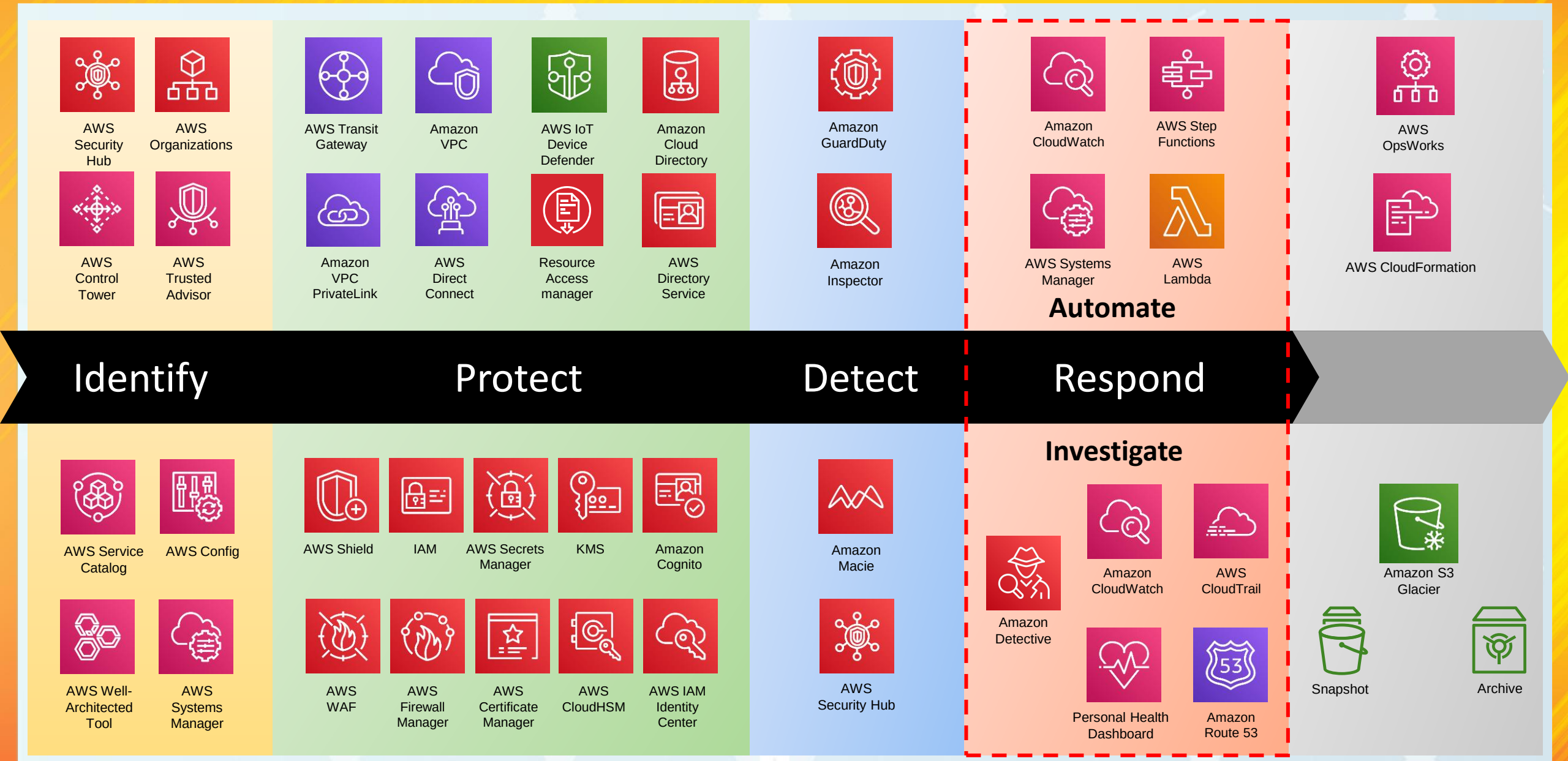
Respond

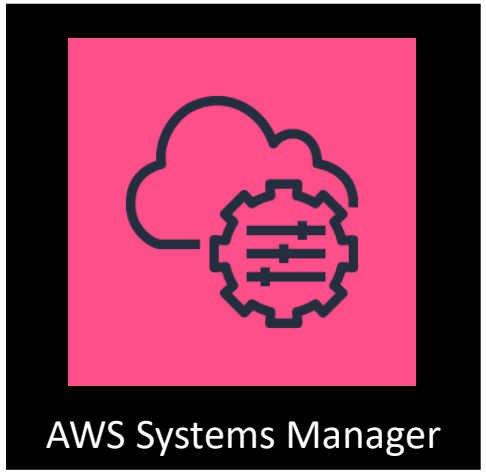
AWS Foundational and Layered Security Services



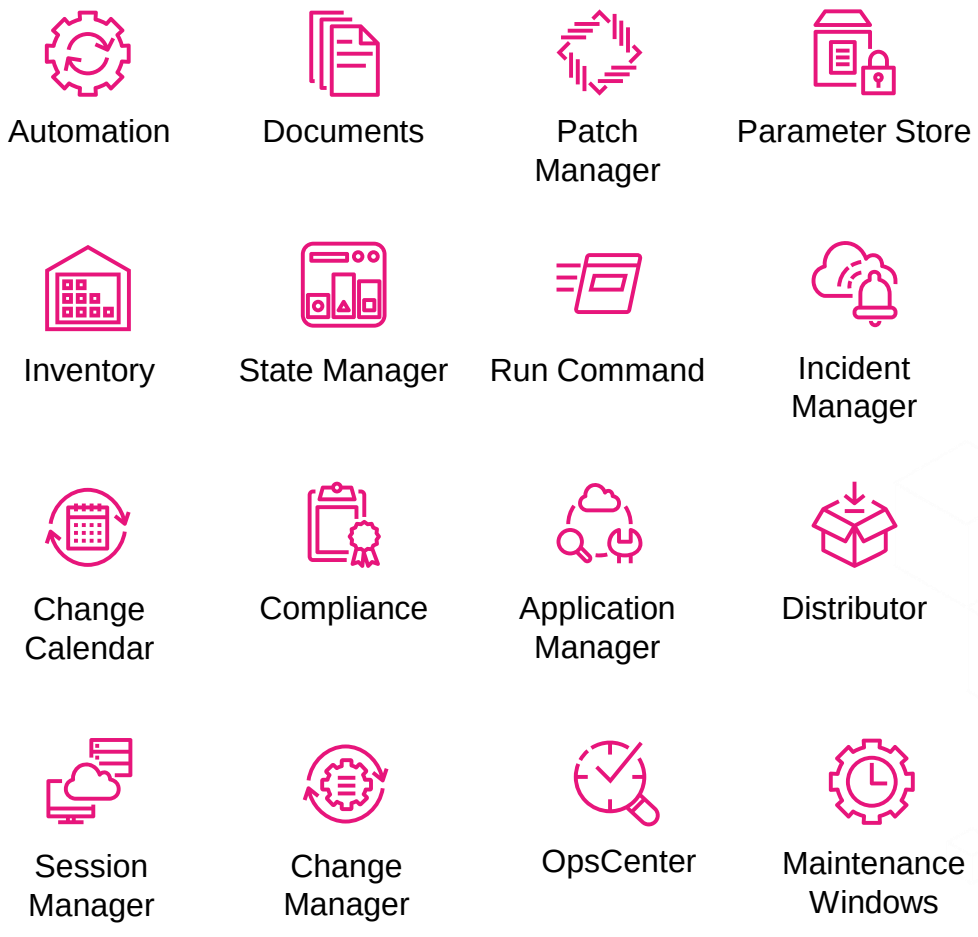
AWS Systems Manager

AWS Systems Manager

- AWS Systems Manager is the operations hub for your AWS applications and resources and a secure end-to-end management solution for hybrid and multicloud environments that enables secure operations at scale.

