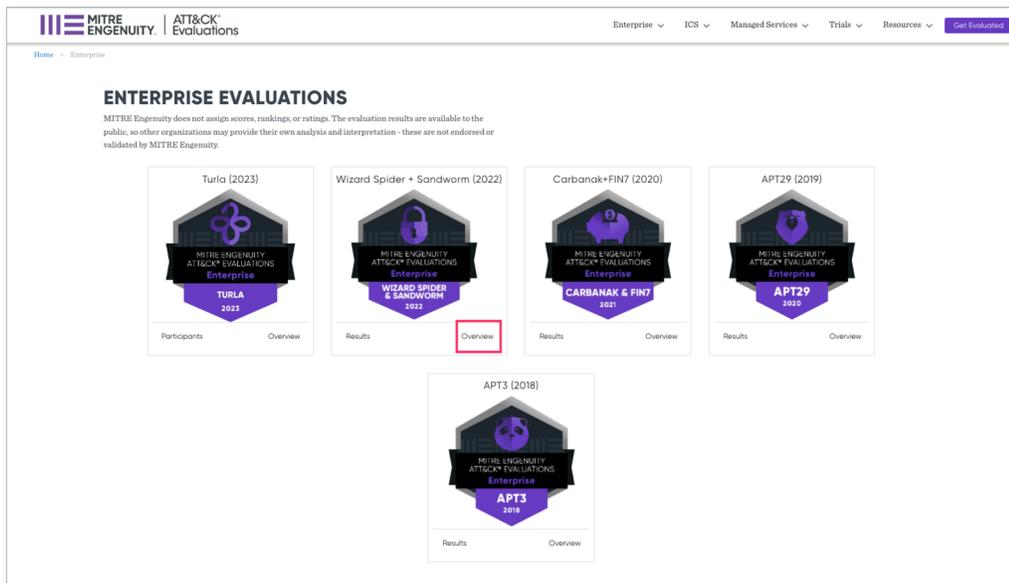


A PAGE-BY-PAGE OVERVIEW:

HOW TO EFFECTIVELY REVIEW MITRE ENGENUITY ATT&CK® EVALUATIONS: ENTERPRISE

Here's a downloadable guide on how to simplify your review to meaningfully analyze relevant data and best inform an effective cybersecurity strategy that addresses your precise needs:

STEP 1: GO TO EVALUATIONS OVERVIEW PAGE



HOW TO EFFECTIVELY REVIEW MITRE ENGENUITY ATT&CK® EVALUATIONS: ENTERPRISE

Review cyber threat intelligence descriptions around a particular adversary:

- ATT&CK descriptions
- Emulation notes

The screenshot shows the MITRE Engenuity ATT&CK Evaluations Enterprise interface. The main heading is "Wizard Spider + Sandworm Enterprise Evaluation 2022". A progress bar indicates the stages: Call for Participation, Evaluating, Preparing, and Published. Below the heading, there are two sections: "ATT&CK Description" and "Emulation Notes". The "ATT&CK Description" section is highlighted with a red box and contains the following text:

ATT&CK Description
Wizard Spider is a financially motivated criminal group that has been conducting ransomware campaigns since at least August 2018 against a variety of organizations, ranging from major corporations to hospitals.^{[1][9]}
Sandworm Team is a destructive Russian threat group that has been attributed to Russian GRU Unit 74455 by the U.S. Department of Justice and U.K. National Cyber Security Centre. Sandworm Team's most notable attacks include the 2015 and 2018 targeting of Ukrainian electrical companies and 2017's NotPetya attacks. Sandworm Team has been active since at least 2009.^{[1][9][14]}

The "Emulation Notes" section contains the following text:

Emulation Notes
This round will focus on how multiple groups abuse Data Encrypted For Impact (TI486). In Wizard Spider's case, they have leveraged data encryption for ransomware, including the widely known Tyral malware (S0146). Sandworm, on the other hand, leveraged encryption for the destruction of data, perhaps most notably with their NotPetya malware (S0368) that disguised itself as ransomware. While the common thread to this year's evaluations is Data Encrypted for Impact, both groups have substantial reporting on a broad range of post-exploitation tradecraft.

