### ·III Recorded Future®



# **Amazon GuardDuty Installation Guide**

This guide will describe the steps involved in integrating Recorded Future as a threat intelligence detection source in Amazon GuardDuty. Please note that there are expansive permissions required within S3, CloudWatch, Lambda, IAM, SSM Parameter Store, and GuardDuty to complete this integration. If you do not have sufficient permissions, please contact your AWS Administrator.

### **Ensure Amazon GuardDuty Is Enabled**

Search for GuardDuty from within your AWS console. Select "GuardDuty".

History	GuardDuty					Group A-Z
Console Home CloudFormation	GuardDuty Intelligent Threat Detection to Pro	tect Your A	WS Accounts and Workloads			tion Integration
GuardDuty S3 EC2 Billing	EC2 Lightnail (2 ECR ECS EKS		AWS IQ (2 Support Managed Services	Amazon SageMaker Amazon CodeGunu Amazon Comprehend Amazon Forecast Amazon Fraud Detector		Step Functions Amazon EventBridge Amazon MQ Simple Notification Service Simple Queue Service
	Lambda Batch Elastic Beanstalk	000	Blockchain Amazon Managed Blockchain	Amazon Kendra Amazon Lex Amazon Lex		SWF
	Serverles Application Repository AWS Outposts EC2 Image Builder	9	Satellite Ground Station	Amazon Personalize Amazon Personalize Amazon Polly Amazon Rekognition Amazon Textract		AWS Cost Management AWS Cost Explorer AWS Budgets AWS Marketplace Subscriptions
	Storage	838	Quantum Technologies Amazon Braket @	Amazon Transcribe Amazon Translate AWS DeepLens	P	Customer Engagement

#### Next, click "Get Started".

Note: This screen will only be available if Amazon GuardDuty has not been previously enabled. If you do not see this screen, Amazon GuardDuty is most likely already enabled, and you may disregard this step.



# ·III·Recorded Future®

### Click on "Enable GuardDuty"

aws Servic	es 👻 Resource Groups 👻 🏌	N. Virginia 👻 Support 🔹
GuardDuty ×	Welcome to GuardDuty	30 day free trial
Enable GuardDuty	Service permissions	
Partners 🖸	When you enable GuardDuty, you grant GuardDuty permissions to analyze AWS Clou security findings. Learn more View service role permissions	udTrail logs, VPC Flow Logs, and DNS query logs to generate
	Note: GuardDuty doesn't manage AWS CloudTrail logs, VPC Flow Logs, and DNS quer can configure the settings of these data sources through their respective consoles or stop it from processing and analyzing events and logs. Learn more	
	When you enable GuardDuty for the first time, your AWS account is automatically en about GuardDuty pricing.	nrolled in a 30 day GuardDuty free trial. Learn more  Enable GuardDuty

### **Creating a Stack**

Navigate to Cloud Formation within your AWS Console.

History							Carried I	
GuardDuty Console Home	CloudFormation CloudFormation Create and Manage Resources wit	h Template	5			tion	Group	A-Z
CloudFormation S3 EC2 Billing	EC2 Lightsail (2' ECR ECS EKS Lambda Batch Eastic Beanstalk	Lightseil (? Si ECR M ECS EKS Lambda E		Amazon SageMaker Amazon CodeGuru Amazon Comprehend Amazon Forecast Amazon Fraud Detector Amazon Kendra Amazon Lex Amazon Machine Learning	u Amazon EventBr end Amazon MQ Simple Notificatik tector Simple Queue Se SWF		tBridge tation Servi	
	Serverless Application Repository AWS Outposts EC2 Image Builder	<i>I</i> 8	Satellite Ground Station Quantum Technologies	Amazon Personalize Amazon Polly Amazon Rekognition Amazon Textract Amazon Transcribe Amazon Transtribe		AWS Cost N AWS Cost Ex AWS Budgets AWS Marketp	plorer i	
	Storage \$3		Amazon Braket C	AWS DeepLens	P	Customer E Amazon Conr		nt

#### Select "Create Stack"

Stacks (0)	C	Delete Update Sta	ck actions 🔻 Create stack 🔻
Q Filter by stack name			Active 🔻 💽 View nested
			< 1 > 0
Stack name	Status	Created time	• Description
	No	No stacks o stacks to display	

# ·I¦I·Recorded Future®

Select "Template is ready" and "Upload a template file" from the menu screen. Select "Choose File" and upload the Recorded Future Cloud Formation Template. Then select "Next".

