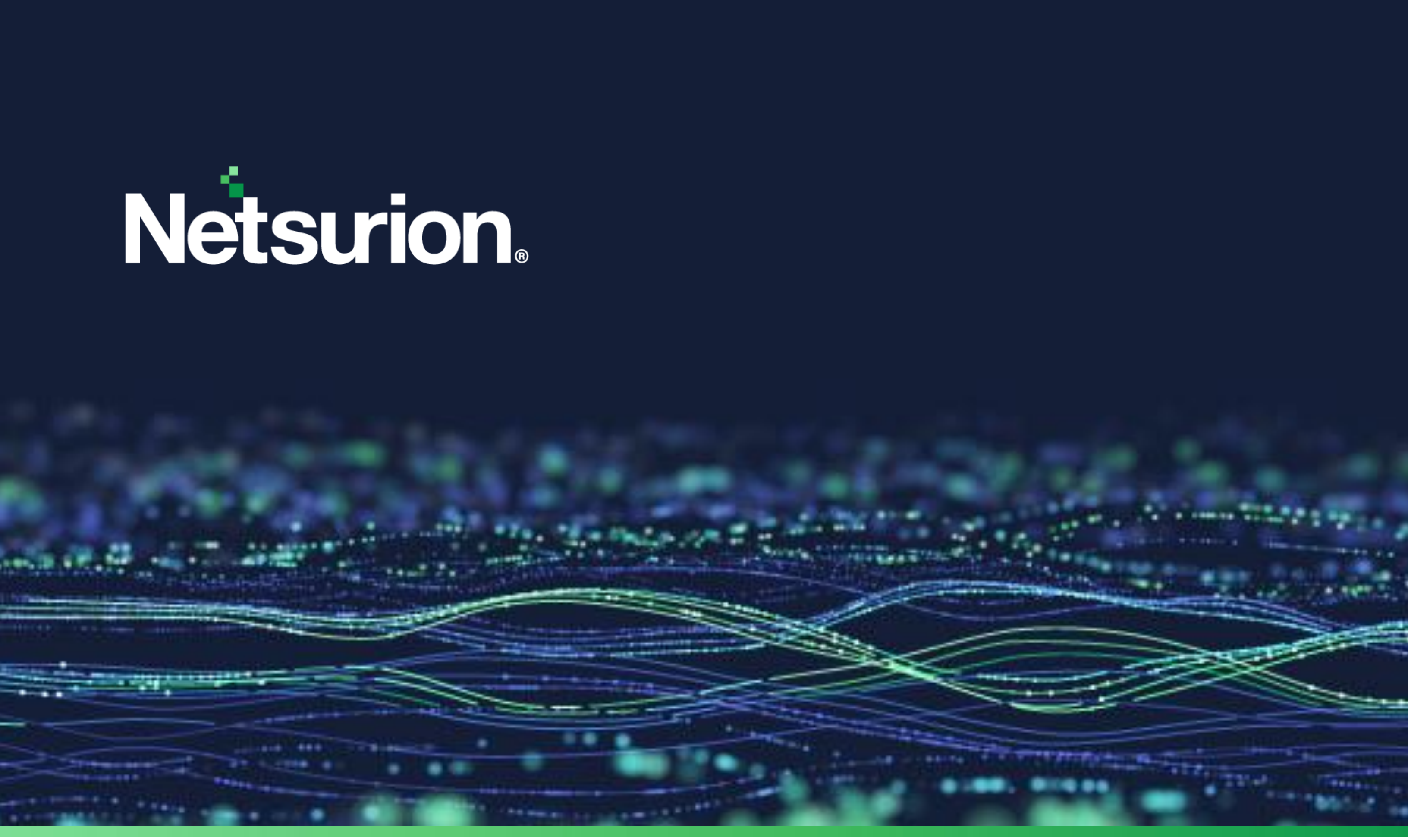

Integration Guide

Integrate Amazon Web Services (AWS) CloudTrail with Netsurion Open XDR

Publication Date:
December 08, 2023

Abstract

This guide provides instructions to configure the required Amazon Web Services (AWS) Data Source Integrations in Netsurion Open XDR to retrieve the Amazon Web services (AWS) logs using Amazon CloudTrail.

Note:

The screen/ figure references are only for illustration purpose and may not match the installed product UI.

Scope

The configuration details in this guide are consistent with Netsurion Open XDR 9.3 or later and AWS CloudTrail.

Audience

This guide is for the administrators responsible for configuring the Data Source Integration in Netsurion Open XDR.

Table of Contents

1 Overview

Amazon Web Services (AWS) is a collection of remote computing services (also called web services) that make up a cloud computing platform offered over the internet by Amazon.com.

