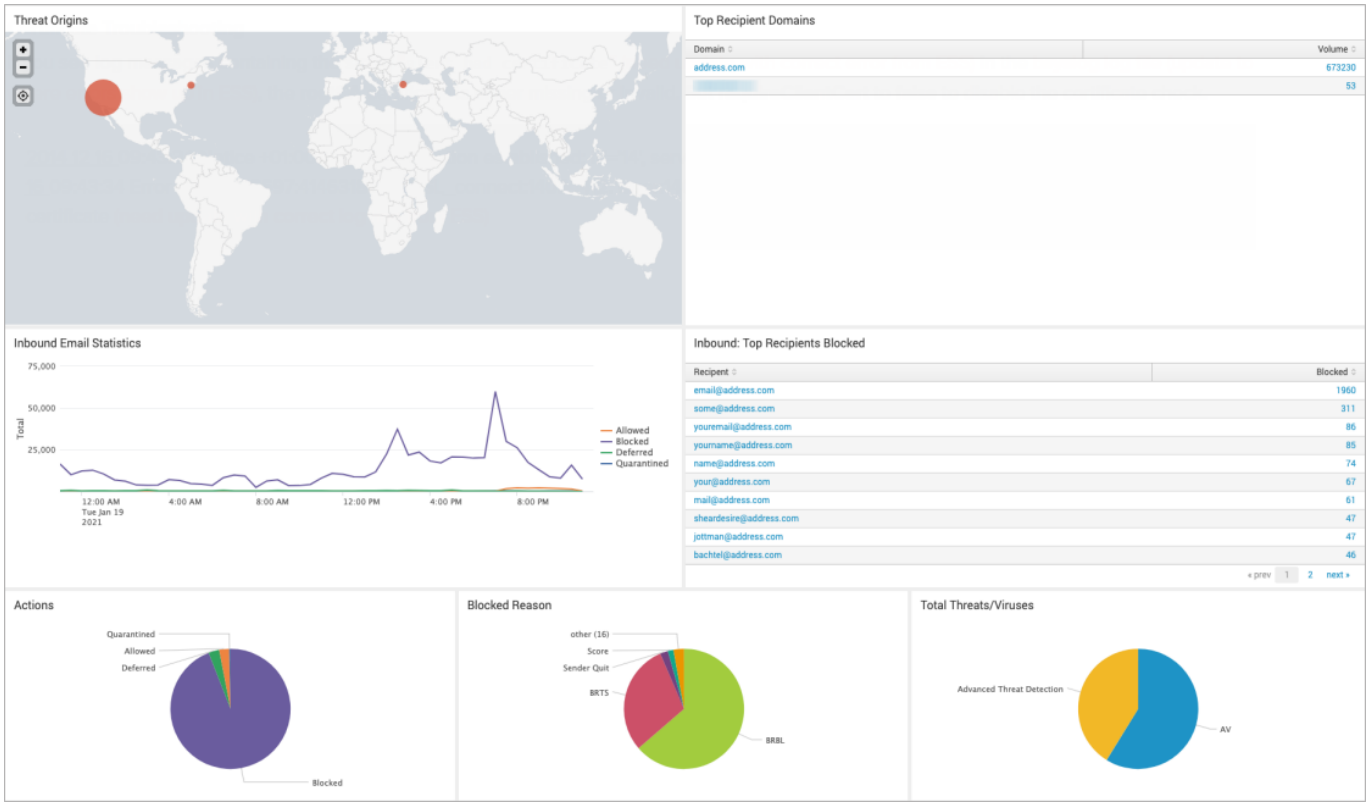
Splunk Integration

https://campus.barracuda.com/doc/94537450/

The Barracuda Email Security Service (ESS) Splunk app collects data from ESS and utilizes Splunk to provide aggregated and individual visualizations. Administrators can view a number of different metrics, including but not limited to inbound and outbound mail, top sender/recipients, actions taken, and detected threats. Data is imported into Splunk via syslog streaming of the Message log. The Splunk dashboard can be exported to PDF format for easy distribution. Currently, Splunk versions 7.1, 7.2, 7.3, 8.0, 8.1 are supported.



