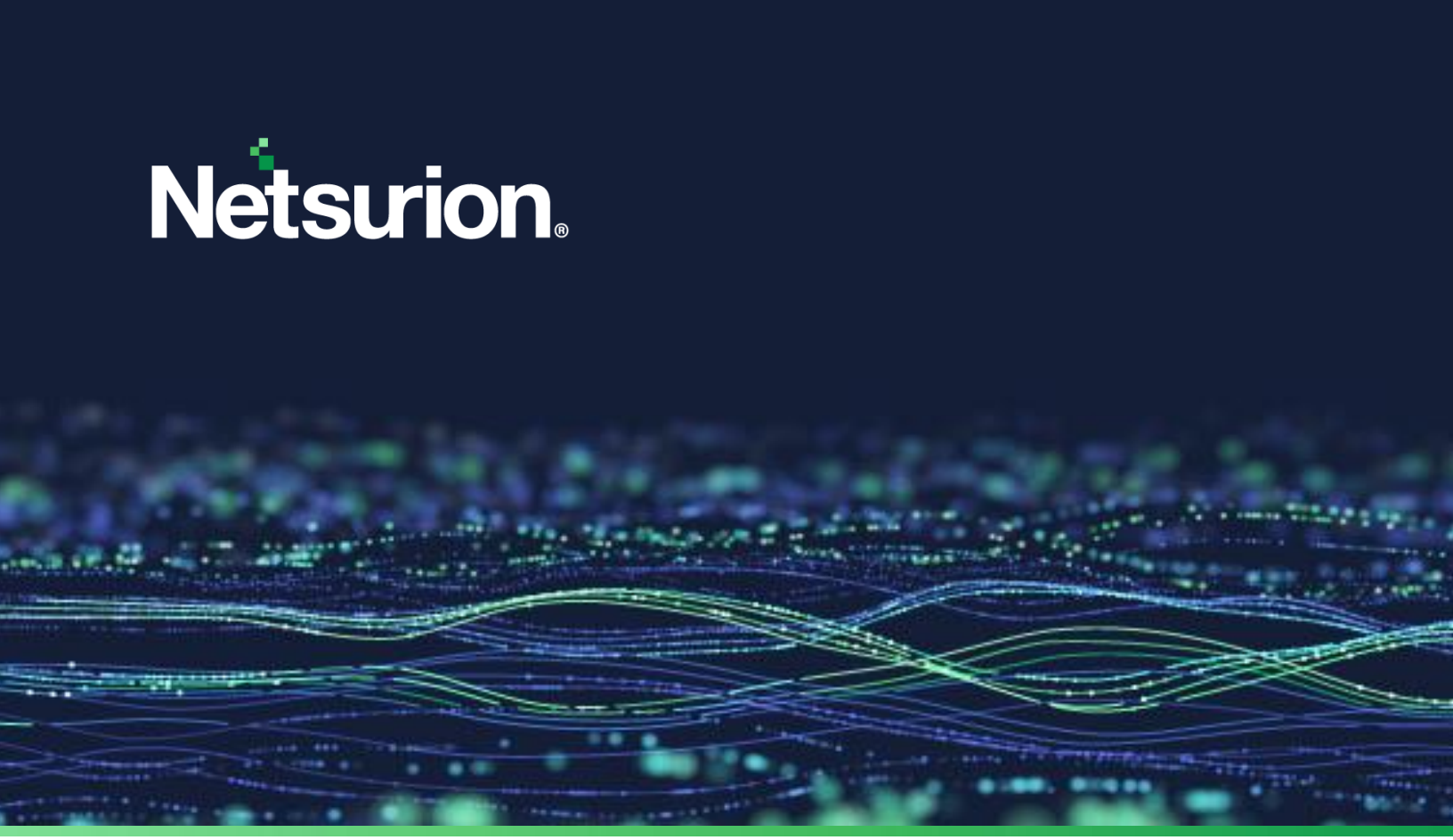


Integration Guide

Integrate AWS Security Hub with Netsurion Open XDR

Publication Date

September 14, 2023

Abstract

This guide provides instructions to configure and integrate AWS Security Hub with Netsurion Open XDR to retrieve its logs and forward them to Netsurion Open XDR.

