

VECTR v5.0.0 Feature Breakdown

Table of Contents

- Generic Detection Rules 2
- Analysis Engine Detection Rules 5
- Detection Behaviors 8
- Organizations 11
- MITRE ATT&CK Heatmap Coverage 13

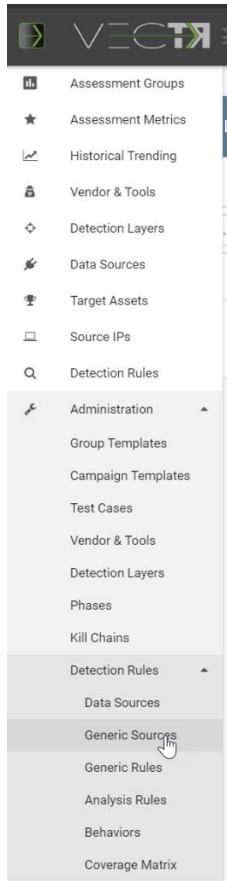
Generic Detection Rules

What is it?

VECTR provides out of the box generic detection rules to assist in the detection of some of the test cases throughout the campaigns.

How does it work?

First, you must define a “Generic Source” for your detection rules. That can be done through the Administration -> Detection Rules -> Generic Sources page:



This will take you to the Data Sources page. From here you can define a new Generic Data Source:

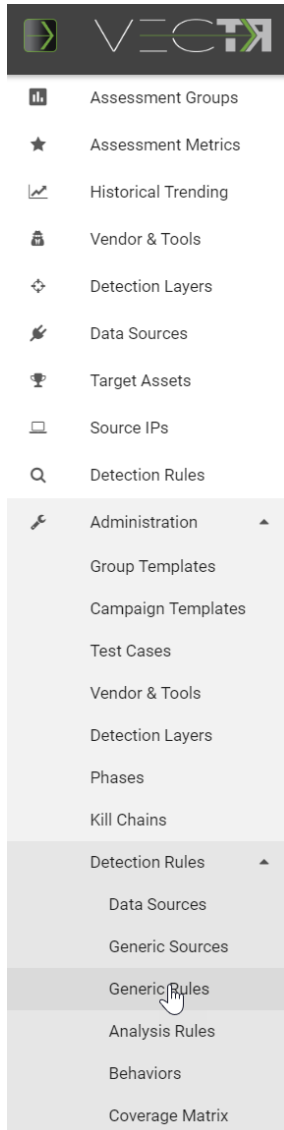
Generic Rule Data Source Summary

NEW

Name	Create Date	Update Date	Action	
search filter ...				
TALR	11/20/2018 14:41:26	11/20/2018 23:03:39		
Sigma	11/20/2018 14:19:51	11/20/2018 14:41:53		

After you fill in the popup, your Generic Source will show up in the list (TALR and Sigma are shown above).

Now that you have a Generic Source, you can use this as the 'parent' of Generic Rules. From the Navigation menu, go to Administration -> Detection Rules -> Generic Rules



This will take you to the Generic Rules page:

