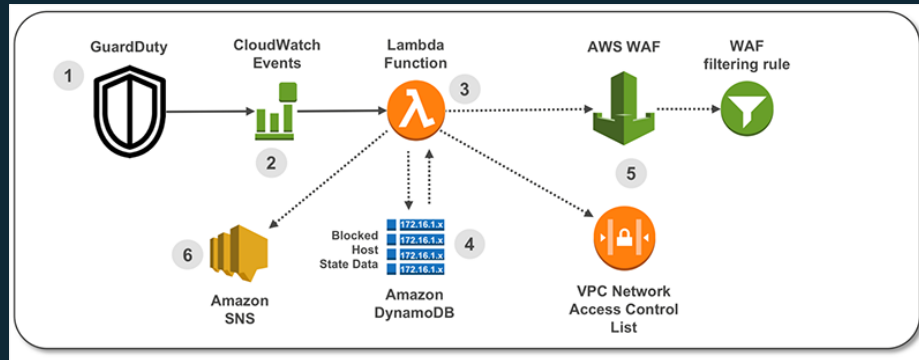


Automate Threat Mitigation Using AWS WAF and Amazon GuardDuty



Alex Tomic, AWS Solutions Architect
Cameron Worrell, AWS Solutions Architect

Agenda

- Intro to AWS Security Services
- AWS Web Application Firewall (WAF)
- Amazon GuardDuty
- Response Automation Patterns
- Demo
- Next Steps and Resources

In AWS:

Move fast

AND

Stay secure

with automation

AWS security solutions



Identity

AWS Identity & Access Management (IAM)
AWS Organizations
AWS Cognito
AWS Directory Service
AWS Single Sign-On



Detective control

AWS CloudTrail
AWS Config
Amazon CloudWatch
Amazon GuardDuty
VPC Flow Logs



Infrastructure security

Amazon EC2
Systems Manager
AWS Shield
AWS Web Application Firewall (WAF)
Amazon Inspector
Amazon Virtual Private Cloud (VPC)



Data protection

AWS Key Management Service (KMS)
AWS CloudHSM
Amazon Macie
Certificate Manager
Server Side Encryption

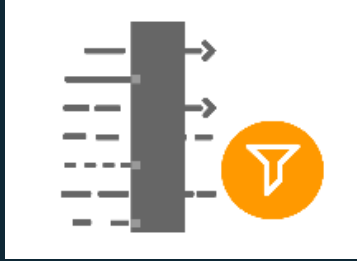


Incident response

AWS Config Rules
AWS Lambda



What is AWS WAF?



**Web traffic filtering
with custom rules**



**Malicious request
blocking**



**Active monitoring
and tuning**

AWS WAF available on



Amazon CloudFront
(Amazon's CDN)



Application Load Balancer
(ALB)

Flexible Rule Language (Combine conditions)

Restrict a rule to specific URIs, such as the login page.

RestrictAdminPage

Edit rule

When a request is not originating from an IP Addresses in [SeattleOffice](#)

IP Addresses in SeattleOffice

IPV4 : 54.234.196.0/24

IPV4 : 54.234.195.0/24

IPV4 : 54.234.1.21/32

And

When a request is matching one of the filters in [AdminLoginPage](#)

