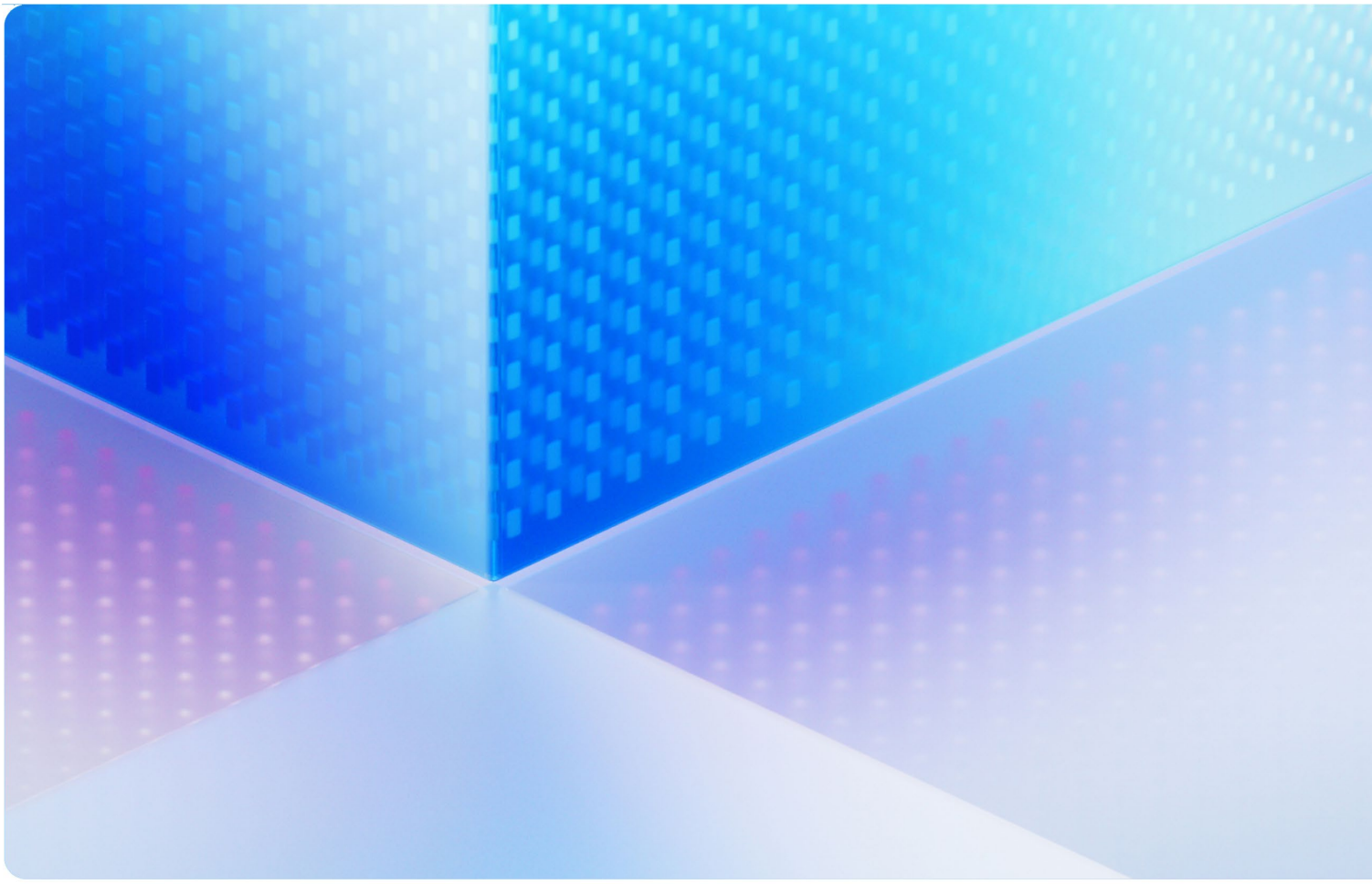
FIELD EFFECT



MITRE Engenuity's ATT&CK® Evaluations: Managed Services

Field Effect Results

Introduction

MITRE Engenuity's ATT&CK® Evaluations is a reliable tool for buyers to identify leading vendors that are committed to the security of their clients while identifying the strengths and weaknesses within each solution.

