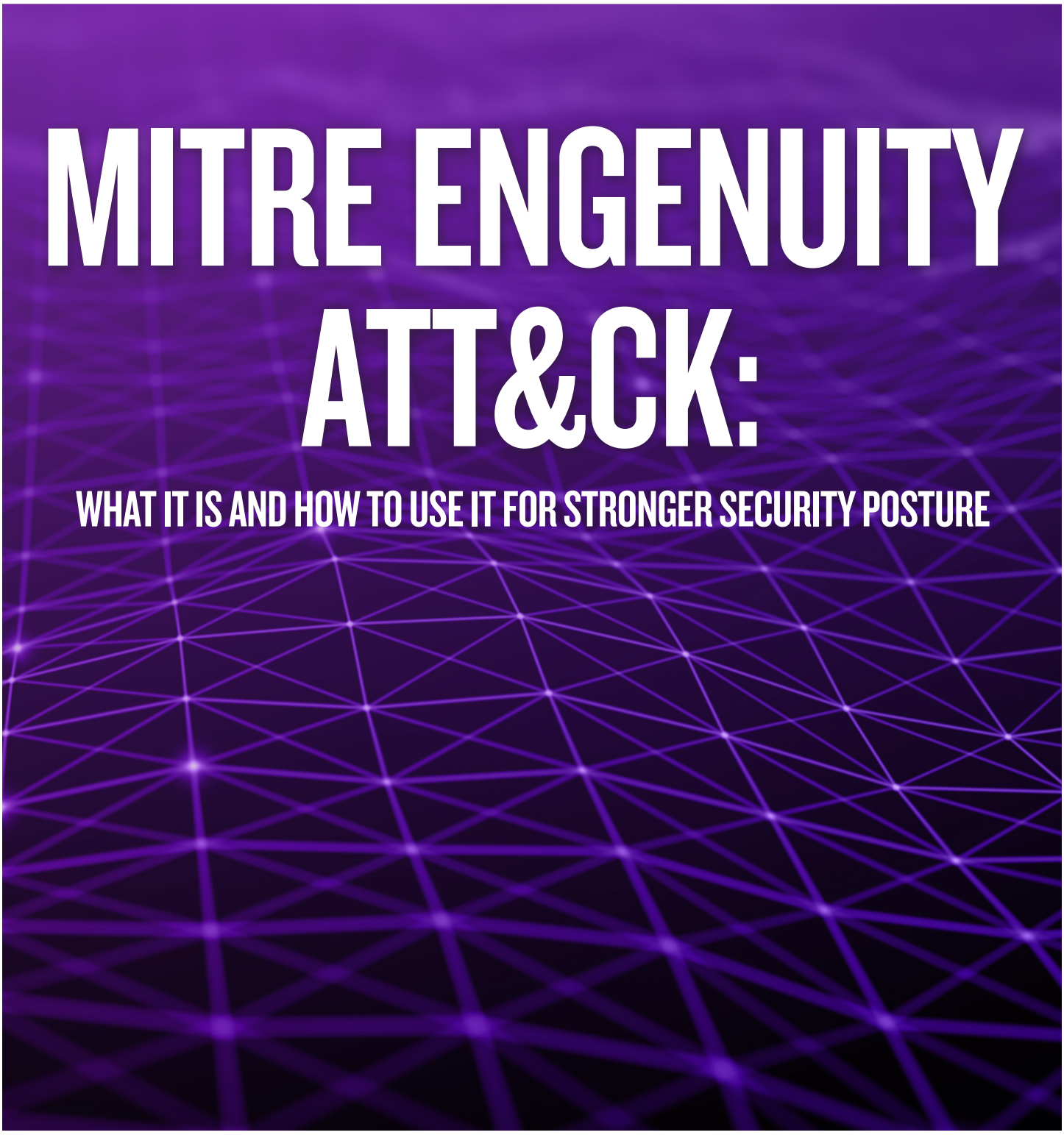
MITRE ENGENUITY ATT&CK:

WHAT IT IS AND HOW TO USE IT FOR STRONGER SECURITY POSTURE



ebook

An SC Media publication

Sponsored by

CISCO

Getting better, with help from MITRE Engenuity ATT&CK

Cisco uses MITRE Engenuity ATT&CK to continuously improve its security products. Individual enterprise security teams can benefit from it as well. Paul Wagenseil explains.

