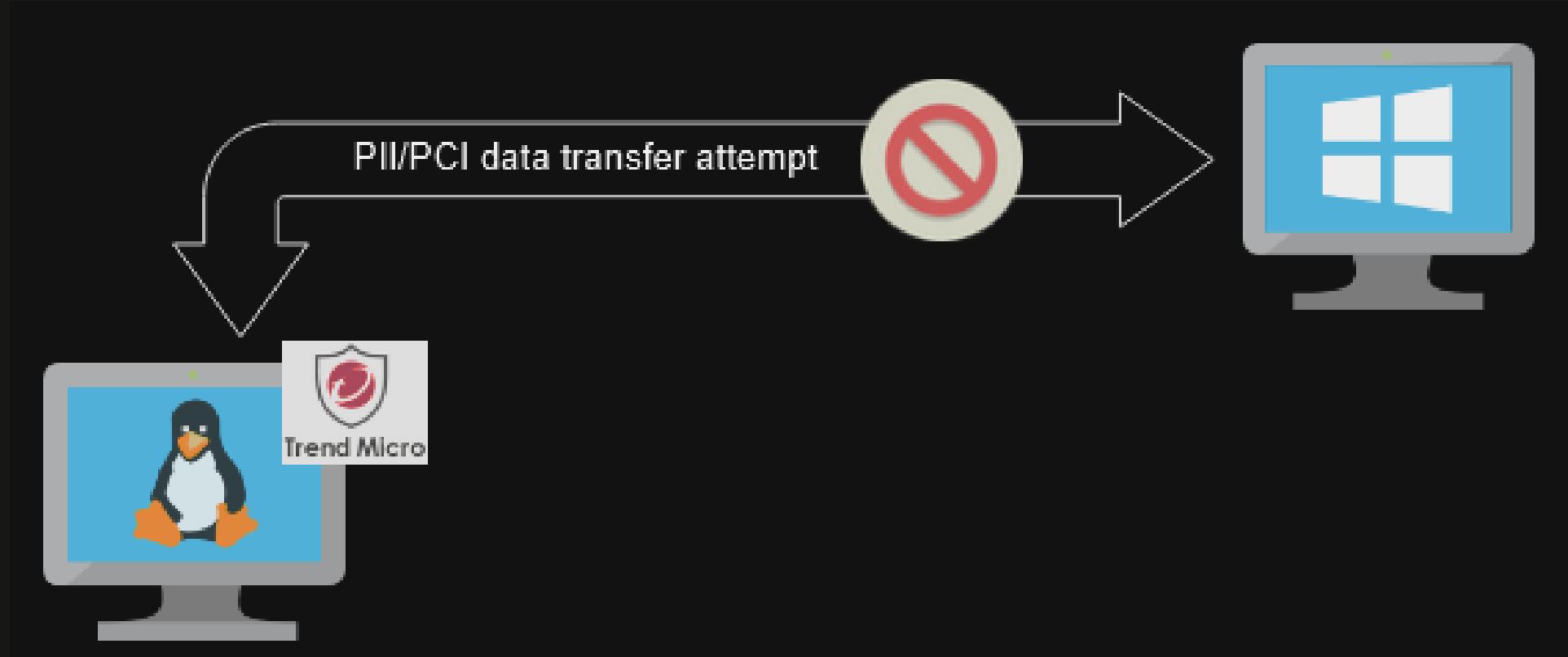
Destination
The destination to which to publish the flow log data.
 Send to CloudWatch Logs
 Send to an Amazon S3 bucket
 Send to Amazon Data Firehose in the same account
 Send to Amazon Data Firehose in a different account

Destination log group [Info](#)
The name of an existing log group or the name of a new log group that will be created when you create this flow log configuration. Log groups are created for each monitored network interface.
 [X](#) [C](#)

IAM role [Info](#)
The IAM role that has permission to publish to the Amazon CloudWatch log group. [Set up permissions](#) [E](#)
 [▼](#) [C](#)

4. Add Data Exfiltration Metric

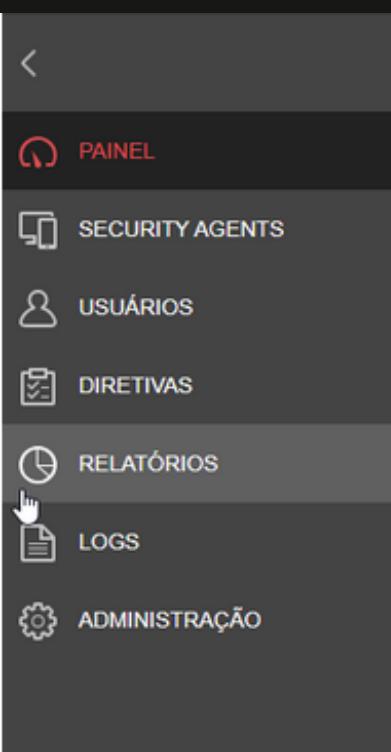
Data Loss Prevention (DLP) Controls



- Select a DLP solution compatible with AWS [Trend Micro].
- Configure policies to detect and prevent the transfer of PII and PCI data.
- Test the DLP solution to ensure it effectively blocks unauthorized data exfiltration.

DLP tool

1. Create Trend Micro account



2. Trend Micro installation

3. Policy configuration

A screenshot of the DLP policy configuration interface. At the top, it says 'Configurações de regras do Prevenção de perda de dados'. It includes sections for 'Configurações gerais' (General settings) with a checked checkbox 'Ativar essa regra' (Enable this rule) and fields for 'Nome da regra:' (Rule name:) and 'Descrição:' (Description); 'Modelo' (Model) with a dropdown showing 'Todos os modelos' (All models) and a search bar with 'dss'; and 'Canal' (Channel) with a checked checkbox 'Canais de rede' (Network channels) and a list of checked items: 'Clientes de e-mail' (Email clients), 'FTP', 'HTTP', 'HTTPS', 'Protocolo SMB', 'Aplicativos IM', and 'Webmail'.

APPLICATION & DEMONSTRATION

DEMO

DOCUMENTATION



Google Docs

Report



Project Repo

THANK YOU