Amazon CloudTrail is enabled on your AWS account when you create it. When an activity occurs in your AWS account, it gets recorded as a CloudTrail event. With CloudTrail, you can get the history of the AWS API calls for your account, including the API calls made via the AWS Management Console, AWS SDKs, command-line tools, and higher-level AWS services (such as AWS CloudFormation). Amazon EC2 and Amazon VPC are examples of a few services integrated with CloudTrail that is, CloudTrail captures the API calls made on behalf of Amazon EC2 and Amazon VPC.

Netsurion Open XDR manages logs delivered to CloudTrail and filters them to get the critical event types. The alerts, reports, dashboard, and saved searches in Netsurion Open XDR are enhanced by reducing the effort of having to manually log in to the AWS account and figure out what events are supposed to be critical. The logs collected by Netsurion Open XDR will include services like Amazon EC2 and Amazon VPC.

2 Prerequisites

- Configure AWS CloudTrail to forward logs to Netsurion Open XDR.
- Ensure Root level access to the AWS console.
- The Data Source Integration package.

Note

To get the Data Source Integration package, contact your Netsurion Account Manager.

- Netsurion Open XDR VCP port must be Network Address Translation (NAT) with the public IP address.

Note:

Refer to the How To Configure AWS CloudTrail guide to configure AWS CloudTrail to forward logs to Netsurion Open XDR.

3 System Extraction

Perform the following process for System extraction.

1. In **Netsurion Open XDR**, hover over the **Admin** menu and click **Manager.**
2. In the **Manager** interface, go to **syslog/ Virtual Collection Point** > **syslog,** hover over the **Gear** icon located adjacent to it, and then click **Extract device id** for extracting the system name.
3. Hover over the **Gear** icon and click the **Extract device Id** for extracting the system name using the below regex:
4. Fill in the following details, (for CloudTrail logs)
   a. **Regular expression:** Organisation:(?P<Tenant>[^,]+).*?"eventSource":"(?P<Computer>[^"]+)
   b. **Token Name:** Computer~Tenant
5. Click the **Update** button to save the extraction logic details.

4 Data Source Integrations (DSIs) in Netsurion Open XDR

After the logs are received by Netsurion Open XDR, configure the respective DSIs in Netsurion Open XDR.

Note

Refer the How To Configure DSI guide for the procedures to configure the respective DSIs in Netsurion Open XDR.

4.1 Console Events

4.1.1 Flex Reports

Name	Description
Amazon AWS Login Failed Activity	Generates a detailed view of the failed or unauthorized logins to the AWS Management Console.
Amazon AWS Login Success Activity	Generates a detailed view of the successful user login or authentication to the AWS Management Console.
Amazon AWS Network Interface Activity	Generates a detailed view of the activity related to the network interface created, deleted, reset, modified, detached, attached, and more.
Amazon AWS User Management Activity	Generates a detailed view of the activities related to the user or group created, deleted, added, removed, and more.
Amazon AWS Bucket-Level Activity	Generates a detailed view of the activities related to the Amazon S3 bucket. This includes CreateBucket, PutBucketPolicy, ListBuckets, and more.
Amazon AWS Policy Activity	Generates a detailed view of the activities related to the policies, that is, AttachUserPolicy, GetPolicy, DetachRolePolicy, CreatePolicy, and more.
Amazon AWS Security Group Activity	Generates a detailed view of the activities related to the security groups, that is, CreateSecurityGroup, AuthorizeSecurityGroupIngress, DeleteSecurityGroup, and more.

4.1.2 Alerts

Name	Description
Amazon AWS: Network Interface Deleted	Triggered if there is any activity related to the VPC network interface deletion.
Amazon AWS: User Deleted	Triggered if a user gets deleted.
AWS CIS Control: AWS Config configuration changed	Triggered when the configuration is changed in the AWS Config. It will help ensure sustained visibility of the configuration items within the AWS account.
AWS CIS Control: AWS Management Console authentication failed	Triggered in the event of any failed or unauthorized login attempt to the AWS Management Console.
AWS CIS Control: Network Access Control Lists (NACL) changed	Triggered in the event any changes to the Network Access Control Lists are detected. Monitoring the changes in the NACLs will help ensure that the AWS resources and services are not unintentionally exposed.
AWS CIS Control: Network gateways changed	Triggered in the event of any changes to the network gateway being detected. Monitoring the changes in the network gateways will ensure all ingress/egress traffic traverses the VPC border via a controlled path.
AWS CIS Control: CloudTrail configuration changed	Triggered in the event of any CloudTrail configuration is changed. Monitoring these changes in the CloudTrail's configuration will help ensure sustained visibility of the activities performed in the AWS account.
AWS CIS Control: Disabling or scheduled deletion of customer created CMKs detected	Triggered in the event of any disabling or scheduled deletion of customer created CMKs. Monitoring these changes in the CloudTrail's configuration will help ensure sustained visibility to activities performed in the AWS account.
AWS CIS Control: IAM policy changed	Triggered in the event of any IAM policy changes. Monitoring these changes in the IAM policies will help ensure authentication and authorization controls remain intact.

