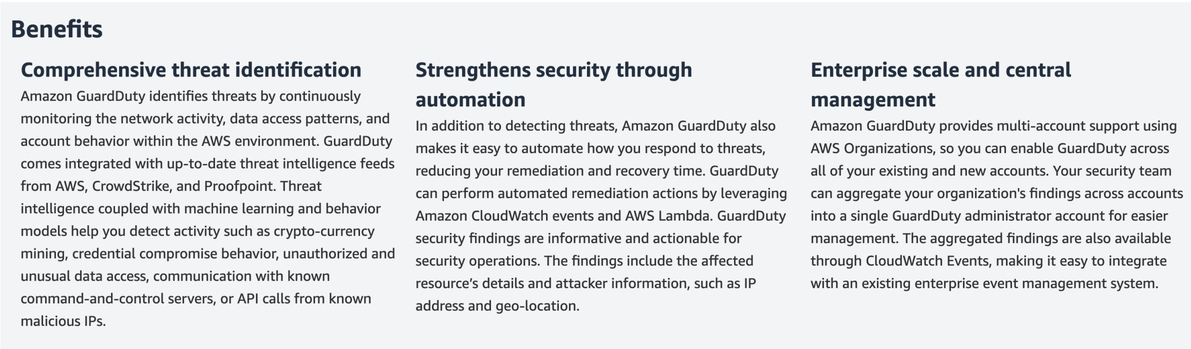
AWS - Guard Duty

https://aws.amazon.com/guardduty/

- Amazon GuardDuty is a threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect your AWS accounts, workloads, and data stored in Amazon S3.
- With the cloud, the collection and aggregation of account and network activities is simplified, but it can be time consuming for security teams to continuously analyze event log data for potential threats.
- With GuardDuty, you now have an intelligent and cost-effective option for continuous threat detection in AWS.
- 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, Cloud trail S3 data events
  - Amazon VPC Flow Logs, and
  - DNS logs.
- With a few clicks in the AWS Management Console, GuardDuty can be enabled with no software or hardware to deploy or maintain.
- By integrating with Amazon CloudWatch Events, GuardDuty alerts are actionable, easy to aggregate across multiple accounts, and straightforward to push into existing event management and workflow systems



Benefits

Comprehensive threat identification

Amazon GuardDuty identifies threats by continuously monitoring the network activity, data access patterns, and account behavior within the AWS environment. GuardDuty comes integrated with up-to-date threat intelligence feeds from AWS, CrowdStrike, and Proofpoint. Threat intelligence coupled with machine learning and behavior models help you detect activity such as crypto-currency mining, credential compromise behavior, unauthorized and unusual data access, communication with known command-and-control servers, or API calls from known malicious IPs.