The MITRE Engenuity ATT&CK evaluation process is an unbiased and transparent way for organizations to gauge the efficacy of a potential security solution. But the detailed and freely available evaluation results it provides can also be a tremendous resource for any organization that wants to train and build out its own security team.

Cisco enthusiastically participates in the MITRE Engenuity ATT&CK evaluation process for two reasons:
1. It wants to establish its own standing among cybersecurity peers and its credibility among potential clients.
2. It believes that Engenuity and the MITRE ATT&CK framework as a whole benefit the entire security community by disseminating knowledge of adversarial threats, tactics and techniques.

Previous Engenuity results have helped Cisco improve its services and products, and this year's MITRE Engenuity ATT&CK results will do the same, company representatives say.

What MITRE Engenuity ATT&CK is and why Cisco participates

MITRE launched its Engenuity evaluation process in 2018, testing the efficacy and methodology of enterprise endpoint security products against known threat actors, using the well-known ATT&CK framework for analysis.

Nearly 40 leading security vendors have participated in MITRE Engenuity ATT&CK evaluations — Evals for short — over the past four years. Thirty did so in the latest round of evaluations, including Cisco, CrowdStrike, McAfee, Microsoft and Symantec. The tests are carried out in Microsoft Azure cloud instances.

Instead of just seeing whether a product stopped an attack at all, the Engenuity evaluations break down the dozens of steps in a sophisticated attack kill chain into discrete segments.

The ATT&CK framework helps explain where and how a product detected or prevented a step in the chain; each segment of the kill chain is treated as a new attack and assumes that the threat actor was successful in a previous part of the kill chain.

This is tremendously informative for both security vendors and their current and potential customers because it shows them how well an endpoint product fared against each step of the kill chain. It's much more granular than standard antivirus testing.

"One of the greatest gaps in the industry is when customers procure a product," says Shyue Hong Chuang, product manager for

OUR EXPERTS: MITRE Engenuity ATT&CK

Shyue Hong Chuang, product manager, Cisco Secure Endpoint.
Eric Howard, lead technical engineer, Cisco Secure Endpoint
Dr. Joel Fulton, co-founder and CEO, Lucidum
Adam Tomeo, senior product marketing manager, Cisco Secure Endpoint
Brad LaPorte, advisor, Morphisec
Dave Cundiff, CISO, Cyvatar

Cisco Secure Endpoint. "They spend good money, and they really don't know if the product's effective."

AV tests don't reflect the requirements of the advanced threat actors we have today, especially evaluating capabilities of EDR products, Chuang explains, adding:

"They may potentially help evaluate a protection product, like a traditional AV from a traditional AV vendor. But when it comes to the stuff that got past, what did your product tell me? It's the MITRE evaluation, it's the AV-Comparatives EPR [Endpoint Prevention and Response] test that gives a bit more visibility (across the attack kill chain)."

Shyue Hong Chuang, product manager for Cisco Secure Endpoint.

2022 evaluation insights

This year's MITRE Engenuity ATT&CK evaluations analyzed how well endpoint security products fared against two hypothetical attacks. The first was by Wizard Spider, a prolific Russian-speaking criminal group known to use BazarLoader, Conti, Emotet, Ryuk and Trickbot malware.

The 2022 evaluations also tested how well each endpoint product handled an attack by Sandworm, the Russian state-sponsored group thought to be, among other things, behind the worldwide NotPetya wiper attacks in 2017. The end goal of the MITRE Engenuity Sandworm simulation was deployment of NotPetya.

However, Engenuity evaluation results, released in March 2022 for the latest round, do not rank the security products tested, and do not give overall scores. There are no winners or losers. Overall, Engenuity is more concerned with how an endpoint security solution works rather than how well it works.