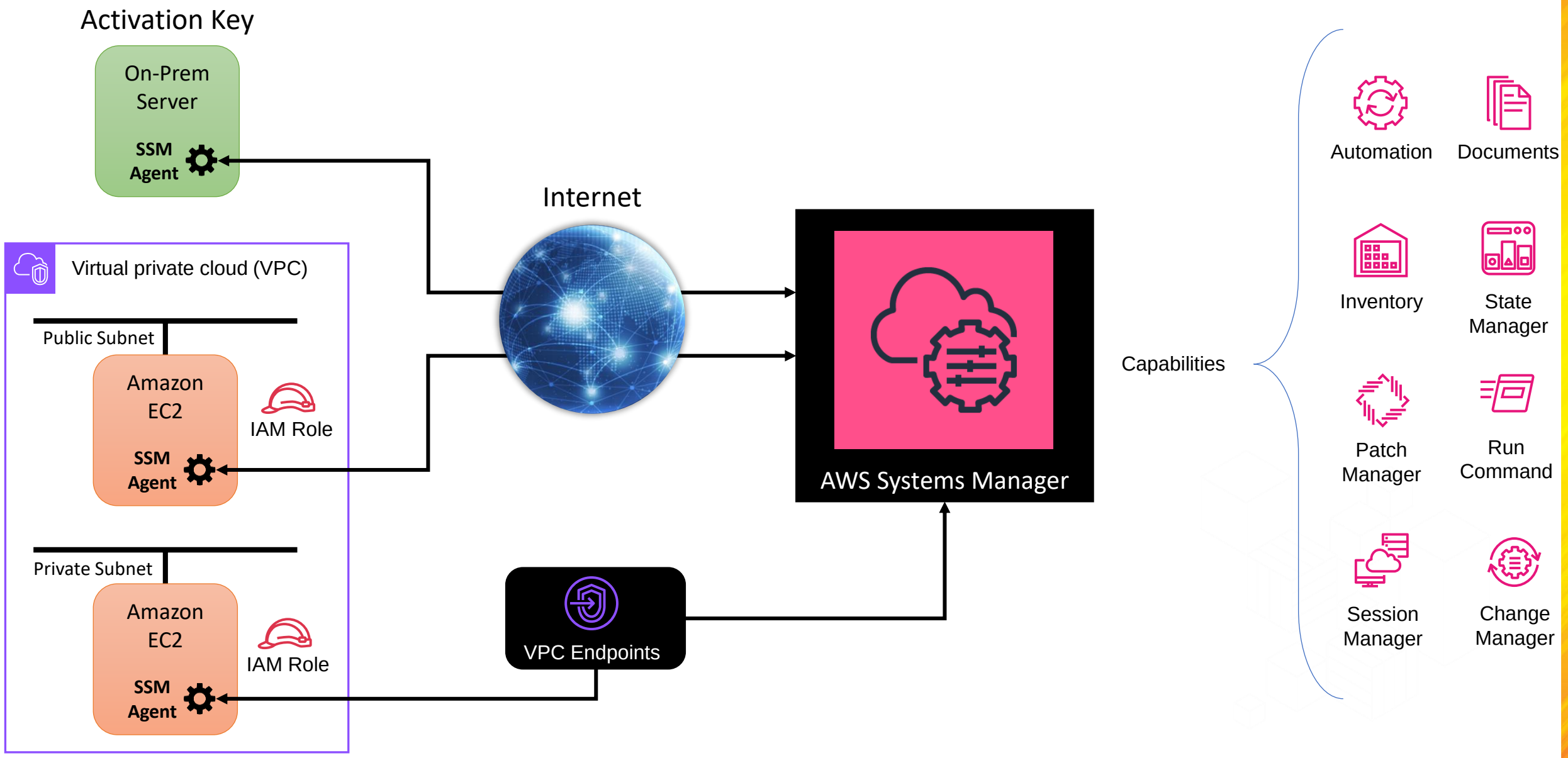


Capabilities



Workshop

Managing nodes using the AWS Systems Manager agent



Session Manager

- Session Manager lets you manage your EC2 instances, on-premises servers, edge devices, and virtual machines (VMs), including VMs in other cloud environments, through an interactive one-click browser-based shell or through the AWS CLI.
- Session Manager provides secure and auditable instance management without the need to open inbound ports, maintain bastion hosts, or manage SSH keys.

Session Manager

Documents

- An AWS Systems Manager document (SSM document) the configuration options, policies, and the actions that Systems Manager performs on your managed instances and other AWS resources.

- Documents use JavaScript Object Notation (JSON) or YAML, and they include steps and parameters that you specify.

- You can use pre-defined AWS managed documents or create your own depending on your use case.

Example

Documents

State Manager

- State Manager automates the process of keeping your managed nodes and other AWS resources in a state that you define.
- State Manager offers the following benefits for managing your nodes
  - Bootstrap nodes with specific software at start-up.
  - Download and update agents on a defined schedule, including the SSM Agent.
  - Join nodes to a Microsoft Active Directory domain.
  - Patch nodes with software updates throughout their lifecycle.
  - Run scripts on managed nodes throughout their lifecycle.
- An association includes three components and one optional set of components:
  - A Command or Automation document that defines the state.
  - Target(s), which can be managed nodes or other AWS resources.
  - A schedule for when or how often to apply the state.
  - (Optional) Runtime parameters specific to the document.

State Manager

Patch Manager

- You can patch Amazon EC2 instances, edge devices, and on-premises servers and virtual machines (VMs), including VMs in other cloud environments.
- You can scan instances to see only a report of missing patches, or you can scan and automatically install all missing patches.
- You can target instances individually or in large groups by using resource tags or Resource Groups.
- Patch Manager doesn’t support upgrading major versions of operating systems, such as Windows Server 2016 to Windows Server 2019, or SUSE Linux Enterprise Server (SLES) 12.0 to SLES 15.0.

Patch Manager

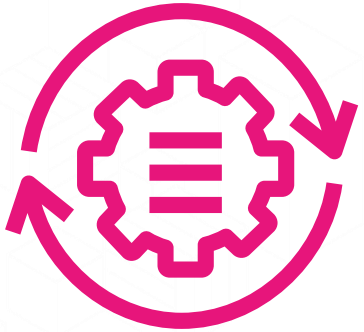
Run Commands

- Run Command lets you remotely and securely manage the configuration of your managed instances. Run Command enables you to automate common administrative tasks and perform ad-hoc configuration changes at scale.
- You can use Run Command from the AWS Management Console, the AWS Command Line Interface, AWS Tools for Windows PowerShell, or the AWS SDKs.
- Administrators use Run Command to install or bootstrap applications, build a deployment pipeline, capture log files when an instance is removed from an Auto Scaling group, join instances to a Windows domain, and more.