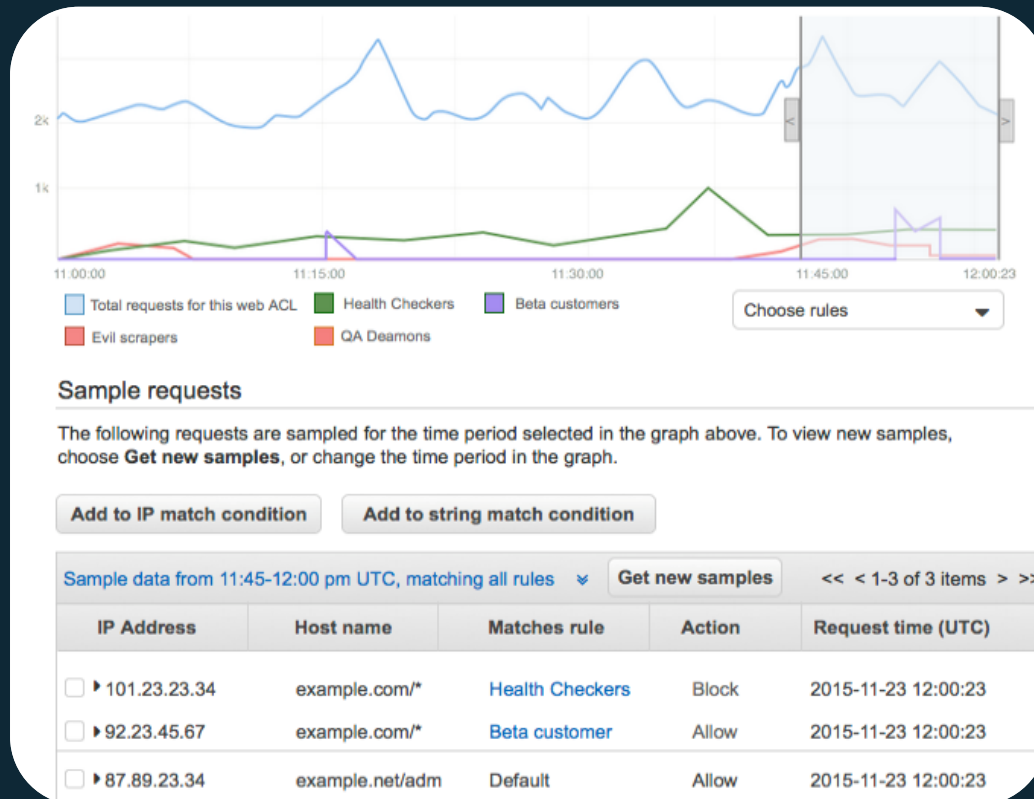
Filters in AdminLoginPage

URI matches STARTS_WITH '/admin/login.cgi' with LOWERCASE transformation.

IP match

String match

AWS WAF - Dashboard





Amazon GuardDuty

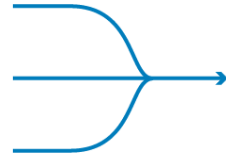
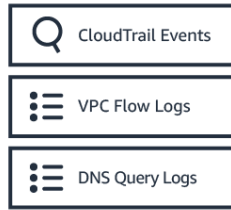
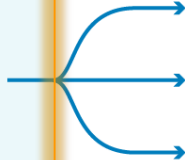
Intelligent threat detection and
continuous security monitoring.



