GuardDuty

AWS Certified Security Specialty SCS-C02

Amazon GuardDuty is an anomaly detection service that uses machine learning, threat detection, and integrated threat intelligence, used to help protect your AWS accounts, workloads, and data from threats.

It has machine learning algorithm, performs anomaly detection and uses third party data to find these threats.

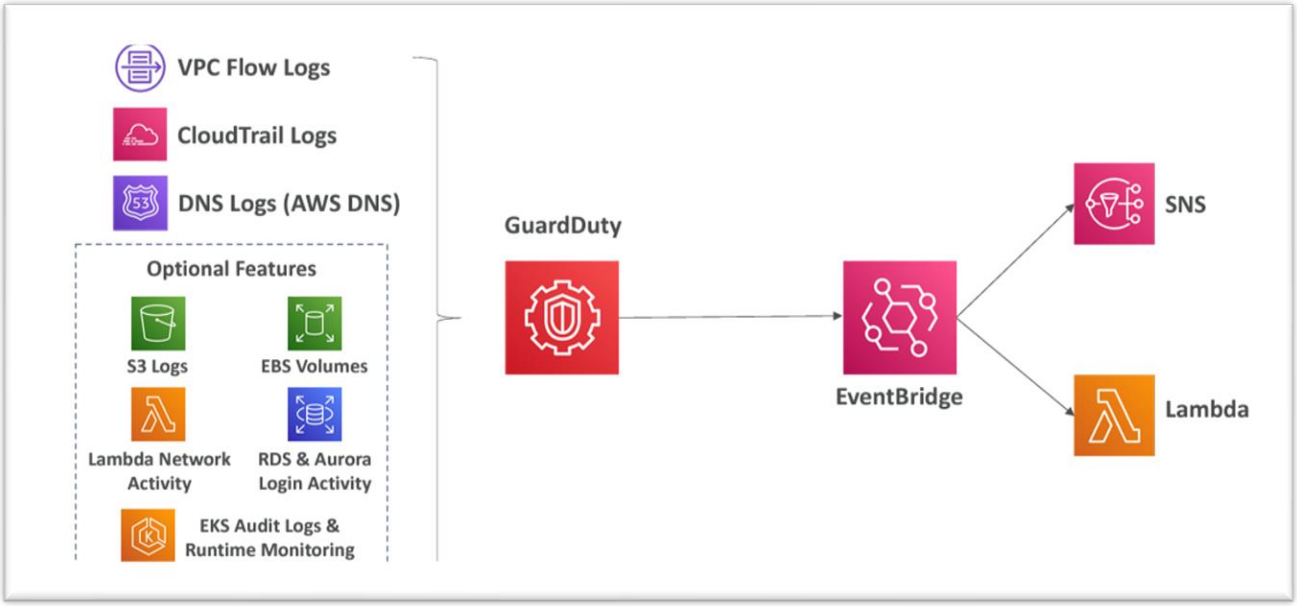
Is an excellent tool for protecting against cryptocurrency attacks, as it has a specific finding type for this purpose. It can analyze input data to detect cryptocurrency attacks effectively.

Input data includes:

CloudTrail Events Logs unusual API calls, unauthorized deployments

- **CloudTrail Management Events** create VPC subnet, create trail,
- **CloudTrail S3 Data Events** get object, list objects, delete object,

- **VPC Flow Logs** unusual internal traffic, unusual IP address
- **DNS Logs** compromised EC2 instances sending encoded data within DNS queries
- **Optional Feature** EKS Audit Logs, RDS & Aurora, EBS, Lambda, S3 Data Events…