Name	Description
AWS CIS Control: Management console signed in without MFA	Triggered in the event of any user signs in without the MFA. Monitoring these single factor console logins will increase the visibility into the accounts that are not protected by the MFA.
AWS CIS Control: Route table changed	Triggered in the event of any Route table changes. Monitoring these changes in the route tables will ensure all the VPC traffic flows through an expected path.
AWS CIS Control: S3 bucket policy changed	Triggered in the event of the S3 bucket policy changes. Monitoring these changes in the S3 bucket policies may reduce the time to detect and correct the permissive policies on sensitive S3 buckets.
AWS CIS Control: Security group changed	Triggered in the event of the S3 bucket policy changes. Monitoring these changes in the security group will ensure that the resources and services are not unintentionally exposed.
AWS CIS Control: Unauthorized API calls detected	This alert is triggered in the event of unauthorized API calls being detected. Monitoring these unauthorized API calls will reveal the application errors and may reduce the time to detect the malicious activity.
AWS CIS Control: Usage of root account detected	Triggered in the event of root account usage detection. Monitoring the root account logins will provide visibility into the use of a fully privileged account and an opportunity to reduce its use.
AWS CIS Control: VPC changes detected	Triggered in the event of the VPC changes. Monitoring these changes in the IAM policies will help ensure authentication and authorization controls remain intact.

4.1.3 Dashboard

Name	Description
Amazon AWS Login Success Activity By the User Type	Displays user attempts to successfully sign into the AWS Management Console.
Amazon AWS Login Failed Activity By Failed Reason	Displays user attempts to unsuccessfully log into the AWS Management Console.
Amazon AWS Policy Activity By the Source IP Address	Displays identity-based policy that denies access to all AWS actions in the account.
Amazon AWS Policy Activity By the User Type	Displays the data about all policy activities within AWS by user agent.
Amazon AWS Login Failed Activity By the User-Agent	Displays the data about AWS console login failure per user agent.
Amazon AWS All Operations Activity By the Event Name	Displays the data of all operation activities of AWS console by event name.
Amazon AWS Login Failed Activity By City	Displays geo location map of login failure.
Amazon AWS User Management Activity by the User Added	Displays the data of new user added into AWS account.
Amazon AWS User Management Activity by the User Deleted	Displays the data of the user deleted from AWS account.
Amazon AWS Policy Activity By the Service Name	Displays the data of all policy related activities by service name in AWS.
Amazon AWS Bucket and Object Activity by the Error Codes	Displays the data about bucket and its related object activity by the error code where error codes define what type of exception thrown.
Amazon AWS Critical Security Activity by the Source IP Address	Displays the data of critical security activity by source IP address.
Amazon AWS VM Instances Activity by the User Type	Displays the data about VM instance activities like create, delete by user type like admin, reader, writer.

4.2 Amazon Kinesis

4.2.1 Flex Reports

Name	Description
Amazon Kinesis - Analytics application modifications	Provides the details of all the actions carried out in relation to the Kinesis analytics service. It gives information about the action name, the time it was initiated, and by whom, among some other details related to the application and the user.
Amazon Kinesis - Data stream activities	Provides the details of all the actions related to the data streams in Kinesis, which includes information like the stream name, the action initiated against it, the timestamp for the action, and the user information for the same.

4.2.2 Alerts

Name	Description
Amazon Kinesis: Data preprocessor deleted	Triggered when a data pre-processing function is removed from the configuration settings of a Kinesis analytics application.
Amazon Kinesis: Application stopped	Triggered when a Kinesis Analytics application is stopped.
Amazon Kinesis: Stream shard count updated	Triggered when the shard count for a particular Kinesis data stream is updated.
Amazon Kinesis: Stream enhanced metrics disabled	Triggered when the enhanced monitoring for a Kinesis stream is disabled.
Amazon Kinesis: SQL I/O configuration deletion	Triggered when an output stream or a reference output data source is deleted.