Run Command

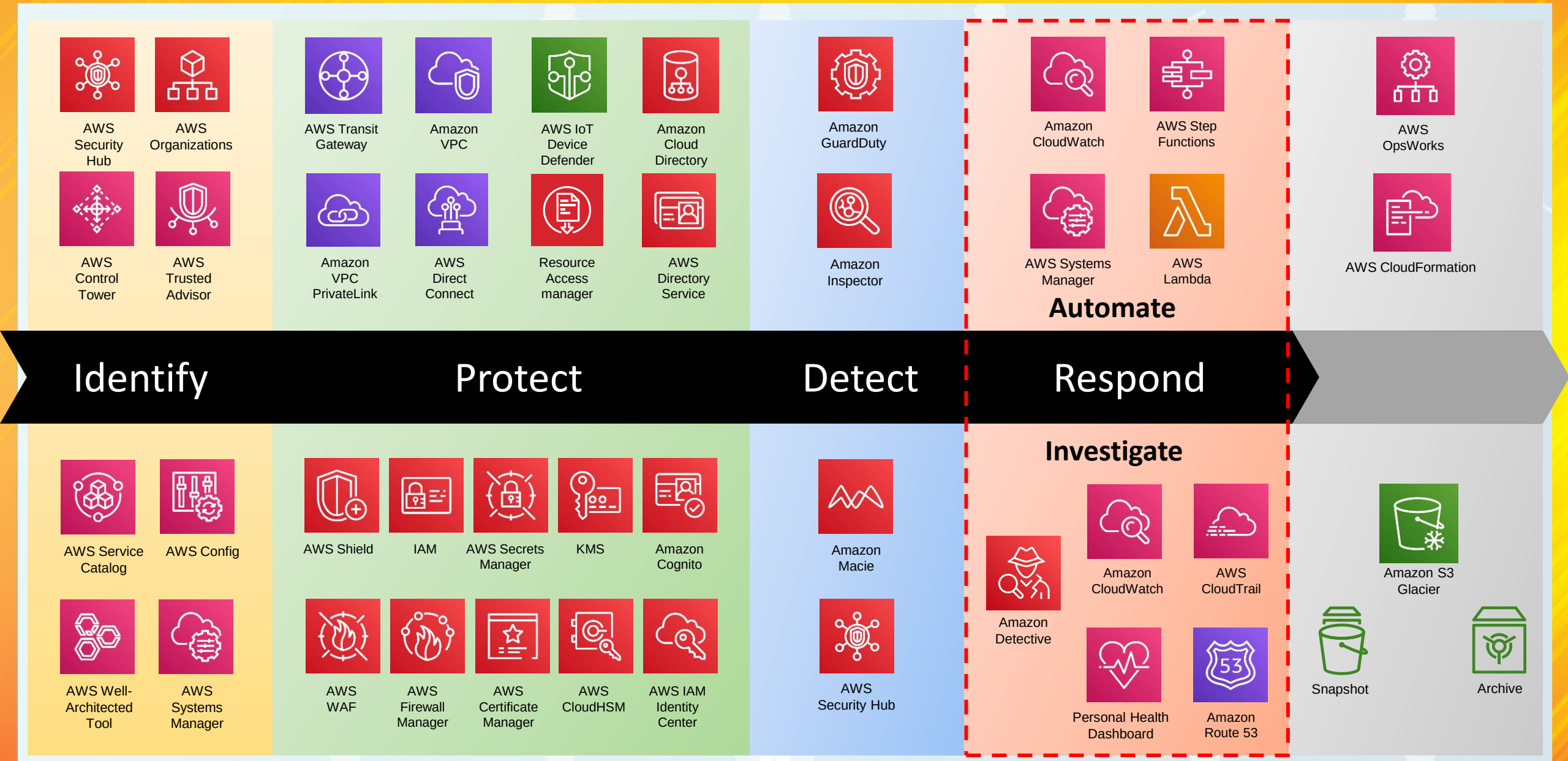
Change Manager

- Change Manager, a capability of AWS Systems Manager, is an enterprise change management framework for requesting, approving, implementing, and reporting on operational changes to your application configuration and infrastructure.
- With Change Manager, you can use preapproved change templates to help automate change processes for your resources and help avoid unintentional results when making operational changes.
- Change templates can be helpful during audits to show how standard changes are made.



Change Manager

AWS Foundational and Layered Security Services



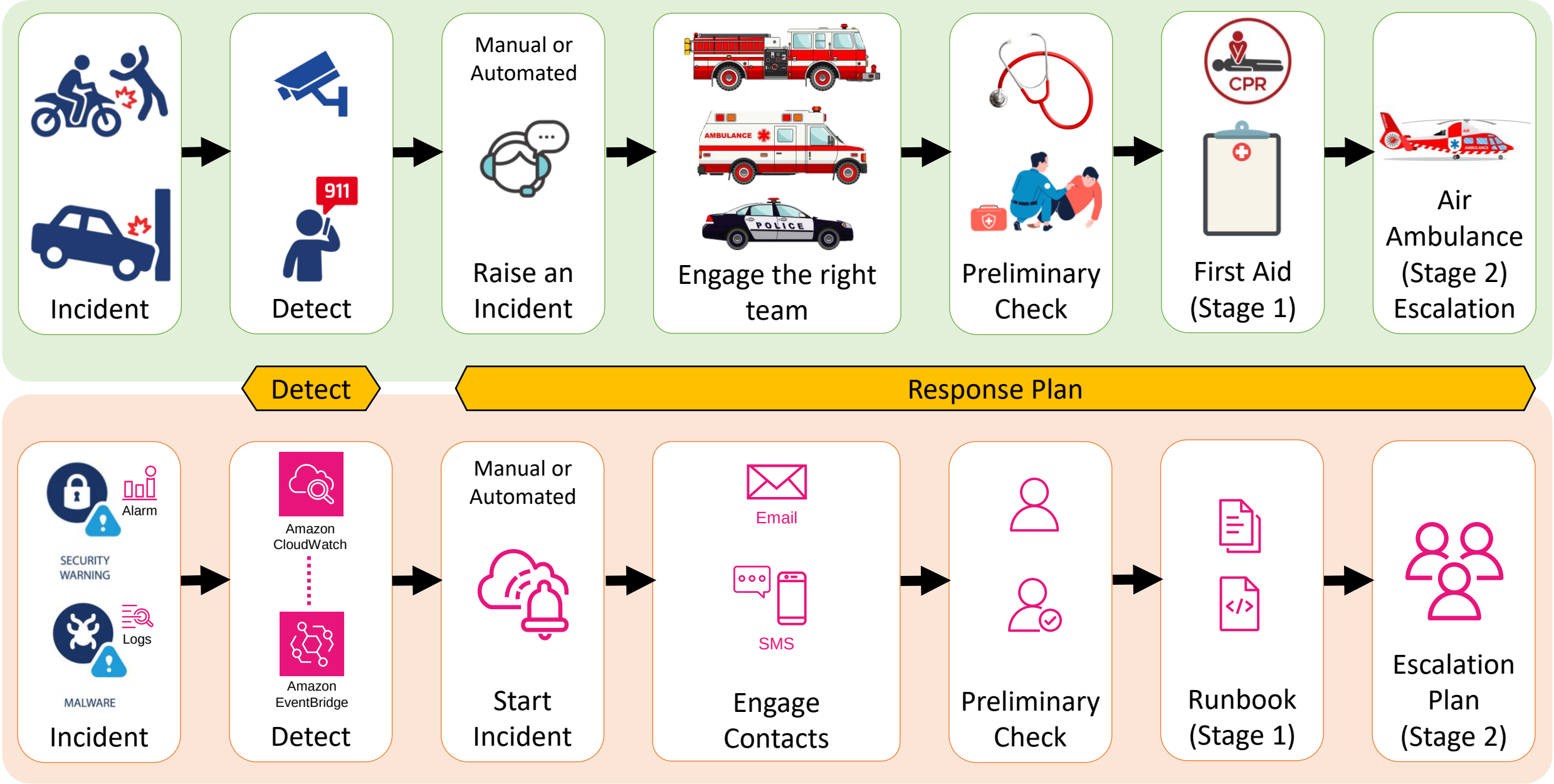
Incident Manager

- Incident
  - General Definition – Unusual or unexpected happening
  - IT Definition – An issue with application or service
- AWS Systems Manager Incident Manager provides a step-by-step framework based on best practices to identify and react to incidents, such as service outages or security threats.
- The primary focus of Incident Manager is to help restore affected services or applications to normal as quickly as possible through a complete incident lifecycle management solution.

