OpenSearch SIEM Deployment guide

Status	IN PROGRESS
Owner	@ Quentin Hatcher
Contributors	~~@Bryan Diaz~~ ~~@ Rod Castillo~~

On this page	• OpenSearch SIEM deployment steps
	  • Setting Up the AWS CDK Execution Environment
	  • Setting Environment Variables
	  • Creating an AWS Lambda Deployment Package
	  • Setting Up the Environment for AWS Cloud Development Kit (AWS CDK)
	  • Setting Installation Options with the AWS CDK
	  • Running the AWS CDK
	  • Configuring OpenSearch Dashboards
	  • Loading logs into OpenSearch Service
	• Non AWS Native Log Sources
	  • Okta Log Ingestion
	  • Add an AWS EventBridge log stream
	  • Configure the Amazon EventBridge log stream in the AWS console
	  • ForcePoint (CASB) Log Ingestion
	  • Register a user in AWS and retrieve credentials
	  • Implementation - Traditional
	  • Setup the environment - Traditional
	  • Setup CASB AWS Security Hub Services - Traditional
	• Source files

OpenSearch SIEM deployment steps

Steps listed below use the AWS CDK to configure and deploy the AWS OpenSearch SIEM solution. Multiple configuration options are listed below, read carefully.

Step	Description

1.	**Setting Up the AWS CDK Execution Environment**
	
	• Deploy an Amazon Elastic Compute Cloud (Amazon EC2) instance that runs Amazon Linux 2 (x86)
	  • The EC2 instance must be deployed on the account you intend to deploy the AWS OpenSearch SIEM solution, this is account specific and does not deploy resources to other accounts.
	• Create a role with Admin permissions in AWS Identity and Access Management (IAM) and attach it to the Amazon EC2 instance
	• Log in to the shell; install the development tools, Python 3.8 and development files, git, jq and tar; and get the source code from GitHub
	
	`sudo yum groups mark install -y "Development Tools"`
	`sudo yum install -y amazon-linux-extras`
	`sudo amazon-linux-extras enable python3.8`
	`sudo yum install -y python38 python38-devel git jq tar`
	`sudo update-alternatives --install /usr/bin/python3 python3 /usr /bin/python3.8 1`
	`git clone https://github.com/aws-samples/siem-on-amazon-opensearch-service.git`

2.

Setting Environment Variables

```
export CDK_DEFAULT_ACCOUNT=<AWS_ACCOUNT> # your AWS account
export AWS_DEFAULT_REGION=<AWS_REGION> # region where the
distributable is deployed
```

3.

Creating an AWS Lambda Deployment Package

The AWS Lambda functions that you use in SIEM on OpenSearch Service make use of third party libraries. The script below will download these libraries and create a deployment package locally. Ensure that you have Python 3 installed.

```
cd siem-on-amazon-opensearch-service/deployment/cdk-solution-
helper/
chmod +x ./step1-build-lambda-pkg.sh && ./step1-build-lambda-pkg.
sh
```

4.

Setting Up the Environment for AWS Cloud Development Kit (AWS CDK)

The script below will install a variety of software in user mode which is needed to run the AWS CDK.

```
chmod +x ./step2-setup-cdk-env.sh && ./step2-setup-cdk-env.sh
source ~/.bashrc
```

Software to be installed:

- Node Version Manager (nvm)
- Node.js
- AWS SDK for Python (Boto3)
- AWS Cloud Development Kit (AWS CDK)

5.

Setting Installation Options with the AWS CDK

From the root directory of the repository, navigate to the directory containing the AWS CDK code to prepare for configuration of options and installation

```
cd ../../source/cdk/
source .venv/bin/activate
cdk bootstrap
```

If the execution fails with an error, verify that your Amazon EC2 instance has the appropriate permissions role assigned.

6.

Deploying SIEM on OpenSearch Service in an Amazon VPC

If you are deploying SIEM on OpenSearch Service in an Amazon VPC, copy and edit the AWS CDK sample file for Amazon VPC:

```
cp cdk.json.vpc.sample cdk.json
```

Edit cdk.json.