4.2.3 Dashboard

Name	Description
Amazon Kinesis – Application activity	Displays the about all application related activities of Kinesis.
Amazon Kinesis – Activity by IP Address	Displays the count of activity associated with the kinesis based on IP addresses of the users who are accessing in amazon kinesis.
Amazon Kinesis – User activity	Displays the users interacting with amazon kinesis.
Amazon Kinesis - Data streams activities overview	Displays an overview of the actions related to Kinesis data streams
Amazon Kinesis - Data stream critical activities	Displays the occurrence of sensitive and critical activities related to Kinesis data streams

4.3 Amazon DynamoDB

4.3.1 Flex Reports

Name	Description
Amazon DynamoDB - Database activity	Provides a detailed overview of all the activities related to the DynamoDB service.
Amazon DynamoDB - DAX cluster activity	Provides the details of all the activity related specifically to the DAX cluster in the DynamoDB.

4.3.2 Alerts

Name	Description
Amazon DynamoDB: Table deletion attempt	Triggered when an attempt is made to delete a DynamoDB table in the AWS.
Amazon DynamoDB: Backup deletion attempt	Triggered when an attempt is made to delete a manual on-demand backup.
Amazon DynamoDB: DAX cluster deletion	Triggered when an attempt is made to delete a DAX cluster.

Name	Description
attempt	
Amazon DynamoDB: Parameter group deletion attempt	Triggered when an attempt is made to delete a parameter group of a DAX cluster in the DynamoDB.
Amazon DynamoDB: DAX subnet deletion attempt	Triggered when an attempt is made to delete a subnet in a DAX cluster in the DynamoDB.

4.3.3 Dashboard

Name	Description
Amazon DynamoDB - Database activities	Displays the overall activity occurring in a DynamoDB database in a day.
Amazon DynamoDB - DAX activity	Displays the overall activity related to DynamoDB Accelerators in a day.
Amazon DynamoDB - Activity overview	Displays the activities occurring in DynamoDB based on the IP addresses of the users accessing the instance.
Amazon DynamoDB - User activity	Displays the users interacting with DynamoDB in the AWS instance.

4.4 Amazon EKS

4.4.1 Flex Reports

Name	Description
Amazon EKS - Cluster activity	Provides a detailed overview of the actions that are being triggered in all the AWS EKS instances. It gives information about the action, the time in which the action was triggered, user information related to it, and other cluster-related information

4.4.2 Alerts

Name	Description
Amazon EKS: Addon deletion attempt	Triggered if an attempt to delete an add-on to the EKS cluster is detected.
Amazon EKS: Cluster deletion attempt	Triggered if an attempt to delete an EKS cluster is made.
Amazon EKS: Fargate profile deletion attempt	Triggered if an attempt to delete a Fargate profile is made in an EKS cluster.
Amazon EKS: Nodegroup deletion attempt	Triggered if an attempt is made to delete a node group in an EKS cluster.

4.4.3 Dashboard

Name	Description
Amazon EKS - User activity	Displays the users interacting with EKS in a day.
Amazon EKS - Cluster activity	Displays the overall activity occurring in the EKS clusters**.**
Amazon EKS - Critical activities	Displays the critical activities occurring in the EKS clusters.
Amazon EKS - Activity overview	Displays the activity occurring in Amazon EKS clusters based on IP addresses of the users accessing the instance.

4.5 AWS Elastic Load Balancing (ELB)

4.5.1 Flex Reports

Name	Description
AWS ELB - Elastic load balancer activities	Provides details of the actions triggered by the AWS ELB service. It gives information about the action, the time at which the action was triggered, user information, etc.

4.5.2 Alerts

Name	Description
AWS ELB: Instance deregistered	Generated when an instance is removed from the list of associated instances in a load balancer.
AWS ELB: Load balancer deleted	Generated when a load balancer is purged and removed from the ELB service.
AWS ELB: Load balancer listener deleted	Generated when a listener is deleted from a particular load balancer.
AWS ELB: Load balancer subnet/AZ removed	Generated when a subnet or Availability Zone (AZ) is removed from the configuration settings of a load balancer.
AWS ELB: Target group deleted	Generated when a target group is deleted from the load balancer configuration.

4.5.3 Dashboard

Name	Description
AWS ELB - Load balancer activities	Displays data about the major actions by count, and triggers related to all Elastic Load Balancers for a day.
AWS ELB - Load balancer critical activities	Displays data about the critical activities related to all Elastic Load Balancers that could potentially cause downtime.
AWS ELB - Activity by IP	Displays data about the count of activity associated with the ELB based on the IP addresses of the users who are accessing the instance.
AWS ELB - User activity	Displays data about the users interacting with ELB in a day.

4.6 Amazon EC2

4.6.1 Alerts

Name	Description
Amazon EC2: Security group rules changed to unrestricted	Generated when a change is detected in the security group configuration.
Amazon EC2: Snapshot deletion attempt	Generated when an attempt is made to delete a snapshot for a specified account and region.
Amazon EC2: Sensitive VPC settings modification attempt	Generated when an attempt is made to change the VPC configuration.
Amazon EC2: Instance termination attempt	Generated when an attempt is made to shut down the specified instances.