STEP 2: SELECT A PROVIDER

On the Evaluations Overview page, scroll down and select a provider in the Results section. This takes you to that provider's overview page.

The screenshot shows the "Results" section of the MITRE Engenuity ATT&CK Evaluations Enterprise interface. It displays a grid of provider logos, each with the text "ACME". The logo in the second row, fifth column is highlighted with a red box.

HOW TO EFFECTIVELY REVIEW MITRE ENGENUITY ATT&CK® EVALUATIONS: ENTERPRISE

STEP 3: PICK AN ADVERSARY

Pick an adversary to see specific results against that adversary for this provider.

ACME Cybersecurity Overview
Participant Configuration: Carbanak-FIN7, Wizard Spider + Sandworm

Select Adversaries [Dropdown] Download JSON

Adversary Results to Download

MITRE Engenuity does not assign scores, rankings, or ratings. The evaluation results are available to the public, so other organizations may provide their own analysis and interpretations - these are not endorsed or validated by MITRE Engenuity.

Overview | APT3 (2018) | APT29 (2020) | Carbanak-FIN7 (2021) | Wizard Spider + Sandworm (2022) | Turla (2022)

Evaluation Summary
These are the evaluations that Cisco has participated in:

Evaluations	Analytic Coverage 1	Telemetry Coverage 1	Visibility 1	Detection Count 1
APT3 (2018)	---	---	---	---
APT29 (2020) Incident MSP	---	---	---	---
Carbanak-FIN7 (2021)	42 of 174 subtypes	112 of 174 subtypes	122 of 174 subtypes	160 across 174 subtypes
Wizard Spider + Sandworm (2022)	74 of 109 subtypes	26 of 109 subtypes	90 of 109 subtypes	---

Evaluation Overview
Choose an evaluation to drill down into the procedures used to test each tactic and technique. The clipboard on each cell will allow you to view the detection results. These are the evaluations that Cisco has participated in:

This will take you to the provider's Results page, where you'll want to dive in deeply.

STEP 4: UNDERSTANDING SCENARIOS

Focus on a particular scenario by clicking on it.

ACME Cybersecurity Overview
Participant Configuration: Wizard Spider + Sandworm

Download Wizard Spider + Sandworm JSON

MITRE Engenuity does not assign scores, rankings, or ratings. The evaluation results are available to the public, so other organizations may provide their own analysis and interpretations - these are not endorsed or validated by MITRE Engenuity.

Overview | APT3 (2018) | APT29 (2020) | Carbanak-FIN7 (2021) | Wizard Spider + Sandworm (2022) | Turla (2022)

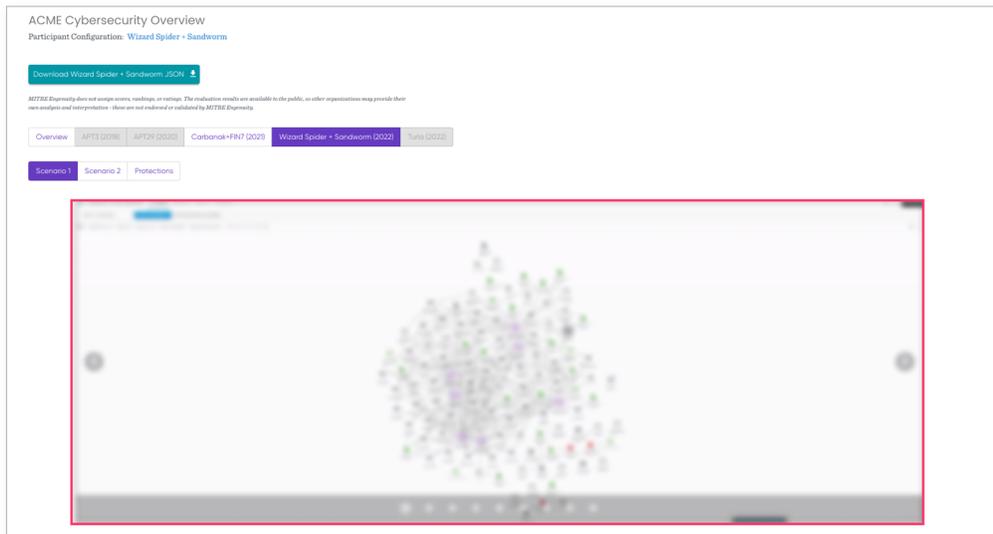
Scenario 1 | Scenario 2 | Protections

Scenario 1

There are multiple scenarios within each evaluation. Read each scenario to gain an understanding of how the provider performed during that specific scenario, within the specific evaluation round you are in.

