# SA-mitre Installation Guide

Contents

[SA-mitre Installation Guide 1](#_Toc40869014)

[Revision history 2](#_Toc40869015)

[Supporting Add On for MITRE – SA-mitre 3](#_Toc40869016)

[Sourcetypes 3](#_Toc40869017)

[Hardware and software requirements for the SA-mitre 3](#_Toc40869018)

[Install SA-mitre 3](#_Toc40869019)

[Configure SA-mitre 4](#_Toc40869020)

[How to use mitre\_techniques KVStore 5](#_Toc40869021)

[Appendix A: mitre\_techniques KVStore Schema 7](#_Toc40869022)

# Revision history

Following table describes changes to the document over time.

|  |  |  |  |
| --- | --- | --- | --- |
| **Revision** | **Revision Date** | **Notes** | **Author** |
| 1.0 | 5/20/2020 | Initial Release | Tony.s@bitsioinc.com |

## Supporting Add On for MITRE – SA-mitre

This app provides a method to ingest MITRE ATT&CK tactics, techniques, and subtechniques into Splunk events. The app contains a mitre\_techniques KVStore with the metadata provided from MITRE to help enrich alerts and ES Correlations without needing to navigate back to MITRE.

### Sourcetypes

|  |  |
| --- | --- |
| **Source type** | **Description** |
| mitre:techniques | MITRE ATT&CK tactic and techniques as defined <https://raw.githubusercontent.com/mitre/cti/master/enterprise-attack/enterprise-attack.json> |
| mitre:subtechniques | MITRE ATT&CK sub techniques as defined <https://raw.githubusercontent.com/mitre/cti/subtechniques/enterprise-attack/enterprise-attack.json> |

### Hardware and software requirements for the SA-mitre

Outbound internet access to the following URLs:

<https://raw.githubusercontent.com/mitre/cti/master/enterprise-attack/enterprise-attack.json>

<https://raw.githubusercontent.com/mitre/cti/subtechniques/enterprise-attack/enterprise-attack.json>

### Install SA-mitre

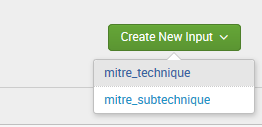
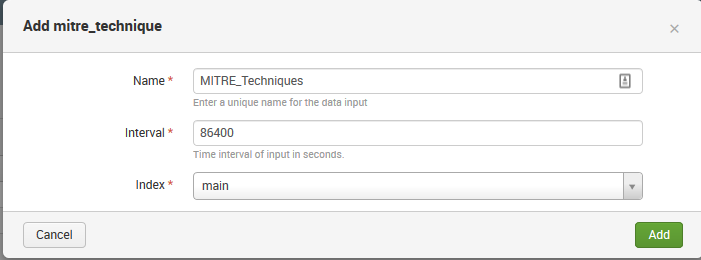
**Where to install this add-on**

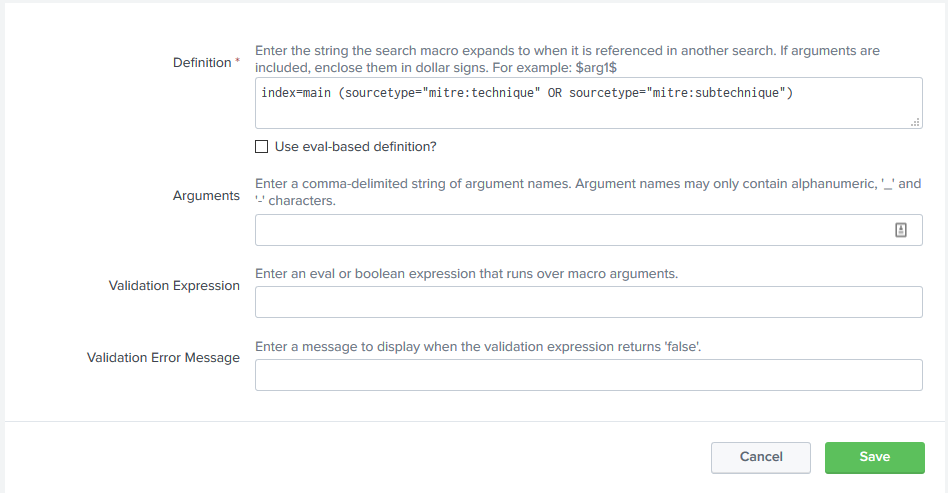
This table provides a reference for installing this specific add-on to a distributed deployment of the Splunk platform.

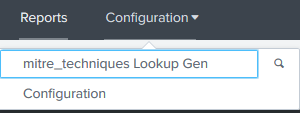
|  |  |  |  |
| --- | --- | --- | --- |
| **Splunk instance type** | **Supported** | **Required** | **Comments** |
| Search Heads | Yes | Yes | Install this add-on to all search heads where MITRE knowledge management is required. |
| Indexers | No | No | KVStore replication to indexers does not require this to be deployed directly on indexers. |
| Heavy Forwarders | No | No | This add-on does not contain any knowledge objects needed on forwarding tier. |
| Universal Forwarders | No | No |

### 

## Configure SA-mitre

1. Install SA-mitre on the search head(s) you would like the enriched MITRE ATT&CK data on.
2. Navigate to the SA-mitre app > Inputs tab.
3. Create new input > mitre\_technique  
     
   
4. Provide a name for the modular input, frequency you want to download and ingest the framework data and index you want to save the data too.   
     