Name	Description	Rule Source	Data Sources	Contributors	Tags	Last Updated	Actions
Antivirus Password Dumper Detection	Detects a highly relevant Antivirus alert that reports a password dumper	Sigma	antivirus	Florian Roth	attack.credential_access	11/15/2018 23:46:27	EDIT
User Added to Local Administrators	This rule triggers on user accounts that are added to the local Administrators group, which could be legitimate activity or a sign of privilege escalation activity	Sigma	windows_security	Florian Roth	attack.privilege_escalation	11/15/2018 23:46:27	EDIT
Suspicious SYSVOL Domain Group Policy Access	Detects Access to Domain Group Policies stored in SYSVOL	Sigma		Markus Neis	attack.credential_access	11/15/2018 23:46:27	EDIT
Suspicious PowerShell Invocations - Generic	Detects suspicious PowerShell invocation command parameters	Sigma	windows_powershell	Florian Roth (rule)	attack.execution	11/15/2018 23:46:27	EDIT
PsExec Tool Execution	Detects PsExec service installation and execution events (service and Sysmon)	Sigma	windows	Thomas Patzke	attack.execution	11/15/2018 23:46:27	EDIT
Antivirus Exploitation Framework Detection	Detects a highly relevant Antivirus alert that reports an exploitation framework	Sigma	antivirus	Florian Roth	attack.command_and_control attack.execution	11/15/2018 23:46:27	EDIT
WMI Persistence	Detects suspicious WMI event filter and command line event consumer based on event id 5861 and 5859 (Windows 10, 2012 and higher)	Sigma	windows_wmi	Florian Roth	attack.persistence attack.execution	11/15/2018 23:46:27	EDIT
MSBuild Invoked by Non-Development Application	This rule is designed to alert on use of the MSBUILD.EXE utility by a non-development application. The majority of legitimate invocations of this Windows utility occur as a compilation task requested by a development application, such as Microsoft Visual Studio. Manual use by most end users should be considered suspect and investigated.	TALR	windows_sysmon	Tyler Frederick	attack.persistence attack.execution	11/20/2018 17:00:21	EDIT
Suspicious PowerShell Parameter Substring	Detects suspicious PowerShell invocation with a parameter substring	Sigma	windows_sysmon	Florian Roth (rule), Daniel Bohannon (idea)	attack.execution	11/15/2018 23:46:27	EDIT
Pandemic Registry Key	Detects Pandemic Windows Implant	Sigma	windows_sysmon	Florian Roth	attack.lateral_movement	11/15/2018 23:46:26	EDIT
Scheduled Task Creation	Detects the creation of scheduled tasks in user session	Sigma	windows_sysmon	Florian Roth	attack.persistence attack.execution	11/15/2018 23:46:27	EDIT
PowerShell PSAttack	Detects the use of PSAttack PowerShell hack tool	Sigma	windows_powershell	Sean Metcalf (source), Florian Roth (rule)	attack.execution	11/15/2018 23:46:27	EDIT

Here you can create new rules by clicking the New button in the top right or Edit existing rules by clicking EDIT.

How can this feature help me?

Having Generic Rules can help users of the platform to have remediation recommendations for Test Cases.

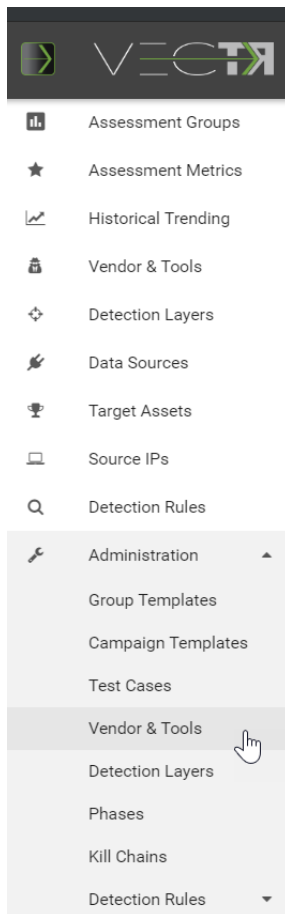
Analysis Engine Detection Rules

What is it?

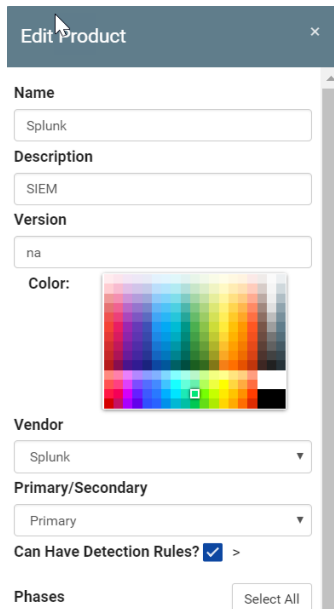
VECTR provides the ability to define product specific detection rules to assist in the detection of some of the test cases throughout the campaigns.

How does it work?

