Security and Analytics Services

Deep Dive

Kevin Liang
2/13/25

Table of contents

- Types of Security Controls
- Security Services
  - AWS Guard Duty
  - AWS Inspector
  - AWS Security Hub
- AWS Analytics Services
  - AWS Glue
  - Athena
  - Amazon OpenSearch
  - Amazon Quick Sight
- Immersion Day - Reference Architectures

What are Security Controls ?

A safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements.

Types of Security Controls:

- Preventive Controls – *e.g. IAM Roles, Service Control Policies*
- Detective Controls – *e.g. AWS Config for auditing and AWS Inspector*
- Responsive Controls – *e.g. AWS Config for remediating*

Security Services Used in Immersion Day

Amazon Inspector

- Automatically discover and scans known software vulnerabilities
- Monitor and process findings with other services and systems

Amazon GuardDuty

- Threat detection service that continuously monitors for malicious activity
- In-built AI/ML to find the threats in your environments

AWS Security Hub

- Comprehensive view of your security state in AWS
- Better prioritize the response and remediation efforts by accounts and resources

Analytics Services Used in Immersion Day

AWS Glue

- Serverless data integration service
- Simplifies complex, and expensive traditional data integration processes

Amazon Athena

- Simplified, flexible way to analyze and query your data
- Runs federated queries, prepares data for ML models

Amazon OpenSearch

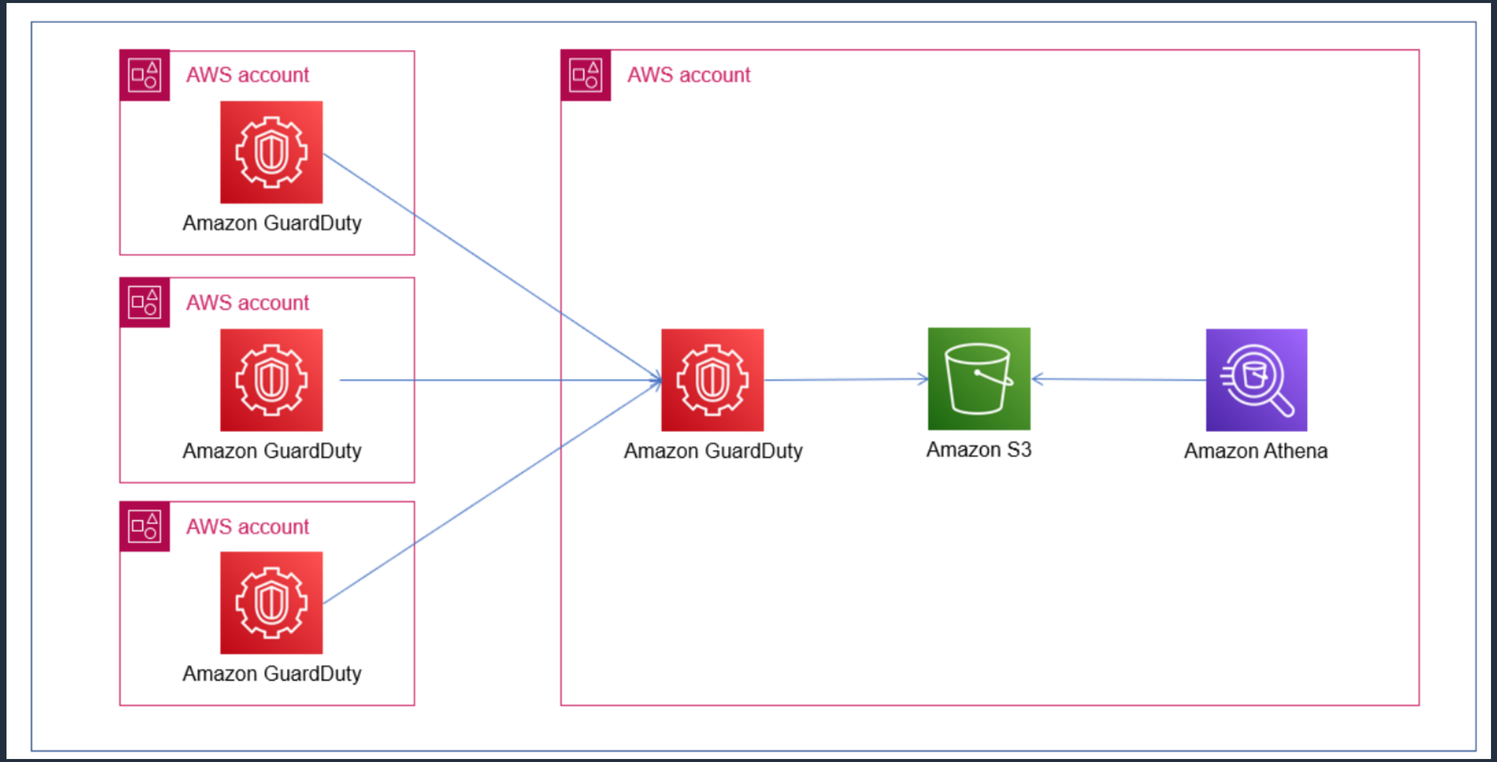
- Managed service for OpenSearch clusters
- Easy to perform interactive log analytics, real-time application monitoring etc.

