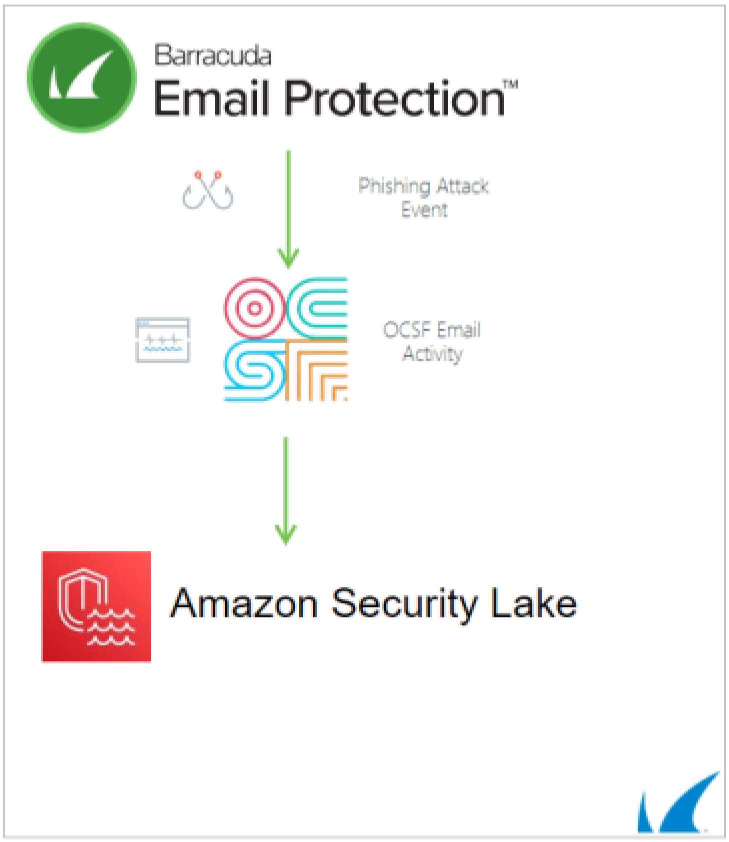
Integrate Amazon Security Lake with Email Protection

https://campus.barracuda.com/doc/98214513/

Note that Amazon Security Lake integration currently only supports receiving threat data (email detections) by Barracuda Impersonation Protection. Additional Barracuda Networks data sources will be supported in the future.

Amazon (AWS) Security Lake centralizes security data from cloud, on-premises, and custom sources into a purpose-built data lake stored in customer accounts. Barracuda Email Protection supports sending events to Amazon Security Lake when new phishing email attacks are detected. Barracuda Email Protection customers can receive these events within their own Amazon Security Lake instance.



Complete the following sections to set up Amazon Security Lake with Barracuda Email Protection.

1. Set Up Amazon Security Lake

Amazon Security Lake must first be enabled in your AWS account. See the Amazon Security Lake User Guide for help.

2. Add Barracuda Email Protection Products as an External Data Source

To start receiving data from a Barracuda Email Protection product in your Amazon Security Lake instance, follow the instructions provided by AWS to add Barracuda Networks as a custom source here: https://docs.aws.amazon.com/security-lake/latest/userguide/custom-sources.html#adding-custom-sources.

You will need to provide the following information:

- The event class that will be sent – **Email Activity**
- The AWS account with permission to write data – AccountID of the custom source

3. Set Up Barracuda Email Protection Products

Once you have added Barracuda Email Protection products as an external data source within your AWS account, provide Barracuda Networks with the following information:

- The ARN (Amazon Resource Name) for the assume-role Barracuda Networks will use to deliver data into your Amazon Security Lake S3 bucket.
    - Run the following command to find the ARN:

      ```
      aws iam list-roles --query "Roles[?
      contains(RoleName,'AmazonSecurityLake-Provider')].Arn"
      ```

- The Amazon Security Lake S3 bucket name and path Barracuda Networks will be delivering data to.
    - This information can be found on the **Custom sources** page.

Contact Barracuda Networks Technical Support

The Amazon Security Lake integration with Email Protection products is currently available as a beta release for select customers. If you would like to enable this integration for your account or require setup assistance, contact Barracuda Networks Technical Support.

Note the information from the above section titled **Set Up Barracuda Email Protection Products** when contacting Barracuda Networks Technical Support.

Integration Data Mapping

The following table maps Open Cybersecurity Schema Framework (OCSF) fields for log data coming from Barracuda Networks.

Barracuda Networks Syslog Field	OCSF Field	Notes
	activity_id	Always a value of 3, which means "A scan was performed."
	category_uid	Always a value of 4, which means "Network Activity"
	class_uid	Always a value of 4009, which means "Email Activity"
timestamp	time	The time of the event
	direction_id	The direction of the email relative to the scanning host or organization
	email.from	The email header **From** values as defined by RFC 5322
	email.to	The email header **To** values as defined by RFC 5322
	email.subject	The email header **Subject** values as defined by RF 5322
	metadata.version	The version of the event class
	metadata.product.vendor_name	The name of the vendor (Barracuda Networks)
	metadata.product.name	The name of the Barracuda Networks product that made the security finding
	severity_id	Always a value of 0
	type_uid	Always a value of 400903: Email Activity: Scan

Maintenance of Components

Barracuda Networks hosts all components associated with the Amazon Security Lake integration. Customer AWS accounts do not require any maintenance.

Figures