Step 1 Specify template	Create stack			
Step 2 Specify stack details	Prerequisite - Prepare template			
Step 3	Prepare template Every stack is based on a template. A template is a	JSDN or YAMs file that contains configuration information	about the AWS resources you want to include in the stack.	
Configure stack options	<ul> <li>Template is ready</li> </ul>	<ul> <li>Use a sample template</li> </ul>	Create template in Designer	
Réview	Specify template A template is a JSON or YMML file that describes y Template source Selecting a template governes an Amazon S3 UR			
	Amazon S3 URL	O Upload a t	template file	1
	Upload a template file Choose file  JSGN or YAML formatted file			
	Choose file 🕀 No file chosen		View in Designer	

#### Specify stack parameters and select "Next" to continue.

Note: An API token from Recorded Future is required for this step. Please reach out to your account manager to obtain an API token for this integration.

Step 1 Specify template	Specify stack details	
Step 2 Specify stack details	Stack name	
Step 3	Stack name	
Configure stack options	RecordedFutureGuardDuty	
	Stack name can include letters (A-2 and a-a), numbers (D-B), and dashes (-).	
Review	Parameters Parameters Parameters and defined in your template and allow you to induct custom values when you create or update a stack.  Recorded Future Information Recorded Future API Token Instart Recorded Fut	
	Risk Lists Finant a common-detimited list of Recorded Potum Risk Lists (contact your Inderv consultant for more information)	
	phishing_host_riskrule, recent_insikt_group_riskrule, recent_intrusion_method_riskrule, ip_risklist_gt_65	
	Advanced Settings Update Schedule Invert the number of flows between executions - when the solution downlasts a new Risk Lot (min 1 - max 170)	
	24 8	

Configure any desired stack options. The defaults within this page should be sufficient for the integration.

CloudFormation > Stacks >	Create stack	
Step 1 Specify template	Configure stack options	
Step 2 Specify stack details	Tags You can specify tags Rep-value paint to apply to resources in your stack. You can add up to 50 unique tags for each stack. Learn more 🔀	
Step 5 Configure stack options	Xoy Value Remove	
Step 4 Review	Add tag	
	Permissions Ovase an IMM-relic to explicitly define how Claud Termation can create, modify, or delete resources in the stack. If you don't choose a rule, Claud Termation uses permissions based on your user createrization. Learn more 🔀	
	IAM role - optional	
	IAM role - optional Choose the IAM role for CloudFormation to use for all operations performed on the stack.	
	Choise the LMM role for CloudFormation is use for all operations performed on the stack.           IAM role name         Sample-role-name         Remove	
	IAM role name           Sample-role-name           Remove	

Review the stack configurations you previously selected.

aws Services - Res	source Groups 🐱 🕈	N. Virginia + Support
CloudFormation > Stacks >	Create stack	
Step 1 Specify template	Review RecordedFutureGuardDuty	Edit
Step 2 Specify stack details	Step 1: Specify template Template	Leit
Step 3 Configure stack options	Templare UIL	
Step 4 Review	https://Si-external-1-amazonaws.com/c5-templates-1158/950540/d-us-kass-1/20200702/bu-inline-integration.joon Sterk: description - Estimate cost not available	
	Step 2: Specify stack details	Edit
	Parameters (3) Q. Separa parameters	٥
	Key A Value	*
	Frequency 24	
	RFAPITokan ********	
	RiskLists phishing_host_risknule, recent_insikt_group_risknule, recent_intrusion_method_risknule, ip_risklist_gt_65	

At the bottom of the stack configuration review page, you will be required to acknowledge that AWS CloudFormation might create IAM resources with custom names. Check the box as shown and select "Create stack".

