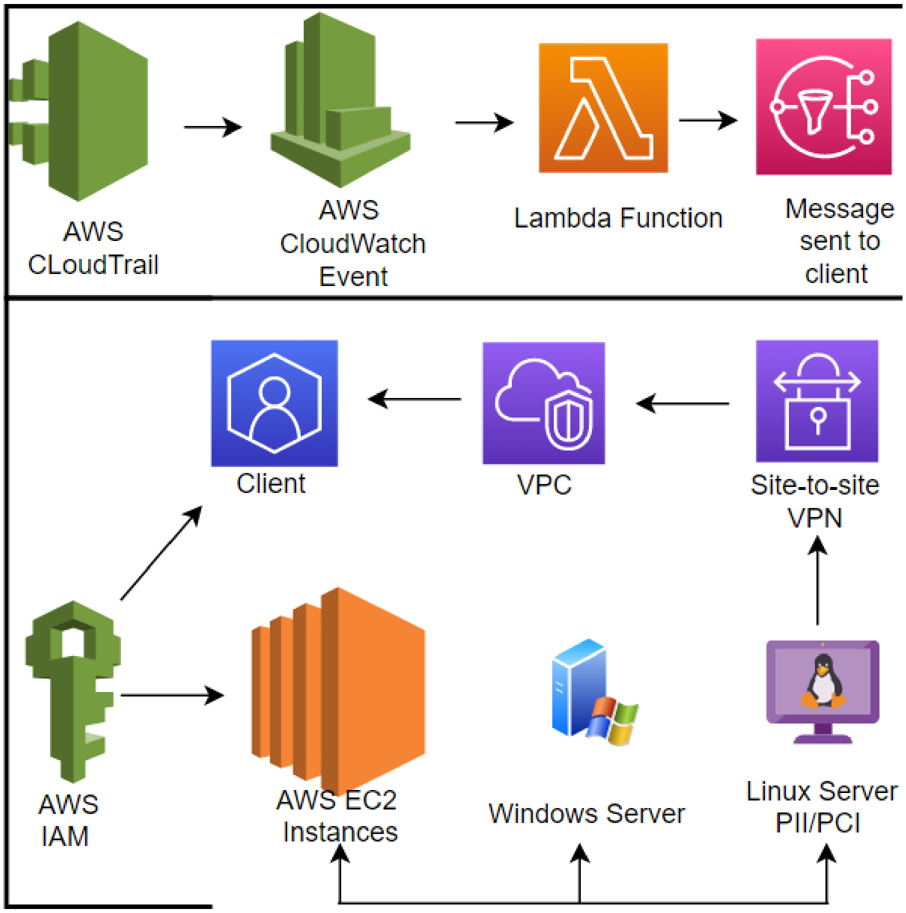
Written Explanation

Authored by Team

Utilizing two AWS EC2 instances, one Windows and one Linux base, we created a virtual private gateway for each instance to connect using a site-to-site VPN. We deployed each instance with their respective private subnets. The site-to-site VPN allows for secure communication. We will log and monitor using AWS CloudTrail and AWS GuardDuty.



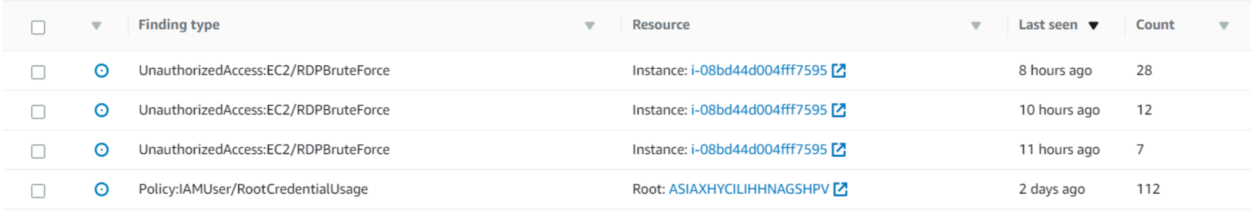
AWS Identity and Access Management (IAM)

IAM is responsible for managing user identities and their permissions within the AWS environment. It ensures that only authorized users have access to AWS services, helping to maintain a secure environment.