Amazon QuickSight

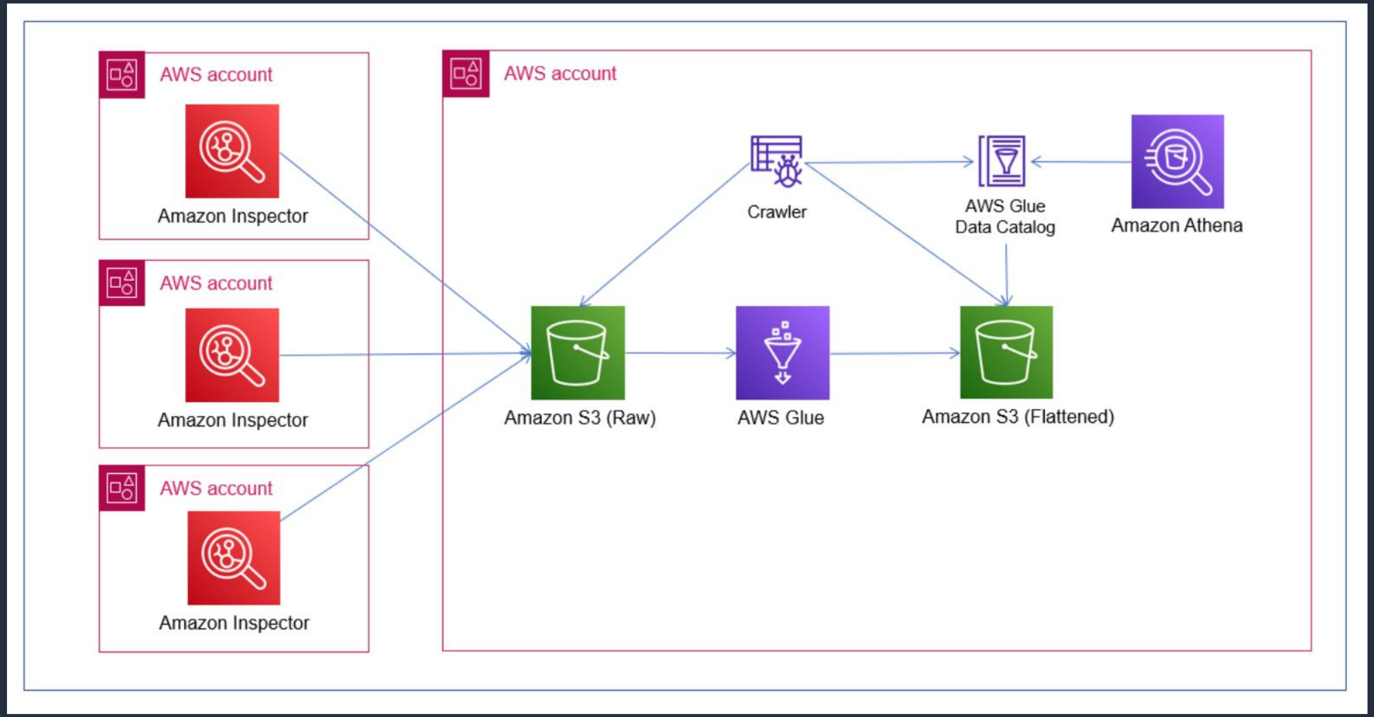
- Unified BI for all your analytics needs
- Provides consistent high performance with auto scale.