Incident Manager

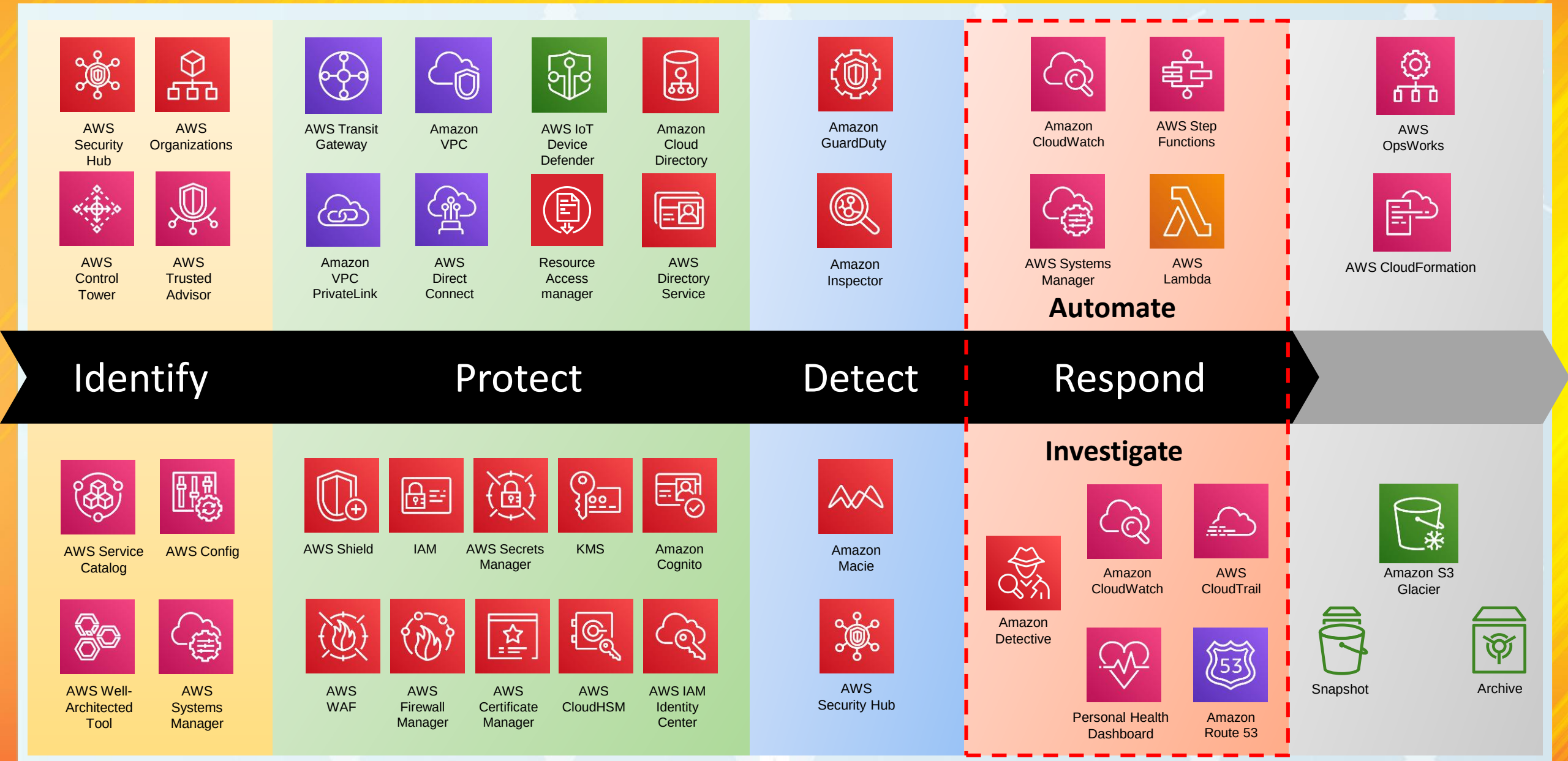
Example

Incident Management

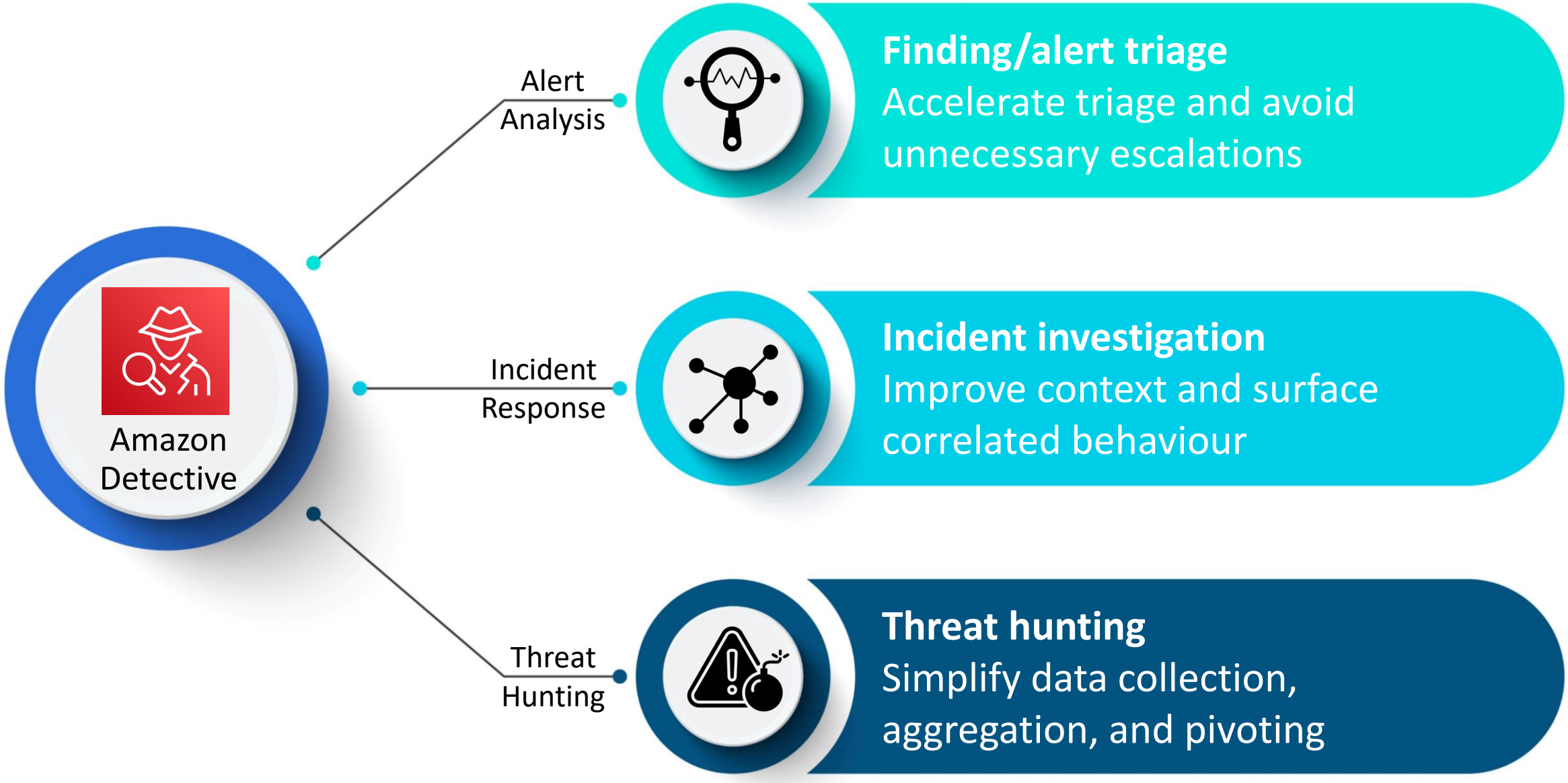


Amazon Detective

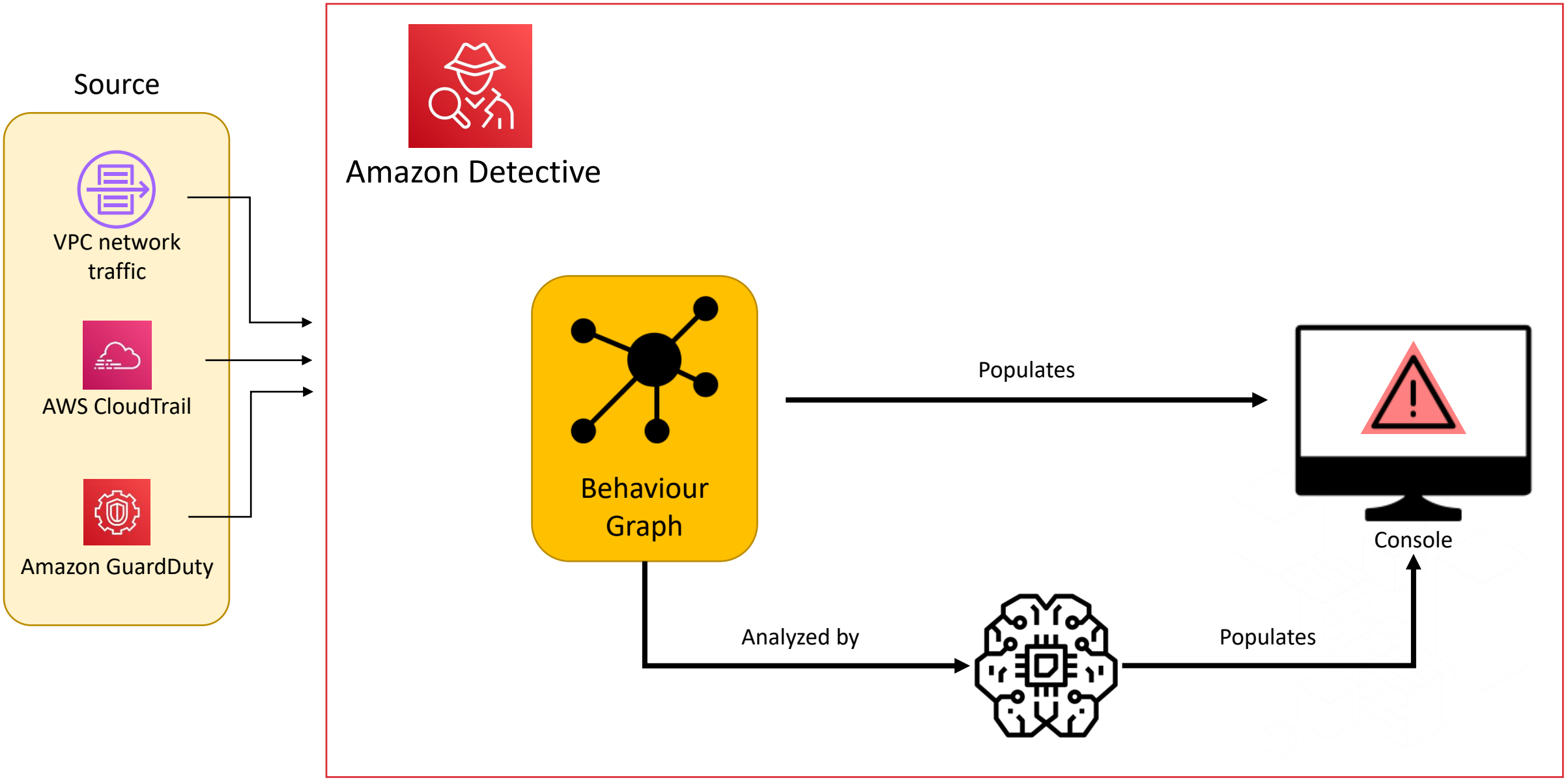
AWS Foundational and Layered Security Services



