System Log events for Okta ThreatInsight

Okta ThreatInsight records requests from potentially malicious IP addresses in the System Log. It records the following types of events:

- Sign-in attempts from suspicious IP addresses
- Security threat detected
- Org Under Attack

View System Log events

1. In the Admin Console, go to **Security > General**.
2. Under **Okta ThreatInsight settings**, click **System Log**. The search field is pre-populated with the query `eventType eq "security.threat.detected"`. You can customize this query to find other types of events.
3. Configure the date range.
4. Click the magnifying glass icon beside the **Search** field.

Sign-in attempts from suspicious IP addresses

If Okta ThreatInsight detects sign-on attempts from a potentially suspicious IP address, it sets the `ThreatSuspected` field to `true`.

Paste this query into the System Log **Search** field to find sign-in attempts from suspicious IP addresses:

```
debugContext.debugData.threatSuspected eq "true"
```

The `ThreatSuspected` field also appears in the `user.session.start` and `security.threat.detected` System Log events.

Security threat detected

The `security.threat.detected` event only appears in the System Log if a request is deemed a high threat.

Okta ThreatInsight evaluates sign-in activity before the user can be identified, so `security.threat.detected` events don't include a username.

The `outcome.result` field describes how Okta ThreatInsight handled the request:

- **DENY**: Okta ThreatInsight terminated the request to prevent malicious actors from consuming the rate limit for your org.