



# Security Analytics Overview

Security Analytics Immersion Day

Sam Burton

February 13, 2025



# Agenda

- Security Analytics Overview
- Common Use Cases
- Analyze Security logs Using Analytics Services
- Log Enrichment and Data Augmentation
- Q&A

# Security Analytics Overview and Use Cases

# Security Analytics Overview

## What

- Approach to cybersecurity that uses data ingestion, data aggregation
- Leverage analysis tools for threat detection and security monitoring.

## Why

- Detect potential threats before they negatively affect company's infrastructure and reduce risk.
- Reduce Risk and Increases compliance

## How

- Combines big data capabilities with threat intelligence
- Leverage data processing techniques such as log enrichment and data augmentation

# Benefits



## Security incident and anomaly detection and response

- By making connections between different events and alerts to detect security incidents or cyberthreats in real time.



## Regulatory compliance

- Comply with government and industry regulations, such as the Health Insurance Portability and Accountability Act ([HIPAA](#)) of 1996 and the Payment Card Industry Data Security Standard ([PCI DSS](#)).



## Enhanced forensics capabilities

- Insights into where attacks originated from, how their systems were compromised, what assets were compromised and identify any data loss, for example.

# Common Use Cases and Challenges

# Common Use Cases

- Companies can deploy security analytics for a wide variety of use cases. Some common use cases include the following:

Analyzing  
network traffic  
to detect  
threats

Monitoring  
suspicious  
Activity

Detecting Data  
Exfiltration

Identifying  
Compromised  
Accounts

Investigating  
malicious  
activity






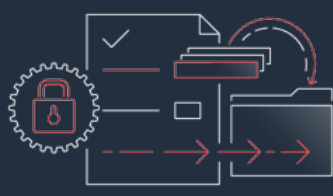
Investigating  
cybersecurity  
incidents

Detecting  
insider threats

# Analyze Security logs Using Analytics Services



# AWS security, identity, and compliance solutions

					
Identity and access management	Detective controls	Infrastructure protection	Data protection	Incident response	Compliance
<div>AWS Identity and Access Management (IAM)</div> <div>AWS Identity Center</div> <div>AWS Organizations</div> <div>AWS Directory Service</div> <div>Amazon Cognito</div> <div>AWS Resource Access Manager</div>	<div>AWS Security Hub</div> <div>Amazon GuardDuty</div> <div>Amazon Inspector</div> <div>Amazon CloudWatch</div> <div>AWS Config</div> <div>AWS CloudTrail</div> <div>VPC Flow Logs</div> <div>AWS IoT Device Defender</div>	<div>AWS Firewall Manager</div> <div>AWS Network Firewall</div> <div>AWS Shield</div> <div>AWS WAF</div> <div>Amazon VPC</div> <div>AWS PrivateLink</div> <div>AWS Systems Manager</div>	<div>Amazon Macie</div> <div>AWS Key Management Service (KMS)</div> <div>AWS CloudHSM</div> <div>AWS Certificate Manager</div> <div>AWS Secrets Manager</div> <div>AWS VPN</div> <div>Server-Side Encryption</div>	<div>Amazon Detective</div> <div>Amazon EventBridge</div> <div>AWS Backup</div> <div>AWS Security Hub</div> <div>AWS Elastic Disaster Recovery</div>	<div>AWS Artifact</div> <div>AWS Audit Manager</div>