Immersion Day - Reference Architectures

Module#1 - Query logs from Amazon GuardDuty and Amazon Inspector

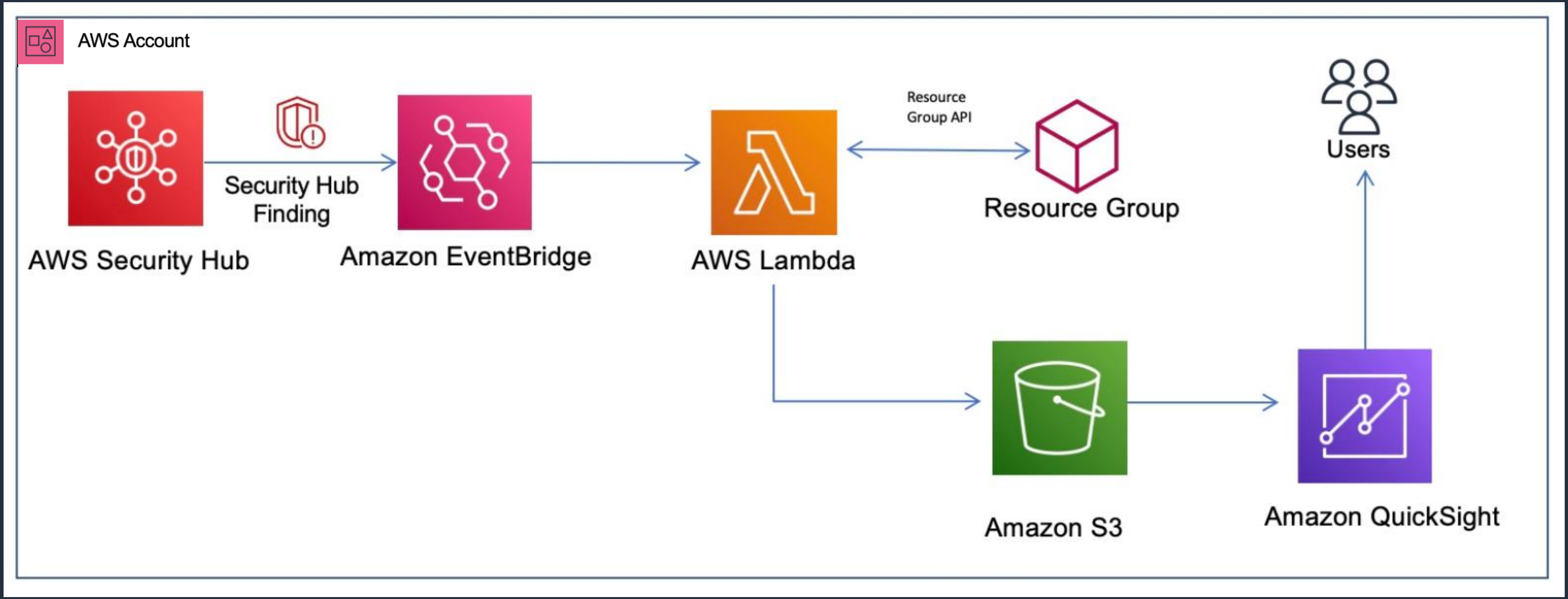


Analyze GuardDuty logs