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 version 9.3 or later and AWS Services.

Audience

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

Table of Contents

1 Overview

AWS Security Hub is a cloud security posture service that automates security checks and brings security alerts into a central location.

Netsurion Open XDR manages logs retrieved from AWS Security Hub. The alerts, reports, dashboards, and saved searches in Netsurion Open XDR are enhanced by capturing important and critical activities in AWS Security Hub.

2 Prerequisites

- Must enable AWS CloudTrail to forward logs to Netsurion Open XDR.
- Ensure Root level access to the AWS console.
- Netsurion Open XDR VCP port must be NAT (Network Address Translation) with the public IP address.

3 System Extraction

Perform the following process for system extraction.

1. In **Netsurion Open XDR console**, 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. Extract the system name using the below regex:

   Fill in the following details, (for CloudTrail logs)

   Regular expression: (?is)Organisation:(?P<Tenant>[^,]+).*?"eventSource":"(?P<Computer>[^"]+)

   Token Name: Computer~Tenant

   Regular expression: (?is) Organisation:(?P<Tenant>[^,]+).*?"source":"(?P<Computer>[^"]+)

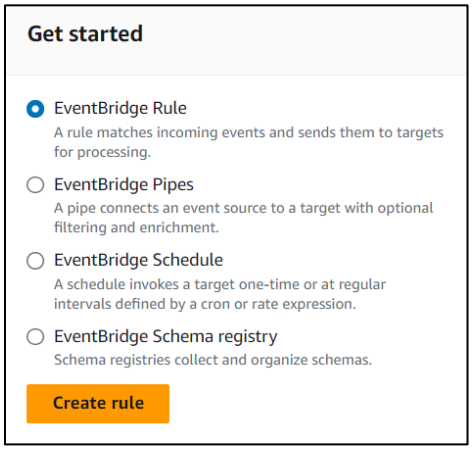
   Token Name: Computer~Tenant

4. After providing the regex details, click the **Update** button to save the extraction logic details.

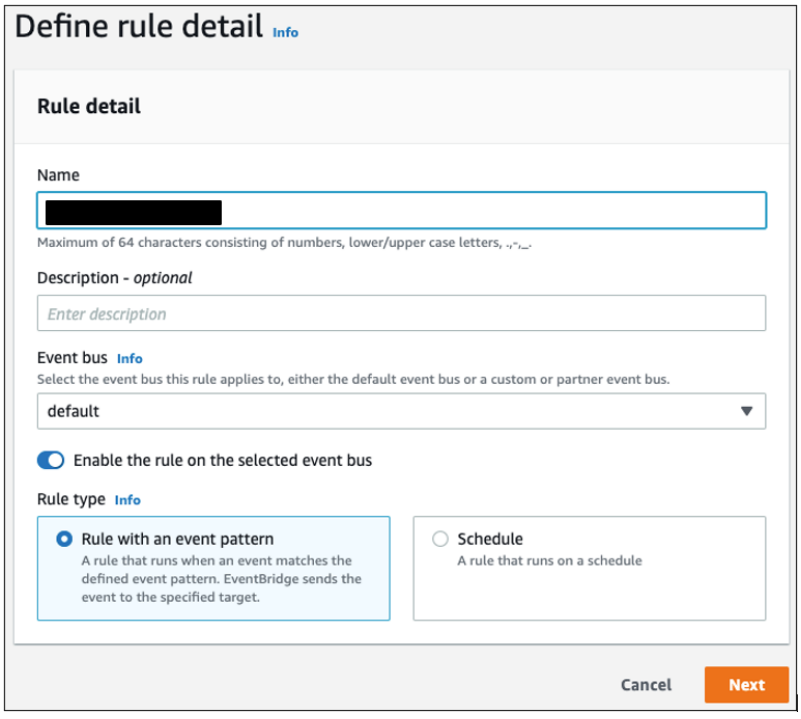
4 Integrating AWS Security Hub with Netsurion Open XDR

Perform the following procedure to integrate AWS Security hub with Netsurion Open XDR.

