AWS Guard Duty

Amazon GuardDuty is a threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect AWS accounts, workloads, and data stored in Amazon S3.

The managed cloud-hosted service immediately begins analyzing the AWS environment once an IT or security administrator enables GuardDuty within the AWS Management Console.

GuardDuty is not a free service, although enabling GuardDuty initiates a 30-day free trial. After that, pricing is based on the number of AWS CloudTrail events analyzed per month and the volume of VPC Flow Log and DNS Log data analyzed per month.

How Does It Work?

The service uses machine learning, anomaly detection, and integrated threat intelligence to identify and prioritize potential threats. GuardDuty analyzes tens of billions of events across multiple AWS data sources, such as AWS CloudTrail event logs, Amazon VPC Flow Logs, and DNS logs.

GuardDuty detects three main types of threats:

- **Compromised instances.** GuardDuty will detect any unusual spikes in network traffic, as well as hijacked resources — such as an external IP address hijacking EC2 instances.
- **Reconnaissance.** Reconnaissance is when an attacker gathers information about the network. GuardDuty detects activity that suggests reconnaissance, such as unblocked port probing from a known malicious IP, VPC port scanning, and unusual API activity.

- **Compromised accounts.** GuardDuty will detect common patterns that indicate an account compromise, such as API calls from unusual locations, updates that weaken the account's password policy and API calls from known malicious IPs.

The service categorizes its alerts into three severity levels: low, medium and high.

- Low severity threats are typically threats that have been blocked without compromising resources.
- Medium severity threats indicate suspicious activity. This can include a spike in traffic directed to bitcoin-related domains, which could be a sign of cryptocurrency mining.
- High severity threats indicate a compromised resource and should be immediately remediated.

Configuring GuardDuty

GuardDuty configuration requires administrators to create an Identity and Access Management (IAM) role to allow GuardDuty to query various services including EC2, S3, VPC Flow, and Organizations. It also enables CloudWatch to query the AWS event bus to read GuardDuty events and put those events into a kinesis data stream.