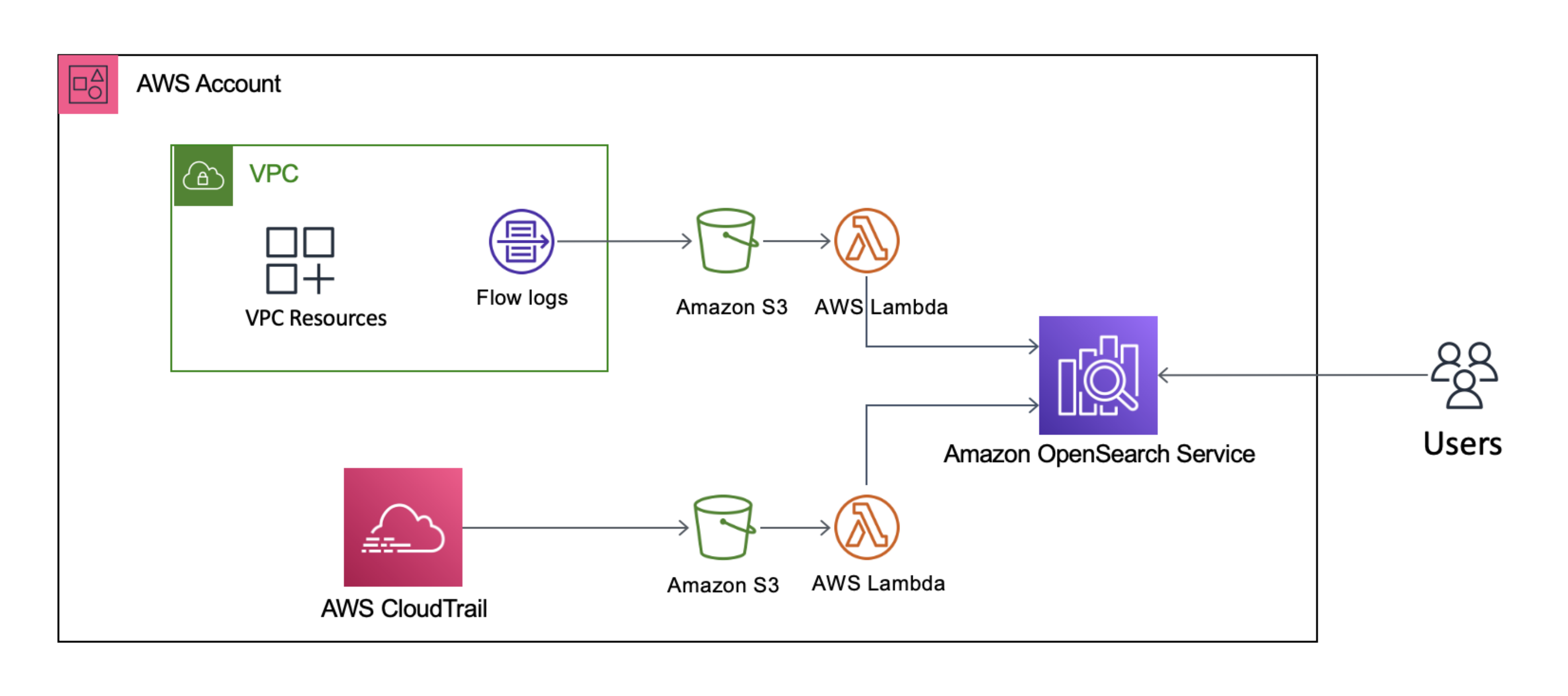


Transform & Analyze Inspector Logs

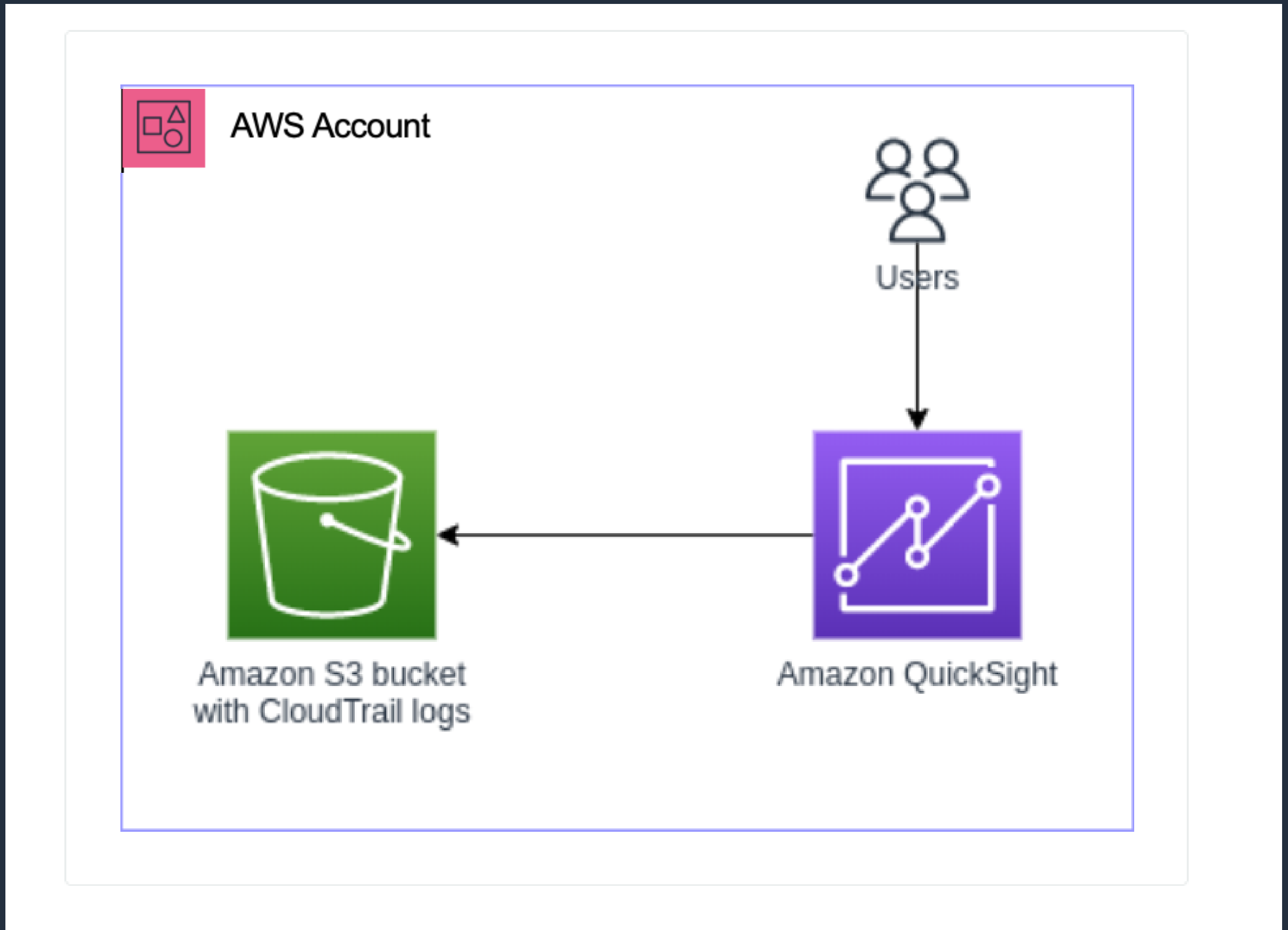
Module#2 - Analyze Security Hub Findings With Athena