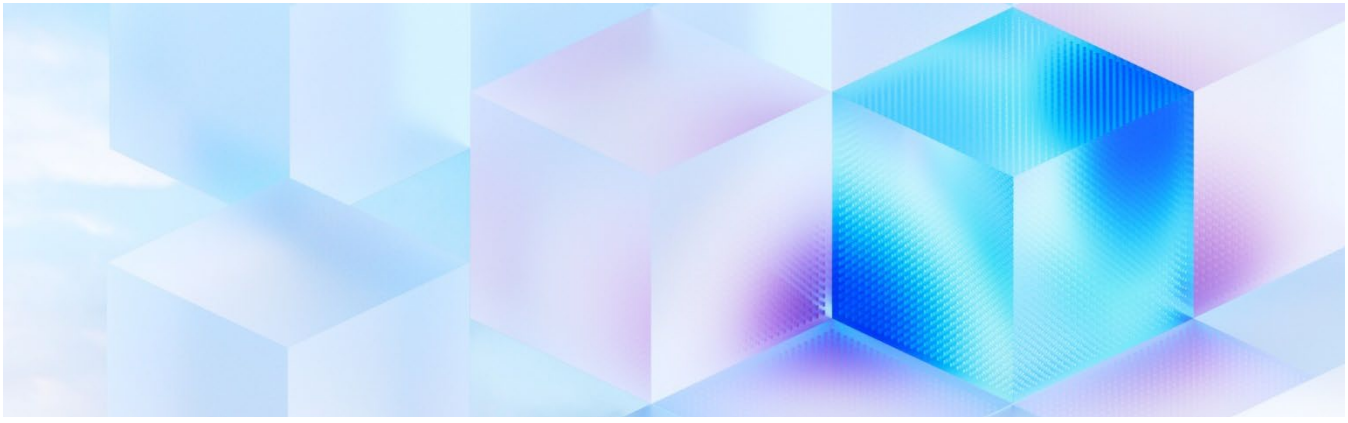
As a solution purpose-built for small and medium sized enterprises (SMEs) and the partners who protect them, Field Effect participated in *MITRE Engenuity's ATT&CK® Evaluations: Managed Services - Round 2* to prove that our approach is the best fit for the SME market—and our results showed exactly that.

We're proud to say that in a real-life attack, like that simulated through the ATT&CK® Evaluations, Field Effect's customers would have been protected from the tactics and techniques deployed in each of the steps therein. Key highlights include:

- Immediately upon deployment and before the simulation began, Field Effect communicated the need to address several vulnerabilities and risks, which were exploited during the simulation
- Field Effect reported actionable detections across 100% of steps in the attack, with a 11-minute Mean Time To Detect (MTTD), allowing for immediate remediation in a real-life scenario
- Field Effect detected the very first indicator of compromise (IoC) in two minutes, at which point in a real environment the attack would have been stopped
- True to our approach to cybersecurity, Field Effect delivered actionable alerts without noise and unnecessary complexity

As our first year participating in the MITRE Engenuity's ATT&CK® Evaluations, our results validate our approach to the market and affirm our confidence in our ability to protect our clients by focusing on prevention, and on early detection and containment.

In light of participating in this year's evaluation, we have been able to identify areas where we can alter our alert information for our analyst team to better align to the evaluation for future rounds, while keeping our service to SMEs consistent with our approach!



MITRE Engenuity's ATT&CK® Evaluations: Managed Services

MITRE Engenuity's ATT&CK® Evaluations: Managed Services evaluates vendors on their 'ability to analyze and describe adversary behavior' in a controlled security simulation. Vendors are evaluated in the same way and face all tactics and techniques with the same approach, regardless of whether the vendors had detected previous indicators of compromise. Blocking, remediating, or engaging in preventative measures is strictly prohibited, as is communicating with the MITRE team acting as the client.

***MITRE Engenuity's ATT&CK® Evaluations: Managed Services* does not evaluate vendors on their response capabilities, quality of support, or overall user experience.**

Methodology

MITRE Engenuity's ATT&CK® Evaluations: Managed Services executed a cybersecurity event consisting of 15 steps and 174 sub steps, emulating attack techniques from menuPass (steps 1-9) and BlackCat (steps 10–15.) Vendors had to allow each sub step to proceed for the purposes of the evaluation, regardless of whether it would have been blocked and the attack terminated in a normal deployment.

MITRE Engenuity evaluated each vendor on their ability to report 43 of the techniques from the 174 sub steps. A technique, or sub step, was rated as 'detected' based on whether there was an alert reported to the 'client' via email or the vendor's console, with extra details provided around actionability of those alerts.

Using the ATT&CK® Evaluations as a Small and Medium Sized Enterprise or Service Provider

MITRE Engenuity's ATT&CK® Evaluations: Managed Services provides an evaluation of potential security vendors and their capabilities around reporting adversarial behavior. **While "detections" can indicate the complexity of alerts that your MDR vendor will share directly with your team, it's also important to focus on your security outcomes.**

With the expense and availability of cybersecurity analysts and resources impacting SMEs and the partners that protect them, consider the following questions when reviewing vendor results:

- Did the vendor detect critical steps required to stop the attack, in a timeframe that minimized the attack and accelerated your recovery efforts?
- In a real-life scenario, would the vendor be able to block and/or neutralize the threat on your behalf?
- Would the volume and complexity of the alerts be suitable for your team's level of expertise?

