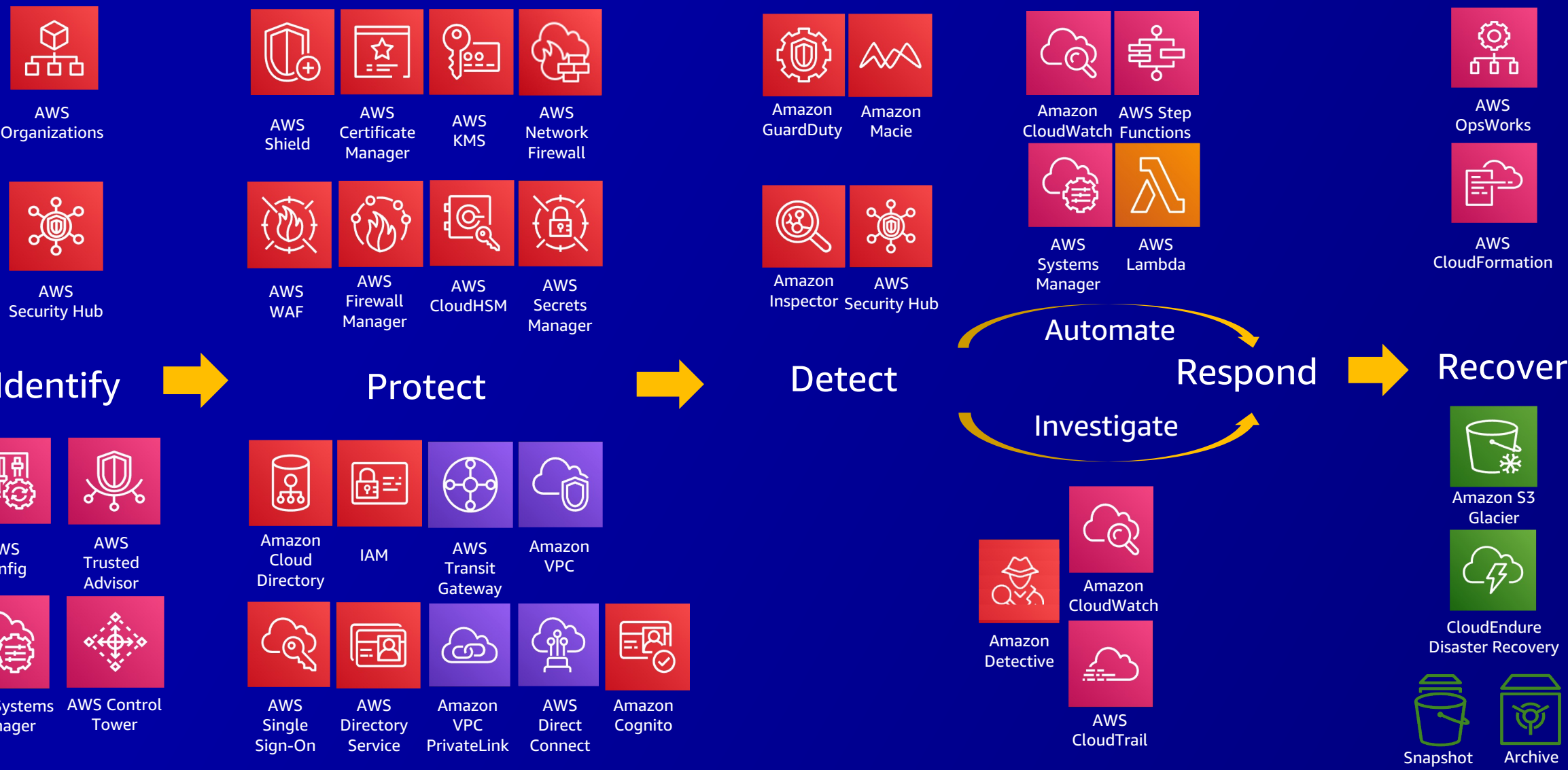
Real-world lessons on how to operationalize security findings