Module#3 - Analyze Logs with OpenSearch



Module#4 - Analyze Cloud Trail Logs with Quicksight Q

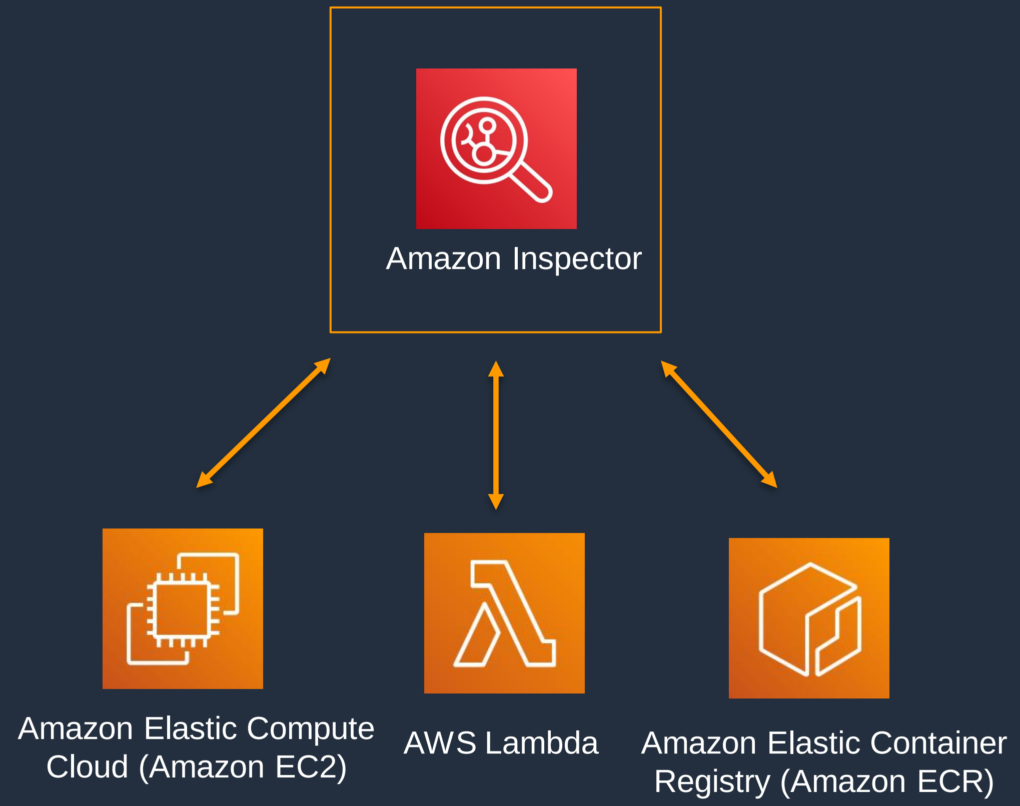


Thank You!

Appendix

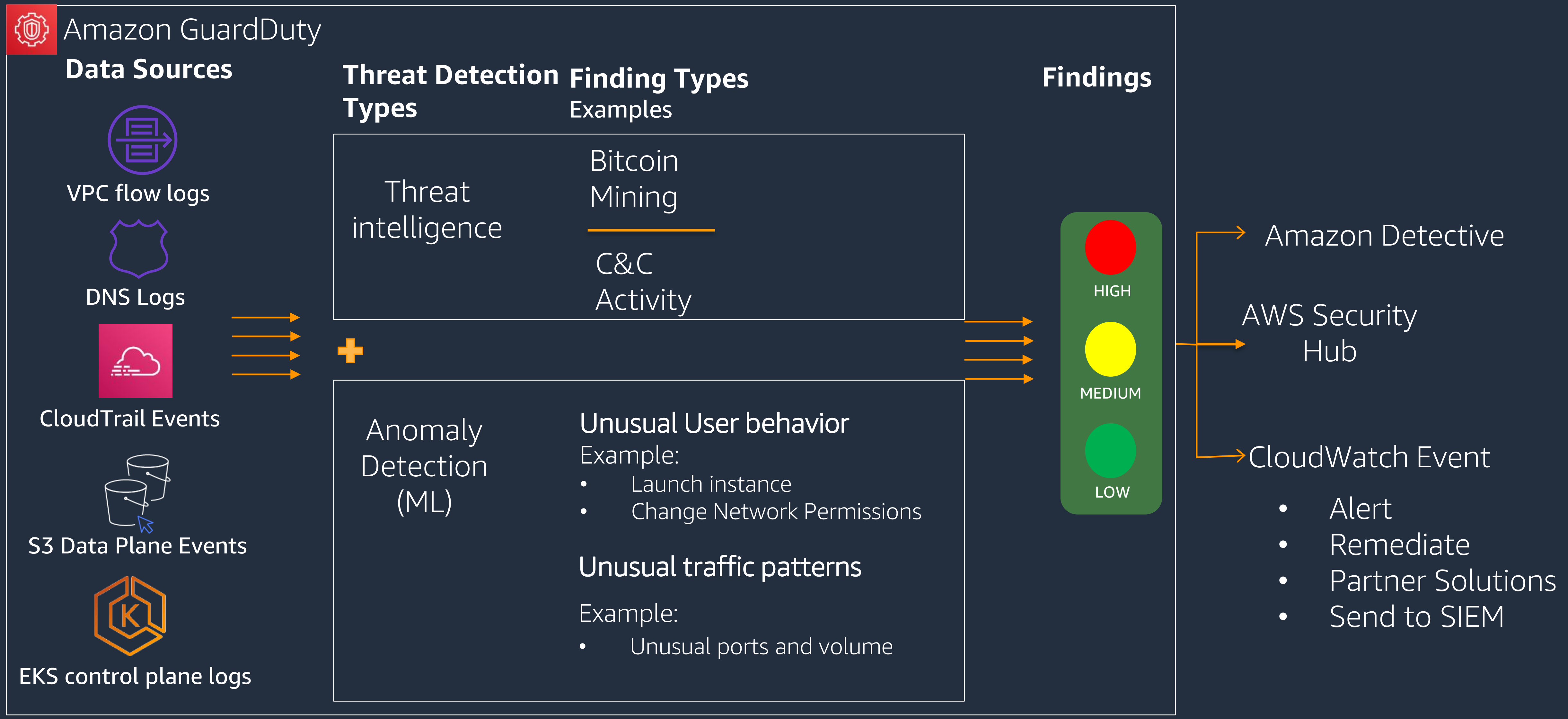
AWS Inspector

- An automated vulnerability management service that continuously scans your workloads for any unintended network exposure or software vulnerabilities.
- Determine prioritization order based on Inspector risk score.
- Integrate to Amazon EventBridge and AWS Security Hub to reduce the time necessary for remediating vulnerabilities.