"Defenders use Evals to make better-informed decisions on leveraging the products that secure their networks," states the MITRE Engenuity ATT&CK evaluations website. "Each vendor evaluation is independently assessed on their unique approach to threat detection. Evaluation rounds are not a competitive analysis; they do not showcase scores, rankings, or ratings and are transparent and openly published."

The Eval results are difficult to interpret, and it helps to have a thorough understanding of the MITRE ATT&CK framework to make sense of them. Yet even though MITRE frowns on the practice, many security vendors do end up touting their "scores" to show that they "beat" competitors. And even those security vendors who don't brag about their results may feel the need to participate just to get a seat at the table.

MITRE and Engenuity: A common language

Cisco admits that one reason it participates in the MITRE Engenuity ATT&CK evaluation process is because, as a top security vendor, it has to.

> "One of the greatest gaps in the industry is when customers procure a product. They spend good money, and they really don't know if the product's effective."
>
> *– Shyue Hong Chuang, product manager for Cisco Secure Endpoint*

"Why does Cisco even participate in the Engenuity ATT&CK?" asks Eric Howard, lead technical engineer on Cisco Secure Endpoint. "And why do we believe in the framework that's been built? Certainly, it's not altogether altruistic."

But, Howard adds, using and interpreting

the Engenuity evaluation results is the natural next step from using the MITRE ATT&CK framework. ATT&CK set up a common language that security practitioners could use to communicate with each other, and with the C-suite executives who must approve funding requests.

"Most CISOs will ask for investments and increases in budget to respond to either current events or long-standing security concerns, but they don't have sufficient data points to support the ask," says Dr. Joel Fulton, co-founder and CEO of Lucidum, an asset discovery company. "By using the MITRE ATT&CK framework as a guide for these conversations, CISOs will be able to effectively explain the severity of threats and the actions to mitigate them while allowing CIOs to be active participants."

Eric Howard, lead technical engineer on Cisco Secure Endpoint

> "Why does Cisco even participate in the Engenuity ATT&CK? And why do we believe in the framework that's been built? Certainly, it's not altogether altruistic."
>
> *-Eric Howard, lead technical engineer on Cisco Secure Endpoint*

Cisco's Shyue Hong Chuang says participation alone gets his company a seat at the table and then allows them to articulate the values that a product brings to the customer. Analyzing the Engenuity evaluation results furthers that communication, Howard says.

"Engenuity has become a very good common language where miscommunication rules the day," Howard says. "Quite often, miscommunication is the root cause of exposed risk vulnerabilities that remain uncovered for long periods of time. That's why we participate — not just for the other reasons that we can get product in front of customers, but also the ability to provide to customers that need good security across the board a common language that helps them do things well and work across their own internal teams."

How Cisco performed in the most recent Eval

Cisco's results from the 2022 MITRE Engenuity ATT&CK evaluations were good, but not flawless. While Cisco Secure Endpoint Advantage, the specific product being tested, detected Wizard Spider activity in 10 out of 10 steps, and Sandworm activity in 9 out 9 steps, there were still two noteworthy compromises.

First, Wizard Spider managed to dump the Active Directory database in the fourth segment of its attack. Because each segment in the Engenuity evaluations is independent and assumes successful compromise in previous segments, it's likely that a real-world attack would have been stopped much further up the kill chain.

Indeed, Cisco Secure Endpoint Advantage blocked the Emotet initial access that made up the first part of the first segment. Subsequent independent segments, including deployment of the Trickbot malware and lateral movement to the domain controller, were also blocked.

"This is assuming that endpoint is a silver bullet for anything and everything," says Adam Tomeo, senior product marketing manager for Cisco Secure Endpoint. "There could have been places where Wizard Spider could have been blocked before it even got in. Because this is an email compromise, Cisco Secure Email might have picked it up as well before it even had a chance to come in."

The more significant compromise was on the first segment of the Sandworm attack,

where Cisco failed to block a user with stolen credentials from installing command-and-control malware, and gaining persistence on a Linux server.

In the second segment, Cisco Secure Endpoint blocked a lateral move to Windows, and blocked a pivot to the domain controller in the third segment.

Brad LaPorte, advisor, Morphisec

While the product did alert with granular analytic detections at the technique level during the Linux initial compromise, Chuang says that Cisco will use this result to improve its own products.