신 은 수

Security Specialist Solutions Architect

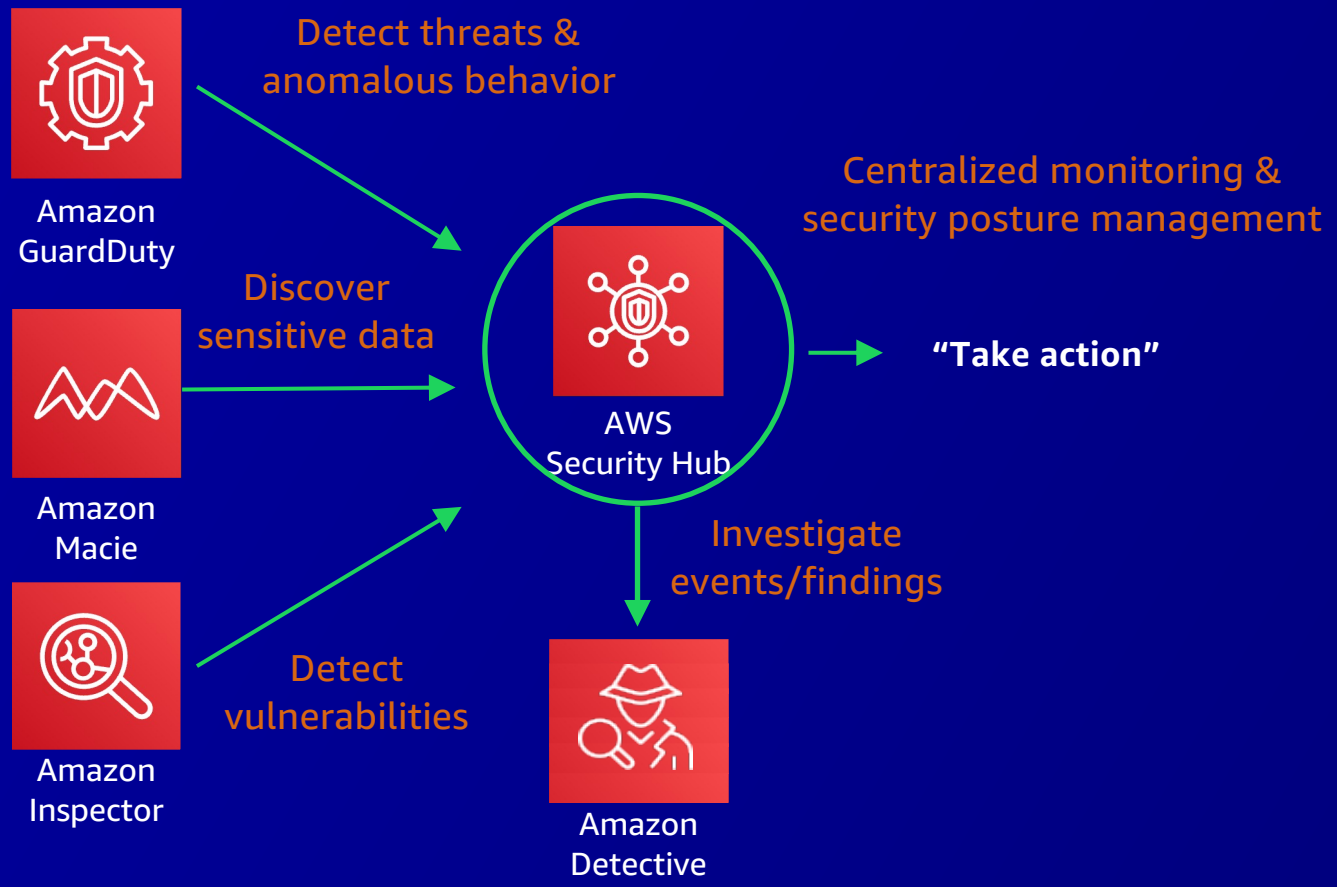
AWS foundational and layered security services



AWS threat detection and monitoring services

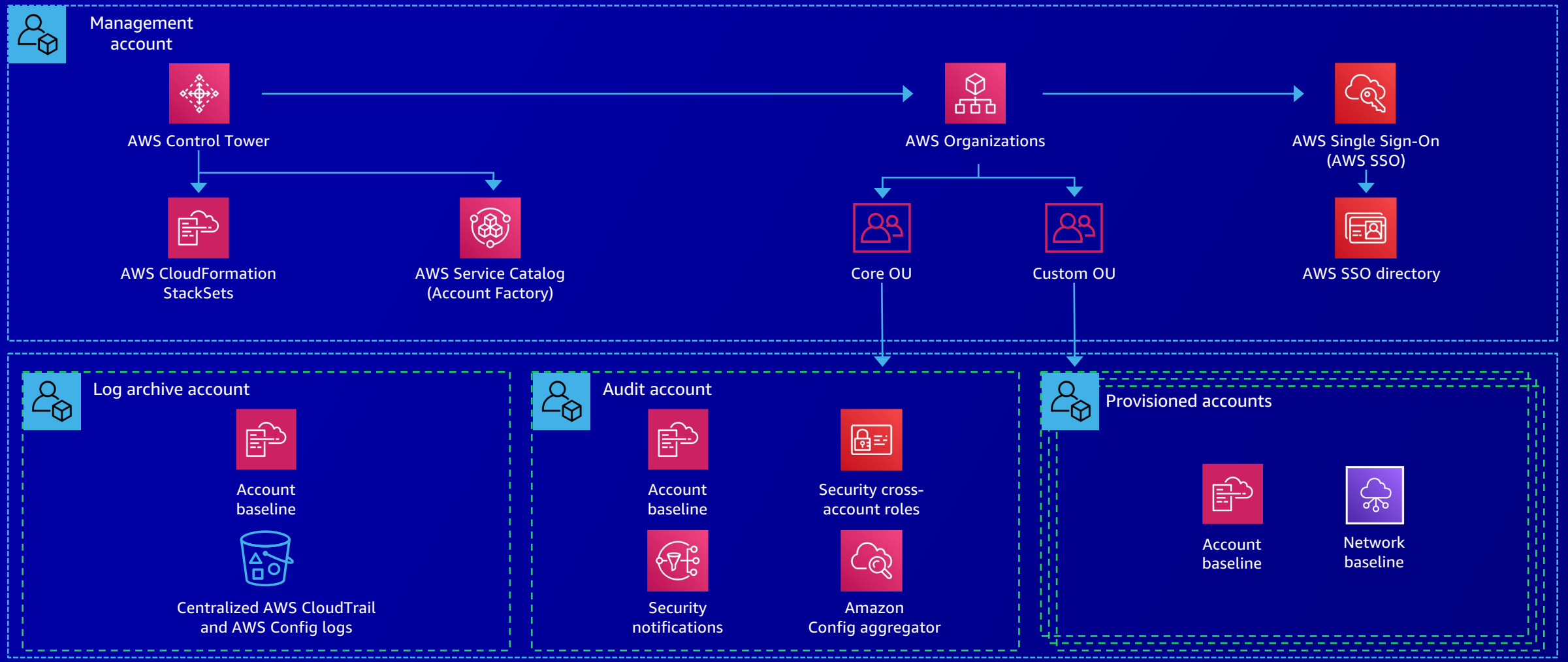
Security monitoring and threat detection