4.6.2 Reports

Name	Description
Amazon EC2 - VPC changes	Provides details related to the modifications made to the VPC configuration in Amazon EC2.
Amazon EC2 - Security group modifications	Provides information related to the changes made in the security group configuration in Amazon EC2.
Amazon EC2 - Activity overview	Provides information related to all the instance activities in Amazon EC2.

4.6.3 Dashboard

Name	Description
Amazon EC2 - Activity overview	Displays all the information related to the actions related to Amazon EC2.
Amazon EC2 - Critical activity	Displays all the information related to critical configuration changes that may alter the way EC2 works.
Amazon EC2 - VPC configuration	Displays all the information related to VPC configuration

Name	Description
	changes.
Amazon EC2 - Security group changes	Displays all the information related to any changes made to the inbound and outbound settings for the security group.
Amazon EC2 - Instance termination	Displays all the information about the user by whom the EC2 instance has been terminated.
Amazon EC2 - Instance backup delete	Display all the information by whom snapshots, and AMI have been deleted.

4.7 Amazon EC2 Auto Scaling

4.7.1 Flex Reports

Name	Description
Amazon EC2 Auto Scaling - Activity overview	Provides relevant information related to all activities for configuration of instance in Amazon EC2 Auto Scaling.

4.7.2 Dashboard

Name	Description
Amazon EC2 Auto Scaling - Activity overview	Displays user performed any action in amazon autoscaling service.
Amazon EC2 Auto Scaling - Critical activity	Displays major configuration changes or deletions in amazon autoscaling service.
Amazon EC2 Auto Scaling -Instance protection	Displays if a user changes the instance protection configuration on the server.
Amazon EC2 Auto Scaling - Scaling policies	Displays any changes in the autoscaling service.

4.8 Amazon SQS

4.8.1 Flex Reports

Name	Description
Amazon SQS - Activity overview	Provides relevant information related to all activities for configuration changes in SQS service.

4.8.2 Dashboard

Name	Description
Amazon SQS - Activity overview	Displays what actions were performed in the simple queue service.
Amazon SQS – CreateQueue with user details	Displays by whom this SQS CreateQueue was created.
Amazon SQS – SetQueueAttributes with user information	Displays SetQueueAttributes by whom this service was created.

4.9 Amazon SNS

4.9.1 Flex Reports

Name	Description
Amazon SNS - Activity overview	Provides relevant information related to all activities for configuration in SNS service.

4.9.2 Dashboard

Name	Description
Amazon SNS – Activity overview	Displays what actions were performed in SNS service.
Amazon SNS – Subscriptions	Displays subscription and unsubscription activity for SNS.
Amazon SNS – Topic created user details	Displays SNS topic created by which user.

4.10 Amazon S3

4.10.1 Alerts

Name	Description
Amazon S3: Bucket encryption disabled	Generated when an attempt is made to disable the server-side encryption on the S3 bucket.

Name	Description
Amazon S3: Inventory configuration changes detected	Generated when an attempt is made to edit or delete the S3 inventory configuration.
Amazon S3: Bucket ownership settings changed	Generated when an attempt is made to edit or delete the S3 bucket ownership settings.
Amazon S3: Public access block settings changed	Generated when an attempt is made to edit or delete the S3 bucket public access settings.
Amazon S3: Bucket replication changes detected	Generated when an attempt is made to change the bucket replication settings for S3.
Amazon S3: Access points modified	Generated when an attempt is made to modify the access point settings for the S3 bucket.
Amazon S3: New lifecycle policy added	Generated when a new life cycle policy is added for the S3 bucket which has a limited object expiration period and may supersede existing policies.
Amazon S3: Bucket policy changed	Generated based on the request of a privileged user for the activities related to modifications in the S3 bucket policy are detected.

4.10.2 Flex Reports

Name	Description
Amazon S3 - Unauthorized user activities	Provides details of the specific actions carried out related to the S3 service, which failed due to one or more errors related to access management or data misconfiguration.
Amazon S3 - Activity overview	Provides details of all the actions carried out related to S3 service. This alert includes details like the action name, the activity-initiated time, the individual who performed it, and other information related to the application and the user.
Amazon S3 - Bucket level activity	Provides the details of all the actions carried out in the S3 service. This alert includes details like action name, the time it was initiated, the individual who performed it, including other details related to the application and the user.

4.10.3 Dashboard

Name	Description
Amazon S3 - Critical activities	Displays all the details of any critical or sensitive actions carried out related to the S3 service.
Amazon S3 - Configuration changes by IP	Displays all the details of the WRITE actions related to S3 bucket configuration mapped to the IP addresses of the users.
Amazon S3 - Failed API calls	Displays the details of any failed API calls mapped to the user's ARN that occurred due to insufficient or unauthorised access.

