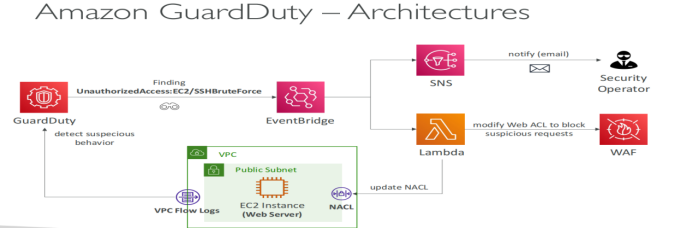
**AWS Guard Duty**

AWS Guard Duty is a managed threat detection service that continuously monitors AWS accounts and workloads for malicious activity and unauthorized behaviour. Leveraging machine learning algorithms and threat intelligence feeds, Guard Duty analyses events and logs from various AWS data sources, including CloudTrail, VPC Flow Logs, and DNS logs, to identify potential security threats such as compromised instances, unauthorized access attempts, and unusual network traffic patterns.

**Guard duty Architecture**

.



**Which Logs Are Analysed By Default?**

**When you enable Guard Duty in your AWS account, Guard Duty automatically starts to monitor these log sources.**

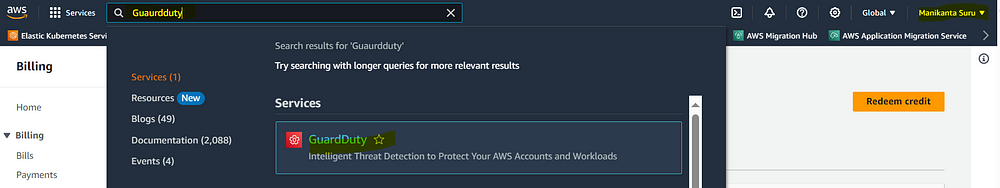
* AWS CloudTrail event logs
* AWS CloudTrail management events
* VPC Flow Logs
* DNS logs

**The following are the supported types of findings available:**

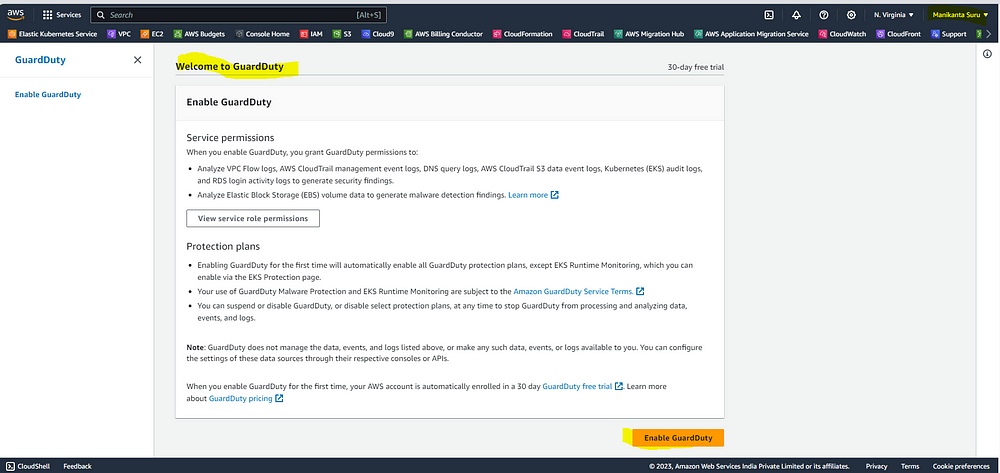
* EC2 finding types
* EKS Runtime Monitoring finding types
* IAM finding types
* Kubernetes audit logs finding types
* Lambda Protection finding types
* Malware Protection finding types
* RDS Protection finding types
* S3 finding types

**Let's deep dive into the practical,**

* Log in to the AWS console and navigate to the Guard duty service.