Introducing Amazon GuardDuty Threat Detection and Notification



ACCOUNT 1
ACCOUNT 2
ACCOUNT 3



Enable GuardDuty

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

Continuously analyze

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

Intelligently detect threats

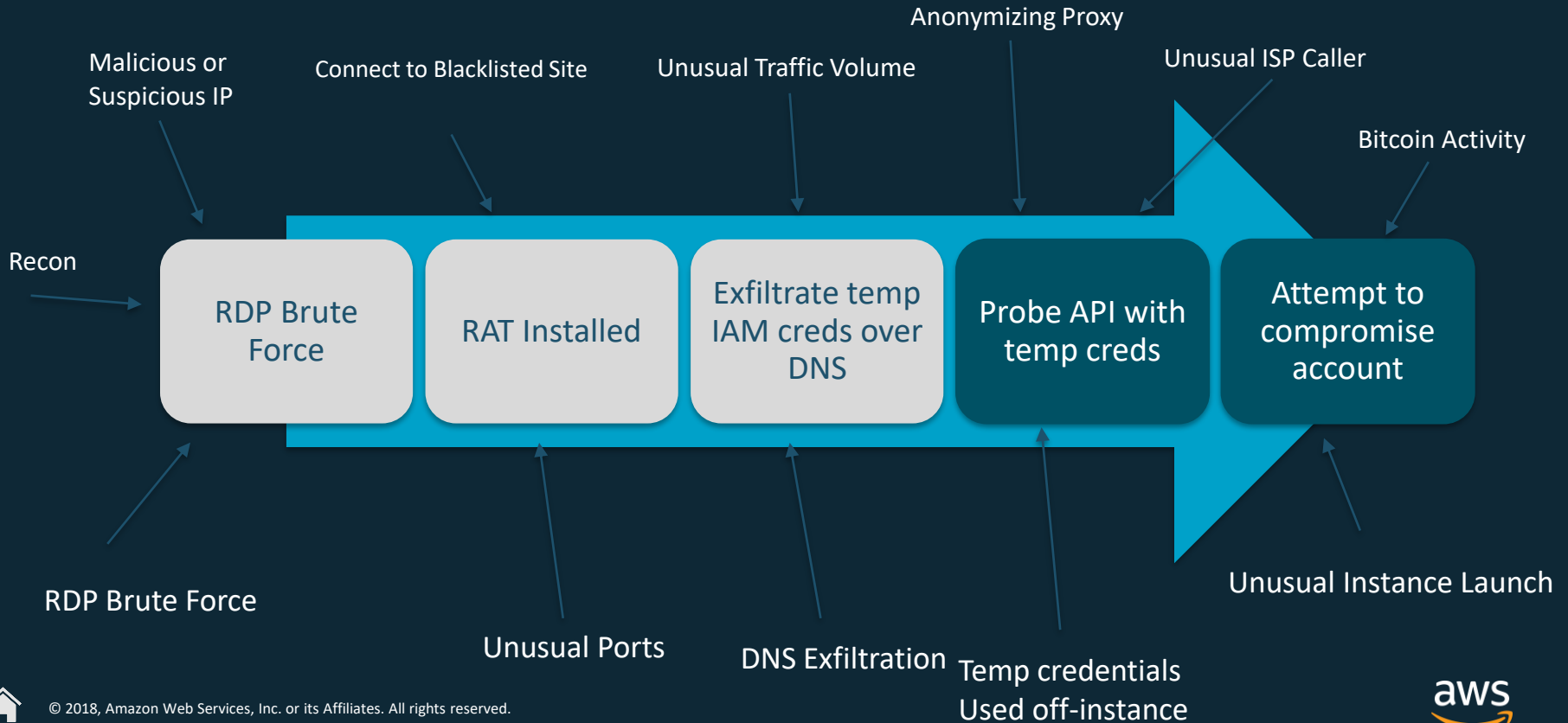
Utilize managed rule-sets, integrated threat intelligence, anomaly detection, and machine learning to intelligently detect malicious or unauthorized behavior