"We're going to increase our ability to mitigate living-off-the-land abuse by introducing more advanced behavioral protection on the Linux platform," Chuang says. "It's something we have seen extensively in the Windows world [and] we're now going to come around and double down to bring that technology into the Linux platform as well. We believe when we introduce behavioral protection into the Linux platform, we'd be able to see these events firing and kick in to kill that process there, (to protect earlier in the adversary's attack kill chain.)"

Does this mean Cisco did poorly? Not at all. A third-party overview of the 2022 MITRE Engenuity ATT&CK evaluations results by Morphisec's Brad LaPorte helps put Cisco's overall results — 100% detection, and 78% prevention — in context.

"Vendor detection rate percentages were as high as 100% and as low as 57%," LaPorte says. "Prevention rates ranged from a high of almost 90% to as low as 3.67%.

Eight of the vendors opted not to participate in the prevention tests. Of those who did, many had mediocre scores, even if they had strong detection scores." Furthermore, Chuang adds, some vendors chose not to take the Linux part of the Sandworm test.

Cisco is most proud of its demonstrated ability to protect against Wizard Spider and Sandworm and provide analytic detections at each step of the adversary's respective attack chains to accelerate incident response, Chuang adds.

In terms of how well Cisco Secure Endpoint performed compared to the 2021 evaluations, Chuang says the product delivered a 3x improvement in its ability to deliver analytic detections across the kill chains. He attributed this to improved MITRE ATT&CK Tactic, Technique and Sub-technique mappings, enhancing its behavioral-protection capabilities, and exposing behavioral telemetry to customers.

> "Vendor detection rate percentages were as high as 100% and as low as 57%. Prevention rates ranged from a high of almost 90% to as low as 3.67%. Eight of the vendors opted not to participate in the prevention tests. Of those that agreed to participate in prevention tests, many had mediocre scores, even if they had strong detection scores"
>
> *– Brad LaPorte, advisor, Morphisec*

How organizations can use MITRE Engenuity ATT&CK

Even if your company isn't looking for a new security vendor, the MITRE Engenuity ATT&CK evaluation results can be tremendously useful in training your security teams.

This year's evaluations mapped out the entire kill-chain process of the Wizard Spider and Sandworm attacks; the 2021 evaluations did the same for the Carbanak and Fin7 criminal threat groups. (Carbanak and Fin7

have links to each other, but MITRE treated them separately.)

The 2020 evaluations ran through an attack by the Russian state-sponsored group APT29, also known as Cozy Bear, the Dukes or Nobelium and thought to be behind the SolarWinds attack of late 2020; 2018's also tested against an attack by Chinese state-sponsored APT3.

Dave Cundiff, CISO at Cyvatar

In other words, you have a full overview of how these attacks work against the MITRE ATT&CK framework, and you can compare it to your own organization's security stance as defined by MITRE ATT&CK.

"Here is a true-to-form attack in sequence with the kill chain, the way that Sandworm or Wizard Spider actually facilitated these opportunities," says Cisco's Tomeo. "You can go back to any previous version of Engenuity to look at those again as an attack simulation in a box."

This is, from the beginning of initial compromise to end-data filtration, already scoped out, he adds. "At this point, regardless of where you can potentially stop it on the kill chain, you can leverage each one of these sub-steps to help strengthen your security posture in your organization."

All these threat actors are still active, and while their current attack strategies may not match exactly the simulations that the MITRE Engenuity ATT&CK evaluations used, running through these attacks with your own security teams can only be beneficial.

"Understanding the ways a potential attacker will take advantage of an organization is critical in being able to repel those very same attackers, and if not repel, identify more quickly when they have been successful," says Dave Cundiff, CISO at Cyvatar.

The granularity of the MITRE ATT&CK framework helps any organization find its own weak points.

"By viewing the MITRE ATT&CK framework as a 'board game' or checklist, security teams can thoroughly understand where their vulnerabilities lie and take the appropriate action to prevent attacks," says Lucidum's Dr. Joel Fulton. "The security leader would lay out the board game populating each of the techniques corresponding to each phase of an attack, and it is immediately apparent where there are gaps, the consequences of those oversights, and even where they have invested beyond the apparent threat."