Integrated with AWS workloads in an AWS account along with identities and network activity

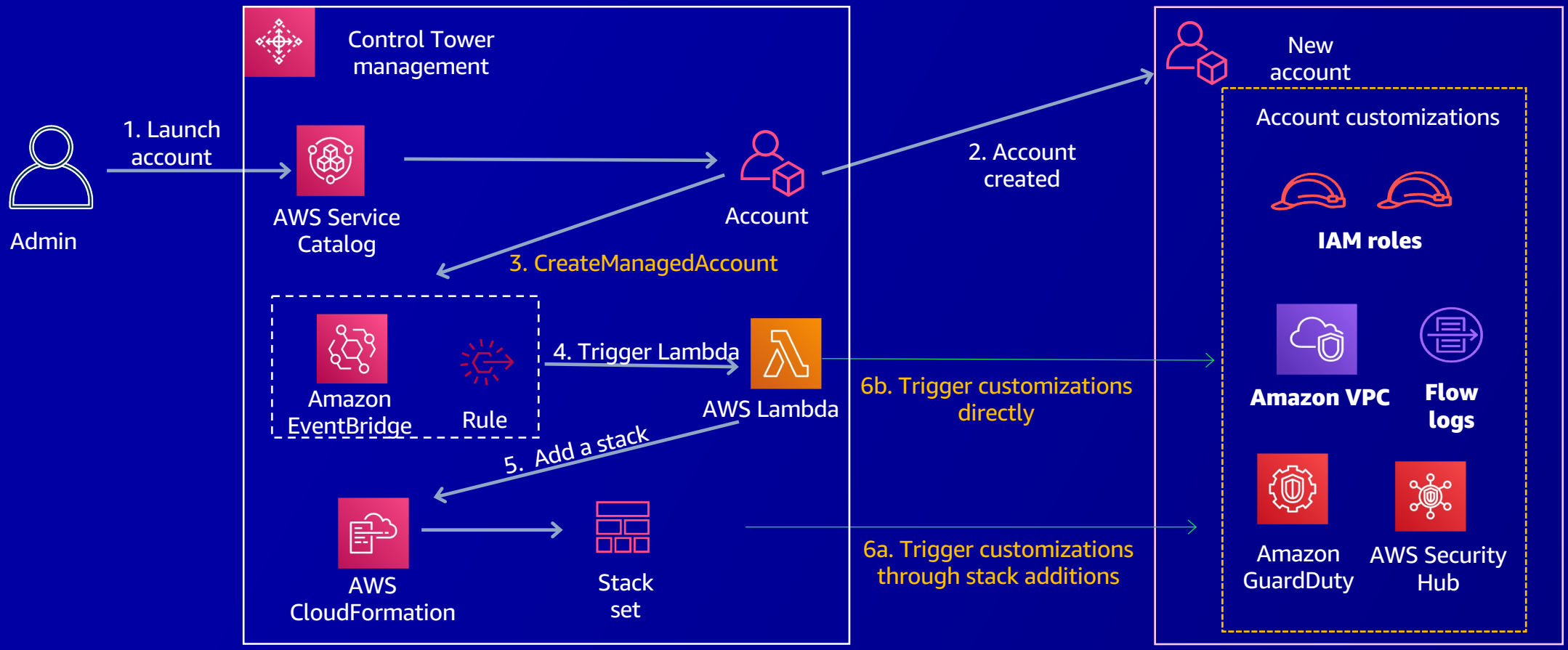


Top 10 security use cases

1 Maintain an accurate inventory of accounts, resources, and applications



2 Verify the configuration of assets by identifying and enabling preventative and detective controls



3 Automatically enable security features and monitor their coverage

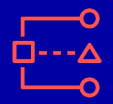
Amazon GuardDuty

Amazon Macie

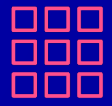
AWS Firewall Manager

AWS Config

Amazon Inspector



IAM Access Analyzer



Third-party integrations

AWS Security Hub

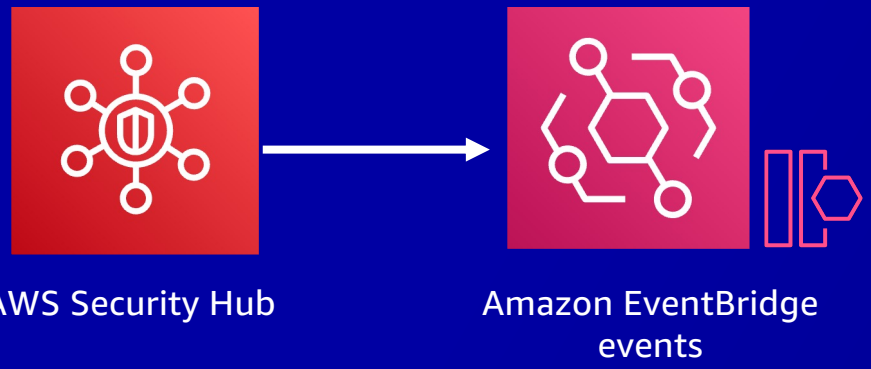
Aggregate and prioritize findings

Conduct automated security checks against benchmarks

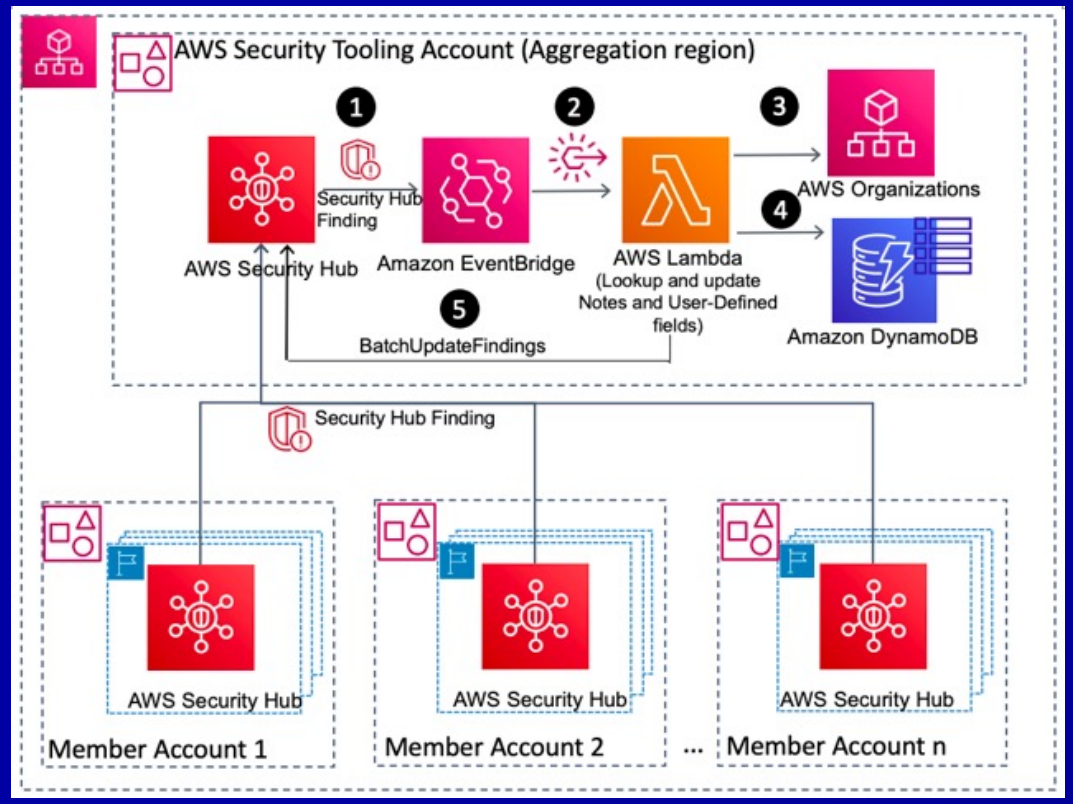
Take action to investigate or respond & remediate