User name	Groups	Permissions/Policy	MFA
Alex_E	AdministratorAccess	AdministratorAccess CloudWatchAgentServerPolicy IAMUserChangePassword	YES
Anthony_W	AdministratorAccess	AdministratorAccess AWSMarketplaceFullAccess IAMUserChangePassword	YES
Dylan_D	LambdaUsers	AdministratorAccess AWSLambdaRole AWSLambdaExecute AWSLambda_FullAccess AmazonSNSFullAccess	YES
Dericus_D	AdministratorAccess	AdministratorAccess IAMUserChangePassword	YES
Geneva_K	AdministratorAccess	AdministratorAccess IAMUserChangePassword CloudWatchAgentServerPolicy	YES

AWS Guard Duty

Guard Duty is a threat detection service that continuously monitors various AWS services for potential security issues. It identifies and alerts you about suspicious activities or policy violations, enabling you to respond quickly to any potential threats.



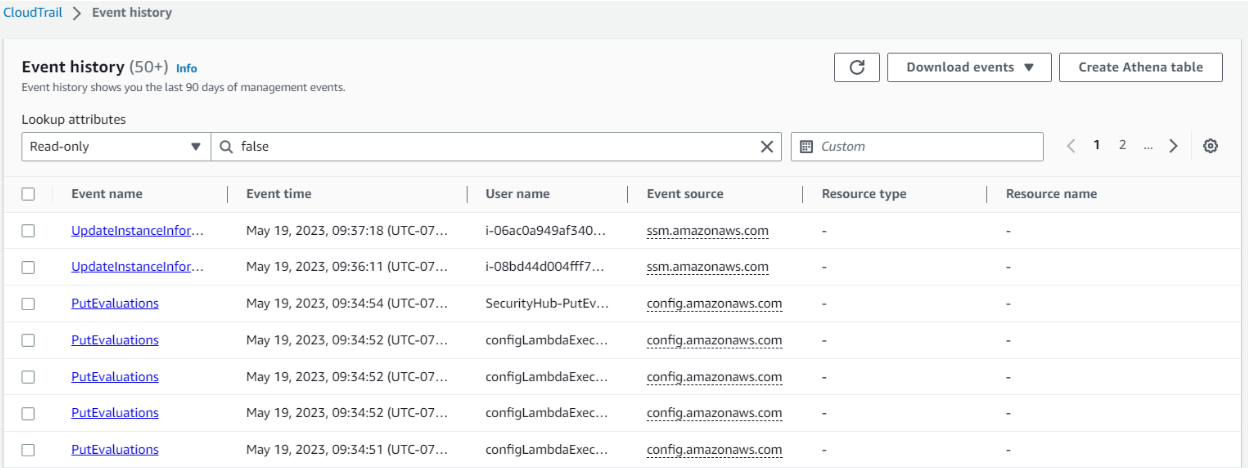
□		Finding type	Resource	Last seen	Count
□	⊙	UnauthorizedAccess:EC2/RDPBruteForce	Instance: i-08bd44d004fff7595	8 hours ago	28
□	⊙	UnauthorizedAccess:EC2/RDPBruteForce	Instance: i-08bd44d004fff7595	10 hours ago	12
□	⊙	UnauthorizedAccess:EC2/RDPBruteForce	Instance: i-08bd44d004fff7595	11 hours ago	7
□	⊙	Policy:IAMUser/RootCredentialUsage	Root: ASIAXHYCILIHHNAGSHPV	2 days ago	112

AWS Virtual Private Cloud (VPC)

VPC provides a private and isolated network environment for your AWS resources. It allows you to define and control network settings, such as IP addressing, subnets, and routing tables. By utilizing a private subnet and VPN tunnels, you enhance the security of your resources and establish secure connections between users and Windows Server DC.

AWS CloudTrail

CloudTrail captures and logs API activity within your AWS account. It helps with governance, compliance, and auditing by providing detailed information about user actions, resource changes, and more. Storing the logs in S3 allows for further analysis and integration with third-party services like Splunk.


CloudTrail > Event history

Event history (50+) Info

Event history shows you the last 90 days of management events.