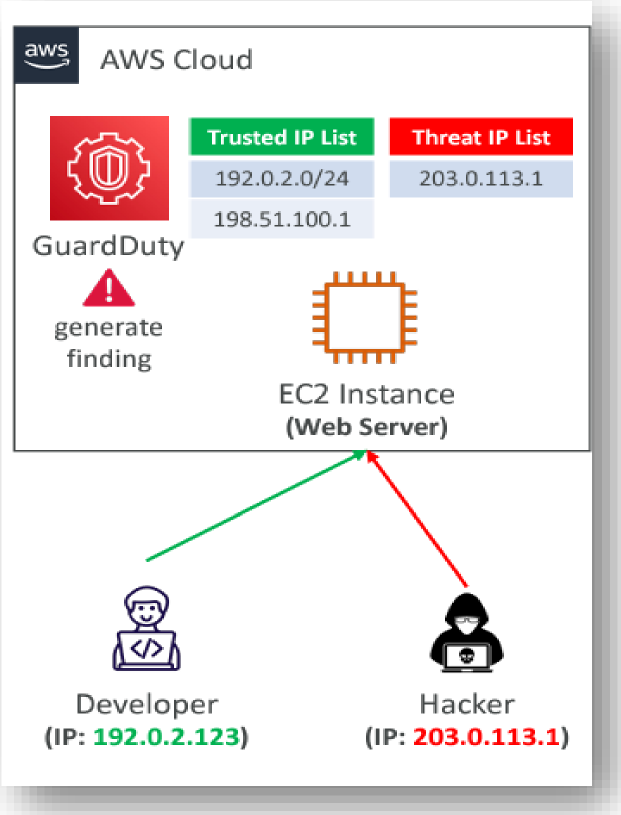
GuardDuty generates findings from these data sources. When a finding is detected, an event is created in Amazon EventBridge. From EventBridge, we can set up rules to trigger automations, such as using Lambda functions, or send notifications using SNS.

Examples of Types of Findings:

- EC2: Unauthorized access or a brute-force attack on SSH, or a cryptocurrency mining attack.
- IAM: Disabling CloudTrail logging or using root credentials.
- Kubernetes: Accessing Kubernetes credentials from a malicious IP address.
- S3: Is public access enabled? Or an attempted penetration test on S3.

Amazon GuardDuty Trusted and Threat IP Lists

This only works for public IP addresses, and we can define a trusted IP list, which is a list of IP addresses and CIDR blocks that we trust. In that case, GuardDuty will not generate findings for these trusted lists.
For example, this allows one of your developers to perform tests on our EC2 instance without generating security findings.



It also has a threat IP list, which is a list of known malicious IP addresses and CIDR ranges. GuardDuty will generate findings based on these threat lists. They can be provided by a third-party intelligence provider, or you can create custom lists yourself. Therefore, if a hacker tries to access your EC2 instance from a malicious IP, GuardDuty will detect it and generate a finding.

Amazon GuardDuty Suppression Rules

Suppression rules allow you to automatically filter and archive new findings. But why would you want to archive new findings, given that GuardDuty provides security findings?

For example, some findings may be of low value, false positives that you've already investigated and know you don't need to see again, or threats that you don't plan to act on. In such cases, you can suppress them by setting up a suppression rule. You can either suppress entire finding types or define more granular criteria, such as suppressing a finding for a specific EC2 instance. When you suppress a finding, it will not be sent to Security Hub, Amazon S3, Amazon Detective, or EventBridge. However, you can still view these findings within GuardDuty.

So for example, if you have an SSH brute-force attempt with a tag value of 'DevOps,' it means that for your DevOps instances, GuardDuty won't generate a finding if someone is trying to brute-force SSH access.

where GuardDuty is activated but it doesn't generate any DNS based findings?

GuardDuty only processes DNS logs if you use the default VPC DNS resolver. Any other DNS resolver you set up within AWS will not generate DNS-based findings for GuardDuty, so that's important to know. Additionally, if you disable or suspend GuardDuty, no findings will be generated.

Finally, as a best practice, it's advisable to enable GuardDuty even in regions you don't actively use, just in case an attack occurs in regions other than the one you're using.