Before You Begin

- Download the Barracuda Email Security Service Splunk app from the Splunk Marketplace.
- Install the Barracuda Email Security Service Splunk app on your Splunk Server. For more information about Splunk add-ons, see https://docs.splunk.com/Documentation/AddOns/released/Overview/AboutSplunkadd-ons.

Step 1. Configure Data Input on Splunk

The Splunk server must be configured to receive the syslog data. Verify that you have a **Data input** entry for TCP port 6515 (SSL) that listens for the incoming syslog streaming connections. By default, port 6515 is used by the Barracuda Email Security Service Splunk app to process data. To use a different port, you must modify the `inputs.conf` configuration file for the Barracuda Email Security Service Splunk app. For more information, see https://docs.splunk.com/Documentation/Splunk/8.1.1/Data/Configureyourinputs.

1. Log into the Splunk server via SSH.
2. Edit `$SPLUNK_HOME/etc/apps/BarracudaESS/default/inputs.conf` and update the `[default]` section to use the desired port:
   ```
   [default]
   [tcp-ssl://6515]
   sourcetype = BarracudaESSJSON
   ```
3. Restart Splunk.

Step 2. Enable SSL Encryption for Barracuda Email Security Service Splunk App

The Barracuda Splunk app requires you to configure SSL encryption for communication between Barracuda and Splunk. To configure SSL, run the following commands.

1. Log into the Splunk server via SSH.
2. Run `/opt/splunk/bin/genRootCA.sh -d /opt/splunk/etc/certs`
3. Run `/opt/splunk/bin/genSignedServerCert.sh -d /opt/splunk/etc/certs -n splunk -c splunk -p`
4. When prompted for a password, enter a value such as `password`.
5. Edit `/opt/splunk/etc/apps/BarracudaESS/default/inputs.conf` and add a section for SSL:
   ```
   [SSL]
   serverCert = /opt/splunk/etc/certs/splunk.pem
   password = password
   requireClientCert = false
   rootCA = /opt/splunk/etc/certs/cacert.pem
   ```
6. Restart Splunk.

Certificate Troubleshooting

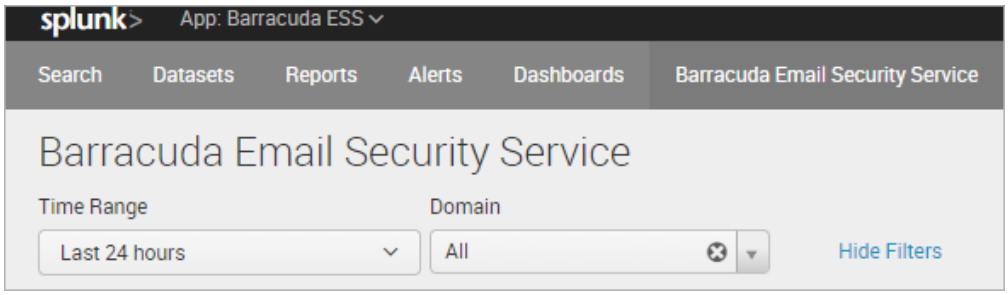
Most syslog servers can be configured to check client certificates. Barracuda syslog clients currently use a self-signed client certificate. Thus, if the syslog server validates client certificates, syslog messages can be rejected. To avoid this error, turn off syslog client certificate validation for the Barracuda Email Security Service or add the certificate to a trusted certificate configuration.

Step 3. Configure Syslog Streaming on the Barracuda Email Security Service

See Barracuda Email Security Service Syslog Integration for instructions.

