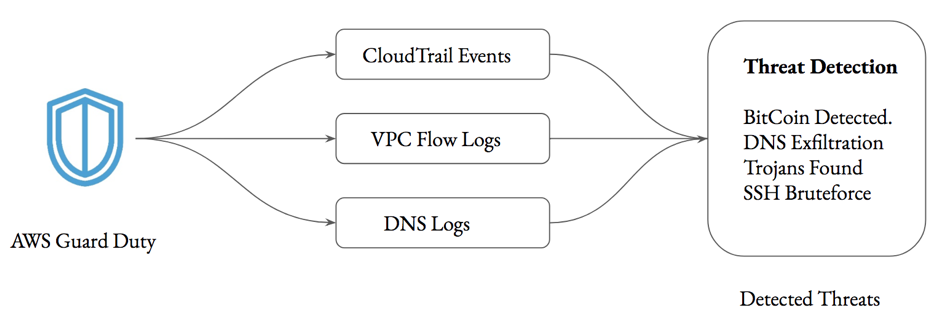
**6. AWS GuardDuty**

AWS Guard Duty is a threat intelligence service by AWS which monitors for malicious behaviour to help customers protect their AWS workloads.

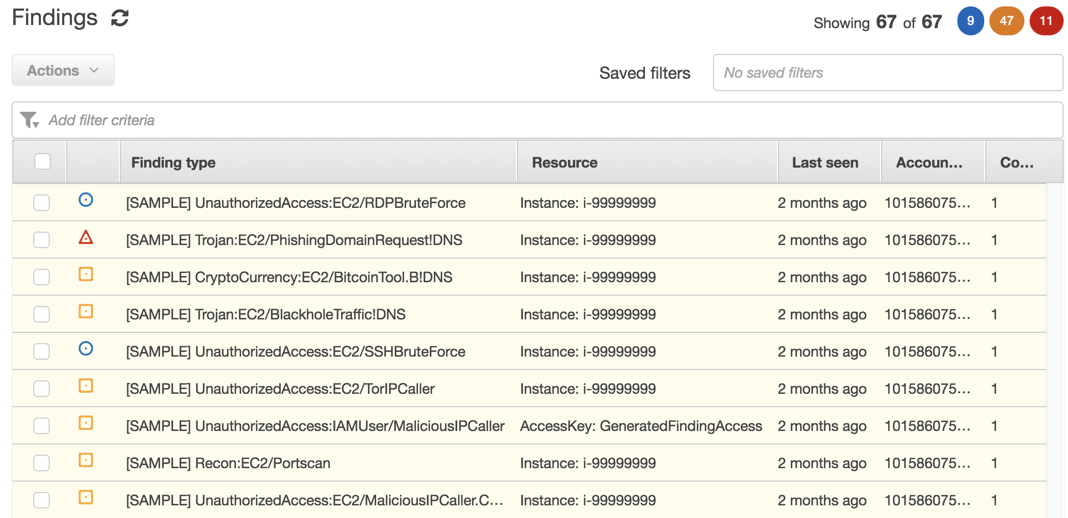


--- Guard Duty Service basically monitors for multiple log files so it can be cloud trail event. It can be VPC flow logs. It can be DNS logs.

--- Now, once it monitors all of them, it will go ahead and analyse it, according to the rules that has been configured and from this, it will go ahead and detect threats. The below eg threat detections.

* Bitcoin detected.
* DNS exfiltration.
* Trojans found
* SSH Bruteforce…etc.

**Sample Guard Duty Findings**



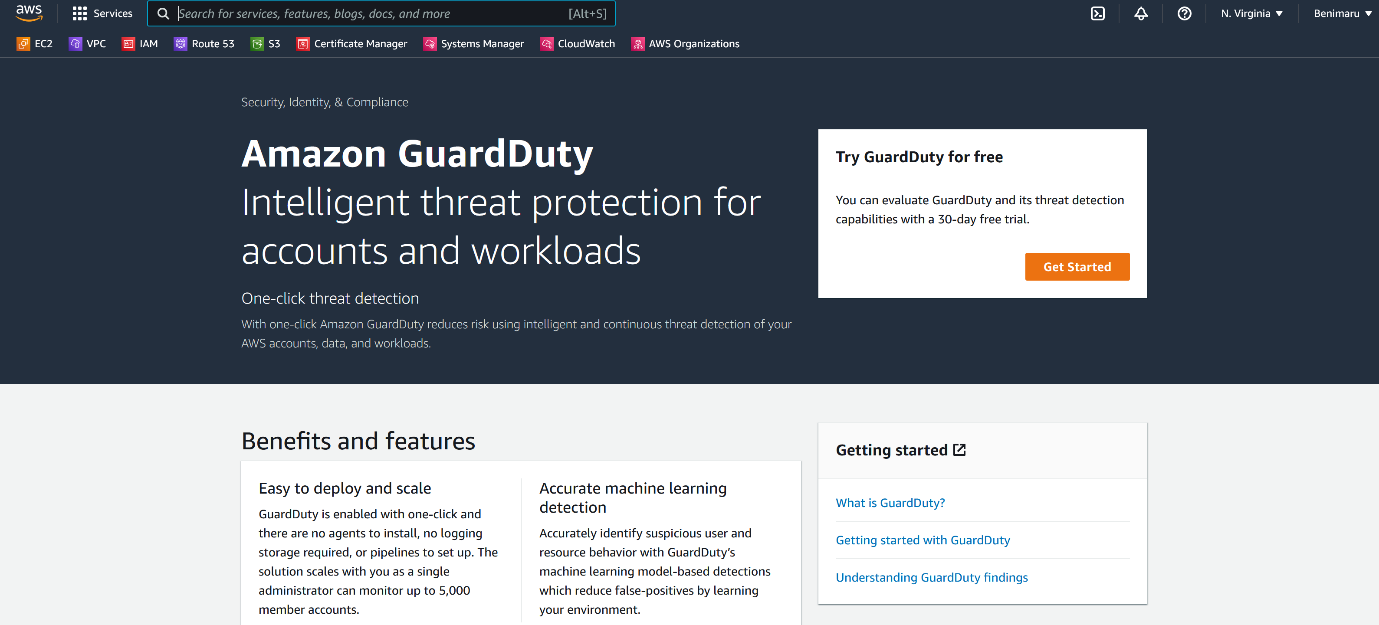
--- **note** – this is what guard duty alerts looks like, guard duty categorises the alert into multiple findings. some can be critical, some can be important, some can be informational

**Important Pointers for Guard Duty**

* Guard Duty will only monitor the Route53 for DNS Logs.
* A lot of organizations make use of Active Directory DNS. The logs from these servers will not be monitored.

**Guard duty**

--- go to aws console.



--- click on get stated.