Parameters and descriptions for Amazon VPC:

Parameter	Description
vpc_typ	If you create a new Amazon VPC, enter [**new**], and if you use an existing Amazon VPC, enter [**import**]. The parameter to edit is new_vpc_xxxx for a new VPC and imported_vpc_xxxx for an existing VPC
imported_vpc_id	Enter the ID of the Amazon VPC where you want to deploy SIEM on OpenSearch Service
imported_vpc_subnets	Enter three or more "VPC subnet IDs" in list form
imported_vpc_subnetX	(Deprecated) Enter three parameters, namely [VPC subnet ID], [Availability Zone], and [route table ID]
new_vpc_nw_cidr_block	Enter the IP and CIDR block for the new Amazon VPC that you create. The format is the IP address/the number of subnet masks. Example) 192.0.2.0/24
new_vpc_subnet_cidr_mask	Subnet CIDR block. For scalability, we recommend /27 or larger.

7.

Other common configurations

You can change the following parameters as common configurations. No modification is required if there are no changes.

Parameter	Initial value	Description
aes_domain_name	aes-siem	Changes the SIEM on OpenSearch Service domain
s3_bucket_name	Changes the S3 bucket name from the initial value	
log	aes-siem-*[AWS Account ID]*-log	S3 bucket name for logs
snapshot	aes-siem-*[AWS Account ID]*-snapshot	S3 bucket name for snapshots
geo	aes-siem-*[AWS Account ID]*-geo	S3 bucket name for GeoIP downloads
kms_cmk_alias	aes-siem-key	Changes the alias name of the AWS KMS customer-managed key
organizations	Automatically generates an S3 bucket policy by using the AWS Organizations information entered here. No input is required if you manage another S3 bucket by yourself	
.org_id	Organizations ID. Example) o-12345678	
.management_id	The AWS account ID that is the administrator account in Organizations	
.member_ids	The AWS account IDs that are member accounts in Organizations, separated by commas	
no_organizations	Automatically generates a bucket policy for accounts that are not managed by Organizations, by using the account information entered here. No input is required if you manage another S3 bucket by yourself	
.aws_accounts	Enter comma-separated AWS account IDs that are not managed by Oarganizations	
additional_s3_buckets	Enumerates S3 bucket names separated by commas	
additional_kms_cmks	Enumerates the ARNs of AWS KMS customer-managed keys, separated by commas	

8. Finally, validate the JSON file. If JSON is displayed after execution and there is no error, the syntax of the JSON file is fine.

```
cdk context  --j
```

9. **Running the AWS CDK**

Deploy the AWS CDK:

```
cdk deploy --no-rollback
```

10. You can specify the same parameters as for the CloudFormation template. The parameters can also be changed from the CloudFormation console after deployment with the CDK command.

Parameter	Description
AllowedSourceIpAddresses	The IP addresses that you want to allow access from when deploying SIEM on OpenSearch Service outside of your Amazon VPC. Multiple addresses are space-separated
SnsEmail	Email address. Alerts detected by SIEM on OpenSearch Service will be sent to this email address via SNS
ReservedConcurrency	The maximum number of concurrency executions for es-loader. The default value is 10. Increase this value if you see delays in loading logs or if you see constant throttling occur even though there are no errors
GeoLite2LicenseKey	Maxmind license key. It will add country information to each IP address
OtxApiKey	If you wolud like to download IoC from AlienVault OTX, please enter OTX API Key.
EnableTor	Would you like to download Tor IoC? Value is "true" or "false" (default)
EnableAbuseCh	Would you like to download IoC from abuse.ch? Value is "true" or "false" (default)
IocDownloadInterval	Specify interval in minute to download IoC, default is 720 miniutes

Syntax) --parameters Option1=Parameter1 --parameters Option2=Parameter2 If you have more than one parameter, repeat --parameters

Example of deployment with parameters)

```
cdk deploy --no-rollback \
    --parameters AllowedSourceIpAddresses="10.0.0.0/8
192.168.0.1" \
    --parameters GeoLite2LicenseKey=xxxxxxxxxxxxxxxx
```

The deployment takes about 30 minutes. When this is done, proceed to “11. Configuring OpenSearch Dashboards.”

