

# Threat Miner for SDL

## User Manual

---

# Contents

---

1	Introduction .....	4
2	Ontologies .....	5
3	Threat Indicators .....	7
4	Feeds .....	8
5	Administrator Management .....	9
6	Tying it all Together .....	10

## ***Revision History***

---

<b>Document Number</b>	<b>Revision Number</b>	<b>Description</b>	<b>Revision Date</b>
XXXX	0.1	Initial version	July 24, 2018

# ***1 Introduction***

---

This document contains instructions on how the front-end of the Threat Miner for SDL application is to be used. It will contain the information necessary to perform daily operations as well as more advanced administration.

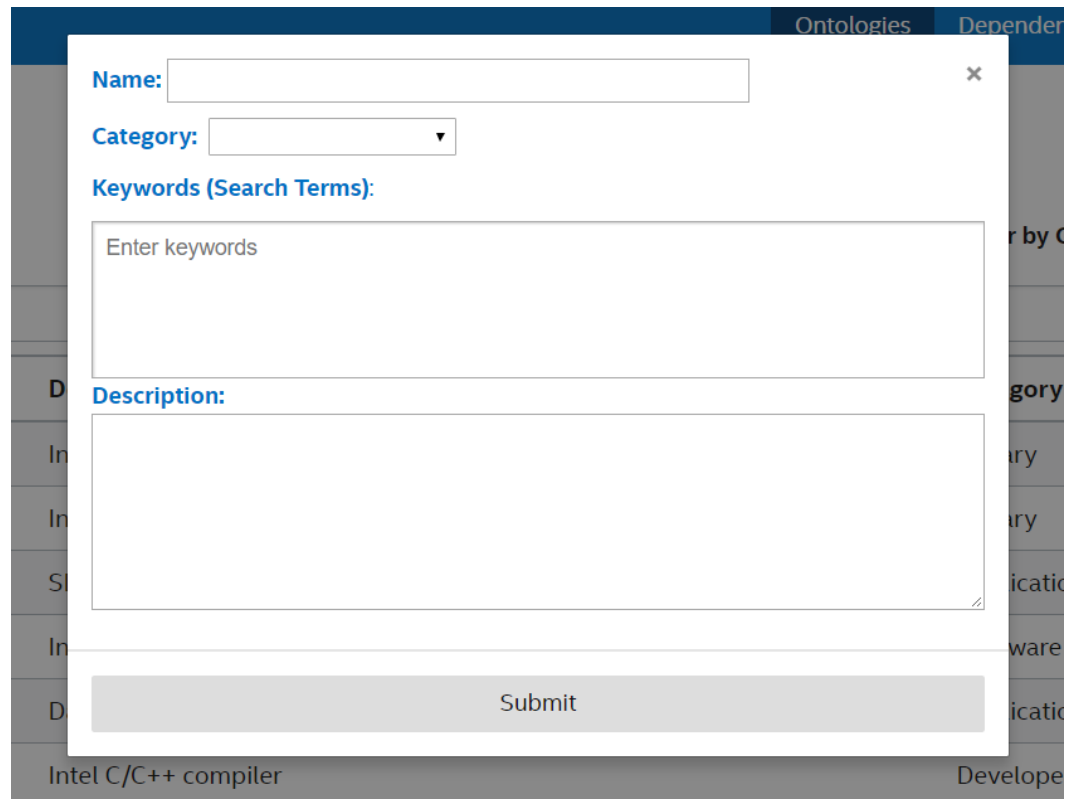
The purpose of the application is to look for threats indicators related to products and their dependencies. This tool automates the process of threat detection and provides updates on the most recent and relevant threat information.

## 2 Ontologies

This page shows the table of all of the ontologies that are recorded in the database.

