Syslog Options Settings

https://campus.barracuda.com/doc/93195062/

Syslog Integration supports syslog version 3.

Syslog Integration enables you to export your event data to a syslog server or a security information and events management (SIEM) system. With Syslog Integration, you can store your information and use it for tracking, analysis, and troubleshooting.

Setting Up Syslog Integration

To configure Syslog Integration:

1. Log into Incident Response.
2. From the menu, select **Settings**.
3. Select the **Syslog Options** tab.
4. Select the **Active** checkbox.
5. Enter the **IP Address/Hostname** and **Port** for your syslog server/SIEM system. The default port is 6514.
   Incident Response public IP addresses are: 3.232.50.116 and 52.202.236.132
6. Click **Save**.
7. Click **Test** to ensure that Incident Response can connect with your syslog server/SIEM system.
   - *If the test is successful*, your message log data begins transferring to your syslog server/SIEM system.
   - *If the test is not successful*, check the IP Address/Hostname and Port information and reenter it if needed. Then perform the test again.

To deactivate the syslog server, clear the **Active** checkbox.

Notes:

- You can only connect one syslog server/SIEM system at a time. You can delete an existing entry and replace it, but you cannot have multiple entries.
- This feature is available only for Transmission Control Protocol (TCP) with Transport Layer Security (TLS).
- If your syslog server/SIEM system stops responding, data will not spool until the communication is re-established.
- After you enable or disable syslog integration, it can take up to 10 minutes for message transmission to either start or stop.

Data Sent

Incident Response sends the following objects to syslog:

Insight Events

- User-Reported Emails

```
{
 "type": "Email",
 "category": "User Reported Emails",
"reported_by": "user@organization.com",
"reported_date": "2022-06-23 - 21:45:27",
"recipient_email": "recipient@barracuda.com",
"delivered_date": "2022-06-07 - 21:45:27",
"subject": "HW#22.pdf",
"sender_email": "user@example.com",
"sender_name": "John, User"
}
```

- Related Threat

```
{
“type”: “Email",
“category”: "Potential Incident: Related Threat",
"subject": "HW#22.pdf",
"sender_email": "user@example.com",
"sender_name": "John, User",
"attachment": "attachment.pdf",
"matched_email_count": "6"
}
```

- Post-Delivery Threats

```
{
“type”: “Email",
“category”: "Potential Incident: Post-Delivery Threat",
"subject": "HW#22.pdf",
"sender_email": "user@example.com",
"sender_name": "John, User",
"attachment": "attachment.pdf",
"matched_email_count”: "9"
}
```

Remediation Events

- New Incident

```
{
"date": "2022-06-23 - 21:45:27",
"category": "Incident [Manual | Automatic]",
"type": "Email",
"incident_id": "123-456",
"created_by": "user@organization.com",
"subject": "HW#22.pdf",
"attachment": "attachment.pdf",
```

```
"sender_email": "user@example.com",
"sender_display_name": "John, User",
"messages_received": "8","
"affected mailboxes": "2",
}
```

- Continuous Remediation Enabled

```
{
"date": "2022-06-23 - 21:45:27",
"category": "Continuous Remediation Enabled",
"type": "Email",
"incident_id": "123-456",
"created_by": "user@organization.com",
"subject": "HW#22.pdf",
"attachment": "attachment.pdf",
"sender_email": "user@example.com",
"sender_display_name": "John, User",
"continuous_remediation_until": "2022-06-26 - 21:45:27"
}
```

- Deleted/Quarantined Email

```
{
"date":"2022-06-23 - 21:45:27",
"category":"[Deleted | Quarantined] Email",
"type":"Email",
"incident_id": "123-456",
"mailbox": "user@organization.com",
"office_id: "987654",
"ess_id": "1-1-1-1",
"internet_message_id": "<123@ABC>"
"continuous_remediation": true,
}
```

Data Format

Data is sent to the syslog in JSON format. You can parse the data any way you choose to meet the needs of your organization.