11. **Configuring OpenSearch Dashboards**

It will take about 30 mins for the deployment of SIEM on OpenSearch Service to complete. You can then continue to configure OpenSearch Dashboards.

1. Navigate to the AWS CloudFormation console, choose the stack that you've just created, and then choose "Outputs" from the tab menu at the top right. You can find your username, password, and URL for OpenSearch Dashboards. Log into OpenSearch Dashboards using the credentials.
2. When you login for the first time, [Select your tenant] is displayed. Select [**Global**]. You can use the prepared dashboard etc.
3. You can also select [**Private**] instead of [Global] in [Select your tenant] and customize configuration and dashboard etc. for each user. The following is the procedure for each user. If you select Global, you do not need to set it.
    a. To import OpenSearch Dashboards' configuration files such as dashboard, download saved_objects.zip. Then unzip the file.
    b. Navigate to the OpenSearch Dashboards console. Click on "Stack Management" in the left pane, then choose "Saved Objects" --> "Import" --> "Import". Choose dashboard.ndjson which is contained in the unzipped folder. Then log out and log in again so that the imported configurations take effect.

12. **Loading logs into OpenSearch Service**

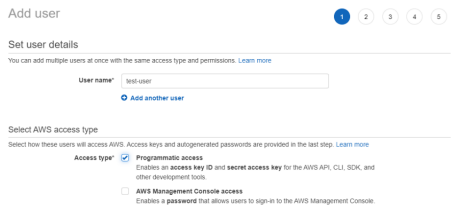
All you need to do to load logs into SIEM on OpenSearch Service is PUT logs into the S3 Bucket named **aes-siem-<YOUR_AWS_ACCOUNT>-log**. Then the logs will be automatically loaded into SIEM on OpenSearch Service. See this for detailed instructions on how to output AWS services logs to the S3 bucket.

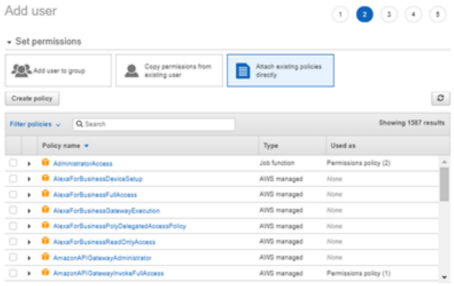
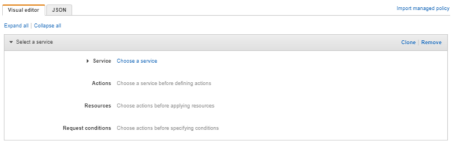
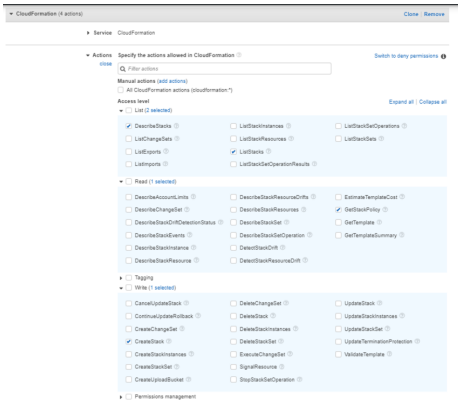
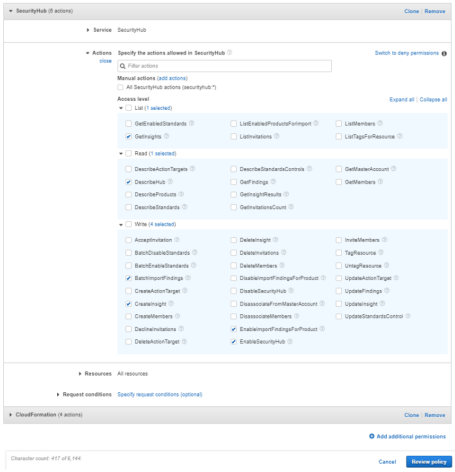
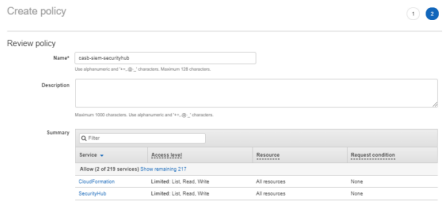
Non AWS Native Log Sources

