



Detect

# AWS Foundational and Layered Security Services



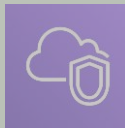
AWS  
Security  
Hub



AWS  
Organizations



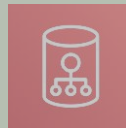
AWS Transit  
Gateway



Amazon  
VPC



AWS IoT  
Device  
Defender



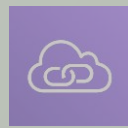
Amazon  
Cloud  
Directory



AWS  
Control  
Tower



AWS  
Trusted  
Advisor



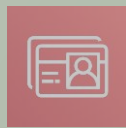
Amazon  
VPC  
PrivateLink



AWS  
Direct  
Connect



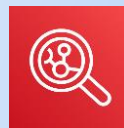
Resource  
Access  
manager



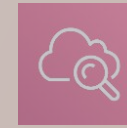
AWS  
Directory  
Service



Amazon  
GuardDuty



Amazon  
Inspector



Amazon  
CloudWatch



AWS Step  
Functions



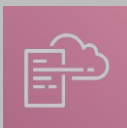
AWS Systems  
Manager



AWS  
Lambda



AWS  
OpsWorks



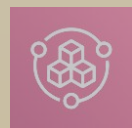
AWS CloudFormation

**Automate**

**Identify**

**Protect**

**Detect**



AWS Service  
Catalog



AWS Config



AWS Shield



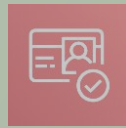
IAM



AWS Secrets  
Manager



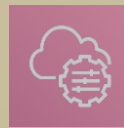
KMS



Amazon  
Cognito



AWS Well-  
Architected  
Tool



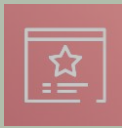
AWS  
Systems  
Manager



AWS  
WAF



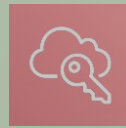
AWS  
Firewall  
Manager



AWS  
Certificate  
Manager



AWS  
CloudHSM



AWS IAM  
Identity  