First, you must enable one of your blue team Products to be capable of using Detection Rules. That can be done through the Administration -> Vendors & Tools page:



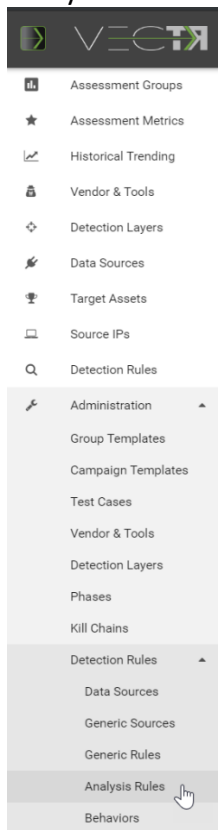
This will take you to the Vendors/Tools page. From here you can edit one of your Products by clicking the cog on the right. In the popup, click the “Can Have Detection Rules” checkbox:



The 'Edit Product' modal form contains the following fields and options:

- Name:** Text input field containing 'Splunk'.
- Description:** Text input field containing 'SIEM'.
- Version:** Text input field containing 'na'.
- Color:** A color selection palette with a small square selected in the bottom-left area.
- Vendor:** A dropdown menu with 'Splunk' selected.
- Primary/Secondary:** A dropdown menu with 'Primary' selected.
- Can Have Detection Rules?** A checkbox that is checked, followed by a right-pointing chevron (>).
- Phases:** A button labeled 'Select All'.

Now that a Product has been identified as an Analysis Engine, you can use this as the ‘parent’ of Analysis Engine Rules. From the Navigation menu, go to Administration -> Detection Rules -> Analysis Rules:



This will take you to the Analysis Engine Rules page:

</

Here you can create new rules by clicking the New button in the top right or Edit existing rules by clicking EDIT.

How can this feature help me?

Having Analysis Engine Rules can help users of the platform to have remediation recommendations for Test Cases.

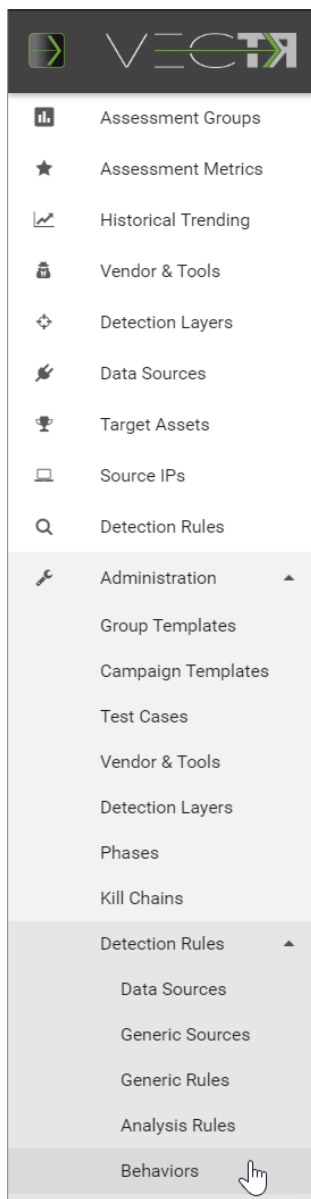
Detection Behaviors

What is it?

VECTR provides the ability to define Detection Behaviors that map Test Cases to Generic Rules and Analysis Engine Rules.

How does it work?

Navigate to the Administration -> Detection Rules -> Behaviors page:



This will take you to the Detection Rule Mapping page.