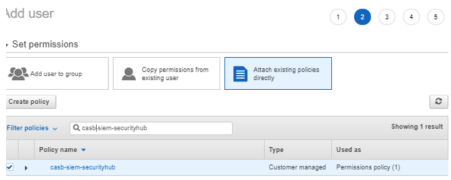
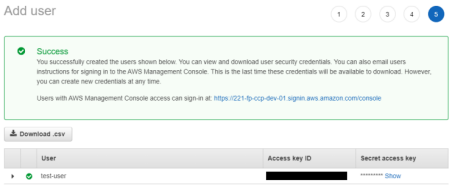
Okta Log Ingestion

Step	Description
	Add an AWS EventBridge log stream
1.	In the Admin Console, go to **Reports** > **Log Streaming**. This page shows all of the log stream targets available in your org.
2.	Click **Add Log Stream** to start the log stream wizard.
3.	Select **AWS EventBridge** from the catalog. Click **Next**.
4.	Fill in the configuration details for your AWS EventBridge log stream: • **Name**: Provide a unique name for this log stream in Okta. • **AWS Event Source Name**: Provide a unique name without any special characters or spaces to identify this event source in Amazon EventBridge. • **AWS account ID**: The 12 digit account identifier provided by AWS. • **AWS region**: Select the AWS region closest to your EventBridge target. Closer geographic regions mean faster stream connection. To send the same events to multiple regions, you must create multiple log stream targets.
5.	Click **Save**. You receive a confirmation message. The log stream that you just added appears on the Log Streaming page with its status as **Active**.
	Configure the Amazon EventBridge log stream in the AWS console
6.	You must configure your Amazon EventBridge log stream to accept partner events from Okta. In the AWS console, go to Amazon EventBridge.
7.	Select **Partner event sources** from the Integration section of the navigation panel.
8.	If you successfully activated an AWS EventBridge log stream in Okta, you should see a partner event source in the Pending status with a name following the format: `aws.partner/okta.com/yourOktaSubdomain/yourAWSEventSourceName`
9.	Select the log stream and click **Associate with an event bus**.
10.	Select the required permissions for the log stream on the Associate with event bus page. Click **Associate**. Your partner event source is active and events are available in the corresponding event bus.
11.	Select **Rules** from the Events section of the navigation panel. For more information, see AWS - Creating a rule that matches SaaS partner events. To ensure that AWS EventBridge receives all logging events from Okta when you create a rule, select **Pre-defined pattern by service** for the **Event matching pattern** and then select **All Events** as your **Service provider**.
12.	Perform an action in Okta to generate an event, such as signing in/out of the Admin Console. Refer to your AWS documentation to find the log containing the corresponding events within the event bus.

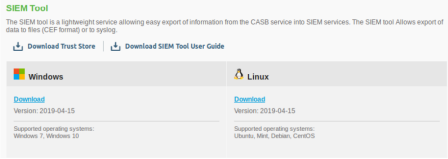
ForcePoint (CASB) Log Ingestion

Step	Description	Screenshots
	Register a user in AWS and retrieve credentials To submit logs into AWS Security Hub, retrieve and configure AWS settings as described in this process. If AWS Security Hub is not already active, it will be activated automatically by the installation script.	
1.	1. Log in to the AWS management console 2. Click on your username in the top right corner and select My Account, look for Account Id at the top of the page and store the ID in a safe location as it is required for configuring the service in the next steps of this guide 3. Navigate to the AWS management console 4. Search for IAM and open it 5. Open the Users section and click Add User in the top left 6. Enter a name for the new user and select Programmatic access in the Access type section	

2.	Select Attach existing policies directly and click Create policy	
3.	On the new page that opens select Choose a service	
4.	Type “CloudFormation” and tick the minimum necessary permissions needed for our setup: ListStacks, DescribeStacks, GetStackPolicy, CreateStack. Under Resources tick All resources.	
5.	Click Add additional permissions and select Choose a service Type “SecurityHub” and tick: GetInsights, DescribeHub, EnableSecurityHub, BatchImportFindings, CreateInsight, EnableImportFindingsForProduct . Select All resources for Resources.	
6.	Click Review policy Type a policy name in the Name field and then click Create policy	