Leverage actionable alerts

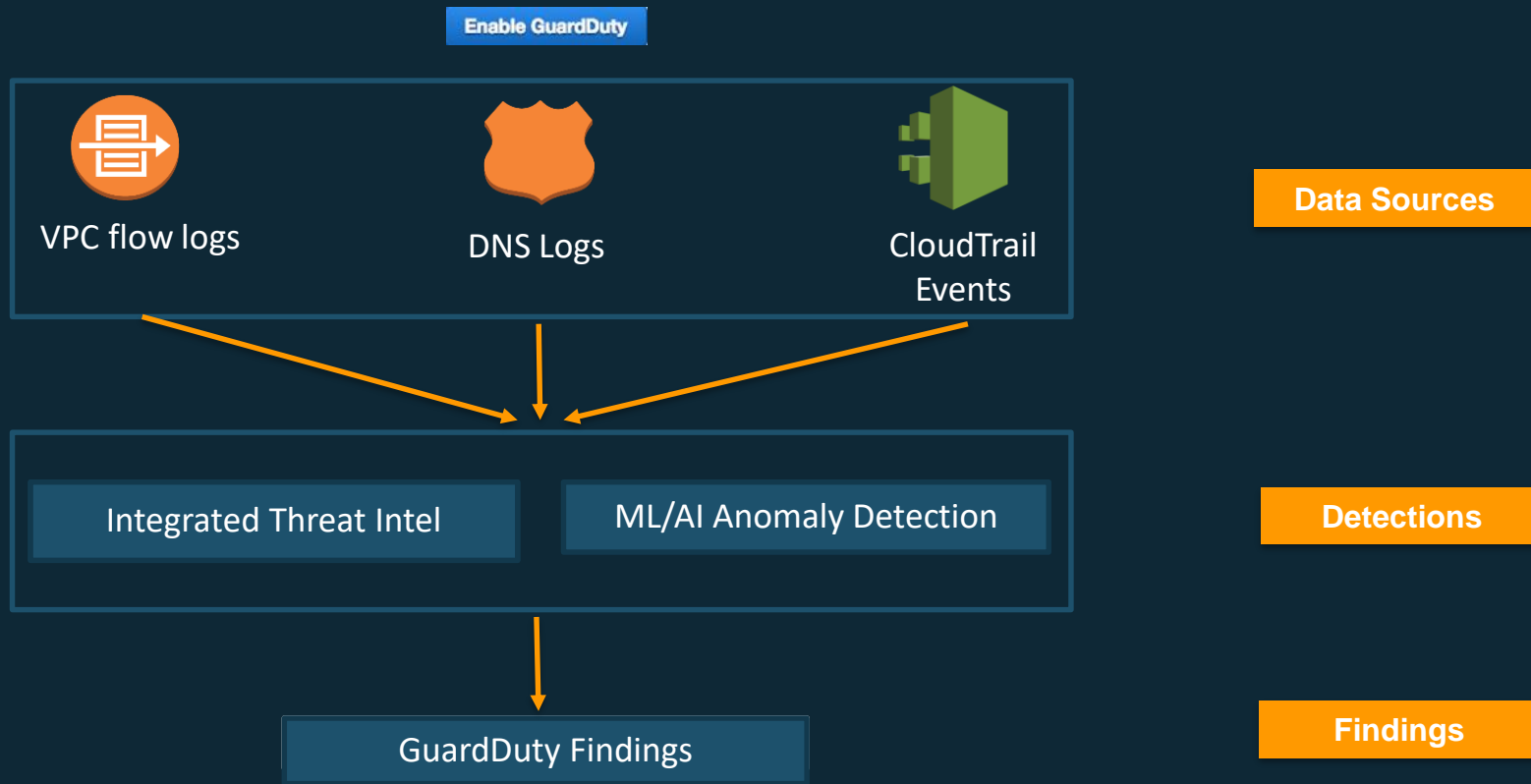
Review detailed findings in the console, integrate into event management or workflow systems, or trigger AWS Lambda for automated remediation or prevention



Covering the Attackers Kill Chain



How Does Amazon GuardDuty Work?



Findings Dashboard



Services ▾

Resource Groups ▾



AdminAccess/tstickle-Isengard ... ▾

Oregon ▾

Support ▾

GuardDuty

Findings

Settings

Lists

Accounts

Usage

Partners

New feature: Consolidated Findings

We've streamlined the navigation and put Current and Archived Findings in one place. Use the filter icon to choose what is shown in the table

Findings

Showing 7 of 7 2 2 3

Actions ▾

Saved filters

No saved filters

Add filter criteria

<input type="checkbox"/>	Finding type	Resource	La...	C
<input type="checkbox"/>	UnauthorizedAccess:EC2/RDPBr...	Instance: i-0e7477409a	11 mi...	1
<input type="checkbox"/>	UnauthorizedAccess:EC2/SSHBr...	Instance: i-0fe8954a34	12 mi...	1
<input type="checkbox"/>	Recon:EC2/Portscan	Instance: i-067db4866c	13 mi...	1
<input type="checkbox"/>	UnauthorizedAccess:EC2/SSHBr...	Instance: i-067db4866c	13 mi...	1
<input type="checkbox"/>	Backdoor:EC2/C&CAActivity.B!DNS	Instance: i-067db4866c	an ho...	75
<input type="checkbox"/>	Trojan:EC2/DNSDataExfiltration	Instance: i-067db4866c	an ho...	3
<input type="checkbox"/>	CryptoCurrency:EC2/BitcoinTool...	Instance: i-067db4866c	an ho...	1

Useful?