- The table lists each ontology, along with its description, category and the last time it was updated.
- A similar table is displayed under “PenTest Arsenal”
- Users are able to filter by category as well as search through all of the listed ontologies in the table.
- Clicking on the name of an ontology will take you to a profile page for that ontology.
- **Only Admins have the ability to delete ontologies.**

### Adding an Ontology



The screenshot shows a web application interface with a dark blue header. The 'Ontologies' tab is selected, and a modal form for adding a new ontology is displayed. The form has a white background and a close button (X) in the top right corner. It contains the following fields:

- Name:** A text input field.
- Category:** A dropdown menu.
- Keywords (Search Terms):** A large text area with the placeholder text 'Enter keywords'.
- Description:** A large text area.
- Submit:** A grey button at the bottom of the form.

The background of the application shows a table with columns for ontology details, including 'Name', 'Category', 'Description', and 'Last Updated'. Some visible entries include 'Intel C/C++ compiler' and 'Developed by C++'.

- Adding an ontology is a very simple process.
  - The user must provide a name for the ontology.
  - The user can provide a category, keywords and description if they feel it is applicable.

- Note: Keywords are very important. These are words and phrases that the datamining algorithm will look for in the **RSS feeds**. It is recommended that they are included when creating an ontology.

### **Ontology Detail Page**

- This page contains a more detailed look at an ontology.
- All the keywords are listed along with all of the potential threats associated with the ontology.
- The top left-hand side of the app offers the ability to delete the ontology as well as add it to your watch list.
- Clicking on the title of a threat will take a user to a more detailed page about the threat.

### **Watchlist**

- This page lists all of the threats/ontologies that a particular user has chosen to watch closely.
- The page provides easy access to the ontologies and threats that are of interest to a user.
- If an ontology on a user's watch list is updated with any new threats, that user will be notified of the threats via email.

## 3 *Threat Indicators*

---

Threat indicators are potential vulnerabilities or security advisories that may affect ontologies listed in the Threat Miner database.

### Threat Detail Page

- Clicking on a threat in the table of an ontology detail page will take a user to a page similar to the one pictured above.
- Here, the link is provided to where more technical details can be found about the vulnerability. A short description, the date it was discovered and a number of other attributes are included as well.
- Admins can edit:
  - Owner: The person who is in charge of pursuing the potential threat
  - Status: Fixed, Under Investigation, Not an Issue, Advisory
  - Severity: The level at which the threat may affect an ontology.
  - Threat Category: Vulnerability, CVE, CWE, Rootkit, etc.
  - Adversary Type: If applicable the threat can be assigned one of the 9 adversary types
- Towards the bottom, other ontologies that may be affected by the same threat.
- The ability to add to a user's watch list also applies to threats.
- ***Only Admins have the ability to delete threats.***

### Machine Learning

- Threat Miner uses various machine learning techniques to retrieve the most relevant threat information.
- ***Only admins have the ability to train the classifier.***
- Threats that are marked -Under Investigation-, -Fixed-, and -Not an Issue- and -N/A- are used as training data.
  - Marking threats as "-N/A-" marks them as irrelevant and not applicable to the application as a whole. If the threat is not applicable to a certain ontology but is to the application as a whole, simply delete it.
  - Marking them otherwise (-Under Investigation-, -Fixed-, and -Not an Issue-) causes the training to mark them as relevant.
  - When the new threats are inserted into the DB they are either labeled "-New-" or "-New N/A-". -New- means that the classifier determined it relevant while "-New N/A-" means that it was determined to be irrelevant.

## 4 Feeds

Feeds are all of the sources that the data mining script searches. These tend to be in the format of xml documents hosted online such as RSS feeds. They are updated on a consistent basis (daily, weekly, etc.).

Threat Feeds

Add Feed +

Delete Selected Feeds

Filter by Type:

search ...