7.	Back on the Add user page, click the refresh icon and type the new policy name	
8.	Select the policy and click Next Add tags if required in your organization (tags are not required by this integration) Review the details and then click Create user In the next screen you will be presented with your new user along with your Access key ID and Secret access key, save these or the CSV file in a secure location, this is the only time the Secret access key will be available	
9.	**Implementation - Traditional** The solution for the traditional implementation described in this chapter below requires the following files available at this link: https://frcpnt.com/casb-securityhub-latest fp-casb-exporter-aws-v1.tar.gz The file fp-casb-exporter-aws-v1.tar.gz contains all files necessary to setup and run Forcepoint CASB connector to AWS Security Hub which automatically monitor, process and upload logs to AWS. We suggest deploying this service on a clean CentOS 7.x or Ubuntu 18.04 machine with at least 2GB RAM, 20GB free storage and the system needs to be 64 bit, the instructions provided in this document are based on a machine running Ubuntu 18.04 which will be referenced as Log Proxy in the rest of this document.	

10.	**Setup the environment - Traditional**
	
	Log into the Log Proxy machine and unpack the integration package using the command
	
	`tar -zxvf ./fp-casb-exporter-aws-v1.tar.gz`
	
	Move into the fp-casb-exporter-aws folder and run the following commands to install the necessary dependencies needed by our integration package, run with a user that has an administrative privileges.
	
	`cd ./deploy`
	
	`./install.sh`	

11.	Setup CASB SIEM Tool – Traditional Obtain the Linux version of the SIEM tool from Forcepoint CASB management portal: go to Settings > Tools and Agents (last icon on the left sidebar) > SIEM Tool and download both the Linux version and the TrustStore file into the Log Proxy machine	
12.	Place both files in the same location Extract the provided SIEM tool archive using the command `unzip ./SIEM-Tool-Linux-*.zip`	
13.	Credentials used by the CASB SIEM Tool are generated using the TrustStore file, this only needs to be done one time. Run the following command to generate a credentials file that will be used by the CASB SIEM Tool to export data from CASB. Change the red parts with the actual credentials of a CASB account with administrator access, and enter a file name for the credentials file that will be generated: `./SIEMClient.sh --set.credentials --username<user> --password<password> --credentials.file<file>`	

14.	Create a directory where the SIEM tool will store the exported logs `mkdir casb-siem-files && sudo chmod ugo+rw $_`	
15.	**Setup CASB AWS Security Hub Services - Traditional** Edit the file cfg.json with all settings as required, more information about the possible values can be found in the Appendix section of this document. We recommend reviewing a selection of CASB logs offline, in order to identify the values which better identify the events that are to be exported into AWS Security Hub.	

16.	Move to the fp-casb-exporter-aws/deploy folder and edit casb-siem-setup.sh with all settings required, more information about the possible values can be found in the Appendix section of this document	**casb-siem-setup.sh**
		
		`_SIEM_HOME_DIR=""`
		`_CREDENTIALS_FILE=""`
		`_HOST="my.skyfence.com"`
		`_PORT=443`
		`_OUTPUT_DIR=""`
		`_TRUST_STORE_PATH=""`

17.	Once all files are edited, install CASB AWS Security Hub Services using the commands below, run with a user that has an administrative privileges.
	
	`cd ./deploy`
	
	`./setup.sh`	

18.	Depending on the number of logs exported from CASB, logs matching all filters will be visible after a few minutes into AWS Security Hub. AWS Security Hub does not store events older than 90 days, so only CASB logs within this timeframe will be processed and sent into AWS Security Hub by our service. Systemd processes are configured to start CASB AWS Security Hub Services at boot of the log proxy machine.	

Source files

Okta Log ingestion - https://help.okta.com/en-us/Content/Topics/Reports/log-streaming/add-aws-eb-log-stream.htm

ForcePoint CASB Log ingestion - https://www.websense.com/content/support/library/bus_dev_integrations/casb/Forcepoint CASB and AWS Security Hub - Integration Guide.pdf