Better visibility into **security issues.** Easier to stay in **compliance.**

4 Detect, normalize, and aggregate security findings and logs

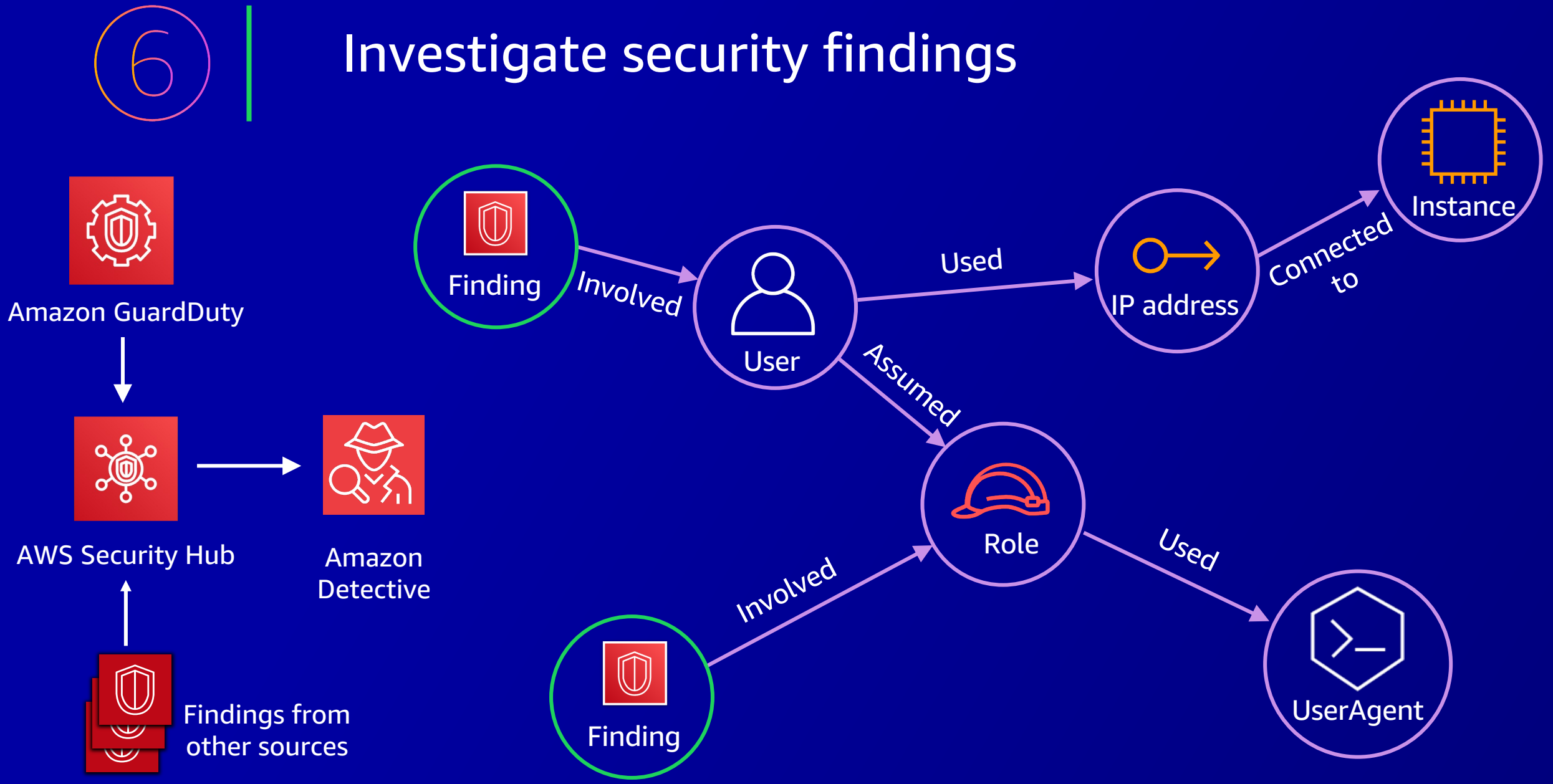


5 Enrich, correlate, and prioritize security findings



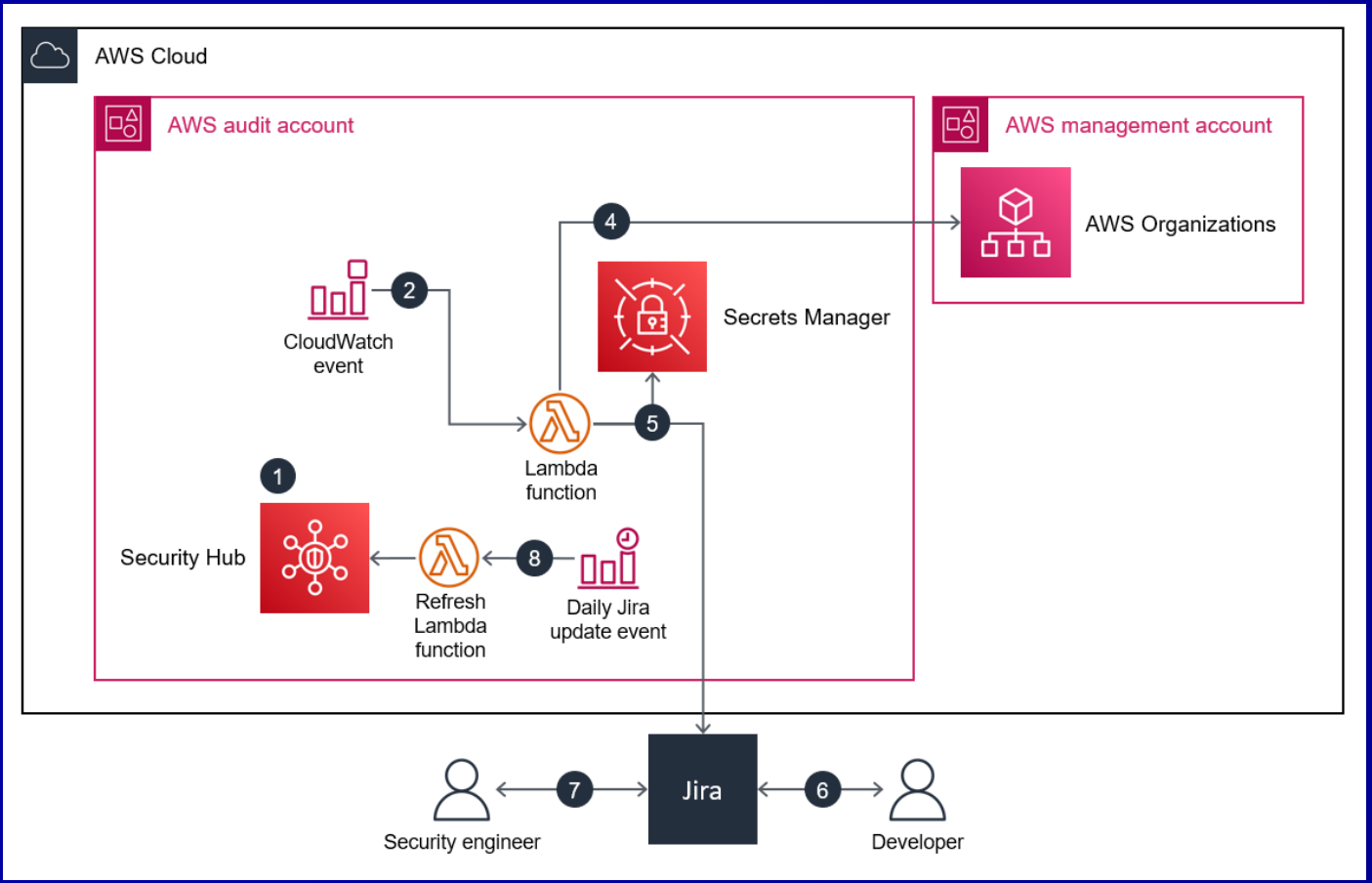
1. Amazon EventBridge rule triggers an AWS Lambda function each time a finding is created or updated
2. Lambda function uses the account ID to retrieve account and alternate contact information using AWS Organizations and account management APIs
3. Lambda function caches the account metadata in an Amazon DynamoDB table for 24 hours
4. Using **BatchUpdateFindings** API, **Note** and **UserDefinedFields** attributes of the Security Hub finding is updated with account metadata