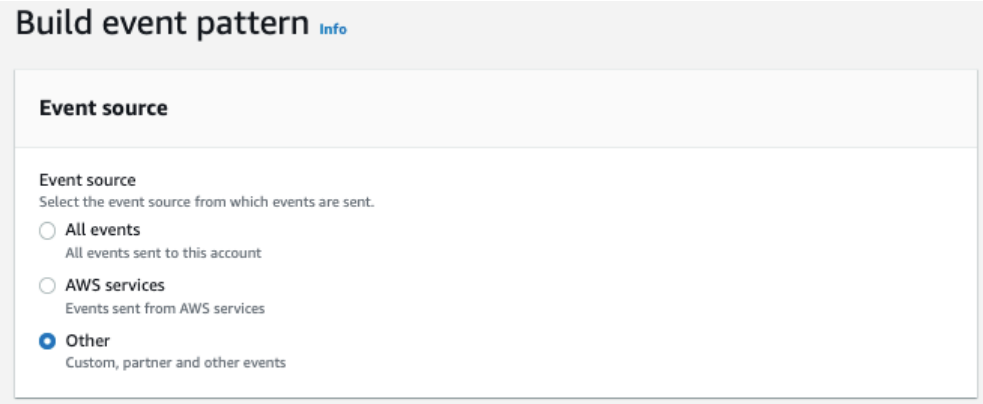
1. Log in to the AWS Management console and go to AWS Event Bridge.
2. In the Event Bridge interface, go to **EventBridge Rule** to create a rule.



3. In **Define rule detail**, provide the following details, and click **Next**.
   - **Name**: Provide a **Name** for the rule. For example, Netsurion-rule.
   - **Event bus**: Specify the **Event Bus** as default.
   - Toggle **Enable the rule on the selected event bus** to active**.**
   - **Rule type**: Select the **Rule type** as **Rule with an event pattern.**

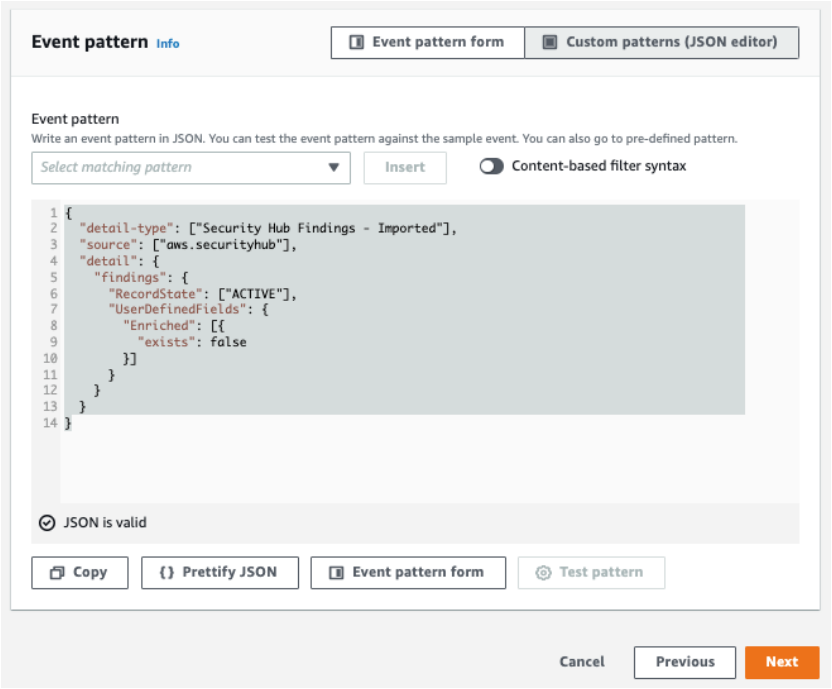


4. In the **Build event pattern** interface, for **Event source**, choose the **Other** option and skip the Sample Event section.