You can also click the rules in the table to have them display in a popup:

The screenshot shows the 'GoldStandard Detection Rule Mapping' application. A table lists detection rules. A popup titled 'TALR:MSBuild Invoked by WMI' is displayed, showing the following details:

```
type: x-detection-rules
id: x-detection-rules--f6957f7b-3bf7-4f03-98d5-efead516be3a
source: TALR
created: '2018-11-15T23:46:27.168Z'
modified: '2018-11-15T23:46:27.168Z'
title: MSBuild Invoked by WMI
revision: 1
revnotes:
- Initial commit
enrichment: None
description: This rule is designed to alert on the use of MSBUILD.EXE to move laterally through WMI, for example; wmic.exe /node:<IP> process call create "msbuild.exe -arguments"
author: Tyler Fredrick and Kevin Foster
logsource:
  product: windows
  service: sysmon
detection:
  selection:
    EventID: 1
    ParentImage:
      - '*\\WIPVSE.EXE'
    Image:
      - '*\\MSBUILD.exe'
  condition: selection
fields:
- CommandLine
- ParentCommandLine
falsepositives:
- unknown
level: high
status: experimental
tags:
- attack.lateral_movement
```

An 'OK' button is at the bottom right of the popup.

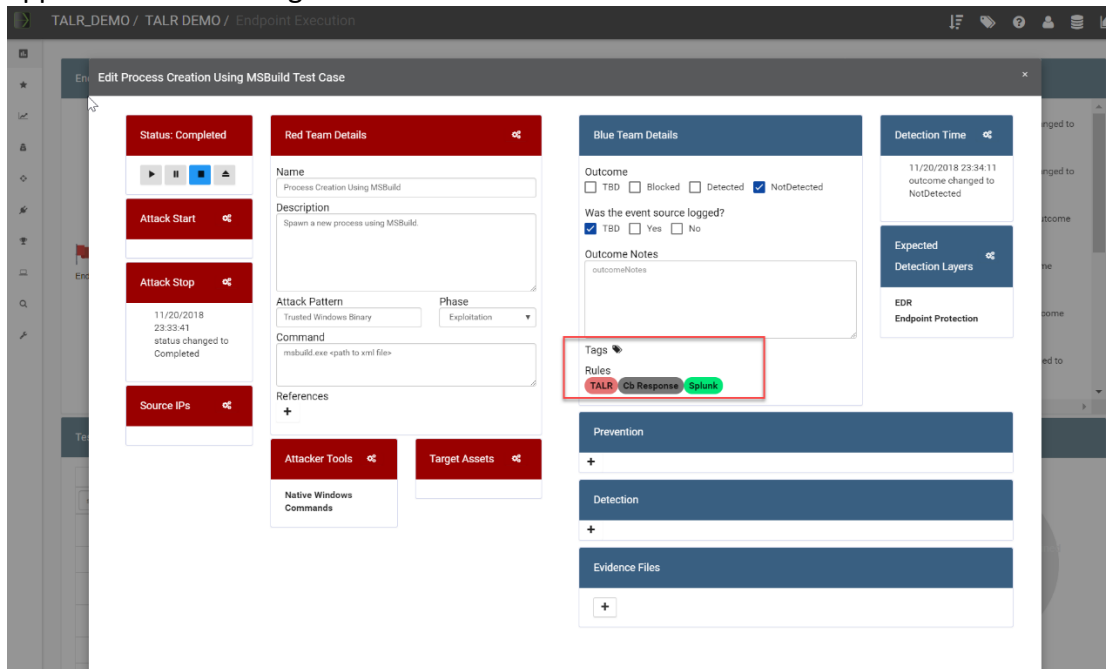
You can also edit one of your Behaviors by clicking the cog on the right. There are 4 tabs. Info, which is metadata, Use Cases which are the Test Case templates the rules will be applied to, Analysis Engine Rules / Generic Rules to associate to the Use Cases:

The screenshot shows the 'GoldStandard Detection Rule Mapping' application. A popup titled 'Edit WMI Invoking MSBuild Detection Rule' is displayed. The 'ANALYSIS ENGINE RULES' tab is selected, showing a table with the following data:

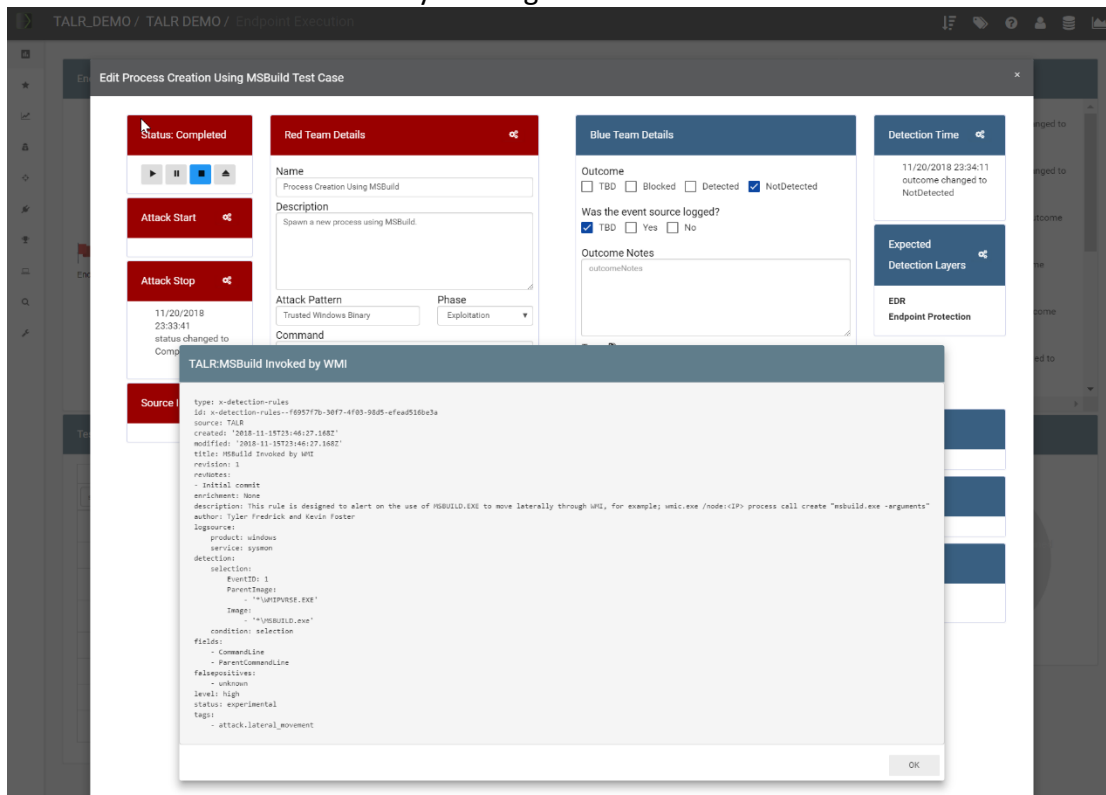
Include	Name	Analysis Engine / Tool	Data Sources
<input checked="" type="checkbox"/>	MSBuild Invoked by WMI	Cl Response	windows_sysmon
<input checked="" type="checkbox"/>	MSBuild Invoked by WMI	Splunk	windows_sysmon

How can this feature help me?

Assuming a Behavior has a Test Case and Rule mapped, you will be able to view the rules applicable to detecting the command in the Test Case:



You can click on the rule for easy viewing:



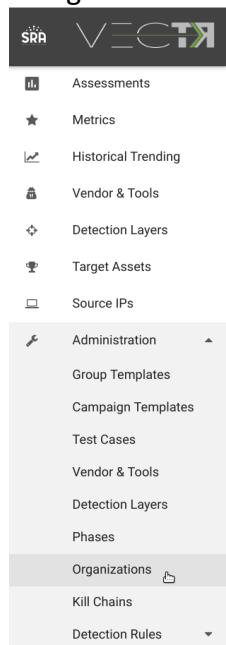
Organizations

What is it?

VECTR provides the ability to define Organizations that will allow content creation to be credited and organized to an Organization.

How does it work?

Navigate to the Administration -> Organizations page:



How can this feature help me?