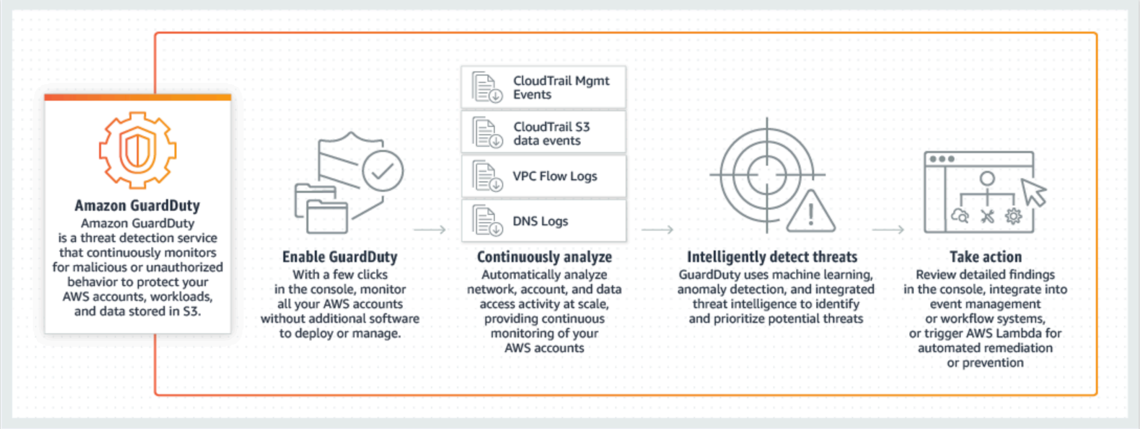
Strengthens security through automation

In addition to detecting threats, Amazon GuardDuty also makes it easy to automate how you respond to threats, reducing your remediation and recovery time. GuardDuty can perform automated remediation actions by leveraging Amazon CloudWatch events and AWS Lambda. GuardDuty security findings are informative and actionable for security operations. The findings include the affected resource's details and attacker information, such as IP address and geo-location.

Enterprise scale and central management

Amazon GuardDuty provides multi-account support using AWS Organizations, so you can enable GuardDuty across all of your existing and new accounts. Your security team can aggregate your organization's findings across accounts into a single GuardDuty administrator account for easier management. The aggregated findings are also available through CloudWatch Events, making it easy to integrate with an existing enterprise event management system.

How it works



Amazon GuardDuty

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

Enable GuardDuty

With a few clicks in the console, monitor all your AWS accounts without additional software to deploy or manage.

CloudTrail Mgmt Events

CloudTrail S3 data events

VPC Flow Logs

DNS Logs

Continuously analyze

Automatically analyze network, account, and data access activity at scale, providing continuous monitoring of your AWS accounts

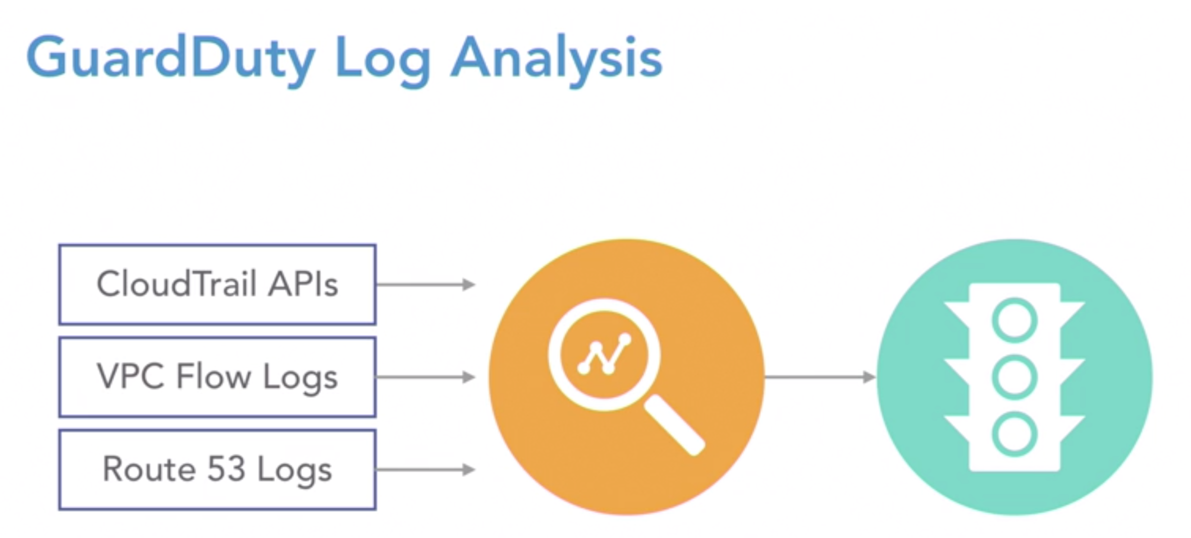
Intelligently detect threats

GuardDuty uses machine learning, anomaly detection, and integrated threat intelligence to identify and prioritize potential threats

Take action

Review detailed findings in the console, integrate into event management or workflow systems, or trigger AWS Lambda for automated remediation or prevention