Center

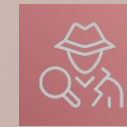


Amazon  
Macie

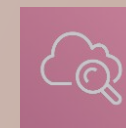


AWS  
Security  
Hub

**Investigate**



Amazon  
Detective



Amazon  
CloudWatch



AWS  
CloudTrail



Personal Health  
Dashboard



Amazon  
Route 53



Amazon S3  
Glacier



Snapshot



Archive

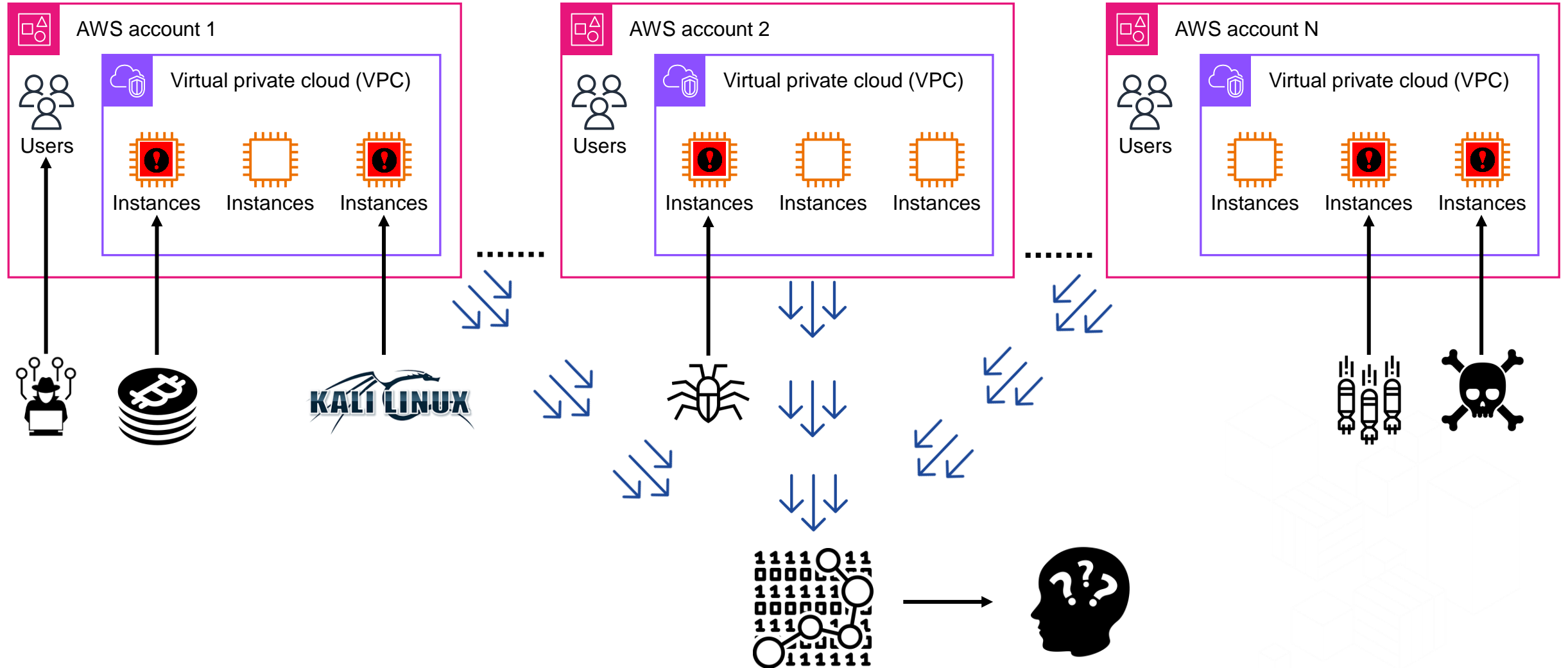


Amazon GuardDuty



# Why we need Amazon GuardDuty?

- A typical enterprise architecture

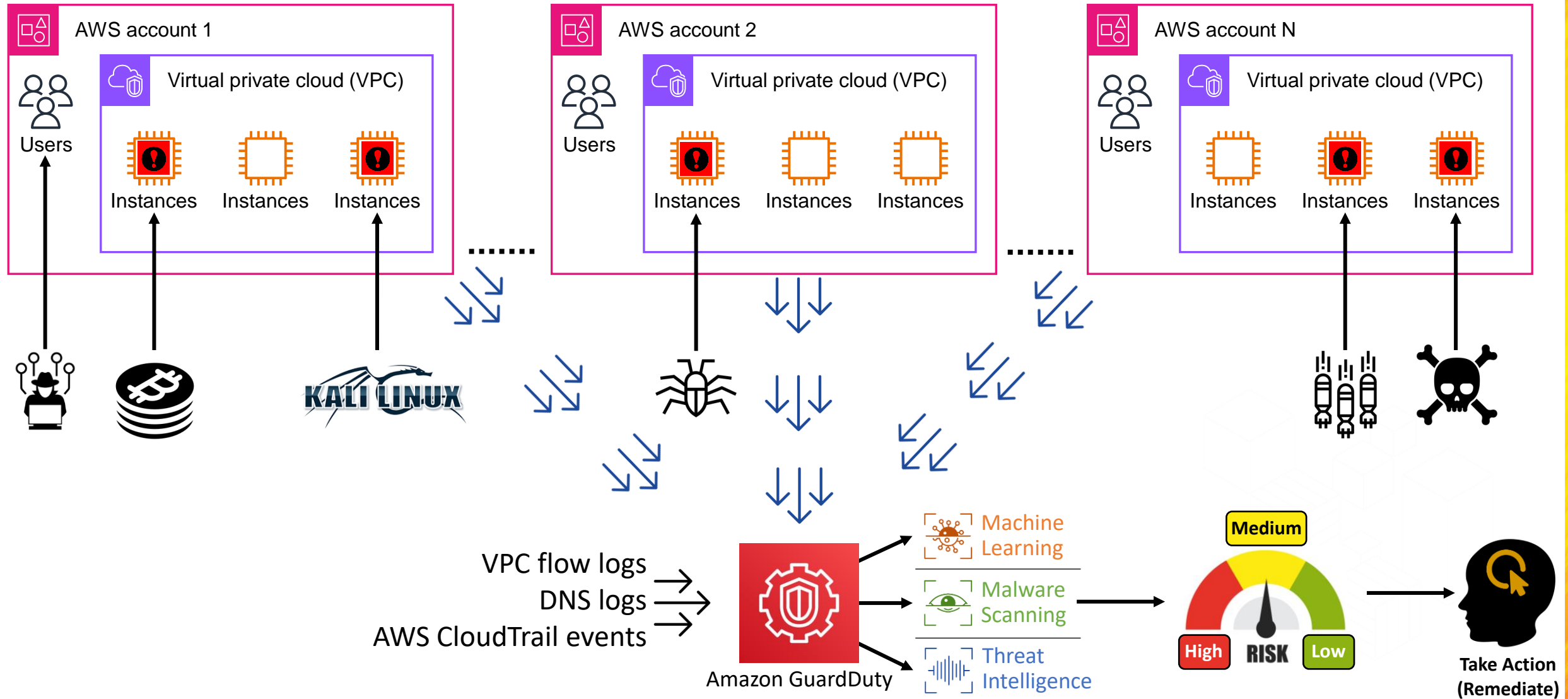


## Finding a needle in the haystack



# Why we need Amazon GuardDuty?

- A typical enterprise architecture





# Amazon GuardDuty

- Amazon GuardDuty is a threat detection service that continuously monitors your AWS accounts and workloads for malicious activity and delivers detailed security findings for visibility and remediation.
- It analyzes and processes Foundational data sources, such as AWS CloudTrail management events, AWS CloudTrail event logs, VPC flow logs (from Amazon EC2 instances), and DNS logs.
- It also processes Features such as Kubernetes audit logs, RDS login activity, S3 logs, EBS volumes, Runtime monitoring, and Lambda network activity logs.
- It uses threat intelligence feeds, such as lists of malicious IP addresses and domains, and machine learning to identify unexpected, potentially unauthorized, and malicious activity within your AWS environment.