There are various screens that will let you sort and filter data by Organization. Two examples are from the:

Assessment Group creation screen:

A screenshot of the 'New Assessment Group' form in the VECTR application. The form has a title bar 'New Assessment Group' with a close button. It contains several input fields: 'Name', 'Description', 'From Template' (a dropdown), and 'Kill Chain' (a dropdown). Below these fields is a table with columns: 'Select', 'Organization', 'Name', 'Description', and '# TestCases'. The table lists several organizations and their associated test cases. The 'Organization' column has a dropdown menu open, showing options: 'All', 'SRA', 'MITRE', and 'Atomic Red Team'. The table data is as follows:

Select	Organization	Name	Description	# TestCases
<input checked="" type="checkbox"/>	SRA	Endpoint Persistence	Activities include creating scheduled tasks on a system using job scheduler utilities to assess endpoint detection rule sets.	6
<input type="checkbox"/>	SRA	Windows Domain Enumeration	Includes Windows domain enumeration techniques ranging from 'net' commands to powershell equivalents and LDAP queries.	4
<input type="checkbox"/>	SRA	Malicious Document Execution	Includes a variety of malicious documents to execute locally on the victim endpoint. Regardless of what made it successfully through the mail gateway, this campaign aims to test the local payload execution to measure endpoint and network detection/blocking capabilities.	12
<input type="checkbox"/>	SRA	App Server Discovery and Exploitation	Includes discovery scans on the internal network for common web server ports and application servers, followed by intrusion attempts against targets such as Tomcat, JBoss, and Jenkins servers.	5
<input type="checkbox"/>	SRA	Network Vulnerability Scanning	Activities include higher volume network and application vulnerability scanning	

Test Case Administration screen:

Test Cases					NEW TEST CASE
<input type="checkbox"/> Show Deprecated					
Phase	Organization	Technique	Test Case	Action	
All	All	All	search...		
Command & Control	All	Remote File Copy	T1105 - scp remote file copy (push)		
Credential Access	SRA	Private Keys	T1145 - Private Keys		
	MITRE				
	Atomic Red Team				
Defense Evasion	Atomic Red Team	Indirect Command Execution	T1202 - Indirect Command Execution - forfiles.exe		
Defense Evasion	Atomic Red Team	Access Token Manipulation	T1134 - Access Token Manipulation		
Persistence	Atomic Red Team	Hooking	T1179 - Hook PowerShell TLS Encrypt/Decrypt Messages		
Defense Evasion	Atomic Red Team	Rootkit	T1014 - Loadable Kernel Module based Rootkit		
Execution	Atomic Red Team	Rundll32	T1085 - Rundll32 execute JavaScript Remote Payload With GetObject		
Defense Evasion	Atomic Red Team	Binary Padding	T1009 - Pad Binary to Change Hash - Linux/macOS dd		
Discovery	Atomic Red Team	Account Discovery	T1087 - View sudoers access		
Defense Evasion	Atomic Red Team	XSL Script Processing	T1220 - WMIC bypass using local XSL file		
Defense Evasion	Atomic Red Team	HISTCONTROL	T1148 - Mac HISTCONTROL		
Defense Evasion	Atomic Red Team	CMSTP	T1191 - CMSTP Executing UAC Bypass		
Discovery	Atomic Red Team	System Owner/User Discovery	T1033 - System Owner/User Discovery		

You can add your organization to previously created content. In the Test Case edit screen, click the gears in the Red Team Details:

Edit T1105 - scp remote file copy (push) Test Case

Status: NotPerformed

Attack Start

Red Team Details

Name

T1105 - scp remote file copy (push)

Description

Utilize scp to perform a remote file copy (push)

In the properties popup, click the gears next to the Organizations:

Edit T1105 - scp remote file copy (push) Test Case

Status: NotPerformed

Attack Start

Attack Stop

Source IPs

Red Team Details

Name

Outcome

Properties

Internal/External

Stealth

Attack Vector

Attack Complexity

Privileges Required

Assign Template

Assign Template

Organizations

Red Canary

Icon

Capec ID

Capec ID

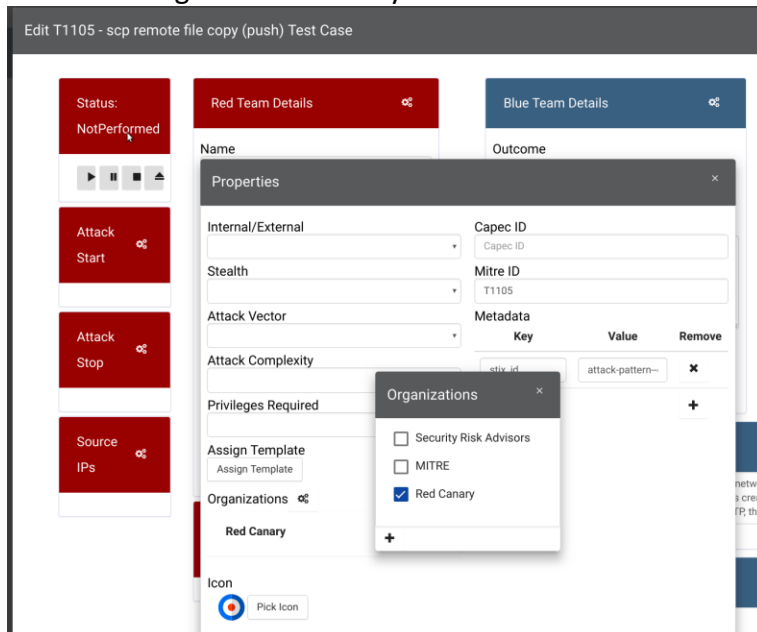
Mitre ID

T1105

Metadata

Key	Value	Remove
stix_id	attack-pattern--	

Select the Organizations that you want to credit with the content:



MITRE ATT&CK Heatmap Coverage

What is it?

VECTR provides the ability to associate Test Cases with a Mitre Technique. You can view coverage of your Assessments and Assessment Groups on the MITRE ATT&CK Matrix.

How does it work?

From the Assessment Group selection screen, click the graph icon next to an Assessment Group:

Assessment Group

NEW

Name	Type	Status	Actions							
Enterprise Purple – 2017 Q1	Campaign	In Progress								
Enterprise Purple – 2017 Q3	Campaign	Completed								
Enterprise Purple – 2018 Q1	Campaign	Completed								
Enterprise Purple – 2018 Q3	Campaign	Completed								
Enterprise Purple – 2019 Q1	Campaign	Completed								

Select Heat Map from the Report selection screen:

Select Report Attributes

Report Type

☐ Toolset Comparison

☐ Campaign Summary

☐ Campaign Detailed

☐ Kill Chain Summary

☐ Kill Chain Detailed

☐ Toolset Summary

☐ Toolset Detailed

☐ Timeline Summary

☐ Timeline Detailed

☐ Tagged Data

☒ Heat Map

☐ Data integrity

Outcome To Include

☒ TBD

☒ Blocked

☒ Detected

☒ NotDetected

Statuses To Include

☒ Completed

☒ NotPerformed

☒ InProgress

☒ Paused

☒ Abandon

Cancel

Select

How can this feature help me?

This will allow you to see the Outcomes of all your Test Cases that have associated Technique IDs on the MITRE ATT&CK Matrix:



You can set a Technique ID to a Test Case by bringing up the Test Case edit screen, then clicking the gears in the Red Team Details:

Edit T1105 - scp remote file copy (push) Test Case

Status: NotPerformed

Red Team Details

Name: T1105 - scp remote file copy (push)

Description: Utilize scp to perform a remote file copy (push)

Attack Start

Fill out the Mitre ID field in the Properties Popup:

Edit T1105 - scp remote file copy (push) Test Case

Status: NotPerformed

Red Team Details

Blue Team Details

Name: T1105 - scp remote file copy (push)

Outcome

Properties

Internal/External: [Dropdown]

Stealth: [Dropdown]

Attack Vector: [Dropdown]

Attack Complexity: [Dropdown]

Privileges Required: [Dropdown]

Assign Template: Assign Template

Organizations: [Dropdown]

Capec ID: [Dropdown]

Mitre ID: T1105

Metadata

Key	Value	Remove
stix_id	attack-pattern--	X