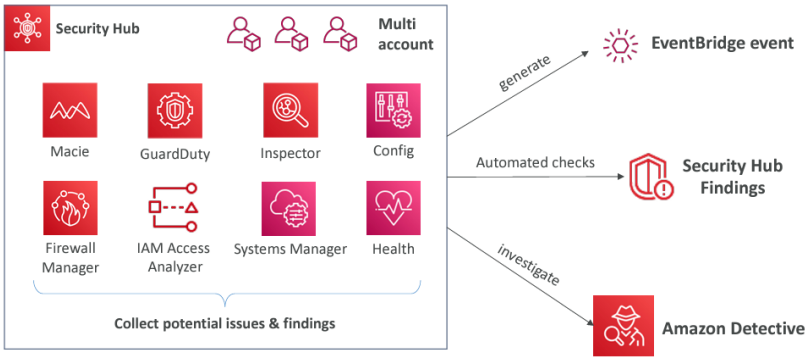
Security Hub & Detective

AWS Certified Security Specialty SCS-C02

AWS Security Hub it's a central security tool that is used to manage the security across several AWS accounts and automate security checks.

this has an integrated dashboard that's going to show us the current security and compliance status that allows us to quickly take actions. So, it's going to aggregate alerts across different services and different partner tools.

So, we are going to get services such as Config, GuardDuty, Inspector,



Macie it just aggregates all these partners tools and all these services into one central dashboard, one central hub. And so, for Security Hub to work, first of all, **we must enable the AWS Config service.**

Main Features

- Cross-Region Aggregation:
  allows you to aggregate security findings, insights, and security scores from multiple AWS Regions into a single, designated aggregation Region. This simplifies monitoring and managing security across a distributed AWS environment, providing a centralized view of your security posture across all Regions.

- AWS Organizations Integration:
  centralize security management across all accounts within an organization. It automatically detects new accounts and adds them to the security monitoring setup. By default, the organization's management account serves as the Security Hub administrator, but you can assign a different account to take on this role. This integration ensures consistent security practices and simplifies the management of security findings across multiple AWS accounts.

- AWS Config must be enabled:
  uses AWS Config to perform its security checks

Amazon Detective:

When you use services like GuardDuty, Macie, and Security Hub in AWS, these services help you identify potential security issues or "findings" that might occur. However, when a security issue arises, you need to understand how it happened and trace it back to its root cause. Often, analyzing the data and connecting the dots to understand the actual cause of the problem can be challenging and time-consuming. In security matters, resolving issues quickly is crucial to avoid vulnerabilities in your infrastructure.

Amazon Detective is specifically designed for this purpose. As its name suggests, Detective analyzes data and swiftly investigates security issues to determine the root cause using machine learning and graph analysis techniques in the background. It automatically collects and analyzes events from sources like VPC Flow Logs, CloudTrail, and GuardDuty to create a unified and comprehensive view of the problem. Then, it provides you with visualizations and details that help you quickly and efficiently identify the cause of the issue.

So, say for example, we have Detective and also GuardDuty and we want to be able to understand how and why CloudTrail would be disabled. So, for example, someone goes in and disables CloudTrail.

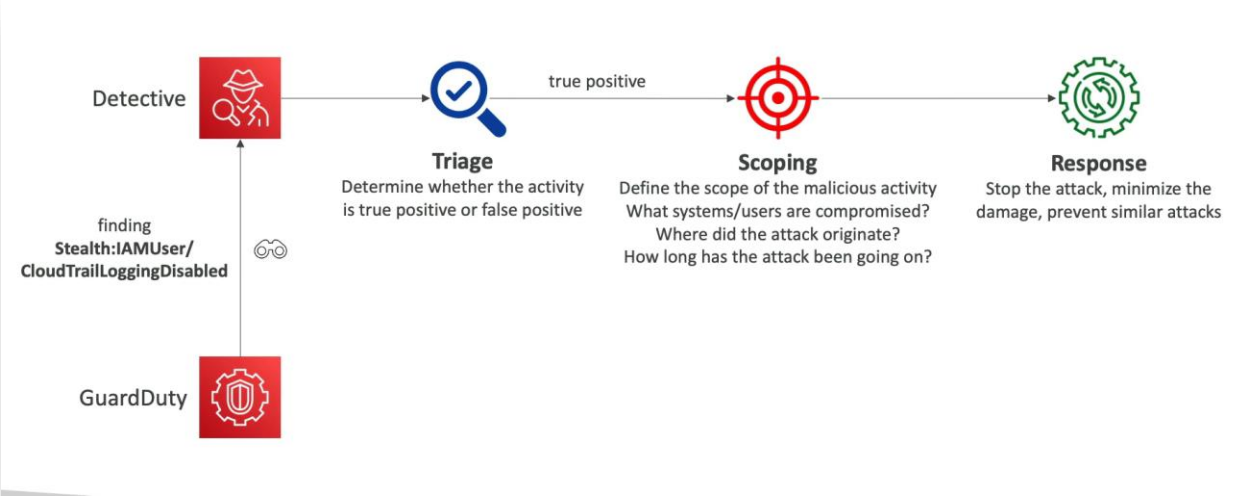
So GuardDuty can generate a finding for it and any findings of Guard Duty will end up into Amazon Detective.

So, from there, we can use Detective and its machine learning capability to

figure out what happens and actually, you know, do triage to determine whether or not this is a true positive or a false positive.

Afterward, we can use Detective to determine the scope of the issue: Which systems were affected? Which users were involved? Who disabled CloudTrail, and from where? How long has this been happening?

Once these details are identified, you can take the necessary actions to stop the attack, such as re-enabling CloudTrail to minimize damage or preventing similar attacks in the future.



In summary, Amazon Detective is the tool that allows you to conduct the necessary investigations and respond effectively and quickly to any findings .generated by GuardDuty