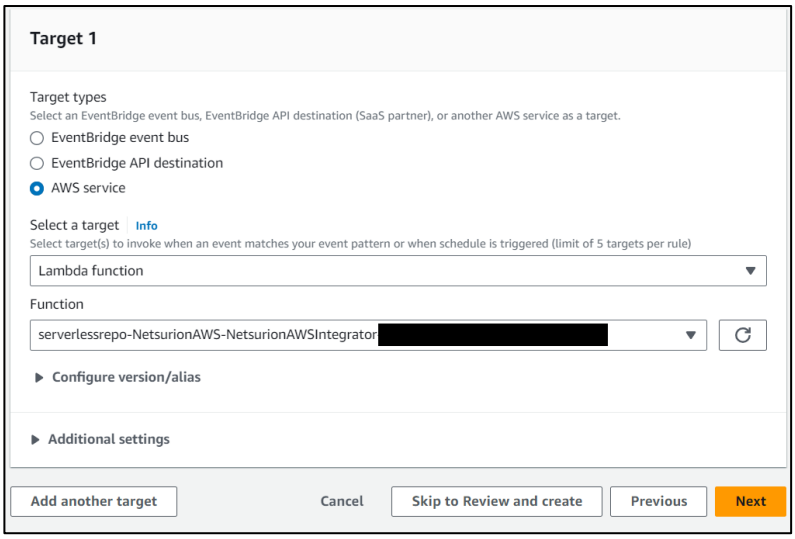
5. In the **Event pattern** interface, choose the **Custom patterns (JSON Editor)** option and paste the following. JSON script, and then click **Next**.

```
{
	"detail-type": ["Security Hub Findings - Imported"],
	"source": ["aws.securityhub"],
	"detail": {
		"findings": {
			"RecordState": ["ACTIVE"],
			"UserDefinedFields": {
					"Enriched": [{
						"exists": false
						}]
					}
				}
		}
}
```



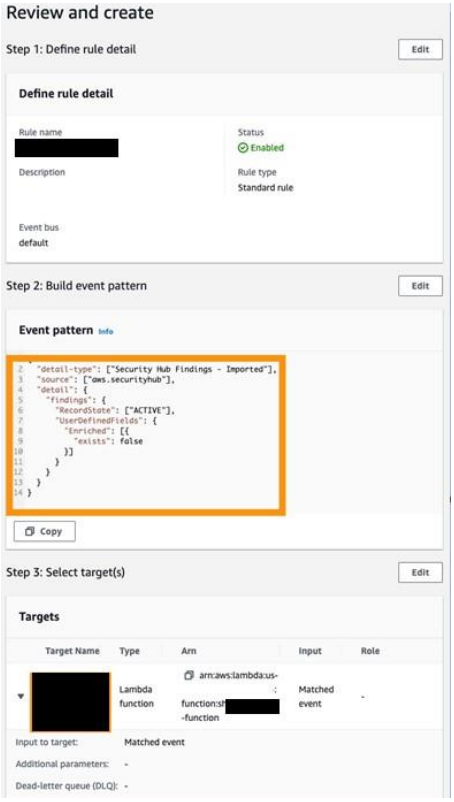
6. In the **Target** interface, provide the following details and click **Next**.

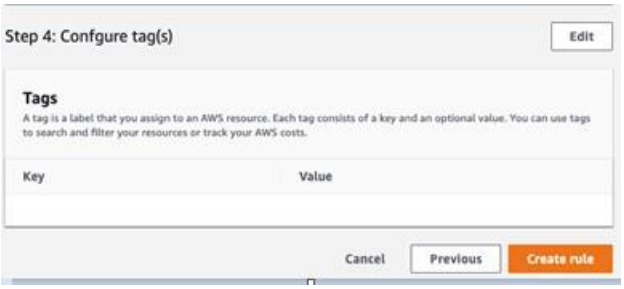
   - **Target types**: Choose the **AWS service** option**.**
   - **Select a target**: Select **Lambda function** from the drop-down list.
   - Function: Choose the name of your function for **AWSNetsurionIntegrator** from the drop-down list.