4.11 Amazon CloudFormation

4.11.1 Flex Reports

Name	Description
AWS CloudFormation - Activity overview	Provides relevant information related to all activities for stacks in AWS CloudFormation.
AWS CloudFormation - Configuration exploit activities	Provides details related to the manipulation of various resources in AWS CloudFormation.

4.11.2 Alerts

Name	Description
AWS CloudFormation: Stack instance manipulation detected	Generated when CloudFormation configurations have been modified or deleted related to stack instances in the specified accounts or in the specified regions.

4.11.3 Dashboard

Name	Description

AWS CloudFormation – Activity overview	Displays all the actions related to CloudFormation.
AWS CloudFormation – Critical Activity	Displays critical configuration changes that may alter the way CloudFormation works.
AWS CloudFormation – User activity by IP	Displays activity performed by a particular user with a specific IP address.
AWS CloudFormation - Actions by user	Displays the actions performed by the different users.

4.12 AWS Lambda

4.12.1 Flex Reports

Name	Description
AWS Lambda - Activity overview	Provides the details of all the actions and API calls related to the different Lambda functions present in the AWS instance.

4.12.2 Alerts

Name	Description
AWS Lambda: Codesign configuration change	Triggered when changes are detected on the codesign configuration which helps to ensure that only trusted code runs on the Lambda functions.
AWS Lambda: Function configuration change	Triggered when an attempt is made to change or update the configuration of a Lambda function.
AWS Lambda: Layer version permission change	Triggered when an attempt is made to change the codesign configuration of a Lambda function.

4.12.3 Dashboard

Name	Description
AWS Lambda -Activity overview	Displays all actions performed in AWS lambda function.
AWS Lambda -Error details	Displays error details while executing the lambda function.
AWS Lambda -User activity by IP	Displays user activities that are performed in lambda function.

4.13 AWS Secrets Manager

4.13.1 Flex Reports

Name	Description
AWS Secrets Manager - Secrets read-write level activity	Provides all details related to activities concerning reading and updating a secret key or its related settings.
AWS Secrets Manager - Resource policy changes	Provides details of any resource policy changes as part of secrets manager.

4.13.2 Alerts

Name	Description
AWS Secrets Manager: Secrets enumeration detected	Generated when multiple attempts related to read, list, or describe actions for different secrets stored are detected within a very short timeframe.
AWS Secrets Manager: Secrets policy changes detected	Generated when the resource policy related to a secret key has been modified.
AWS Secrets Manager: Secrets restored	Generated when a secret key has been restored which was otherwise scheduled for disposal.
AWS Secrets Manager: Secrets value modifications detected	Generated when the secret key or its related settings have been modified.

4.13.3 Dashboard

Name	Description
AWS Secrets Manager -Activity overview	Displays the top 10 activities occurring, related to secrets manager for a duration of 1 day.
AWS Secrets Manager - Settings and permission changes	Displays the data related to any changes made to the secret settings or permissions related to Secrets Manager within a time span of 1 week.
AWS Secrets Manager - User activity by IP	Displays the details of users interacting with secrets manager (top 10) and their respective public IP address for a duration of 1 day.
AWS Secrets Manager - Error details	Displays the details of top errors by count, mapped to their actions related to secrets manager in a day.

4.14 AWS Key Management Service (KMS)

4.14.1 Flex Reports

Name	Description
AWS KMS - Permission management related activity	Provides details of all actions carried out related to permission management in the AWS KMS.
AWS KMS - Read-write access level activity	Provides details of the actions that were carried out which are related to viewing and updating the configuration settings in KMS.

4.14.2 Alerts

Name	Description
AWS KMS: High privileged key created	Triggered when an attempt is made to create a customer managed key which has sensitive permissions like delete and/or update and/or revoke for all resources as part of KMS.
AWS KMS: Key deletion cancelled	Triggered when an attempt is made to cancel the scheduled deletion of a customer managed key.

AWS KMS: Key rotation disabled	Triggered when the setting for an auto change of the cryptographic material of a key has been disabled as part of KMS**.**
AWS KMS: Short window key deletion scheduled	Triggered when a key deletion is scheduled for a customer managed key in KMS, where the timeframe of the deletion is too short.

4.14.3 Dashboard

Name	Description
AWS KMS - Activity overview	Displays what actions were performed in the AWS KMS service.
AWS KMS - User activity by IP	Displays actions performed by a user with a particular IP in the AWS KMS service.
AWS KMS - Permission management level activity	Displays high-permission activity performed by a user in the AWS KMS service.