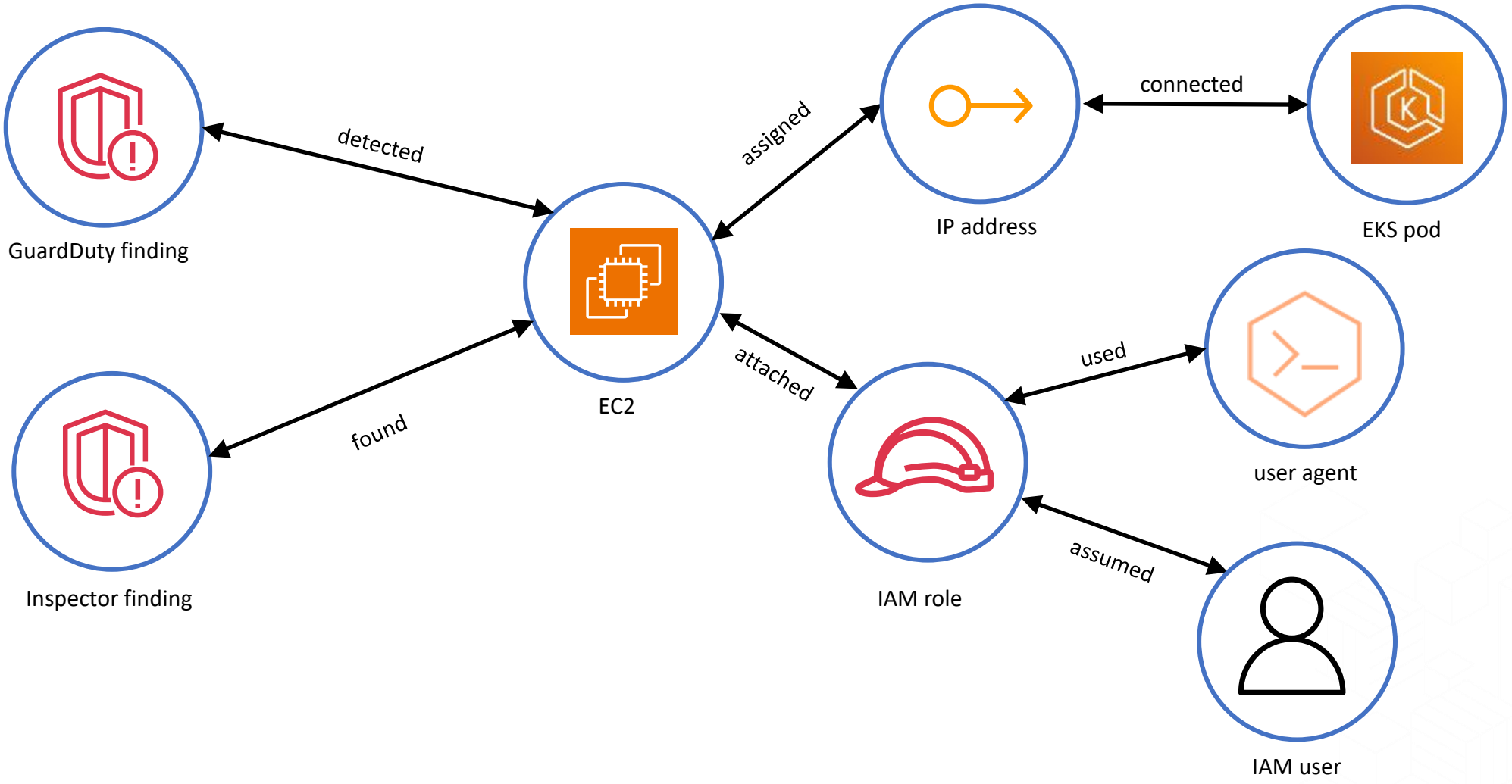
Amazon Detective



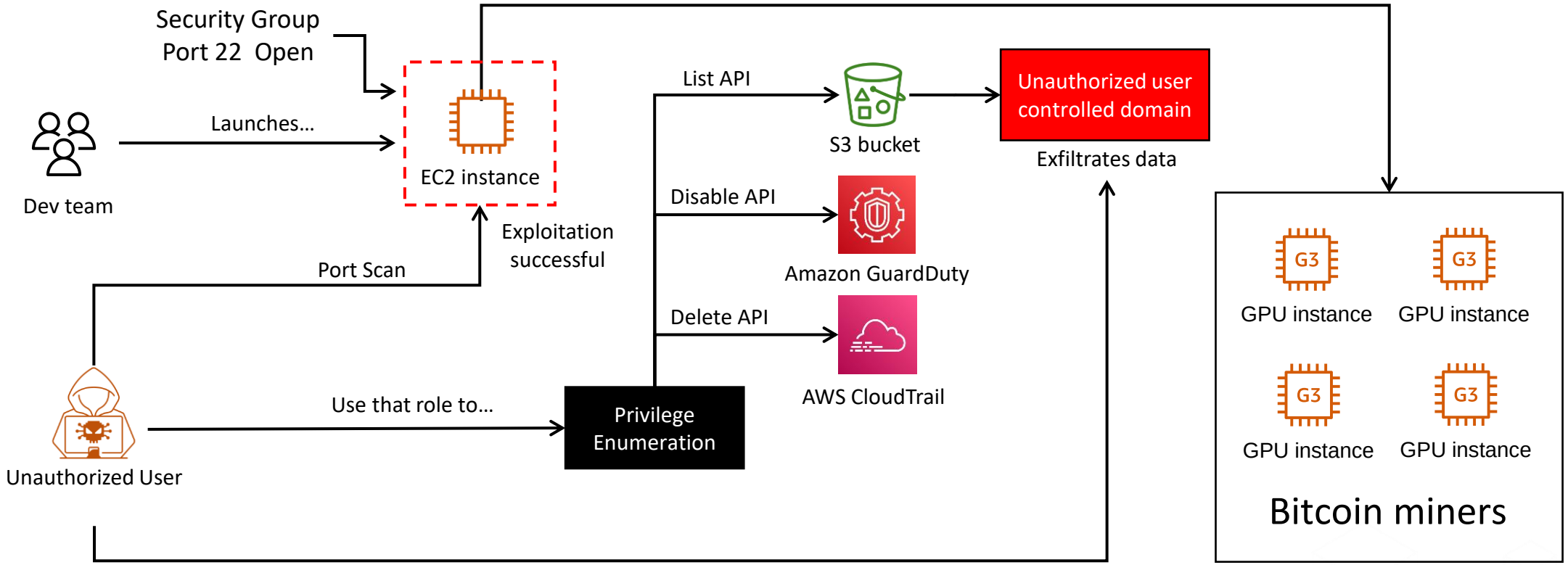
How Amazon Detective processes source data?