← Security Analytics Platform →







# Large community of security partners & solutions

## Network and infrastructure security

## Identity and access control

## Vulnerability and configuration analysis

## Logging, monitoring, SIEM, threat detection, and analytics









## Application security



## Data protection and encryption

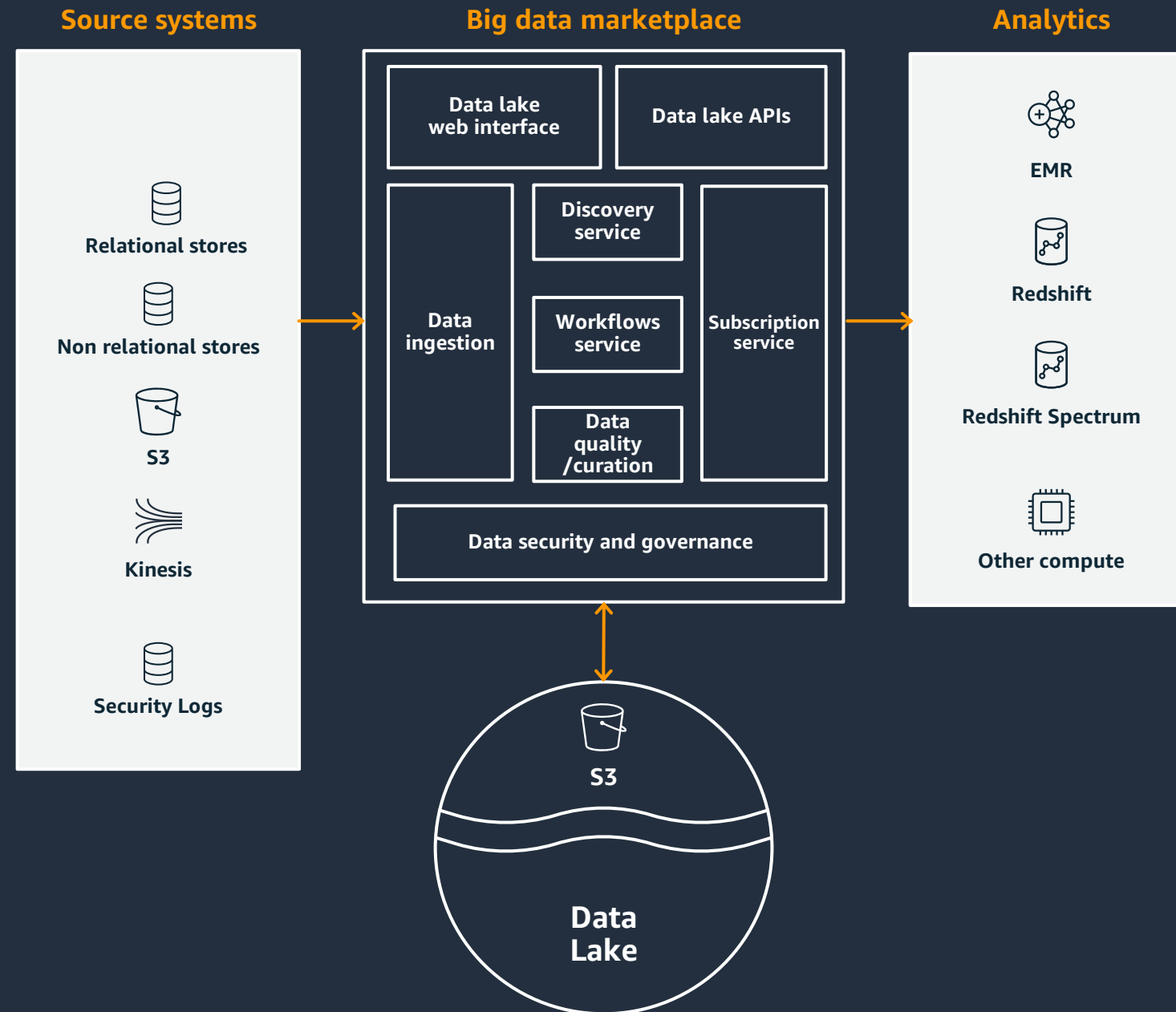