Amazon Inspector
Amazon Elastic Compute Cloud (Amazon EC2)
AWS Lambda
Amazon Elastic Container Registry (Amazon ECR)

Amazon GuardDuty

Amazon GuardDuty is a threat detection service that continuously monitors your AWS accounts and workloads for malicious activity



Amazon GuardDuty

Data Sources

VPC flow logs

DNS Logs

CloudTrail Events

S3 Data Plane Events

EKS control plane logs

Threat Detection Types

Finding Types Examples

Threat intelligence

Bitcoin Mining

C&C Activity

Anomaly Detection (ML)

Unusual User behavior

Example:

- Launch instance
- Change Network Permissions

Unusual traffic patterns

Example:

- Unusual ports and volume

Findings

HIGH

MEDIUM

LOW

Amazon Detective

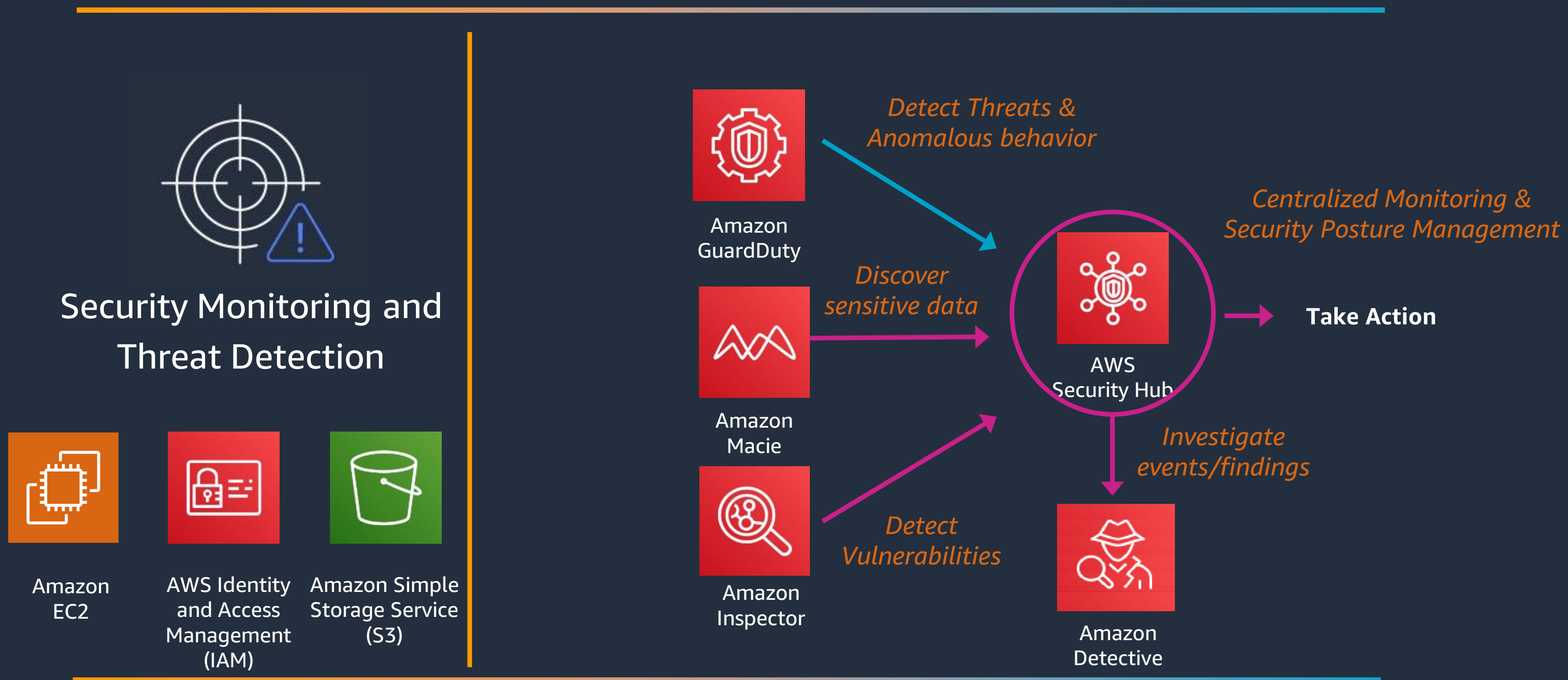
AWS Security Hub

CloudWatch Event

- Alert
- Remediate
- Partner Solutions
- Send to SIEM

AWS Security Hub

A comprehensive view of your security state in AWS by collecting security data from across AWS accounts, services, and supported third-party partner products