Security behaviour graph



Scenario walkthrough



GuardDuty Findings

Recon:EC2/Portscan	Instance: i-089d54d61af097a90
Trojan:EC2/DNSDataExfiltration	Instance: i-0fdd8d8cb49bf3c00
CryptoCurrency:EC2/BitcoinTool.B!DNS	Instance: i-0fdd8d8cb49bf3c00

Investigation - So what happened?

Findings associated with EC2 instance i-0fdd8d8cb49bf3c00 Info

The following findings occurred on this resource around the scope time.

Filter by Finding ID, Title, Finding type, or Account

1

Title	AWS account	Finding type	First observed	Last observed	Finding severity
Data exfiltration through DNS queries from EC2 instance i-0fdd8d8cb49bf3c00		Trojan:EC2-DNSDataExfiltration!DNS	05/25/2022, 17:05 UTC	05/25/2022, 18:05 UTC	High
Outbound portscan from EC2 instance i-0fdd8d8cb49bf3c00		Recon:EC2/Portscan	05/25/2022, 17:05 UTC	05/25/2022, 18:05 UTC	Medium
Command and Control server domain name queried by EC2 instance i-0fdd8d8cb49bf3c00		Backdoor:EC2-C&CActivity.B!DNS	05/25/2022, 17:05 UTC	05/25/2022, 18:05 UTC	High
Bitcoin-related domain name queried by EC2 instance i-0fdd8d8cb49bf3c00		CryptoCurrency:EC2-BitcoinTool.B!DNS	05/25/2022, 17:05 UTC	05/25/2022, 18:05 UTC	High

Investigation

Recon:EC2/Portscan Instance: i-0fdd8d8cb49bf3c00 a mor

Start in GuardDuty, initial event

Choose Investigate with Detective

Open up the impacted EC2 instance

Actions

Save / Edit

Count

15

Recon:EC2/Portscan

Finding ID: 2ac07e18d24cc56268e37cd5580f4027

Feedback

Medium EC2 instance i-0fdd8d8cb49bf3c00 is performing outbound port scans against remote host 10.0.0.128. Info

Investigate with Detective

Investigate with Detective

Detective visualizes the CloudTrail and VPC flow data for the resources affected by this finding

GuardDuty finding
2ac07e18d24cc56268e37cd5580f4027
Investigate trends, new behaviors, and relationships involving the resources and actors present within the finding.

EC2 instance i-0fdd8d8cb49bf3c00
Investigate VPC flow traffic trends or view the activity details. Analyze CloudTrail activity associated with the EC2 Instance and quickly identify any new behavior.

AWS account
Investigate account level CloudTrail activity to identify unusual trends in volume, new activity, and location access patterns.

IP address 34.207.115.92
Investigate CloudTrail activity originating from the IP address to see unusual trends in volume, new activity from this IP address, and determine which resources have used the IP address.

IP address 10.0.0.93
Investigate CloudTrail activity originating from the IP address to see unusual trends in volume, new activity from this IP

bf3c00
:09:13 (a month ago)
:09:18 (a month ago)
bf3c00
8bbf9259
2 AMI 2.0.20220426.0 x86_64 HVM gp2
Launch time 05-25-2022 13:03:54
IAM instance profile

Investigation

Detective > Search > Ec2Instance/i-0fdd8d8cb49bf3c00

i-0fdd8d8cb49bf3c00
EC2 instance Info

Scope time Info
05/25/2022, 17:00 UTC > 05/25/2022, 19:00 UTC

Overview | New behavior

EC2 instance details Info

EC2 instance i-0fdd8d8cb49bf3c00	Creation date 05/25/2022, 17:03 UTC	Created by AWSReservedSSO_AWSAdministratorAccess_d751db6fdef65b0b	Role test-GeneralInstanceRole-2XTI3Z4WO54S
AWS account	ARN arn:aws:ec2:us-east-1: instance/i-0fdd8d8cb49bf3c00	Associated VPC vpc-0099921857ba5b883	

Investigation

Role assumption activity during scope time Info

This role was involved in the following role assumption activity. This panel shows when the role was assumed, and when the role assumed a different role.

Filter by Orgin or Target

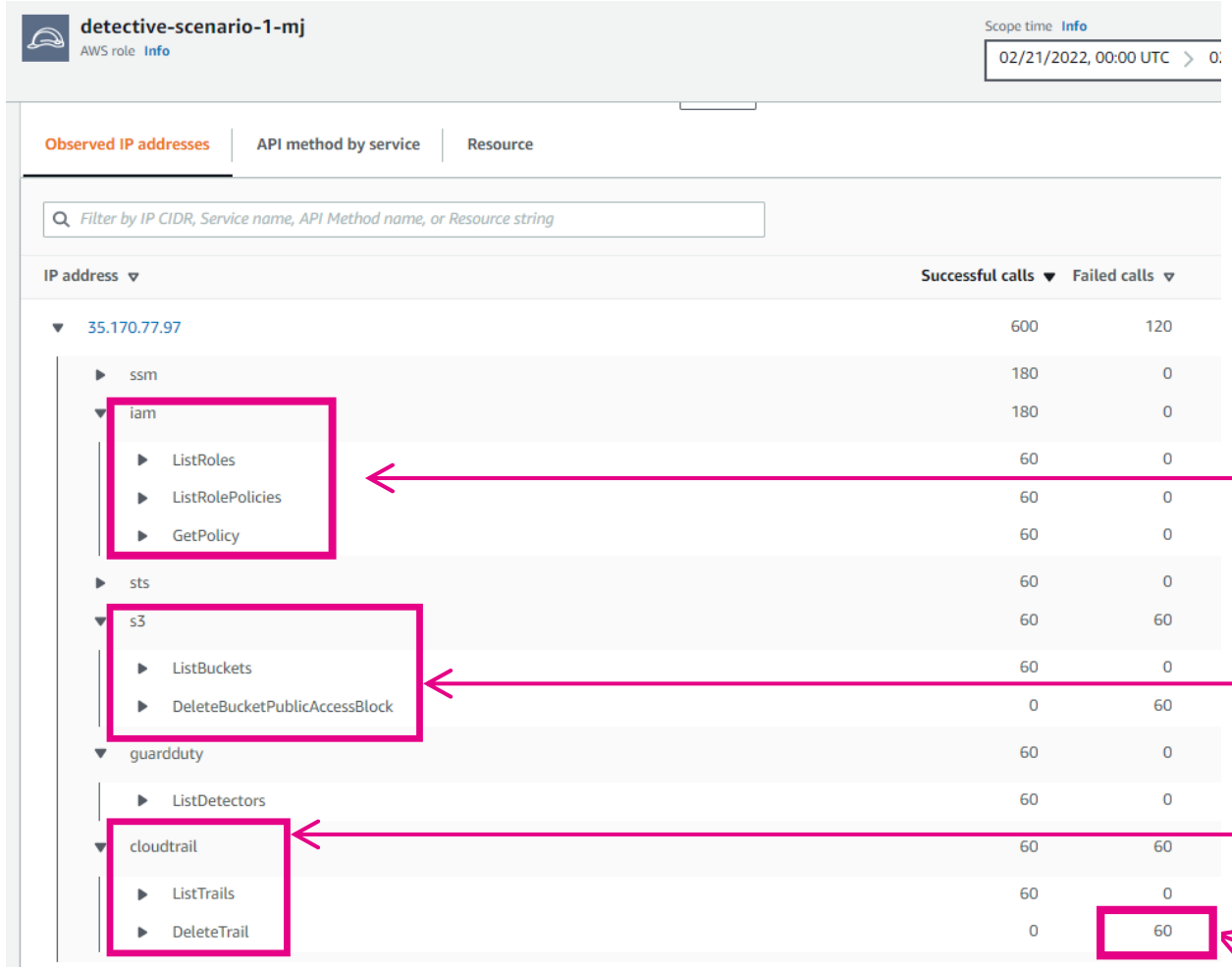
1

Origin	Target	First occurrence	Last occurrence
marshall Federated user	AWSReservedSSO_AWSAdministratorAccess_d751db6fdef65b0b	04/28/2022, 20:00 UTC	06/14/2022, 18:00 UTC

What questions do we need to answer?

- Can we determine what else the role has been doing? Was it successful in other suspicious activity?
- Can we identify the IP associated with the malicious domain?
- Was the IP interacting with other resources in the environment?
- Can we determine what data was exfiltrated?