4.15 AWS Identity & Access Management (IAM)

4.15.1 Flex Reports

Name	Description
AWS IAM - Activity overview	Provides details of all the activities in AWS IAM.

4.15.2 Alerts

Name	Description
AWS IAM: Add policy and roles	Generated when an attempt is made to attach a group, single policy, or a role for the users to access the AWS services.
AWS IAM: Create new user and group	Generated when an attempt is made to create a new user or new group in the IAM console.
AWS IAM: Delete group and user	Generated when an attempt is made to delete or remove a user or group from the IAM console.
AWS IAM: Delete policy and role	Generated when the AWS service policies or role has been deleted by the user from the IAM console.
AWS IAM: Create and delete access key	Generated when the credentials have been deleted or newly created by the user in the IAM console.

4.15.3 Dashboard

Name	Description
AWS IAM - IAM users created	Displays data about the total number of users in the IAM console.
AWS IAM - Critical activity	Displays data about the deletion of a user or group in the IAM service.
AWS IAM - Activity overview	Displays data about the actions performed in the IAM service.

Name	Description
AWS IAM - User group	Displays data about the total number of user groups in the IAM service.
AWS IAM - User policies	Displays data about the new policies added by the user in an IAM environment.
AWS IAM - User roles list	Displays data about the total roles attached to the IAM user.

4.16 Amazon CloudWatch

4.16.1 Flex Reports

Name	Description
Amazon CloudWatch - Activity overview	Provides details of changes in CloudWatch activities in the Amazon CloudWatch service.

4.16.2 Alerts

Name	Description
Amazon CloudWatch: Attempt to delete or disable alarms	Generated when an attempt is made to delete the specified alarms and disable the actions for the specified alarms.
Amazon CloudWatch: Create export task	Generated when a new export file has been created and sent to the database or S3 storage in the CloudWatch service.
Amazon CloudWatch: Delete log groups	Generated when an attempt is made to delete or remove the log group in CloudWatch
Amazon CloudWatch: Log groups subscription or metrics deleted	Generated when the user has deleted the metric filter and subscription filter from the log group in the CloudWatch service.

4.16.3 Dashboard

Name	Description
Amazon CloudWatch - Critical activities	Displays data about the deletion actions performed in the CloudWatch service.
Amazon CloudWatch - Activity overview	Displays data about the actions performed in the CloudWatch service
Amazon CloudWatch - New filters created	Displays data about who created these filters in the CloudWatch service.
Amazon CloudWatch - New log group created	Displays data about the new log group assigned to the CloudWatch service.

4.17 Amazon Relational Database Service (RDS)

4.17.1 Flex Reports

Name	Description
Amazon RDS - Activity overview	Provides details of all the activities in the Amazon Relational Database Service (RDS).

4.17.2 Alerts

Name	Description
Amazon RDS: Backup deletion attempt	Generated when the deleted database backup is detected in the Amazon Relational Database Service (RDS) service.
Amazon RDS: Backup export attempted	Generated when an attempt is made to export data or copy data to a simple storage service(s3) from the RDS console.
Amazon RDS: Database deletion attempt	Generated when an attempt is made to delete or remove a database from the Amazon Relational Database Service (RDS) console.

4.17.3 Dashboard

Name	Description
Amazon RDS - Activity overview	Displays data about the actions performed in the RDS service.
Amazon RDS - Critical activity	Displays data about the deletion actions performed in the RDS service.
Amazon RDS - Data exported by user	Displays data about the relational database data exported by the user to other storage or database.

4.18 AWS Systems Manager

4.18.1 Flex Reports

Name	Description
AWS Systems Manager - Activity overview	Provides relevant information related to any changes in automation of Systems Manager activities in AWS System Manager service.

4.18.2 Dashboard

Name	Description
AWS Systems Manager – Activity overview	Displays the actions performed in systems manager.
AWS Systems Manager – Critical activity	Displays the deletions in systems manager service.
AWS Systems Manager – Node Management	Displays created association in node management service.
AWS Systems Manager – Task update information	Displays updates in systems manage service.

4.19 AWS CloudTrail

4.19.1 Flex Reports

Name	Description
AWS CloudTrail - Activity overview	Provides related to all the activities in AWS CloudTrail Service.

4.19.2 Alerts

Name	Description
AWS CloudTrail: Datalake configuration changes detected	Triggered if there is any change in the Trail settings or any misconfiguration occurred in the CloudTrail.

4.19.3 Dashboard

Name	Description
AWS CloudTrail - Activity overview	Displays all actions performed in CloudTrail service**.**
AWS CloudTrail - Critical activity	Displays security value configurations that have been deleted.
AWS CloudTrail - Trail configurations changed	Displays any configuration changes in the Trail while monitoring critical activities.