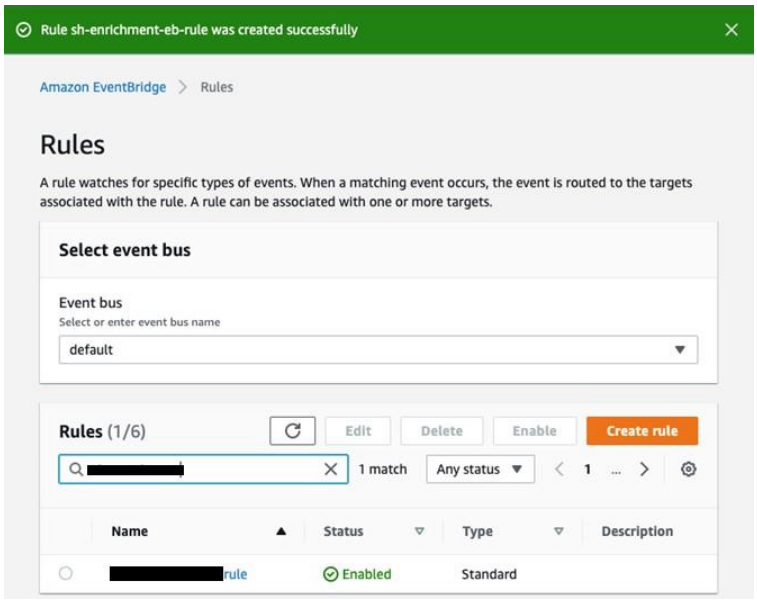
Skip the **Configure tags** (as it is optional) interface.

7. In the **Review and create** interface, validate all the configuration, and click **Create rule.**





8. You will see the rule successfully created and listed in the rules list page.



Note:

After enabling the rule on Event Bridge, it is necessary to integrate CloudTrail with Netsurion Open XDR using the NetsurionAWSIntegrator lambda function. Refer to the How To Configure AWS CloudTrail guide to configure AWS CloudTrail to forward logs to Netsurion Open XDR.

5 Data Source Integration (DSI) in Netsurion Open XDR

After the logs are received in Netsurion Open XDR, configure the DSI in the Netsurion Open XDR.

The DSI package contains the following files for AWS Security Hub.

- Categories_AWS Security Hub.iscat
- Reports_ AWS Security Hub.etcrx
- KO_ AWS Security Hub.etko
- Dashboards_ AWS Security Hub.etwd
- Alerts_ AWS Security Hub.isalt

5.1 Alerts

Name	Description
AWS Security Hub: Critical findings	Generated whenever critical and high severity findings are captured by AWS Security Hub.
AWS Security Hub: Configuration manipulation detected	Generated whenever sensitive configuration(s) related to AWS Security Hub are changed.

5.2 Reports

Name	Description
AWS Security Hub - All findings	Provides information about all security findings generated by AWS Security Hub.
AWS Security Hub - Activity overview	Provides details about all console level activities related to AWS Security Hub.

5.3 Dashboards

Name	Description
AWS Security Hub - Critical severity findings	Displays all critical findings based on its name.
AWS Security Hub - High severity findings	Displays all high severity findings based on its name.
AWS Security Hub - Medium severity findings	Displays all medium severity findings based on its name.
AWS Security Hub - Configuration modification detected	Displays information about configuration modifications based on actions.
AWS Security Hub - Resources configured	Displays the integration of a partner products or AWS services.

5.4 Saved Searches

Name	Description
AWS Security Hub - All findings	Provides information about all security findings generated by AWS Security Hub.
AWS Security Hub - Activity overview	Provides details about all console level activities related to AWS Security Hub.

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