6 Investigate security findings



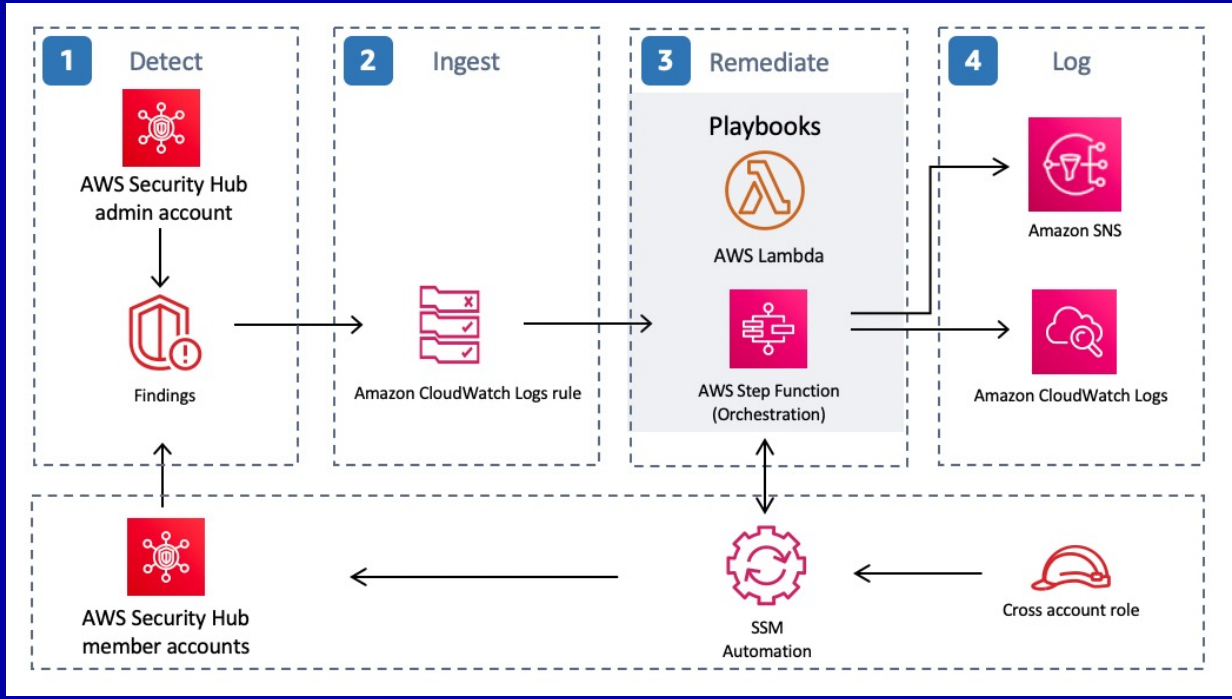
7

Manage exceptions and SLAs for acknowledging and resolving findings



1. Native bi-directional integration between AWS Security Hub and partner tools.
2. Using this solution, you can automatically and manually create and update tickets from Security Hub findings.
3. Security teams can use this integration to notify developer teams of severe security findings that require action.