Security Monitoring and Threat Detection
Amazon EC2
AWS Identity and Access Management (IAM)
Amazon Simple Storage Service (S3)
Amazon GuardDuty
Detect Threats & Anomalous behavior
Amazon Macie
Discover sensitive data
Amazon Inspector
Detect Vulnerabilities
AWS Security Hub
Centralized Monitoring & Security Posture Management
Take Action
Investigate events/findings
Amazon Detective

AWS Glue

Scalable Data Integration Engine

Built-in data transforms

Execution engine

Monitor

Centralized and Unified Data Governance

Glue Data Catalog

Glue Data Quality

Glue crawlers

Lake Formation

Connect and Ingest Data

Glue connectors

Glue connector marketplace

Variety of interfaces

User Productivity and Data Ops

Persona specific tools

Productivity tools

Data ops tools

Amazon Athena

Simple, instant start

Serverless, no setup

Start quickly, optimized for fast results

Interactive analytics

Integrated tooling works where users are

Run queries on **25+** data stores

Open and flexible

Based on open source, optimized for AWS

Supports multiple formats, compression types, data types, and more

Cost effective

Pay only for what you use

Save **30%–90%** on per-query costs through compression

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.

Secure

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

Observability

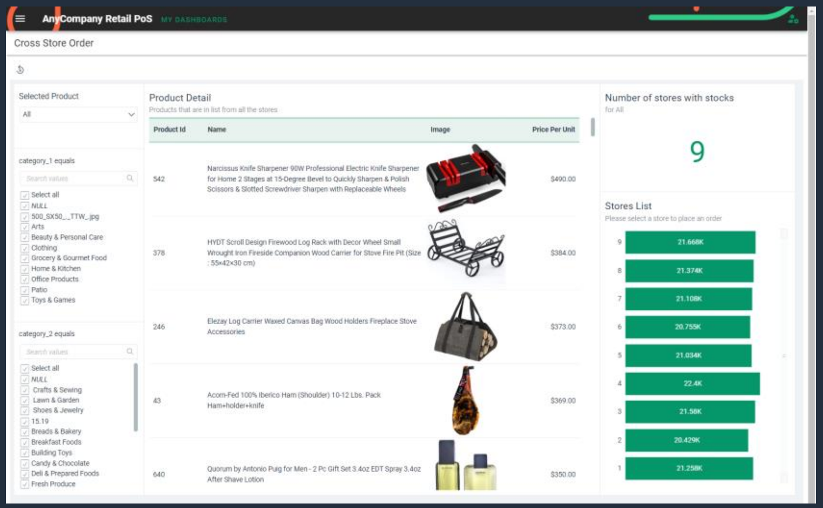
Systematically detect potential threats and react to a system's state

Cost Conscious

Optimize time and resources for strategic work

Amazon QuickSight

Amazon QuickSight service provides unified BI for all your analytics needs and provides consistent high performance with auto scale.



Cross Store Order

Selected Product: All

category_1 equals
- ☑ Select all
- ☑ NULL
- ☑ 500_SX50_._TTW_.jpg
- ☑ Arts
- ☑ Beauty & Personal Care
- ☑ Clothing
- ☑ Grocery & Gourmet Food
- ☑ Home & Kitchen
- ☑ Office Products
- ☑ Patio
- ☑ Toys & Games

category_2 equals
- ☑ Select all
- ☑ NULL
- ☑ Crafts & Sewing
- ☑ Lawn & Garden
- ☑ Shoes & Jewelry
- ☑ 15.19
- ☑ Breads & Bakery
- ☑ Breakfast Foods
- ☑ Building Toys
- ☑ Candy & Chocolate
- ☑ Deli & Prepared Foods
- ☑ Fresh Produce

Product Detail
Products that are in list from all the stores

Product Id	Name	Image	Price Per Unit
542	Narcissus Knife Sharpener 90W Professional Electric Knife Sharpener for Home 2 Stages at 15-Degree Bevel to Quickly Sharpen & Polish Scissors & Slotted Screwdriver Sharpen with Replaceable Wheels		$490.00
378	HYDT Scroll Design Firewood Log Rack with Decor Wheel Small Wrought Iron Fireside Companion Wood Carrier for Stove Fire Pit (Size : 55×42×30 cm)		$384.00
246	Elezay Log Carrier Waxed Canvas Bag Wood Holders Fireplace Stove Accessories		$373.00
43	Acorn-Fed 100% Iberico Ham (Shoulder) 10-12 Lbs. Pack Ham+holder+knife		$369.00
640	Quorum by Antonio Puig for Men - 2 Pc Gift Set 3.4oz EDT Spray 3.4oz After Shave Lotion		$350.00