## Host and endpoint security





# Data Analytics Platform



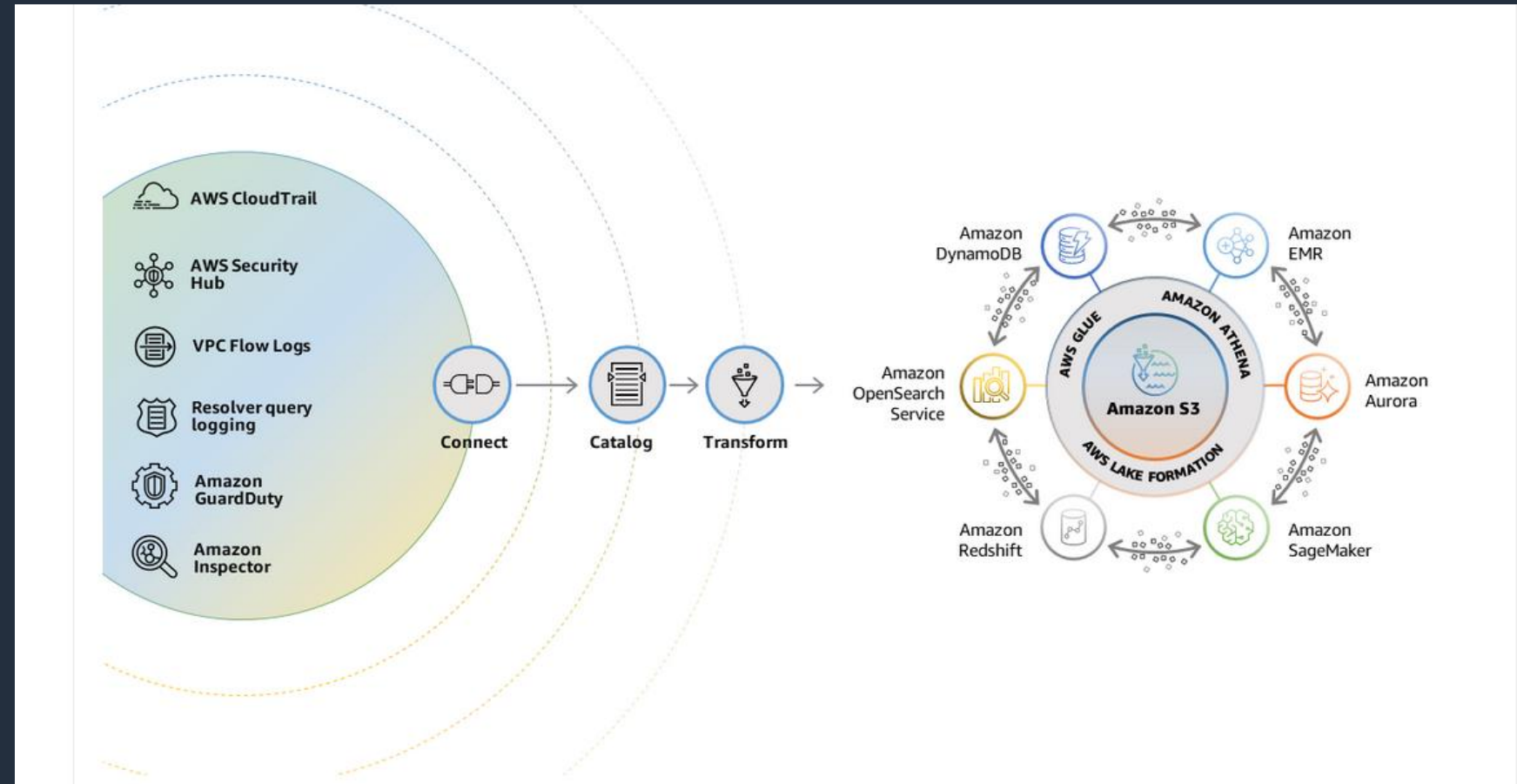
- Ingest Data from multiple sources
- Derive insights from data
  1. LoB Insights
  2. Security Insights

# Consume Security Logs on AWS

“To help customers gain insights in their security controls and **reduce total cost** of ownership of the security insight platform.”