STEP 5: REVIEW THE DETECTION SUMMARY

Review the Detection Summary by scrolling through the carousel of screenshots.



The detection summary gives context and a broad view of the specific scenario that you're looking at. It highlights the experience you would see within your UI and UX if you were to implement this product within your security infrastructure and the specified adversary breached your environment.

Evaluations has the largest global database of product screenshots.

In order to assess UX/UI, ask yourself:

- Do you like what you see?
- Will it work with your team?
- Is the visual representation responsive to your team's needs?

STEP 6: DIVE DEEPER INTO THE RESULTS

Scroll down and dive deeply into these results because they say a lot!

- See specifics regarding the scenario and provider
- Inspect detection categories
- Evaluate products off of the emulation plan
- See the detections in the products
- See how those detections were categorized

Within the results, focus on the data itself. We show a breakdown of achievements across each step and sub step of the overall emulation plan.

- Review detection criteria and categories
- Determine if the provider achieved detection within the emulation
- Review screenshot showing how the actual detection was generated
- Focus on higher-fidelity results to limit your alert fatigue

Step	ATT&CK Pattern	Detection Type	Detection Note
A 1.A.1	B Tactic Execution (TA0002) Technique User Execution (T1204) Subtechnique User Execution: Malicious File (T1204.002)	C Technique	D [1] [1]
1.A.2	Tactic Execution (TA0002) Technique Command and Scripting Interpreter (T1059) Subtechnique Command and Scripting Interpreter: Visual Basic (T1059.005)	Technique (Delayed)	[1] [2]
1.A.3	Tactic Command and Control (TA0011) Technique	Telemetry	[1]

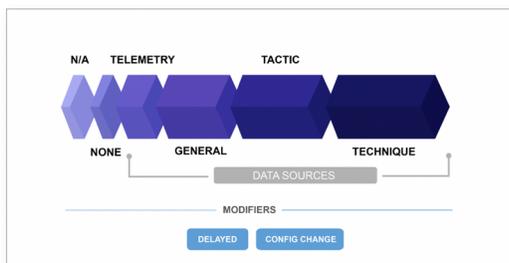
A
Steps & substeps
of emulation plan

B
Tactics, techniques,
and subtechniques

C
Detection Categories
column

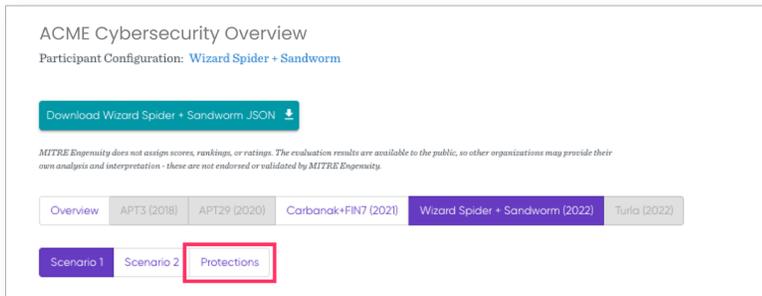
D
Click here to see
screen shots of the
detectors within
the provider's
enviroment

E
Click here for
Detection Criteria
and Data Sources



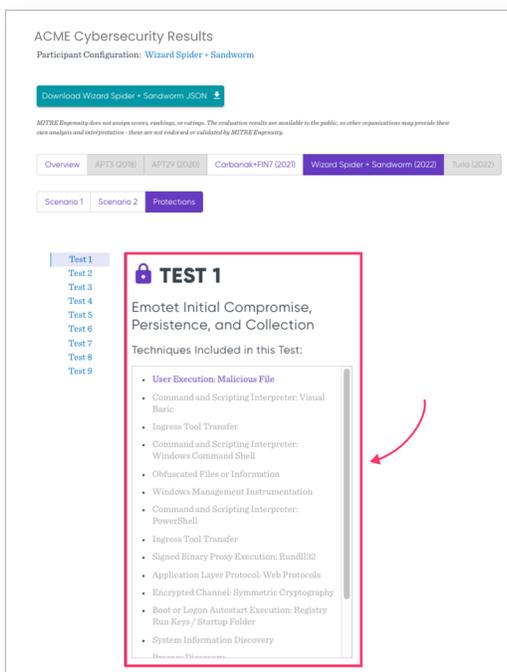
Detection Categories are explained for each adversary. In this instance they can be found [here](#).