8 Automatically export, respond to, and remediate findings



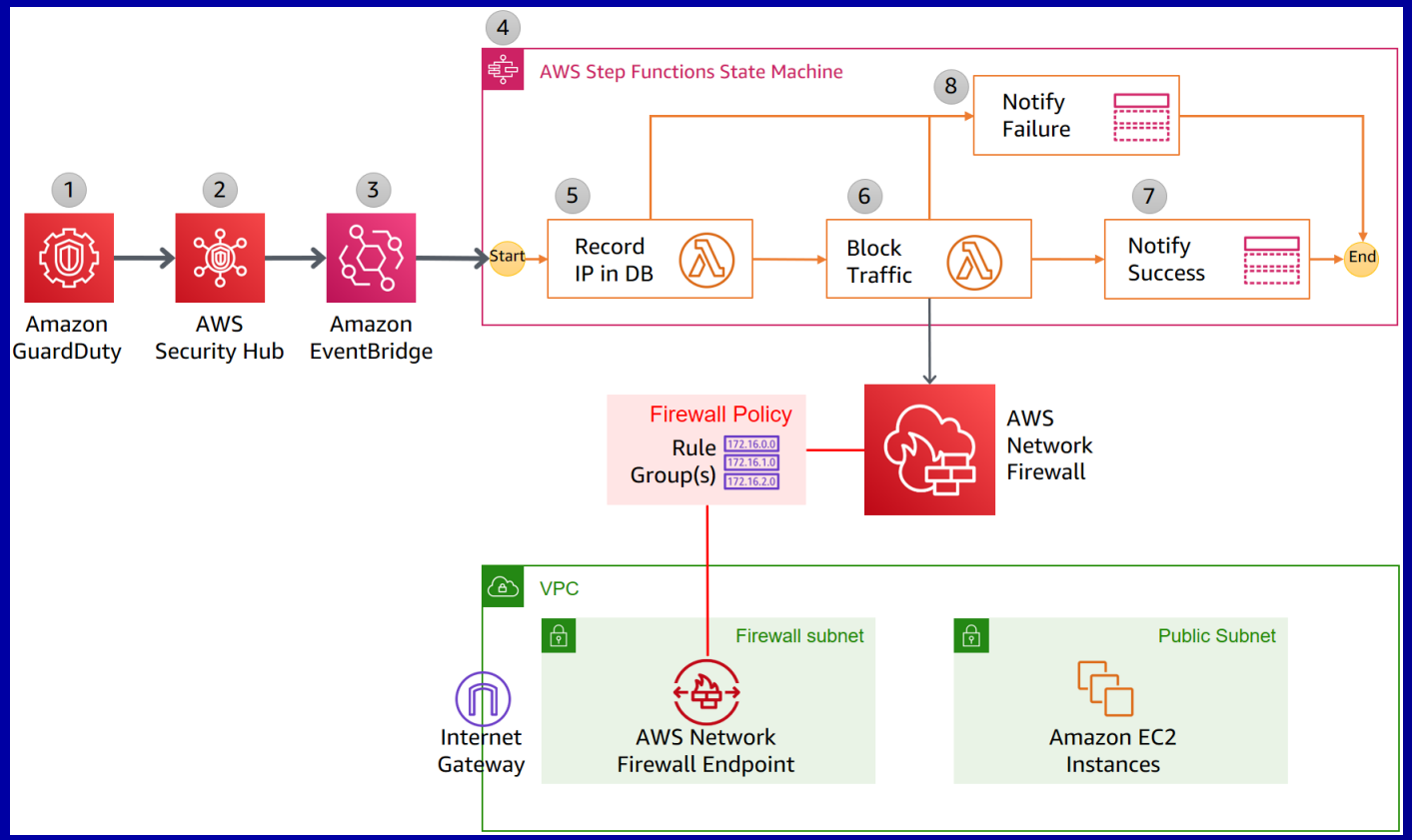
Detect: Security Hub provides a comprehensive view of security alerts and posture across all of your AWS accounts.

Ingest: Findings from Security Hub are sent to Amazon CloudWatch Events/EventBridge. You can then set up rules to be invoked on specific findings or send these findings via a Security Hub Custom Action.

Remediate: CloudWatch Events/EventBridge rules can have AWS Lambda targets, AWS Systems Manager automation documents, or AWS Step Functions to automatically remediate.

Log: Playbooks will log to CloudWatch for a complete audit trail of actions. The findings are updated as **RESOLVED** after the remediation is run.

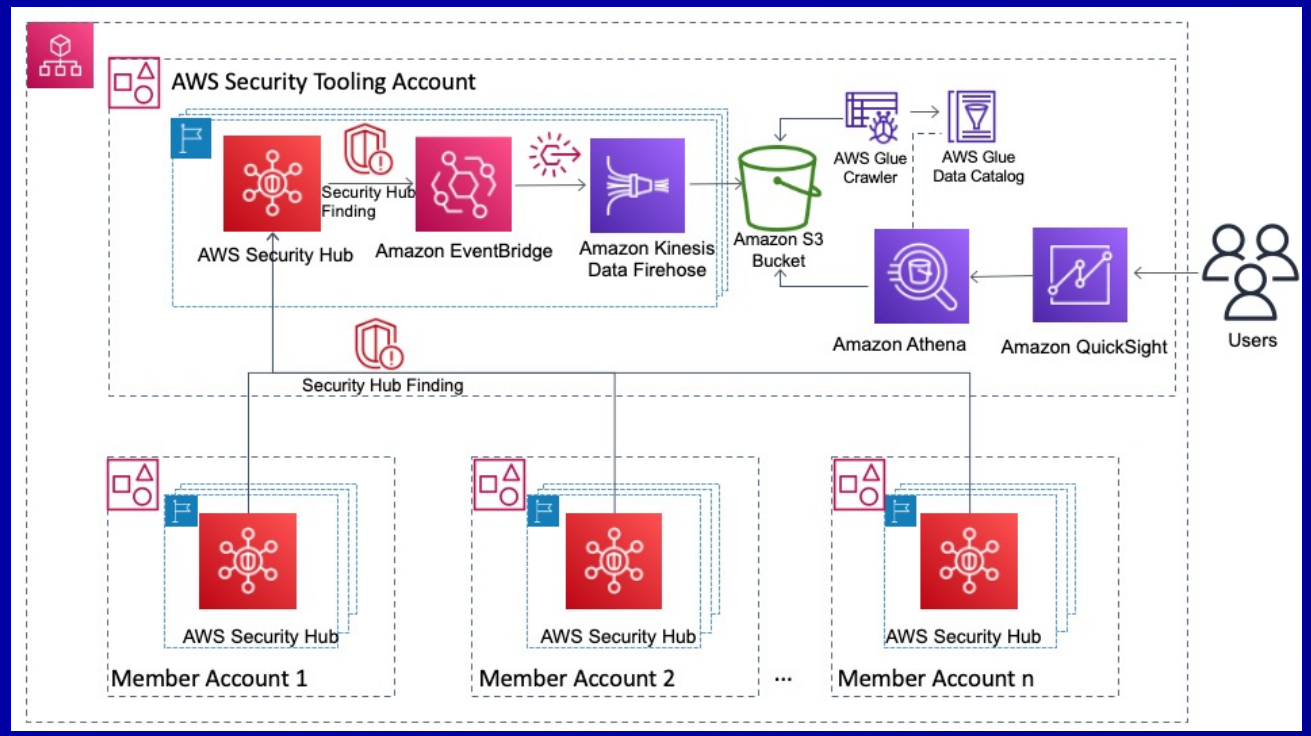
9 Identify, investigate, and recover from security incidents