Close



UnauthorizedAccess:EC2/SSHBruteForce

Finding ID: [62b19bb549b62627ff4778804b8c060](#)



i-067db4866dbf1dafd is performing SSH brute force attacks against 172.16.0.25. Brute force attacks are used to gain unauthorized access to your instance by guessing the SSH password.

Severity

High

Region

us-west-2

Count

1

Account ID

5692-

Resource ID

[i-067db4866db...](#)

Created at

2018-05-06 14:...

Updated at

2018-05-06 14:...

Resource affected

Resource role

ACTOR

Resource type

Instance

Instance ID

[i-067db4866dbf1dafd](#)

Port

35712

Port name

Unknown

Instance type

m4.large

Instance state

running

Availability zone

us-west-2a







Findings Formats

AWS Management Console

API / JSON Format





EC2 Instance [Close](#)    

i-e2f5f524
performing outbound port scans.

Recon:EC2/Portscan [Q](#) [Q](#)

Actions ▾

This finding was:  


⚠ EC2 Instance i-e2f5f524 is performing outbound port scans against remote host 10.0.0.158.

Severity	Region	Count
Medium Q Q	us-west-2	1

Account ID
1851063622... [Q](#) [Q](#)

Resource ID
i-e2f5f524 [Q](#) [Q](#)

Last seen
2017-11-01 15:53:28 (an hour ago)

▼ **Resource Affected** 

Resource role	Resource type
ACTOR	Instance Q Q

Instance ID <u>i-e2f5f524</u> Q Q	Port 38128 Q Q
Image ID ami-494e7279	Launch time 2015-10-14 23:57:18

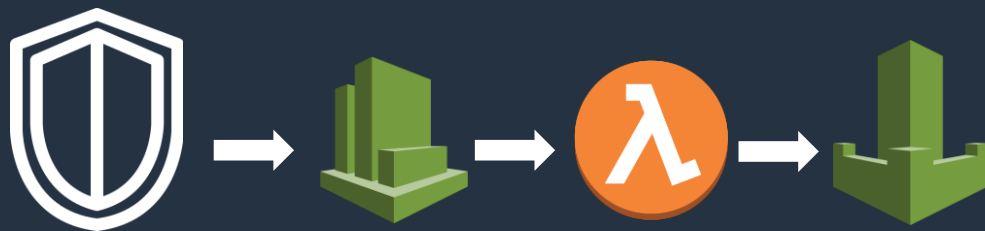
Tags
Name: tester
Inspector: Enabled

Private IP address 10.0.1.224	Private dns name ip-10-0-1-224.us-west-2....
Subnet ID subnet-d44ca8bc	VPC ID vpc-de4ca8b6 Q Q

```
{
  "type": "Recon:EC2/Portscan",
  "resource": {
    "resourceType": "Instance",
    "instanceDetails": {
      "imageId": "ami-494e7279",
      "instanceId": "i-e2f5f524",
    }
  },
  "service": {
    "serviceName": "guardduty",
    "detectorId": "6caf0da04f873e4ab085519f39f7fa88",
    "action": {
      "actionType": "NETWORK_CONNECTION",
      "networkConnectionAction": {
        "connectionDirection": "OUTBOUND",
        "remoteIpDetails": {
          "ipAddressV4": "10.0.0.158",
        }
      }
    },
    "resourceRole": "ACTOR",
    "additionalInfo": {
      "portsScannedSample": [
        140,
        83,
        110,
      ]
    }
  },
  "eventFirstSeen": "2017-11-01T22:52:36Z",
  "eventLastSeen": "2017-11-01T22:53:28Z",
  "severity": 5,
  "createdAt": "2017-11-01T23:00:10.179Z",
  "updatedAt": "2017-11-01T23:00:10.179Z",
  "title": "EC2 Instance i-e2f5f524 performing outbound port",
  "description": "EC2 Instance i-e2f5f524 is performing outbo"
}
```



Response Automation Patterns



Automated Response Pattern

Record It!