STEP 7: CONSIDER PROTECTION RESULTS



These are simpler to review than detection results because these are linear tests that have a defined start and end. These are opt-in tests.

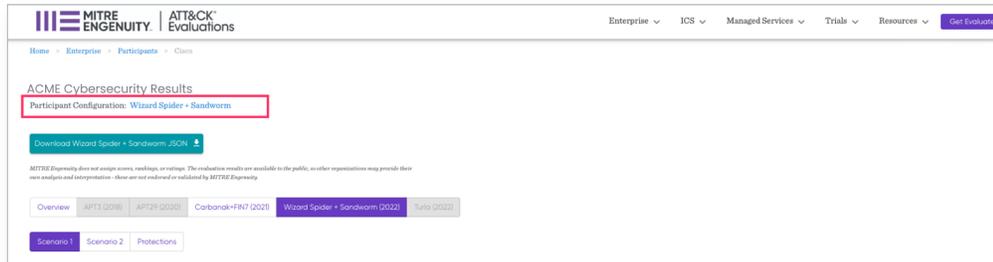
**Note that not every tool reviewed is structured toward detection and protection.*



- **Black text** means the red team won
- **Purple text** means the product stopped the activity
- **Gray text** means the activity was contained before the product could be run
- **Purple locks** means the product successfully protected
- **Unlocked icons** mean the product did not protect

STEP 8: PARTICIPANT CONFIGURATION

You've looked at the results. What do you do now?
Scroll up and go to the **Participant Configuration** page.



The Participant Configuration page:

- See specifics regarding the scenario and provider
- Inspect detection categories
- Evaluate products off of the emulation plan
- See the detections in the products
- See how those detections were categorized

Downloadable JSON file:



Advanced users can download a JSON (Java Script Object Notation) file, a structured data file that allows you to dive more deeply into results. You can use it to build internal analytics to further parse the data

STEP 9: FOLLOW-UP

We don't intend to be a one-stop shop to procure providers and products.

ATT&CK Evaluations results are meant to augment assessments. We hope this is just one component of an overall procurement strategy that takes many factors into consideration, including:

- Cost
- Resources
- Requirements
- And more



ABOUT MITRE ENGENUITY

MITRE Engenuity, a subsidiary of MITRE, is a tech foundation for the public good. MITRE's mission-driven teams are dedicated to solving problems for a safer world. Through our public-private partnerships and federally funded R&D centers, we work across government and in partnership with industry to tackle challenges to the safety, stability, and well-being of our nation.

MITRE Engenuity brings MITRE's deep technical know-how and systems thinking to the private sector to solve complex challenges that government alone cannot solve. MITRE Engenuity catalyzes the collective R&D strength of the broader U.S. federal government, academia, and private sector to tackle national and global challenges, such as protecting critical infrastructure, creating a resilient semiconductor ecosystem, building a genomics center for public good, accelerating use case innovation in 5G, and democratizing threat-informed cyber defense.

www.mitre-engenuity.org

ABOUT MITRE ENGENUITY ATT&CK® EVALUATIONS

ATT&CK® Evaluations (Evals) is built on the backbone of MITRE's objective insight and conflict-free perspective. Cybersecurity vendors turn to the Evals program to improve their offerings and to provide defenders with insights into their product's capabilities and performance. Evals enables defenders to make better informed decisions on how to leverage the products that secure their networks. The program follows a rigorous, transparent methodology, using a collaborative, threat-informed, purple-teaming approach that brings together vendors and MITRE experts to evaluate solutions within the context of ATT&CK. In line with MITRE Engenuity's commitment to serve the public good, Evals results and threat emulation plans are freely accessible.