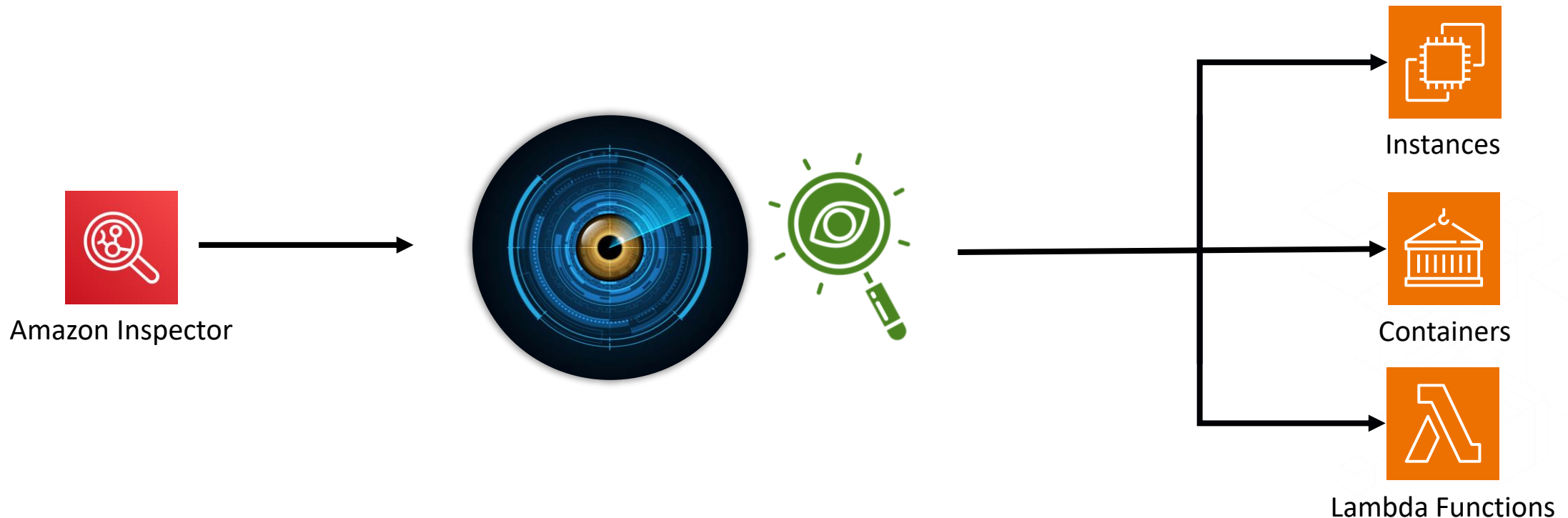


Amazon Inspector

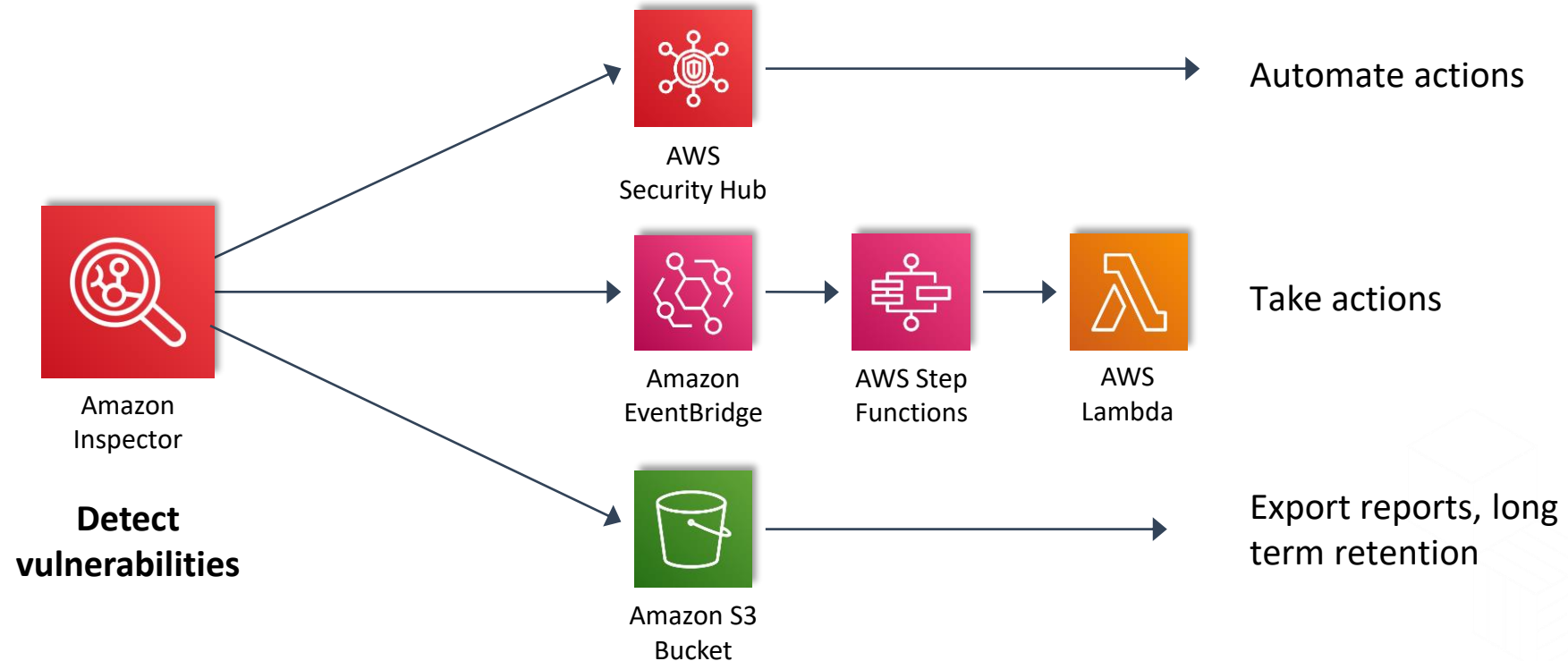


# Amazon Inspector

- Amazon Inspector is an automated vulnerability management service that continually scans AWS workloads for software vulnerabilities and unintended network exposure.
- A vulnerability is a weakness that can be exploited by cybercriminals to gain unauthorized access to a system.