Number of stores with stocks
for All

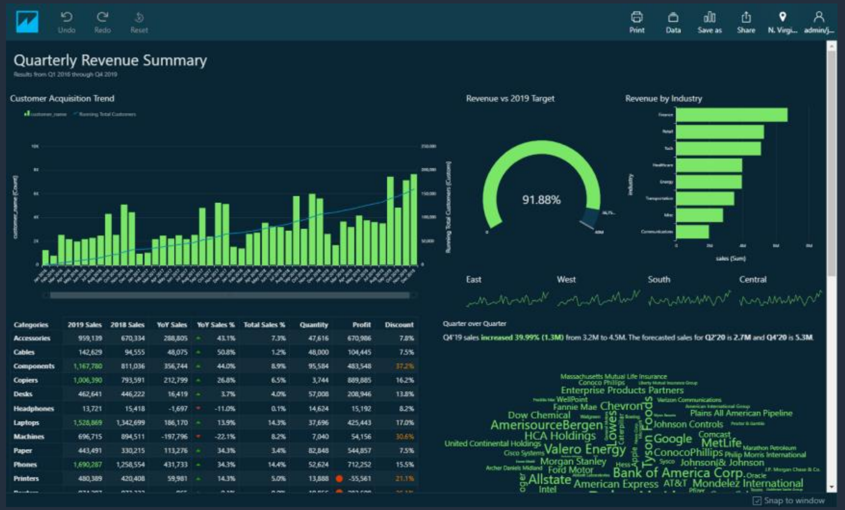
9

Stores List
Please select a store to place an order

9	21.668K
8	21.374K
7	21.108K
6	20.755K
5	21.034K
4	22.4K
3	21.58K
2	20.429K
1	21.258K

Embedded insights

Enhance customer-facing products and monetize data assets



Quarterly Revenue Summary
Results from Q1 2016 through Q4 2019

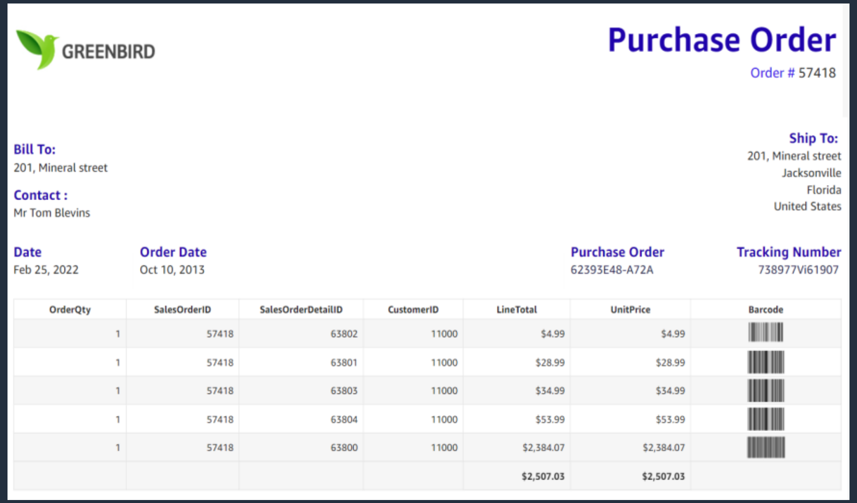
Categories	2019 Sales	2018 Sales	YoY Sales	YoY Sales %	Total Sales %	Quantity	Profit	Discount
Accessories	959,139	670,334	288,805	43.1%	7.3%	47,616	670,986	7.8%
Cables	142,629	94,555	48,075	50.8%	1.2%	48,000	104,445	7.5%
Components	1,167,780	811,036	356,744	44.0%	8.9%	95,584	483,548	37.2%
Copiers	1,006,390	793,591	212,799	26.8%	6.5%	3,744	889,885	16.2%
Desks	462,641	446,222	16,419	3.7%	4.0%	57,008	208,946	13.8%
Headphones	13,721	15,418	-1,697	-11.0%	0.1%	14,624	15,192	8.2%
Laptops	1,528,869	1,342,699	186,170	13.9%	14.3%	37,696	425,443	17.0%
Machines	696,715	894,511	-197,796	-22.1%	8.2%	7,040	54,156	30.6%
Paper	443,491	330,215	113,276	34.3%	3.4%	82,848	544,857	7.5%
Phones	1,690,287	1,258,554	431,733	34.3%	14.4%	52,624	712,252	15.5%
Printers	480,389	420,408	59,981	14.3%	5.0%	13,888	-55,561	21.1%

Quarter over Quarter

Q4'19 sales increased 39.99% (1.3M) from 3.2M to 4.5M. The forecasted sales for Q2'20 is 2.7M and Q4'20 is 5.3M.

Interactive dashboards, meaningful insights

Dashboards, visualizations, and ad-hoc analysis primarily for internal audiences



Purchase Order
Order # 57418

Bill To:
201, Mineral street

Contact :
Mr Tom Blevins

Ship To:
201, Mineral street
Jacksonville
Florida
United States

Date	Order Date	Purchase Order	Tracking Number
Feb 25, 2022	Oct 10, 2013	62393E48-A72A	738977Vi61907

OrderQty	SalesOrderID	SalesOrderDetailID	CustomerID	LineTotal	UnitPrice	Barcode
1	57418	63802	11000	$4.99	$4.99	
1	57418	63801	11000	$28.99	$28.99	
1	57418	63803	11000	$34.99	$34.99	
1	57418	63804	11000	$53.99	$53.99	
1	57418	63800	11000	$2,384.07	$2,384.07	
				$2,507.03	$2,507.03	

Enterprise reporting

Static, highly formatted, email-based reporting distributed to large internal or external audiences