Logging

CloudTrail
CloudWatch Events
Config
VPC FlowLogs
Application Logs
...



Check It!

Detection

Signature Match
Behavior Heuristics
Insecure Config Check
Threshold Alarms
ML Analysis
...



Fix It!

Remediation

Notify Admins
Add Malicious IP to WAF
Add Malicious IP to NACLs
Revert SG Changes
...



Automated Response Pattern

Record It!

Logging



GuardDuty Findings are recorded in CloudWatch Events

Check It!

Detection



CloudWatch Event Rule routes GD findings to a Lambda function

Fix It!

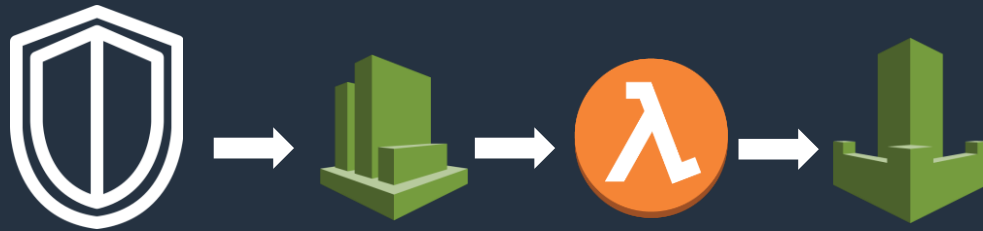
Remediation



Lambda updates WAF ACL, VPC NACL and emails via SES

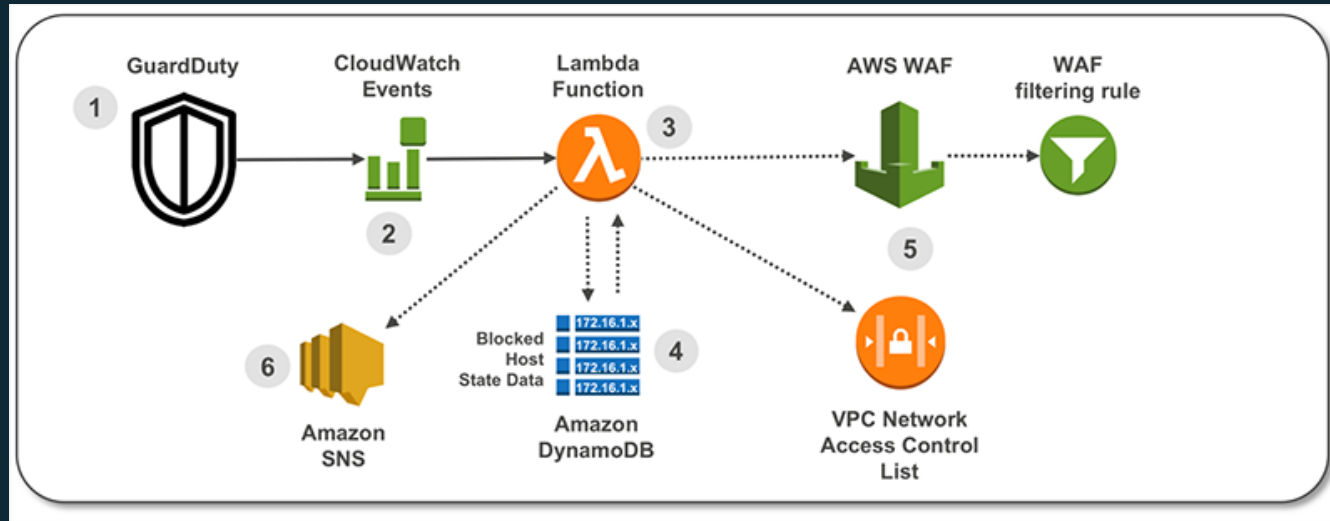


Demo Time!