# Automated vulnerability management through Amazon Inspector



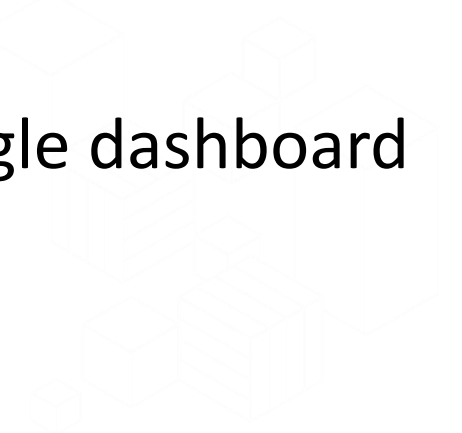


AWS Security Hub

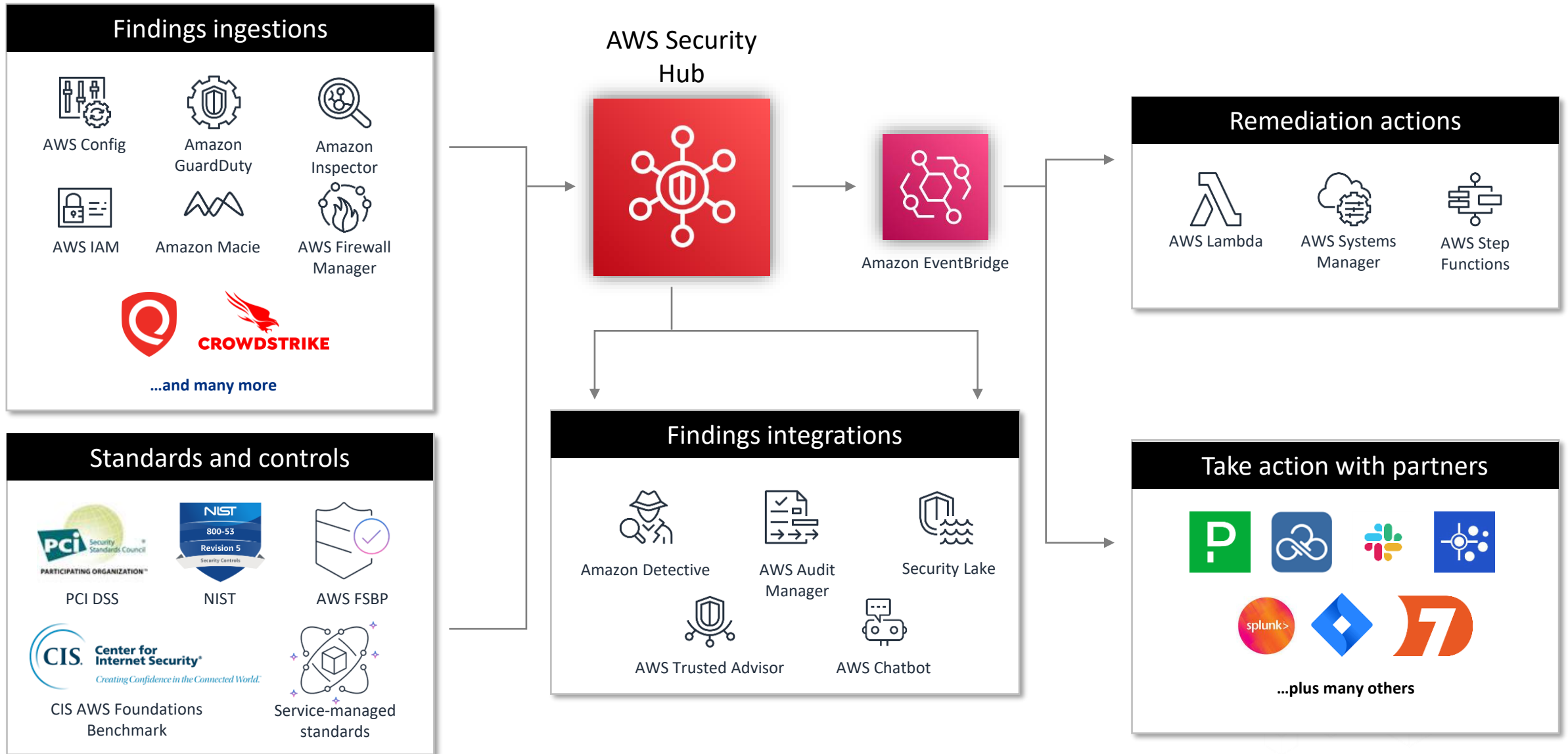


## AWS Security Hub

- AWS Security Hub is a cloud security posture management service that continuously performs security best practice checks and seamlessly aggregates security findings from AWS and third-party services and enables automated response.
- Security Hub ingests findings from multiple AWS services, including Amazon GuardDuty, Amazon Inspector, AWS Firewall Manager, and AWS Health, and also from third-party services.
- It can be integrated with AWS Organizations to provide a single dashboard where you can view findings across your organization.



# AWS Security Hub





Amazon Macie



# Amazon Macie

- Amazon Macie is a data security service that discovers sensitive data by using machine learning and pattern matching, provides visibility into data security risks, and enables automated protection against those risks.
- If Macie detects a potential issue with the security or privacy of your data, such as a bucket that becomes publicly accessible, Macie generates a finding for you to review and remediate as necessary.