Title ↑↓	Link	Description	Type ↑↓
Carnal0wnage	<a href="http://carnal0wnage.attackresearch.com/feeds/posts/default">http://carnal0wnage.attackresearch.com/feeds/posts/default</a>		RSS Feed
Cisco CVRF	<a href="https://tools.cisco.com/security/center/cvrf_20.xml">https://tools.cisco.com/security/center/cvrf_20.xml</a>	Cisco Common Vulnerability Reporting Framework	XML Feed
Cisco event response	<a href="https://tools.cisco.com/security/center/eventResponses_20.xml">https://tools.cisco.com/security/center/eventResponses_20.xml</a>		XML Feed
Cisco OVAL	<a href="https://tools.cisco.com/security/center/oval_20.xml">https://tools.cisco.com/security/center/oval_20.xml</a>	Cisco Open Vulnerability and Assessment Language	XML Feed
Cisco PSIRT alerts	<a href="https://tools.cisco.com/security/center/psirtss20/AlertRSS.xml">https://tools.cisco.com/security/center/psirtss20/AlertRSS.xml</a>		XML Feed
Cisco security advisory	<a href="https://tools.cisco.com/security/center/psirtss20/CiscoSecurityAdvisory.xml">https://tools.cisco.com/security/center/psirtss20/CiscoSecurityAdvisory.xml</a>		XML Feed
Cisco security response	<a href="https://tools.cisco.com/security/center/psirtss20/CiscoSecurityResponse.xml">https://tools.cisco.com/security/center/psirtss20/CiscoSecurityResponse.xml</a>		XML Feed
Command line kungfu	<a href="http://blog.commandlinekungfu.com/feeds/posts/default">http://blog.commandlinekungfu.com/feeds/posts/default</a>		Blog Feed
Dark Net Hackers	<a href="http://feeds.feedburner.com/darknethackers">http://feeds.feedburner.com/darknethackers</a>		Feedburner
DoD CSIAc	<a href="http://iac.dtic.mil/csiac/rss/digest.xml">http://iac.dtic.mil/csiac/rss/digest.xml</a>	DOD Cyber security and information systems	RSS Feed







- **Only admins have the ability to add and delete feeds.**



## 5 Administrator Management





Users with the Administrator role have access to the Administrator Management Page.

**Threat Categories**Add Threat Category +

Name 	Description	
-Rootkit-	No Description	
-CVE-	No Description	
-CWE-	No Description	
-Vulnerability-	No Description	
-Malicious URL-	No Description	

1 2

**Adversary Types**Add Adversary Type +

Name 	Description	
Unprivileged Software Adversary	No Description	
System Software Adversary	No Description	
Startup Code/SMM Software Adversary	No Description	

- Here, Admins are able to manage many aspects of the applications.
- Admins can add/delete:
  - Users
    - Note: Must provide Name and Role
  - Feed Types
  - Threat Categories
  - Adversary Types
  - Ontology Categories

## 6 *Tying it all Together*

---

Threat Miner for SDL web service tool has 4 major components.

- AngularJS based front end GUI webservice has 2 modes, an Admin mode and a User mode. The GUI allows users to build product ontology, add product dependencies, and manage keywords to datamine for relevant threats. The GUI also allows users to add ontologies on the user specific watch-list to receive email alerts for new potential threats found. In the admin mode, the admin can manage threat feeds (add or delete threat feeds), manage users who have access to the tool. The admin has the privilege to manage the status and severity of these threats. The machine learning threat classifier learns only from the threat disposition that the admin has completed to classify new threats as relevant or not.
- MySQL Database to host all the content displayed through the Angular front end.
- A virtual machine can host the python scripts that talk to the database. The ***datamine.py*** script can run once or twice every day to mine for potential threats in opensource threat feeds such as security blogs, twitter, NVD etc. Once datamine is completed based on the ontologies described by the user, a classifier kicks in to identify relevant threats. The user only sees relevant threats output by the classifier. The admin sees both relevant and irrelevant ones. The admin can then override the classifier output and mark irrelevant ones as relevant if needed and this human feedback is used to re-train the classifier constantly. The ***train.py*** script can run once a week to retrain the classifier. The ***emailUpdate.py*** can run once or twice a day after datamine.py completes to inform the users on the watch-list regarding new potential threat indicators relevant to their watch-list.
- RestAPIs to enable communication between the MySQL database & Angular front end.