Threats

A threat is an indication of impending danger or the possibility that something bad or harmful could happen. Threat intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging risk to entities that can be used to inform decisions regarding the subject's response to that threat.

RiskVision allows you to import threat intelligence to:

- Assign risk level to threats;
- Attribute incidents to threats;
- Associate entities with threats;
- Mitigate threats by creating tickets against the threats; and
- Prioritize vulnerabilities by auto-correlating threats to vulnerabilities.

These functions will be discussed in more detail later in this section.

The RiskVision user interface features threats grids and pages. The Threats grids are:

- **My Threats**: Threats the logged in user owns.
- **Recent Threats**: Threats from the last month. This can be configured to show different time periods.
- **All Threats**: Shows all threats.
- **Threat Intelligence**: Data imported from threat intelligence services, excluding malware, threat actors, and vulnerability intelligence. Includes periodic reports, such as weekly and monthly updates, and alerts on important topics.
- **Malware**: Shows threat intelligence on malware.
- **Threat Actors**: Shows threat intelligence on threat actors.
- **Vulnerability Reports**: Shows threat intelligence on vulnerabilities

The Threats grids provide the following information:

- **Source**: Name of the threat intelligence service.
- **Identifier**: The ID that the threat intelligence service assigns to the threat information.
- **Title**: Title assigned by the threat intelligence provider.
- **Type**: Type of report assigned by the threat intelligence provider.
- **Status**: Values can be New, Acknowledged, Investigating, Ignore, Mitigating, and Mitigated.
- **Owner**: Owner of the threat.
- **Risk**: Risk level associated with the threat.
- **Published Date**: Date the threat information was first released.
- **Last Updated Date**: Date the threat information was last updated.
- **Entities at Risk**: Count of entities associated with the threat information. Entities attached to a threat's targeted vulnerabilities will appear in this count, as will entities that have been manually assigned to the threat.
- **Targeted Vulnerabilities**: Count of vulnerabilities associated with the same CVE as the threat.
- **Related Incidents**: Incidents that have been linked to the threat. RiskVision automatically correlates threats with vulnerabilities when such correlation is provided by the threat intelligence provider.
- **Related Tickets**: Tickets that have been filed for the threat information.

The following optional columns can be added to the Threats grids using the **Customize** button:

- **Exploitation Consequence**: The consequence of the threat.
- **Exploited in the Wild**: Whether or not this threat has exploited a company in a real-life setting.
- **Proof of Concept Exploit**: Whether or not the threat has an exploit code.
- **Quantity of Exploits Exploited in the Wild**: The number of exploits that have been exploited in the wild, not the number of times an exploit has been exploited in the wild.
- **Quantity of Proof of Concept Exploits**: The number of proof of concept exploits that exist for this threat.
- **Quantity of Weaponized Exploits**: The number of weaponized exploits that exist for this threat.

- **Reference Count**: The number of references for the threat report. The higher the number, the greater the threat.
- **Risk Rating**: The rating assigned to the threat by the feed.
- **Risk Score**: The threat's quantitative risk score as reported by threat intelligent providers.
- **Threat Subtype**: Subtype of report assigned by the threat intelligence provider.
- **Weaponized Exploit**: Whether or not the threat's exploit has been automated.

The following are threat-related properties that can be added to `%AGILIANCE_HOME%\config\agiliance.properties` if needed:

- **com.agiliance.threatObject.fireEye.forceUpdate=true**: This property is set to **false** by default; however, users can force updates to the existing threat data that has already been imported into RiskVision from FireEye by setting it to **true**.
- **com.agiliance.fireeye.requestRange.inDays=90:** This property controls the maximum age for threat intelligence reports retrieved from FireEye. The default and maximum supported value of this property is **90** (days); however, users can reduce the number of days by adjusting this property.