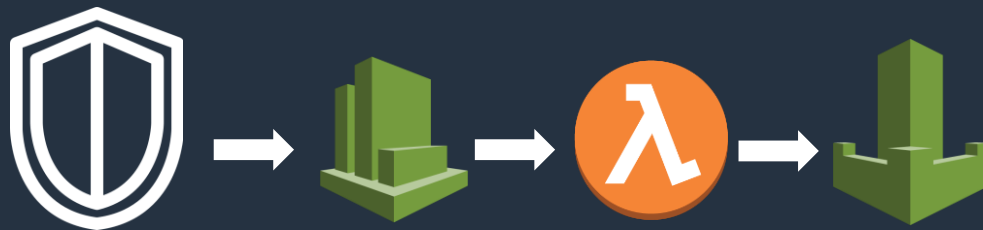


Automated Response Pattern

Based on Blog Post: “How to use Amazon GuardDuty and AWS Web Application Firewall to automatically block suspicious hosts”



Next Steps and Resources



WAF for Web App Protection



Launch



1. Easy to deploy



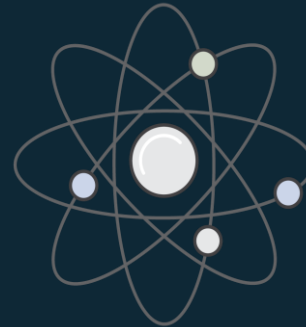
2. Fast Incident Response



3. Affordable



4. Full API Support



5. Managed Service



Turn On GuardDuty!



Welcome to GuardDuty

30 day free trial

Service permissions

When you enable GuardDuty, you grant GuardDuty permissions to analyze AWS CloudTrail logs, VPC Flow Logs, and DNS query logs to generate security findings. [Learn more](#)

[View service role permissions](#)

Note: GuardDuty doesn't manage AWS CloudTrail logs, VPC Flow Logs, and DNS query logs or make their events and logs available to you. You can configure the settings of these data sources through their respective consoles or APIs. You can suspend or disable GuardDuty at any time to stop it from processing and analyzing events and logs. [Learn more](#)

When you enable GuardDuty for the first time, your AWS account is automatically enrolled in a 30 day [GuardDuty free trial](#). Learn more about [GuardDuty pricing](#).

[Enable GuardDuty](#)



Review the Blog Post



AWS Security Blog

How to use Amazon GuardDuty and AWS Web Application Firewall to automatically block suspicious hosts

by Cameron Worrell, Alex Tomic, and Sundar Jayashekar | on 03 AUG 2018 | in [Amazon GuardDuty](#), [AWS WAF](#), [Security](#), [Identity](#), & [Compliance](#) | [Permalink](#) | [Comments](#) | [Share](#)

When you're implementing security measures across your AWS resources, you should use a holistic approach that incorporates controls across multiple areas. In the [Cloud Adoption Framework \(CAF\) Security perspective](#) whitepaper, we define these controls across four categories.

- **Directive controls.** Establish the governance, risk, and compliance models the environment will operate within.
- **Preventive controls.** Protect your workloads and mitigate threats and vulnerabilities.
- **Detective controls.** Provide full visibility and transparency over the operation of your deployments in AWS.
- **Responsive controls.** Drive remediation of potential deviations from your security baselines.



Links to More Resources:

- How to use Amazon GuardDuty and AWS Web Application Firewall to automatically block suspicious hosts: <https://aws.amazon.com/blogs/security/how-to-use-amazon-guardduty-and-aws-web-application-firewall-to-automatically-block-suspicious-hosts/>
- GitHub repo: <https://github.com/aws-samples/amazon-guardduty-waf-ac1>
- AWS WAF Documentation: <https://docs.aws.amazon.com/waf/latest/developerguide/what-is-aws-waf.html>
- AWS GuardDuty Documentation: <https://docs.aws.amazon.com/guardduty/latest/ug/what-is-guardduty.html>

Thank You!

