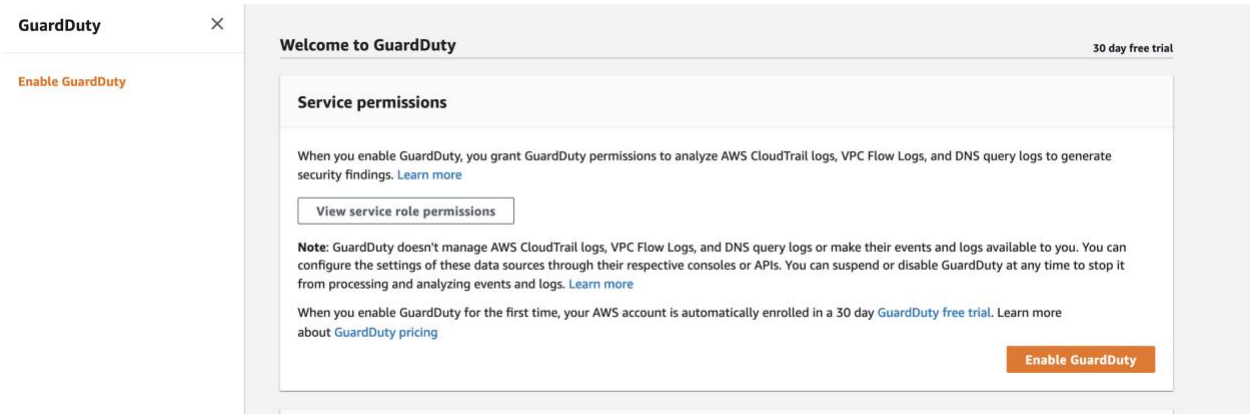
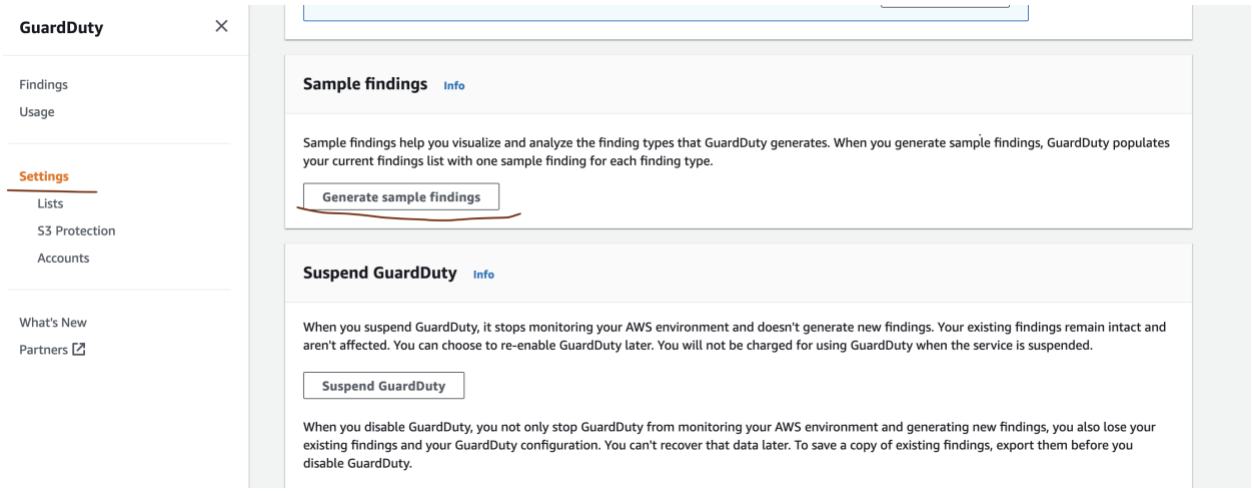
SIEM in AWS

Security: Say you have lot of resources in your account and want to know what happening inside them whether scan for open ports or they are sending some malicious traffic or is there any antivirus or malware causing DDOS attack.

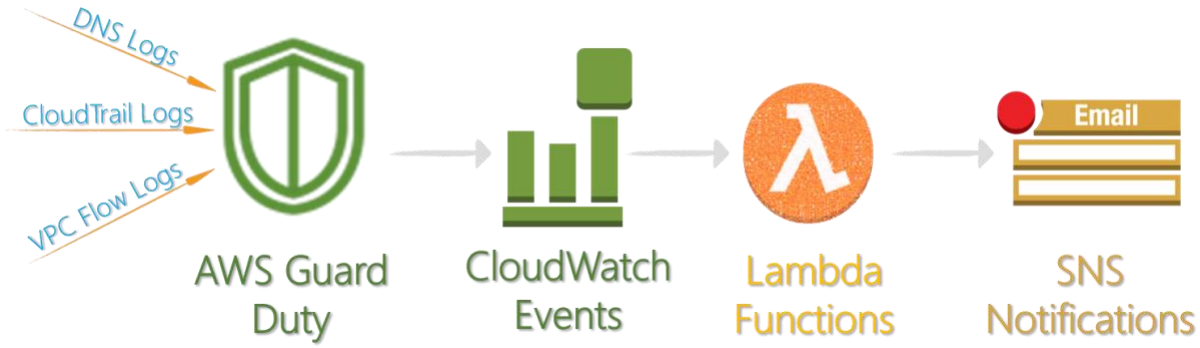
Threat Detection
Event Correlation
Automate Remediation: Ex Blackbox

AWS Guard Duty: SIEM for AWS.
Need to enable it once enabled. {It will be free for 30 days}
It will take DNS logs, Cloud Trail logs and VPC Flow logs.
How to enable:
Search Guard Duty and get started and enable guard duty.
Settings: Generate sample finding to test it out.