Answer questions with Detective



What IAM permissions do I have?

Which S3 buckets can I read?

Can I disable Cloudtrail to cover my tracks?

Failed calls

Answer questions with Detective

Observed IP addresses | API method by service | Resource

Filter by IP CIDR, Service name, API Method name, or Resource string

1 2 3 4 5 6 7 ... 33

IP address	Successful calls	Failed calls	Location
44.197.111.53	148,374	34,777	Ashburn, US
3.234.218.18	114,082	5	Ashburn, US
3.234.215.177	30,454	0	Ashburn, US
3.236.209.147	22,742	0	Ashburn, US
3.228.24.32	16,659	0	Ashburn, US
3.237.11.149	11,617	0	Ashburn, US

Detective > Search

Search

Search for a finding or entity using the suggested identifier or wildcard. All searches are case sensitive.

IP address | 44.197.111.53 | Search | Reset

Enter the IP address in CIDR or dot notation.

(Examples from your data: 1.0.120.97 1.0.132.124 1.0.132.192 *)*

Answer questions with Detective

Findings associated with IP address 35.170.77.97 Info

The following findings occurred on this resource around the scope time.

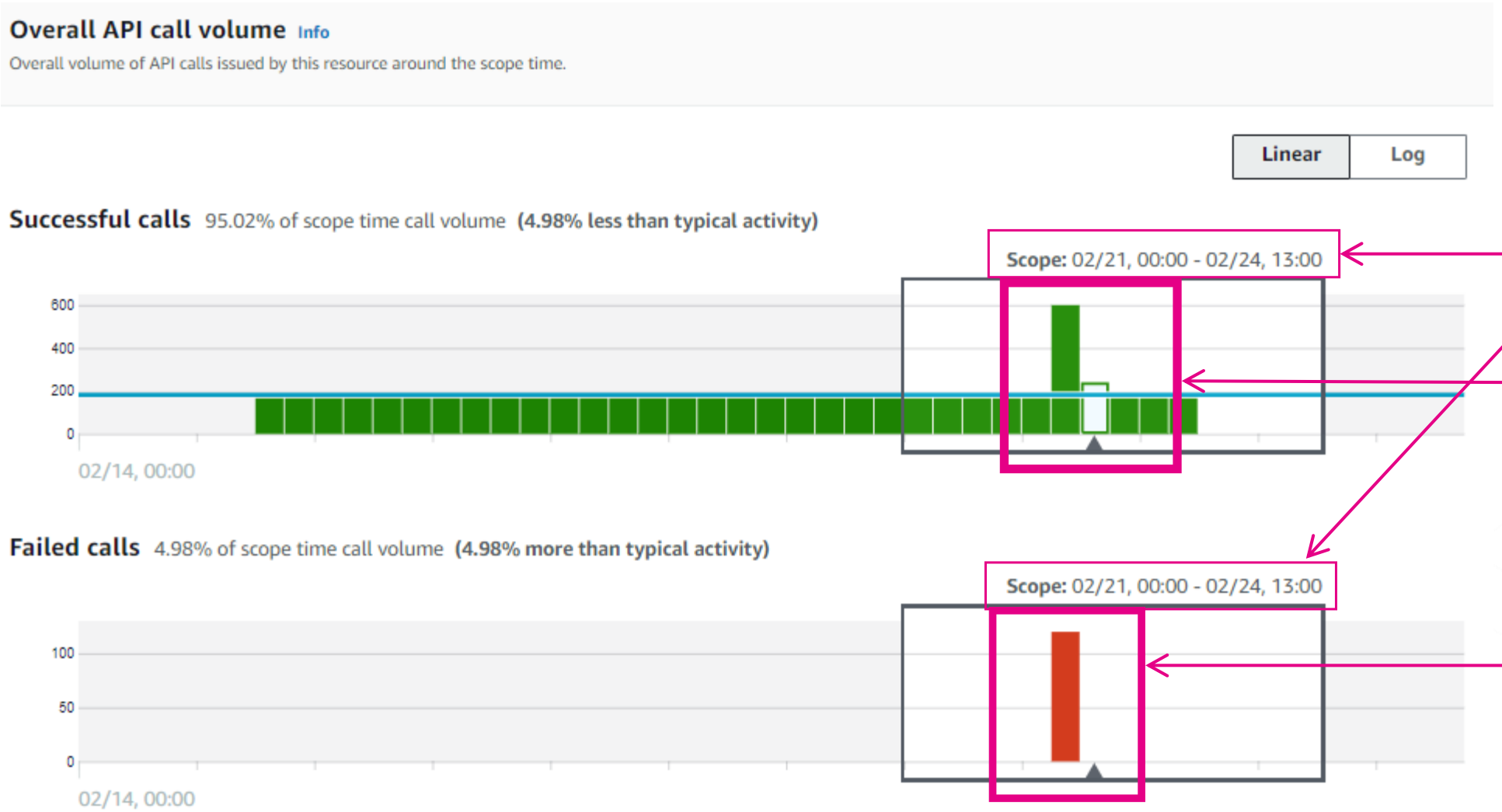
Filter by Finding ID, Title, Finding type, or Account

1

Title	AWS account	Finding type	First observed	Last observed	Finding severity
Data exfiltration through DNS queries from EC2 instance i-096d3ac4dbc6cc940.		Trojan:EC2-DNSDataExfiltration!DNS	02/22/2022, 10:11 UTC	02/22/2022, 11:04 UTC	High

GuardDuty finding of Data Exfiltration to known DNS name

Answer questions with Detective



Timeframe

Successful calls, showing a spike

Some failed calls for services the role doesn't have access to

Answer questions with Detective

Showing activity: **02/21/2022, 00:00 UTC - 02/24/2022, 13:00 UTC** Edit

Observed IP addresses | API method by service | Resource

Filter by IP CIDR, Service name, API Method name, or Resource string

1 2 3 4 5 6 7

Resource	Successful calls	Failed calls
detective-scenario-1-mj:i-0e861489418b1f6e5 Role session	4,596	1,115
detective-scenario-1-mj:i-0bb50c5b70652161a Role session	2,564	0
detective-scenario-1-mj:i-096d3ac4dbc6cc940 Role session	2,290	120
35.170.77.97	2,290	120
ssm	1,810	0
iam	180	0
sts	60	0
s3	60	60
guardduty	60	0
ec2	60	0
RunInstances	60	0
cloudtrail	60	60