   
5. Update indexmitre macro with correct index and sourcetype if you are not using index=main. **Settings > Advanced Search > Search Macros > indexmitre**



1. Once data has been indexed, run the **mitre\_techniques Lookup Gen** to populate the KVStore.  
     
   
2. Optional – Schedule the **mitre\_techniques Lookup Gen** saved search to run on a daily/weekly schedule based on your Interval defined in the input.

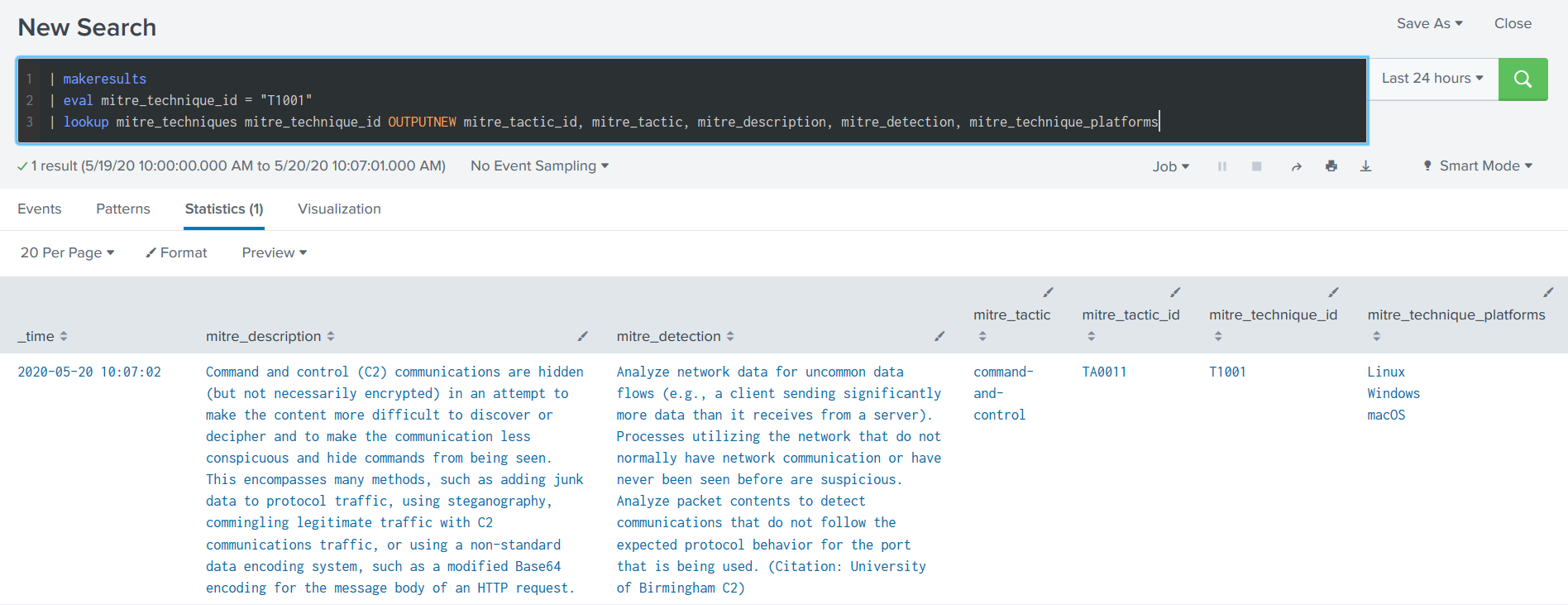
## How to use mitre\_techniques KVStore

Given a MITRE Tactic or Technique you can use this KVStore to enrich events with contextual data.

| makeresults

| eval mitre\_technique\_id = "T1001"

| lookup mitre\_techniques mitre\_technique\_id OUTPUTNEW



# Appendix A: mitre\_techniques KVStore Schema

|  |  |  |
| --- | --- | --- |
| **Field name** | **Data type** | **Description** |
| mitre\_technique\_id | string | The MITRE ATT&CK technique ID such as T1001. |
| mitre\_technique | string | The MITRE ATT&CK technique name such as Data Obfuscation. |
| mitre\_tactic\_id | string | The MITRE ATT&CK tactic ID such as TA0001. |
| mitre\_tactic | string | The MITRE ATT&CK tactic name such as Initial Access. |
| mitre\_description | string | The MITRE ATT&CK technique description. |
| mitre\_url | string | The MITRE ATT&CK technique URL for additional reference material. |
| mitre\_detection | string | The MITRE ATT&CK technique detection information. |
| mitre\_technique\_platforms | string | The MITRE ATT&CK technique platforms such as windows, linux, or mac. |
| mitre\_threat\_group\_name | string | The MITRE ATT&CK technique associated group names such as APT19. |
| mitre\_threat\_group\_aliases | string | The MITRE ATT&CK associated group aliases. |
| mitre\_threat\_group\_url | string | The MITRE ATT&CK group URL for additional reference material. |
| mitre\_threat\_group\_id | string | The MITRE ATT&CK group ID such as G0073. |
| mitre\_software\_name | string | Associated software name such as Mimikatz. |
| mitre\_software\_type | string | Associated software type such as Tool. |
| mitre\_software\_platform | string | Associated software platforms such as windows, linux or mac. |
| mitre\_software\_url | string | Associated software URL for additional reference material. |