1. GuardDuty detects unexpected behavior that includes a remote host IP address
2. Security Hub ingests the finding generated by GuardDuty and consolidates it with findings from other AWS security services
3. EventBridge has a rule with an event pattern that matches GuardDuty events that contain the remote IP address
4. The Step Functions state machine ingests the details of the Security Hub finding published in EventBridge and orchestrates the remediation response

10

Track and report on key security metrics



1. Centralize findings across the organization into Security Hub
2. Publish findings to EventBridge, which delivers those findings to Amazon Kinesis Data Firehose
3. Kinesis Data Firehose will push the findings to an Amazon S3 bucket that has been partitioned by AWS account number, region, date
4. Configure an AWS Glue crawler to pull the schema of the data from Amazon S3 and query the data with Amazon Athena
5. Plug Amazon QuickSight into Amazon Athena to build dashboards of interesting data and trends

How AWS security team operationalizes findings

1. Onboarding & prioritization
2. Enrichment
3. Response
4. Feedback

Onboarding & prioritization

Reminder

ThreatPurpose:ResourceTypeAffected/ThreatFamilyName.DetectionMechanism

Backdoor:EC2/DenialOfService.Tcp

LOW (3.9 - 1.0) | MEDIUM (6.9 - 4.0) | HIGH (8.9 - 7.0)

Finding breakdown & grouping

- Threat purpose
- Threat family name
- Resource (AWS service)

Organization specific data points

- Number of findings in the past 30 days
- GD severity -> Org severity

Enrichment

Reminder

GuardDuty data sources
AWS CloudTrail management event logs, AWS CloudTrail data events for Amazon S3, DNS logs, Amazon EKS audit logs, and VPC Flow Logs

Make findings actionable

- What information would be needed to notify and respond?
  - The right owner (email, team, severity)
- What systems hold this information?

Sample finding


```
[  {
    “AccountId”: “123456789012”
    "CreatedAt": "2022-06-24T15:02:29.871Z",
    "Description": "Credentials…have been used from external IP address 198.51.100.0.",
    "Id": "38c0cb1e3377f530c813345fa5404c52",
"Region": "us-east-1",
"ImageDescription": "GeneratedFindingInstaceImageDescription",
        "ImageId": "ami-99999999",
        "InstanceId": "i-99999999",
"LaunchTime": "2016-08-02T02:05:06.000Z",
      "Archived": false,
      "Count": 1,
      "DetectorId": "5ab09337fe408cbe096b1496e3f007be",
      "EventFirstSeen": "2022-06-24T15:02:29.000Z",
      "EventLastSeen": "2022-06-24T15:02:29.000Z",
      "ResourceRole": "TARGET",
      "ServiceName": "guardduty",
"Type": "default" }},
    "Severity": 8,
    "Title": "Credentials for instance role GeneratedFindingUserName used from external IP address.",
    "Type": "UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS",
    "UpdatedAt": "2022-06-24T15:02:29.871Z”
} ]
```

Enrichment

Other considerations

- IAM role
- Organization severity
- Accounts details
  - Classification (production/non-production)
  - Data classification (business data, customer data, customer metadata)
  - Team-specific routing
  - Individual owners
  - Spend

Response

Runbooks

- Ticketing for the service teams
  - Explaining the finding to the team
- Alerts for the response teams
- Automation

Feedback

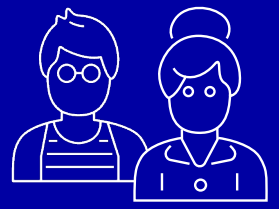
Feedback loop

- Grouping open findings
- Future development efforts
- Human judgement and service team engagement

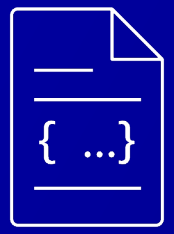
Exemptions

- Account level (customer/service accounts)
- Account level + finding level (by-design services)

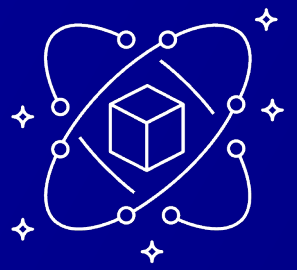
Key takeaways



Identify your key personas



Transition security requirements into user stories



Apply a layered security approach

Thank you!