********* GUARD-DUTY *********

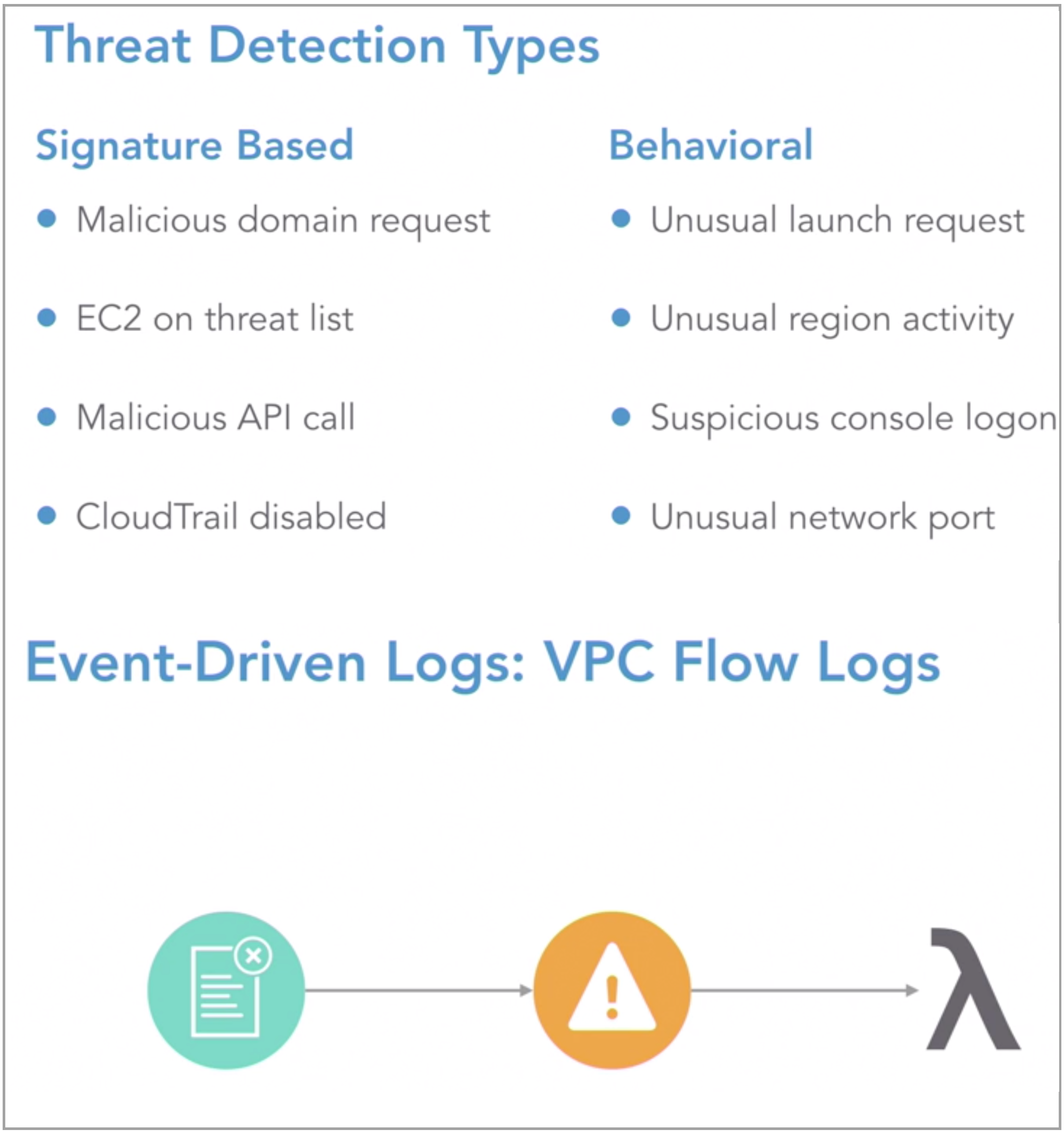


GuardDuty Log Analysis

CloudTrail APIs

VPC Flow Logs

Route 53 Logs



Threat Detection Types

Signature Based

- Malicious domain request
- EC2 on threat list
- Malicious API call
- CloudTrail disabled

Behavioral

- Unusual launch request
- Unusual region activity
- Suspicious console logon
- Unusual network port

Event-Driven Logs: VPC Flow Logs