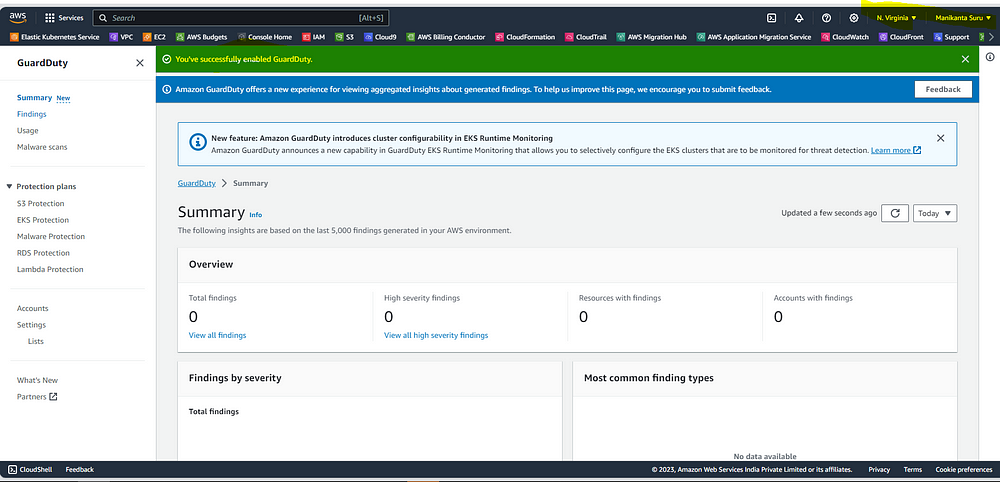
* **Enable Guard Duty**

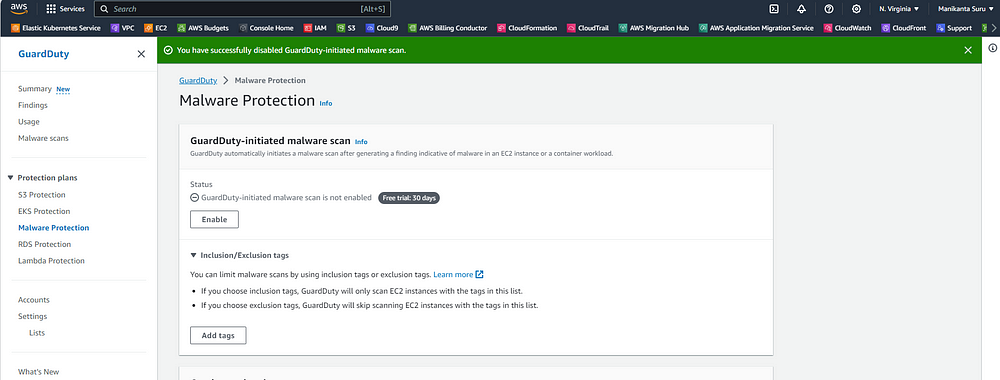


**When you enable Guard Duty, you grant Guard Duty permissions to:**

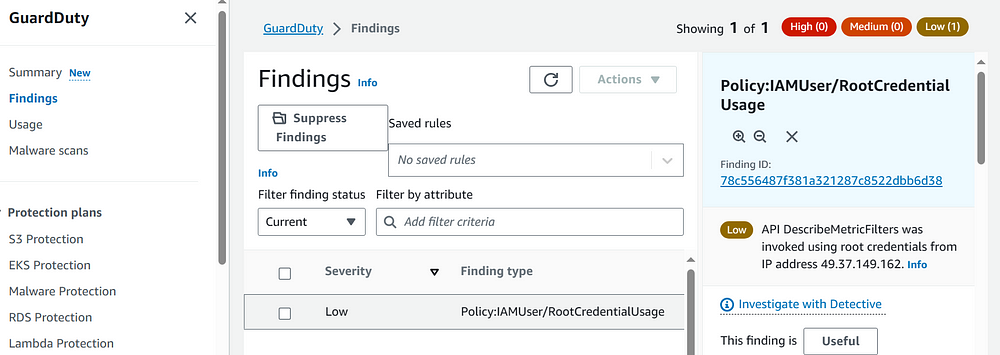
Analyze VPC Flow logs, AWS CloudTrail management event logs, DNS query logs, AWS CloudTrail S3 data event logs, Kubernetes (EKS) audit logs, and RDS login activity logs to generate security findings

**Hit on generating sample findings**





* Navigate to the Findings,
* Details of the Findings look like for more details,



* I want to scan my EC2 using with guard