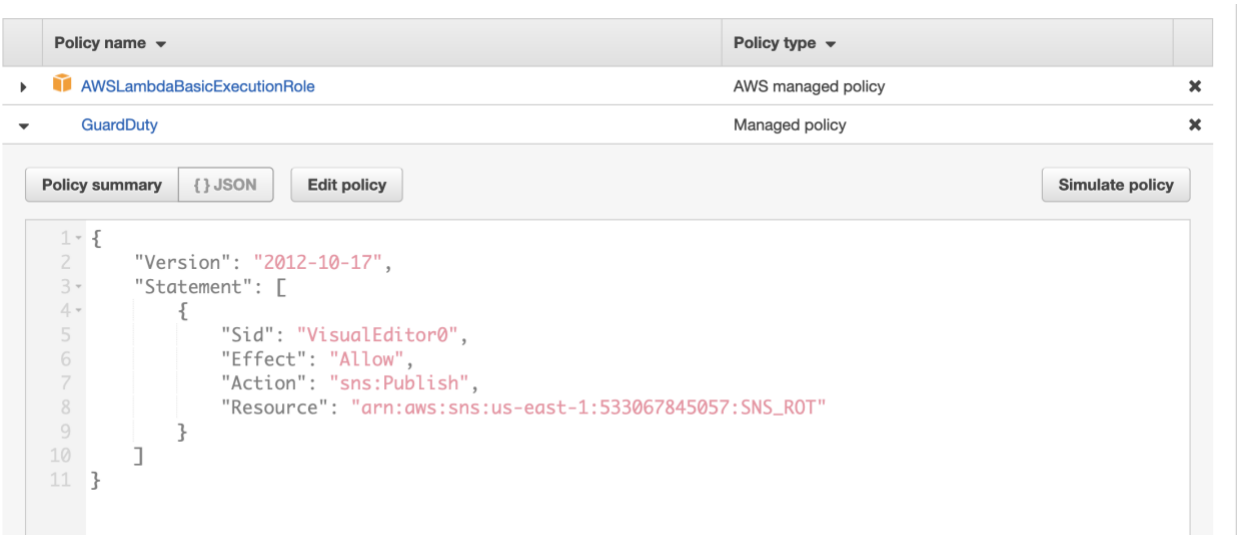
Since not everyone will get access to AWS cloud, but they can get logs through SNS and then they can start investigation. I.e., SECOPS Using Cloud Watch events, Lambda Functions and SNS Notifications. Using Cloud Formation create a stack to send notification through slack channel to the security team.



Requirements:

1) A SNS topic need to be create by assigning email address. {ARN OF YOUR SNS TOPIC}
2) IAM Role - i.e Lambda Service Role - with three permissions

- AWSLambdaBasicExecutionRole
- Inline Policy{ AWS SNSTOPIC Role}

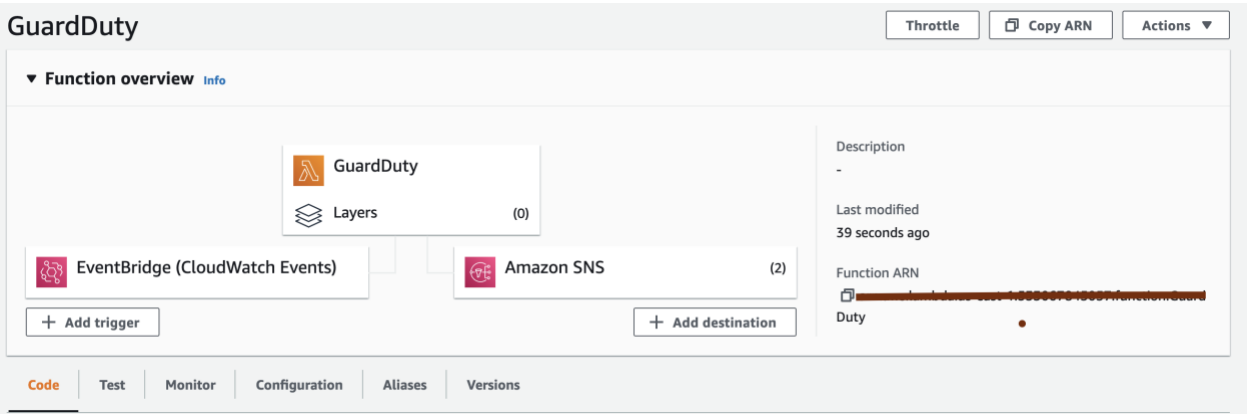


Configure Lambda Function:

Configure lambda trigger:

Goto the EventBridge Dashboard, We are going to use Event Rules

1. Choose Create a new Rule
2. Fill the Rule name
3. In define pattern choose Event pattern
4. Choose Pre-Defined pattern by service
    1. For Service provider, Choose/Type AWS
    2. For Service name, Choose GuardDuty
    3. For Event Type, Choose GuardDuty Finding
5. For Target, Choose Lambda Function
    1. From dropdown select GuardDuty of Lambda Funvtion name
6. In the bottom, Configure Details



Domain related to known malicious domains queried by EC2 instance i-99999999. Inbox ×

RoT <no-reply@sns.amazonaws.com> 10:26 (1 hour ago)

to me

{"version": "0", "id": "0982f042-f0d4-6e1a-cb27-f0e268461738", "detail-type": "GuardDuty Finding", "source": "aws.guardduty", "account": "[redacted]", "time": "2022-01-20T16:25:00Z", "region": "us-east-1", "resources": [], "detail": {"[redacted]partition": "aws", "id": "60bf3c26813b92258b9a443c142bfbdb", "arn": "arn:aws:guardduty:us-east-1:533067845057:detector/acbf3c11bd0dfed03d603461de169faa/finding/60bf3c26813b92258b9a443c142bfbdb", "type": "Impact:EC2/MaliciousDomainRequest.Reputation", "resource": {"resourceType": "Instance", "instanceDetails": {"instanceId": "i-99999999", "instanceType": "m3.xlarge", "outpostArn": "arn:aws:outposts:us-west-2:123456789000:outpost/op-0fbc006e9abbc73c3", "launchTime": "2016-08-02T02:05:06.000Z", "platform": null, "productCodes": [{"productCodeId": "GeneratedFindingProductCodeId", "productCodeType": "GeneratedFindingProductCodeType"}], "iamInstanceProfile": {"arn": "[redacted]", "id": "GeneratedFindingInstanceProfileId"}, "networkInterfaces": [{"ipv6Addresses": [], "networkInterfaceId": "eni-bfcffe88", "privateDnsName": "GeneratedFindingPrivateDnsName", "privateIpAddress": "10.0.0.1", "privateIpAddresses": [{"privateDnsName": "GeneratedFindingPrivateName", "privateIpAddress": "10.0.0.1"}], "subnetId": "GeneratedFindingSubnetId", "vpcId": "GeneratedFindingVPCId", "securityGroups": [{"groupName": "GeneratedFindingSecurityGroup Name", "groupId": "GeneratedFindingSecurityId"}], "publicDnsName": "GeneratedFindingPublicDNSName", "publicIp": "198.51.100.0"}], "tags": [{"key": "GeneratedFindingInstaceTag1", "value": "GeneratedFindingInstaceValue1"}, {"key": "GeneratedFindingInstaceTag2", "value": "GeneratedFindingInstaceTagValue2"}, {"key": "GeneratedFindingInstaceTag3", "value": "GeneratedFindingInstaceTagValue3"}, {"key": "GeneratedFindingInstaceTag4", "value": "GeneratedFindingInstaceTagValue4"}, {"key": "GeneratedFindingInstaceTag5", "value": "GeneratedFindingInstaceTagValue5"}, {"key": "GeneratedFindingInstaceTag6", "value": "GeneratedFindingInstaceTagValue6"}, {"key": "GeneratedFindingInstaceTag7", "value": "GeneratedFindingInstaceTagValue7"}, {"key": "GeneratedFindingInstaceTag8", "value": "GeneratedFindingInstaceTagValue8"}, {"key": "GeneratedFindingInstaceTag9", "value": "GeneratedFindingInstaceTagValue9"}], "instanceState": "running", "availabilityZone": "GeneratedFindingInstaceAvailabilityZone", "imageId": "ami-99999999", "imageDescription": "GeneratedFindingInstaceImageDescription"}}, "service": {"serviceName": "guardduty", "detectorId": "acbf3c11bd0dfed03d603461de169faa", "action": {"actionType": "DNS_REQUEST", "dnsRequestAction": {"domain": "GeneratedFindingDomainName", "protocol": "UDP", "blocked": true}}, "resourceRole": "TARGET", "additionalInfo": {"threatListName": "GeneratedFindingThreatListName", "sample": true}, "evidence": {"threatIntelligenceDetails": [{"threatListName": "GeneratedFindingThreatListName", "threatNames": ["GeneratedFindingThreatName"]}]}, "eventFirstSeen": "2022-01-20T16:23:39.000Z", "eventLastSeen": "2022-01-20T16:23:39.000Z", "archived": false, "count": 1}, "severity": 8, "createdAt": "2022-01-20T16:23:39.895Z", "updatedAt": "2022-01-20T16:23:39.895Z", "title": "Domain related to known malicious domains queried by EC2 instance i-99999999.", "description": "EC2 instance i-99999999 is querying a low reputation domain that is associated with known malicious domains."}}