It certainly beats running one simulation tool after another, Cisco's Eric Howard says.

> "Understanding the ways a potential attacker will take advantage of an organization is critical in being able to repel those very same attackers, and if not repel, identify more quickly when they have been successful."
>
> – Dave Cundiff, CISO at Cyvatar

Vulnerability intelligence

It's not directly tied to the MITRE Engenuity ATT&CK evaluations, but the Cisco team wanted to talk about one of their company's most recent acquisitions, risk-based vulnerability management platform provider Kenna.

"It just so happens Wizard Spider is one of the adversaries in the MITRE evaluations, but Wizard Spider is also known to be attributed to zero-day exploits for a particular CVE — in this case, for the Microsoft HTML engine," says Chuang.

"With CVE-2021-40444, there was basically a remote-code execution vulnerability in that particular engine."

Chuang explained that the MITRE Engenuity Wizard Spider attack simulation used stolen credentials to attack a system, but the attack vector could just have easily been malware that exploited CVE-2021-40444 in Microsoft Office files.

The Kenna system would have alerted customers to the vulnerability, along with links to patches — and given it a higher priority than vulnerabilities that were not being exploited or for which there was no proof-of-concept code.

"In this particular scenario with CVE-2021-40444, it was deemed to be actively exploited by threat actors, Wizard Spider being one of them," Chuang says. "There are proof-of-concept codes available and there are active incidences of this exploitation in the wild that Kenna vulnerability intelligence informs us (of)."

> "Most CISOs will ask for investments and increases in budget to respond to either current events or long-standing security concerns, but they don't have sufficient data points to support the ask. By using the MITRE ATT&CK framework as a guide for these conversations, CISOs will be able to effectively explain the severity of threats and the actions to mitigate them while allowing CIOs to be active participants."
>
> *-Dr. Joel Fulton, co-founder and CEO of Lucidum, an asset discovery company*

This is both more informative and more dynamic than a standard NVD vulnerability listing because the Kenna alert will change over time if a vulnerability is exploited.

The platform also learns what its customer is running and tailors its presentation according to whether the customer's software environment is at risk.

Kenna "prioritizes risk against vulnerability," says Howard. "The business conversation is often not around vulnerability, but around risk. We know the vulnerability's there, we may have to live with it for a moment. But what's our exposure? What's the risk to us? Is there stuff actively out there exploiting this?"

Conclusion

Overall, MITRE Engenuity ATT&CK evaluations provide the following benefits:

They show organizations how security products under consideration work against well-known malware, and furthermore how those products might work in their own organizations.

Even if there's no need to consider new security vendors, security teams can map out the Engenuity results against their own MITRE ATT&CK frameworks to evaluate how well their organizations would have performed — and highlight what might need to be improved.

The prevalence of the ATT&CK framework lets both red teams and blue teams study Engenuity results and share in their understanding of the threats. It provides "the ability to have a common language between both those that know how to test an environment and those that are tasked with defending against the things that are thrown at an environment," Howard says, adding:

"Red and blue teams can speak the same language, reversing the power of the Babel effect so that we can get to the same goal." ■

For more information about ebooks from SC Media, *please contact Bill Brenner, VP, content strategy, at bill.brenner@cyberriskalliance.com.*

If your company is interested in sponsoring an ebook, please contact Dave Kaye, chief revenue officer, at (917) 613-8460, or via email at dave.kaye@cyberriskalliance.com.

Sponsor

Masthead

EDITORIAL
VP, CONTENT STRATEGY
Bill Brenner
bill.brenner@cyberriskalliance.com
SPECIAL PROJECTS MANAGER
Victor Thomas
victor.thomas@cyberriskalliance.com

SALES
CHIEF REVENUE OFFICER
Dave Kaye
(917) 613-8460 *dave.kaye@cyberriskalliance.com*
DIRECTOR, STRATEGIC ACCOUNTS
Robyn Armao
(914) 263-4178 *robyn.armao@cyberriskalliance.com*