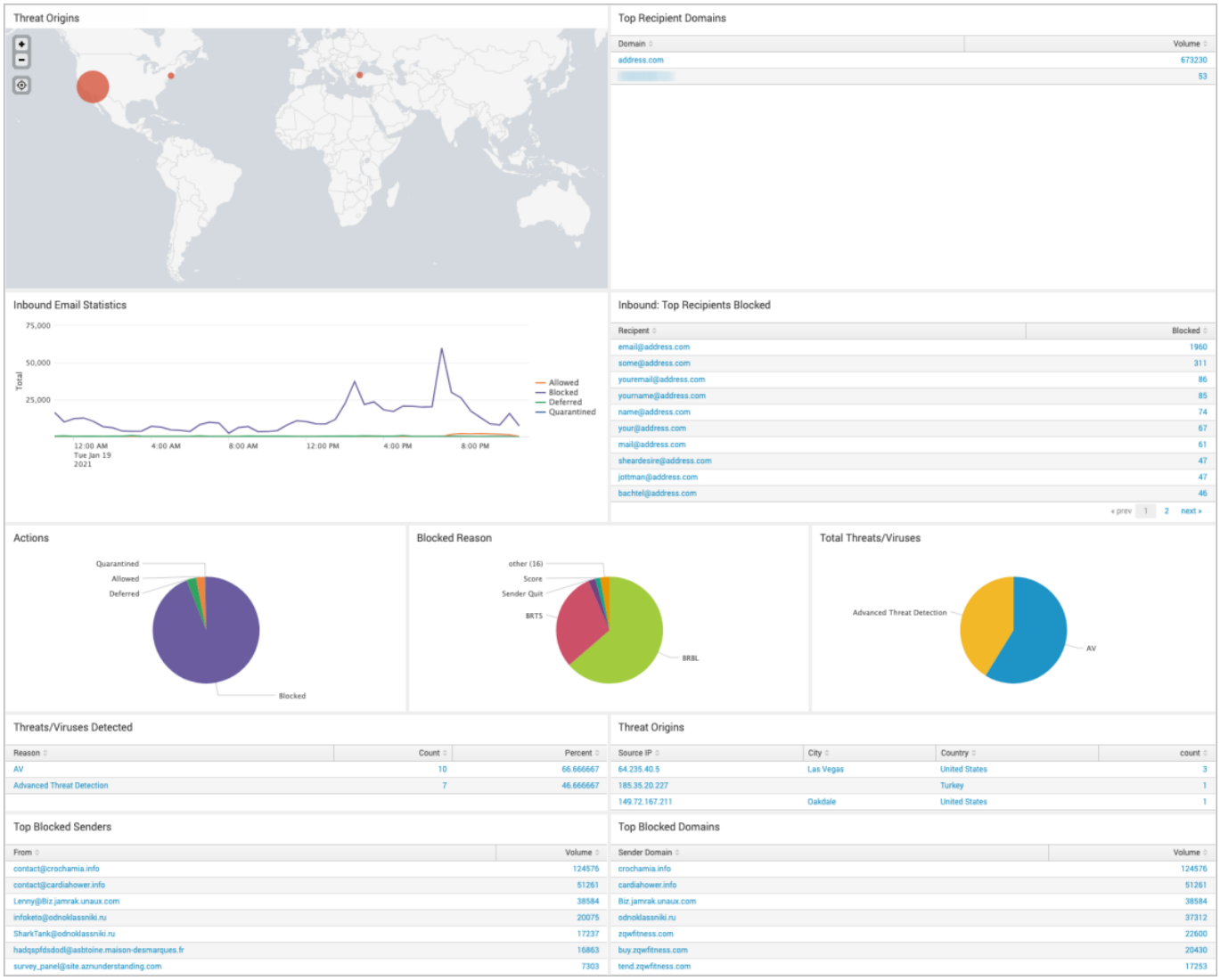
Barracuda Email Security Service Splunk App

Log into Splunk, and click on the Barracuda ESS app on the Splunk dashboard. Select the **Time Range** and **Domain** for the query.



Barracuda Email Security Service Dashboard

The app allows you to display domain statistics information based on a relative period (i.e. last 30 days) or real-time window (i.e. 1 minute).



Examples of Additional Splunk Queries

Top PTR Records

```
sourcetype=BarracudaESSJSON dst_domain=$destDomain$ ptr_record
| where isnotnull(account_id) and len(account_id) > 0
| foreach ptr_record [ eval ptr_record = if(isnull(ptr_record) OR
len(ptr_record)==0, "No PTR Record", ptr_record) ]
| top showperc=false limit=20 ptr_record
| rename "ptr_record" as "PTR Record", "count" as "Volume"
```

Popular Subjects

```
sourcetype=BarracudaESSJSON dst_domain=$destDomain$
```

```
| where isnotnull(account_id) and len(account_id) > 0
| top showperc=false limit=20 "subject"
| rename "subject" as "Subject", "count" as "Count"
```

Figures

1. ess_splunk1.png
2. essSplunkDash.png
3. ess_splunk2.png