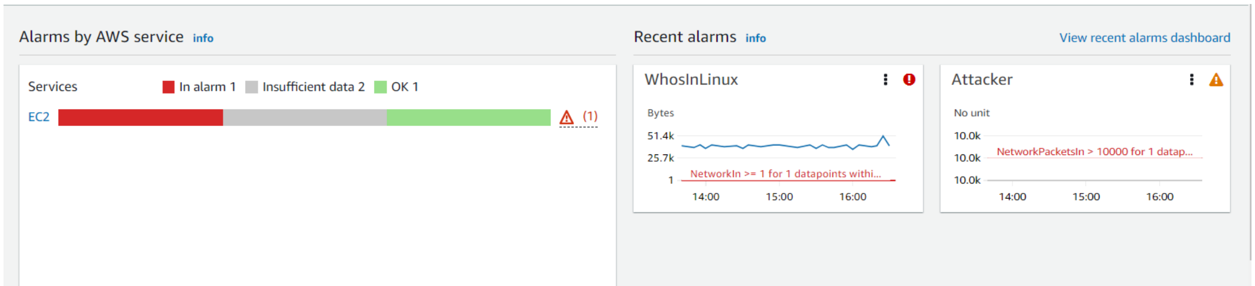
Lookup attributes

Read-only ▼ | false | Custom

□	Event name	Event time	User name	Event source	Resource type	Resource name
□	UpdateInstanceInfor...	May 19, 2023, 09:37:18 (UTC-07...	i-06ac0a949af340...	ssm.amazonaws.com	-	-
□	UpdateInstanceInfor...	May 19, 2023, 09:36:11 (UTC-07...	i-08bd44d004fff7...	ssm.amazonaws.com	-	-
□	PutEvaluations	May 19, 2023, 09:34:54 (UTC-07...	SecurityHub-PutEv...	config.amazonaws.com	-	-
□	PutEvaluations	May 19, 2023, 09:34:52 (UTC-07...	configLambdaExec...	config.amazonaws.com	-	-
□	PutEvaluations	May 19, 2023, 09:34:52 (UTC-07...	configLambdaExec...	config.amazonaws.com	-	-
□	PutEvaluations	May 19, 2023, 09:34:52 (UTC-07...	configLambdaExec...	config.amazonaws.com	-	-
□	PutEvaluations	May 19, 2023, 09:34:51 (UTC-07...	configLambdaExec...	config.amazonaws.com	-	-

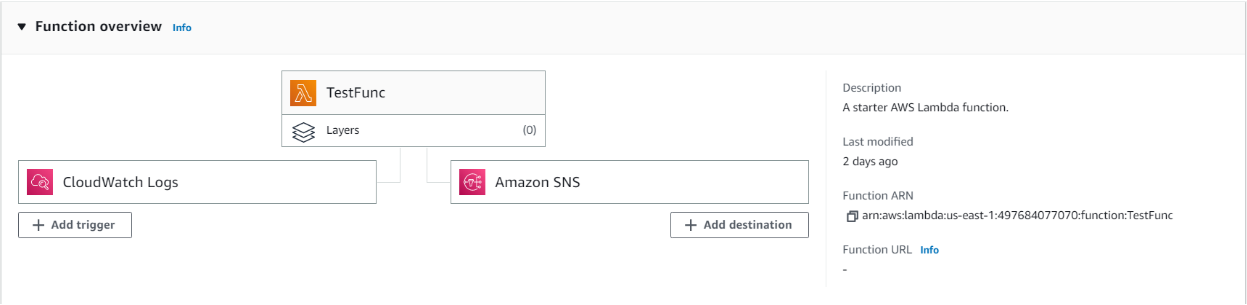
AWS CloudWatch

CloudWatch is a comprehensive monitoring service that collects and tracks various metrics related to your AWS resources. It enables real-time monitoring of metrics like CPU usage, latency, and error counts. By setting up alarms and triggering AWS Lambda functions based on predefined thresholds, you can respond to security threats or abnormal resource usage promptly.



AWS Lambda

AWS Lambda is a serverless computing service provided by Amazon Web Services (AWS). It allows you to run your code without provisioning or managing servers. With AWS Lambda, you can focus on writing your application code while AWS takes care of the underlying infrastructure and scaling.



Description
A starter AWS Lambda function.

Last modified
2 days ago

Function ARN
arn:aws:lambda:us-east-1:497684077070:function:TestFunc

Function URL Info
-