## How

By Aggregating & Correlating various AWS Security Services and 3<sup>rd</sup> Party Security using AWS Analytical Services



# Overview of Log Enrichment and Data Augmentation

# Log Enrichment and Event Augmentation Overview

**What is Log Enrichment?**

Mechanism to build **context** around security logs data in order to better understand meaning, such as intent and scope

**Why is it Important?**

Additional research is often required to fill information gaps and add fidelity to logs in order to reduce research required per incident which results in better informed decisions

**How to achieve it?**

Utilize Security analytics as a mechanism to aid in this research and to automatically associate additional context with an event to provide the analyst with necessary details

# Log Enrichment and Event Augmentation Overview

Common questions often requiring additional research:

- Who owns this IP?
- What country does this IP originate?
- Does this IP route through a country that it should not?
- What routable network does this IP belong?
- What EC2 instance is this IP associated?
- Who owns the EC2 instance associated with this IP?
- What Autonomous System (AS) is this IP's subnet announced from?
- What provider(s) does this AS peer with?
- What is the reputation of this IP? Is it on any public block lists?
- Has this IP touched any honeypots maintained by ISC DShield?
- Is this address space legitimately allocated by a NIC? (eg. ARIN, APNIC, JPNIC, etc)
- What hostnames/domains are associated with this IP?
- What service is this port number?

# Log Enrichment and Event Augmentation

## GeoIP – IP Based Geolocation

Mapping of an IP address to a geographic location.

- Country, Region, City, ZIP
- Latitude/Longitude
- Provider/ISP
- Time Zone

IP: 96.231.179.223  
Network: 96.231.179.0/24  
ISP: Verizon Business  
AS: AS701  
Location: Silver Spring, Maryland 20904 USA  
Time Zone: UTC -05:00  
Hostname: pool-96-231-179-223.washdc.fios.verizon.net  
Lat/Lon: 39.0840/-77.1528

Version	AWS Account	Interface	Source IP	Destination IP	Packets	Bytes	Disposition
Event Data							
▶ 2	41747	eni-b30b9cd5	119.147.115.32	10.1.1.179	6000	22 6 1 40	1442975475 1442975535 REJECT OK
▼ 2	41747	eni-b30b9cd5	169.54.233.117	10.1.1.179	21188	80 6 1 40	1442975535 1442975595 REJECT OK
▼ 2	41747	eni-b30b9cd5	212.7.209.6	10.1.1.179	3389	3389 6 1 40	1442975596 1442975655 REJECT OK
▼ 2	41747	eni-b30b9cd5	189.134.227.225	10.1.1.179	39664	23 6 2 120	1442975656 1442975716 REJECT OK
▼ 2	41747	eni-b30b9cd5	77.85.113.238	10.1.1.179	0	0 1 1 100	1442975656 1442975716 REJECT OK
▼ 2	41747	eni-b30b9cd5	10.1.1.179	198.60.73.8	512	123 17 1 76	1442975776 1442975836 ACCEPT OK

Source Port

Protocol

Start and End Time

Destination Port



# Log Enrichment and Event Augmentation

## Example Service and System Audit Trails and Potential Enrichment Data Sets

### AWS Service Trails

- AWS API Calls - CloudTrail
- IP Communications - VPC Flowlogs
- Domain Name System - Route53
- Application Firewalls - WAF
- Load Balancers - ALB

### Open Source Data Sets

- Internet Routing Table - Routeviews
- Top-Level Domains - Public Suffix, whois
- Anonymous Proxies - TOR Entry/Exit Nodes
- Unallocated Address Space - BOGONs
- Whois and SWIP Assignments - RADDDB

### Infrastructure Management Systems

- Operations and Change Management - ServiceNow
- Cloud Infrastructure Management – AWS VPC and EC2
- Systems Inventory and Management – AD, RH Satellite
- IPAM, DNS, DHCP – InfoBlox, Bluecat, AD
- Security Toolings – Qualys, Tenable

### Commercial Data Sets

- Public Internet Scanning – Shodan, Censys
- Domain Registrations - DomainTools
- Passive Internet DNS - Farsight DNSDB (DT)
- GeoIP Location - MaxMind
- Certificate Sightings - CRT.sh

# Thank you!