4.20 AWS Certificate Manager

4.20.1 Flex Reports

Name	Description
AWS Certificate Manager - Activity overview	Provides information related to all the activities in AWS Certificate Manager Service.

4.20.2 Dashboard

Name	Description
AWS Certificate Manager - Activity overview	Displays all activities in AWS certificate manager.
AWS Certificate Manager - Critical activity	Displays any deletion or modification action performed in AWS certificate manager configuration.
AWS Certificate Manager - Certificate configurations changed	Displays certificates that needs to be renewed and updated certificate details.
AWS Certificate Manager - Certificate transfer to the port	Displays exports pf a private certificate issued by a private certificate authority (CA) for use anywhere.

4.21 AWS Config

4.21.1 Flex Reports

Name	Description
AWS Config - Activity overview	Provides information related to all the activities in AWS Config Service.

4.21.2 Alerts

Name	Description
AWS Config: Configurations and rule changed	Triggered when a modification is detected in the configuration of the config rule settings.

4.21.3 Dashboard

Name	Description
AWS Config - Activity overview	Displays all activities in AWS config.
AWS Config - Critical activity	Displays any deletion and modification action performed in AWS config.
AWS Config - Recording configuration changed	Displays any modification and changes in configurations.
AWS Config - Remediation configurations setup	Displays any remediate noncompliant resources that are evaluated by AWS Config Rules.

4.22 Amazon CloudFront

4.22.1 Flex Reports

Name	Description
Amazon CloudFront – Activity overview	Provides information related to all console activities concerning the CloudFront service.

4.22.2 Alerts

Name	Description
Amazon CloudFront: Configuration manipulation detected	Triggered whenever distributions configuration is deleted or maliciously modified.

4.22.3 Dashboard

Name	Description
Amazon CloudFront – Critical activities by action	Displays information on actions that can disrupt the CloudFront configuration.
Amazon CloudFront – Configuration changes	Displays any modification in CloudFront configuration.
Amazon CloudFront – Origin access control modifications	Displays information on origin access creation and modification in CloudFront distributions.

4.23 Amazon Cognito

4.23.1 Flex Reports

Name	Description
Amazon Cognito - Manipulation in authorized api detected	Provides details of all authorizer manipulation activities that have been performed in the amazon Cognito console.
Amazon Cognito - Identity fedration and userpool configurations modified or deleted	Provides details of all configurations related to Cognito that were deleted or changed.

4.23.2 Alerts

Name	Description
Amazon Cognito: Unauthorized activity detected	Triggered whenever a configuration related to Cognito is deleted or changed.

4.23.3 Dashboards

Name	Description
Amazon Cognito - Admin create a new user internally	Displays information about users created by administrators in amazon Cognito.
Amazon Cognito - Configuration modification deleted	Displays information about configuration modification in userpool or federated identities.
Amazon Cognito - Userpool misconfigurations detected	Displays information while creating userpools that are misconfigured.
Amazon Cognito - Enabled and disabled users in userpool	Displays details on all users enabled and disabled by the administrator in the user pool.
Amazon Cognito - Federated identities and userpools configuration deleted	Displays details about configurations deleted from the Amazon Cognito Service.

4.23.4 Saved Search

Name	Description
Amazon Cognito: Activity overview	Provides details of all user management activities been performed in amazon cognito console.
Amazon Cognito: Configurations modification and deletions	Provides information when any modification or deletion of configuration occurs.
Amazon Cognito: Federated identities and userpool API information	Provides information about API authorization.

About Netsurion

Netsurion® delivers an adaptive managed security solution that integrates our Open XDR platform with your existing security investments and technology stack, easily scaling to fit your business needs. Netsurion's 24x7 SOC operates as your trusted cybersecurity partner, working closely with your IT team to strengthen your cybersecurity posture. Our solution delivers managed threat protection so you can confidently focus on your core business.

Headquartered in Ft. Lauderdale, FL with a global team of security analysts and engineers, Netsurion is a leader in Managed Detection & Response (MXDR). Learn more at www.netsurion.com.

Contact Us

Corporate Headquarters

Netsurion
Trade Centre South
100 W. Cypress Creek Rd
Suite 530
Fort Lauderdale, FL 33309

Contact Numbers

Use the form to submit your technical support tickets. Or reach us directly at 1 (877) 333-1433

Managed XDR Enterprise Customers	SOC@Netsurion.com
Managed XDR Enterprise MSPs	SOC-MSP@Netsurion.com
Managed XDR Essentials	Essentials@Netsurion.com
Software-Only Customers	Software-Support@Netsurion.com

https://www.netsurion.com/support