•	The following resource(s) require capabilities: [AWS::IAM::Role]
	This template contains identity and Access Management (IAM) resources. Check that you want to create each of these resources and that they have
	the minimum required permissions. In addition, they have custom names. Check that the custom names are unique within your AWS account. Learn more
	account. Learn more

# ·II Recorded Future®

The stack will begin to initialize based on the settings selected. The status of the job will be reported on the page below. Once you see a "CREATE\_COMPLETE" note under your stack, your stack will be created. Any errors during this process will be displayed under the "Status Reason" column.

aWS Services - Resource Gr	roupa 👻 🔭				N, Virginia - Support
CloudFormation > Stacks > Recorded	FutureGuardDuty				
Stacks (1)	C	RecordedFutureGuardDuty	1		Delete Update Stack actions V Create stac
Q. Filtur by stack name		Stack Info Events Resources O	utputs Parameters Template	Change sets	
Active View nested	615	Events (23)			-
RecordedFutureGuardButy 2020-05-10 14:30:53 UTC-0400 © CREATE_COMPLETE	0	Q. Search events			C
		Timestamp v	Logical ID	Status	Status reason
		2020-05-10 14:52:42 UTC-0400	RecordedFutureGuardDuty	@ CREATE_COMPLETE	2
		2020-03-10 14:52:40 UTC-0400	UpdateThreatFeedSchedulerInvokeP ermissions	@ CREATE_COMPLETE	11 11
		2020-03-10 14:32:30 UTC-0400	UpdateThreatFeedSchedulerInvokeP ermissions	CREATE_IN_PROGRESS	Resource creation Initiated
		2020-05-10 14:52:29 UTC-0400	UpdateThreatFeedSchodulerInvokeP ermissions		17 I
		2020-03-10 14:32:27 UTC-0400	UpdateThreatFeedScheduler	@ CREATE_COMPLETE	9. 1
		2020-03-10 14:32:00 UTC-0400	UpdateThreatFeedEvent	CREATE COMPLETE	

### **Verify Successful Stack Creation**

Navigate back to "GuardDuty".

aws Service	s 🔺 Resource Groups 👻	*			N. Virgin	ia 👻 Support 👻
History Console Home	GuardDuty					Group A-Z
GuardDuty	GuardDuty Intelligent Threat Detection to Protect Your AWS Accounts and Workloads			er	Computing	
	EC2		AWS IQ C	Athena	WorkSpace	
	Lightsail 🕑		Support	EMR	AppStream	2.0
	ECR		Managed Services	CloudSearch	WorkDocs	
	ECS			Elasticsearch Service	WorkLink	
	EKS			Kinesis		
	Lambda	KICICI	Blockchain	QuickSight (2*		

On the left side menu, select "Lists" to see list management options.

aws	Services	<ul> <li>Resource 0</li> </ul>	àroups v 🕈				N. Virginia 👻	Support	*
GuardDuty	×	Findings C					Showing 1 of	1 💽	00
Findings Settings		Actions V		Sav	red filters / Auto-archive	No saved filters			
Lists		Current 🔻	₽ Add filter criteria						
Accounts What's New			Finding type	*	Resource	Ŧ	Last 🔻	Count	٣
Usage			Behavior:EC2/NetworkPortUnusual		Instance: i-d5baa552		2 months a	2	
Partners 🖸									

# ·I¦I·Recorded Future®

From here, scroll down to "Threat Lists" and ensure the successful creation of the Recorded Future threat lists inputted into the risklist field of the stack parameters. Ensure each list is active.