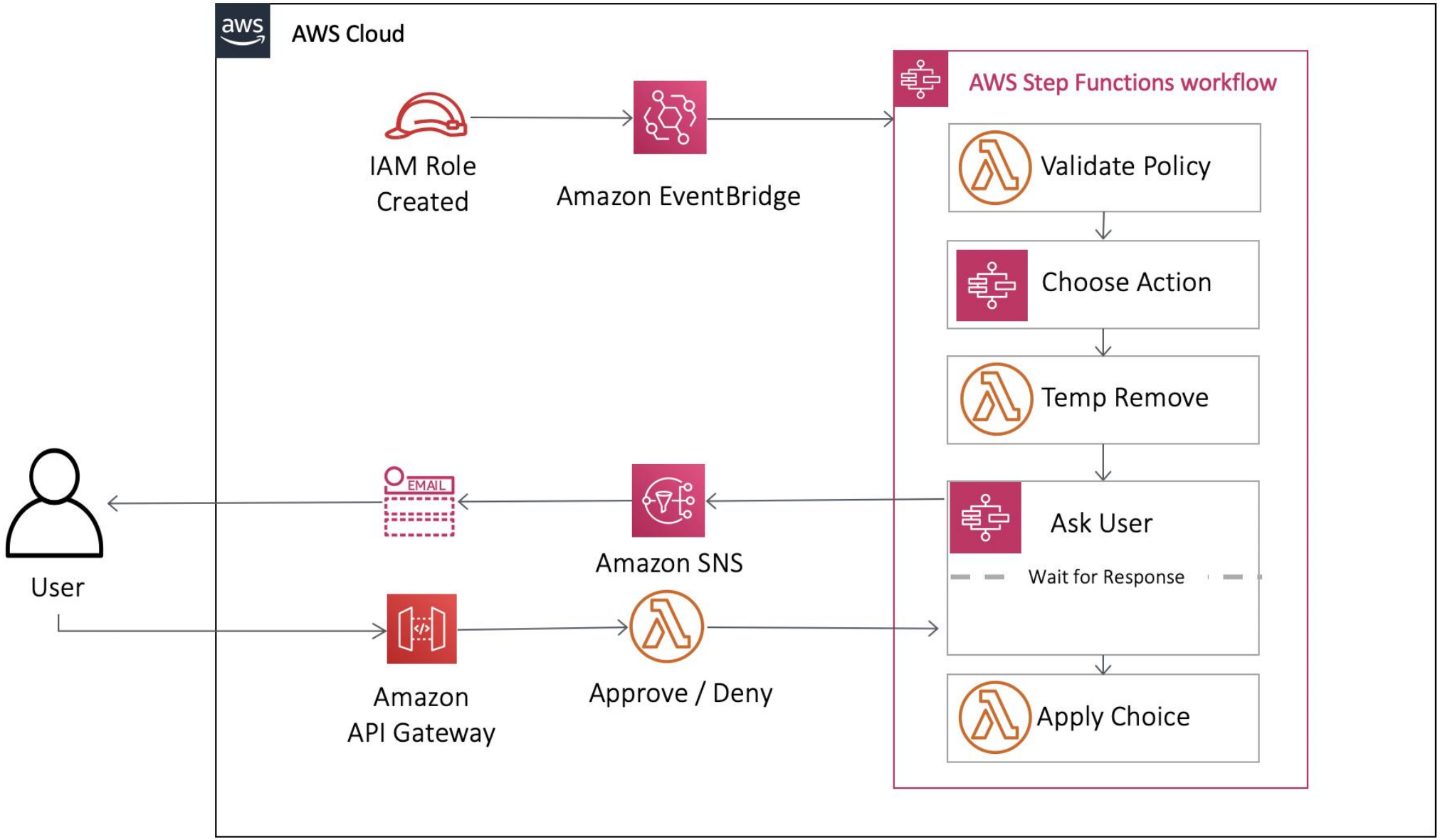
Scope time indicates this occurred on Feb 21

60 successful RunInstances calls indicating 60 bitcoin miners were created

Execute Incident Response

Automating Incident Response

Orchestrating a security incident response with AWS Step Functions



Amazon Route 53 Health Checks

Route 53 health checks

- Route 53 health checks monitor the health and performance of your application's servers, or endpoints, from a network of health checkers in locations around the world.

- You can specify either a domain name or an IP address and a port to create HTTP, HTTPS, and TCP health checks that check the health of the endpoint.

AWS Health Dashboard

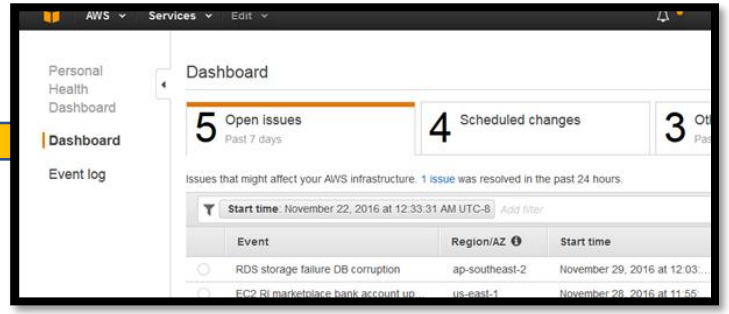
AWS Health Dashboard

- The AWS Health Dashboard is the single place to learn about the availability and operations of AWS services.

AWS Service Health Dashboard

	Apr 16	Apr 15	Apr 14	Apr 13	Apr 12	Apr 11	Apr 10
Amazon Elastic Compute Cloud (API)	✓	✓	✓	—	—	—	—
Amazon Elastic Compute Cloud (Instances)	✓	✓	✓	—	—	—	—
Amazon Flexible Payments Service	✓	✓	✓	—	—	—	—
Amazon Mechanical Turk (Requester)	✓	✓	✓	—	—	—	—
Amazon Mechanical Turk (Worker)	✓	✓	✓	—	—	—	—
Amazon SimpleDB	✓	✓	✓	—	—	—	—
Amazon Simple Storage Service (EU)	✓	✓	✓	—	—	—	—
Amazon Simple Storage Service (US)	✓	✓	✓	—	—	—	—
Amazon Simple Queue Service	✓	✓	✓	—	—	—	—

AWS Personal Health Dashboard



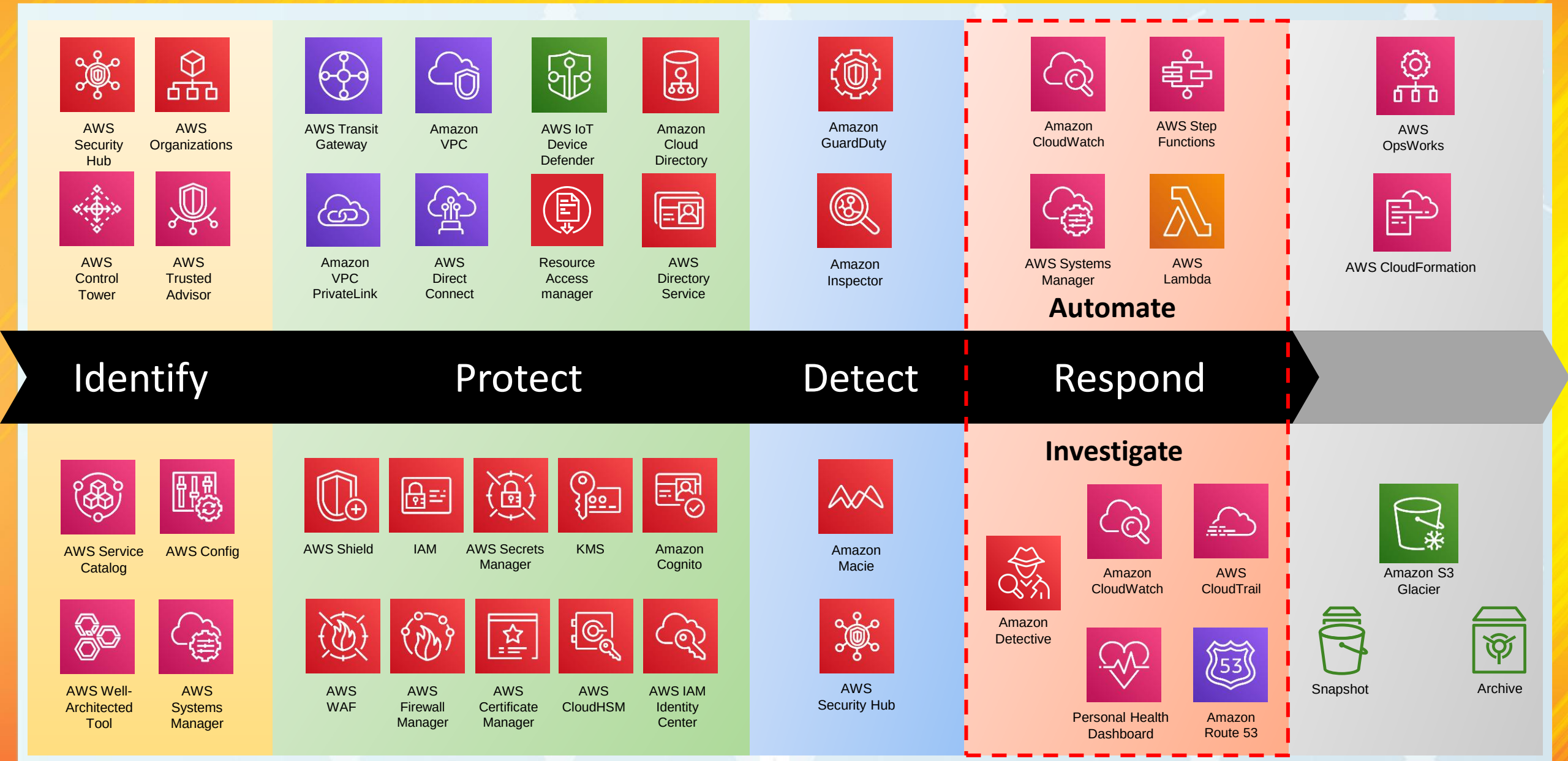
AWS Organizations

Aggregation

AWS Health Dashboard

Integration

Amazon EventBridge

Automate Action

AWS Foundational and Layered Security Services