aws	Services •	<ul> <li>Resource Groups ~</li> </ul>	*						N. 1	firginia -	Support -
GuardDuty	×	List management									
Findings Settings		Trusted IP lists									
Lists Accounts		Trusted IP lists consist of IP addresses that are whitelisted for secure communication with your XWS environment. GuardDury does not generate findings for IP addresses that are included in trusted IP links. Learn room									
What's New		+ Add a trusted IP list									
Free trial		List name	List file URL	Format	Active						
Partners 🖸		generate findings	vist of IP addresses that are whitelisted for scoure communication for IP addresses that are included in trusted IP lists. Learn more maticious IP addresses. GuardDuty generates findings for IP addre								
Partonin LS		Threat lists consist of known	for IP addresses that are included in trusted IP lists, Learn more								
Partonin LS		Threat lists Threat lists Threat lists Add a threat list	for IP addresses that are included in trusted IP lists. Learn more malicious IP addresses. GuardDuty generates findings for IP addre	ases that are included in t	West libts. Ley						
Partonin LS		Trusted IP liets car generate findings Threat lists Threat lists consist of known + Add a threat list List name	for IP addresses that are included in trusted IP lists. Learn more Intellicious IP addresses. GuardDuty generates findings for IP addres List the URE s1//recorded/utvrguardduty-threatfeedbucket-1proot12/31	ases thet are included in t Format TXT	hreat lists. Lea	ett more					
Partners LS		Threat lists Threat lists Threat lists Threat lists Threat lists Ust name O lp_risklar_gt_65 O phabling_rost_riskr	for IP addresses that are included in trusted IP lists. Learn more Intellicious IP addresses. GuardDuty generates findings for IP addres List the URE s1//recorded/utvrguardduty-threatfeedbucket-1proot12/31	Format TXT TXT	Active	m more					

Note: If Recorded Future threat lists have not been created successfully, please check your Lambda function logs for any errors that may appear there under log group ex: /aws/lambda/[StackName]-UpdateThreatFeedFunction-[randomstring]

### **Check for Any Findings from the Threat List**

Navigate to the GuardDuty home page. Select "Findings" and select a finding.

aws Servi	ces	<ul> <li>Resource</li> </ul>	e Gro	ups v 🔭					N. Virginia	ı - Suppo	rt -
GuardDuty	¢	Findings C	1						Showing a	8 of 8 🔘	00
Findings Settings		Actions 7		🔁 Suppress Findings			Saved rules	No saved	rutes		
Lists		Current 🖤	V	Add filter criteria							
Accounts What's New			v	Finding type	*	Resource			Last seen 🔻	Count	v
Usage			٠	UnauthorizedAccess:EC2/MaliciousIPCaller.Custom		Instance: i-Obd89eb3b8b51e8d0			6 hours ago	2	
				UnauthorizedAccess:EC2/MaliciousIPCaller.Custom		Instance: I-076718d2d0acee14e			8 hours ago	1	
Partners 🗹			۰	UnauthorizedAccess:EC2/MaliciousIPCaller.Custom		Instance: 1-0b6fd90105ba7f858			13 hours ago	2	
		0		Recon:IAMUser/UserPermissions		maf: ASIATSFICY6WXDT6TTEC			8 days ago	2	

#### A panel on the right side will display a summary of the hit as well as the threat list this IP was found on.

IP address	Port
64.233.160.0 @ Q	443
Location	
city: London	
country: United Kingdom	
lat: 51.5132	
lon: -0.0961	
Organization	
asn: 41231	
asnOrg: Acme Inc.	
isp: Acme Inc.	
org: Acme Inc.	
• Additional information	on
Threat name	Threat list name
Customer Threat Intel	Recorded Future Threat Detection
Archived	
false	

Use the Recorded Future Browser Extension to provide context as to "why" the indicator is risky.

·I¦I·Recorded Future	0		pport ~
All 6 1   IP Address 3 1 Domain 2	Hash 1   Vulnerabi	lity O	
• 67 64.233.160.0 IP Address		>	
5 recordedfuture.com Domain		>	
74.125.255.255 IP Address			
1cb7cfd2698bae5f8c1a26677a8feb3f Ha	sh		
72.14.192.0 IP Address			
ec2-3-91-157-234.compute-1.amazonaws.	.com Domain		
			(a day ago)
	▼ Actor		
	IP address 64.233.160.0 @ Q	Port 443	
	Location		

#### ABOUT RECORDED FUTURE

Recorded Future is the world's largest intelligence company. Recorded Future's cloud-based Intelligence Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future provides real-time visibility into the vast digital landscape and empowers clients to take proactive action to disrupt adversaries and keep their people, systems, and infrastructure safe. Headquartered in Boston with offices and employees around the world, Recorded Future works with more than 1,400 businesses and government organizations across more than 60 countries. Learn more at recordedfuture.com.

www.recordedfuture.com