The ATT&CK® Evaluation is an excellent tool to identify leading vendors that are committed to the security of their clients and to get a third-party evaluation of their alerting capabilities, however, it should not be used as a singular tool when evaluating vendors. The SME market should pay close attention to the time to detect, usability of the solution, expected level of support, as well as their overall capabilities. In this case, it's also important to understand the nuance between 'detected' and 'reported'.

For the ultimate test of real outcomes, consider deploying a solution in your own environment before making a long-term decision.

Field Effect MDR results

Field Effect MDR demonstrated rapid threat detection and purposeful, actionable alerting throughout the ATT&CK Evaluations that—in a real-life scenario—would have fully protected our clients without undue complexity.

Field Effect reported the first sign of the attack within two minutes of onset and identified four key risks, which were exploited to make the attack possible, before the simulation even began.

We reported malicious behavior early and quickly in all 15 of MITRE's steps while minimizing noise, offering clients the benefit of a fully managed Security Operations Center (SOC) without requiring in-house cybersecurity expertise. Throughout the evaluation, we ensured business continuity for our users, both by detecting threats early and sharing the information that matters most to our target audience—with clear and easy-to-understand language.

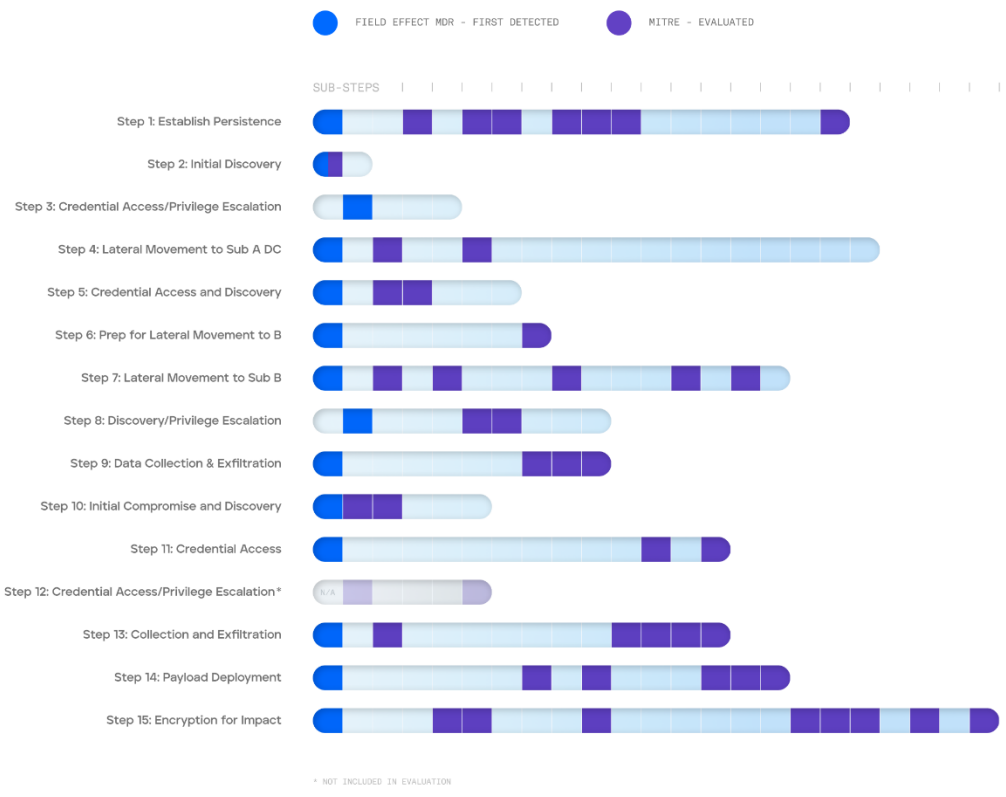
Our results validated our approach to our customers—those who do not have an in-house enterprise SOC. Field Effect delivers sophisticated cybersecurity that is both powerful while simple and noise-free for SMEs and the partners that protect them.

Full protection

During a real attack like that simulated in the ATT&CK Evaluation, Field Effect MDR would not only have neutralized each step to stop spread and business disruption but also would have identified vulnerabilities early on to prevent the attack all together.

As soon as Field Effect MDR was deployed in the simulated environment, we identified multiple risks and vulnerabilities that, as it turns out, were the basis of the attack. In a real-life scenario, our team would've worked with our clients to eliminate these risks before attackers had the opportunity to exploit them, thereby eliminating the opportunity to gain access to their environment.

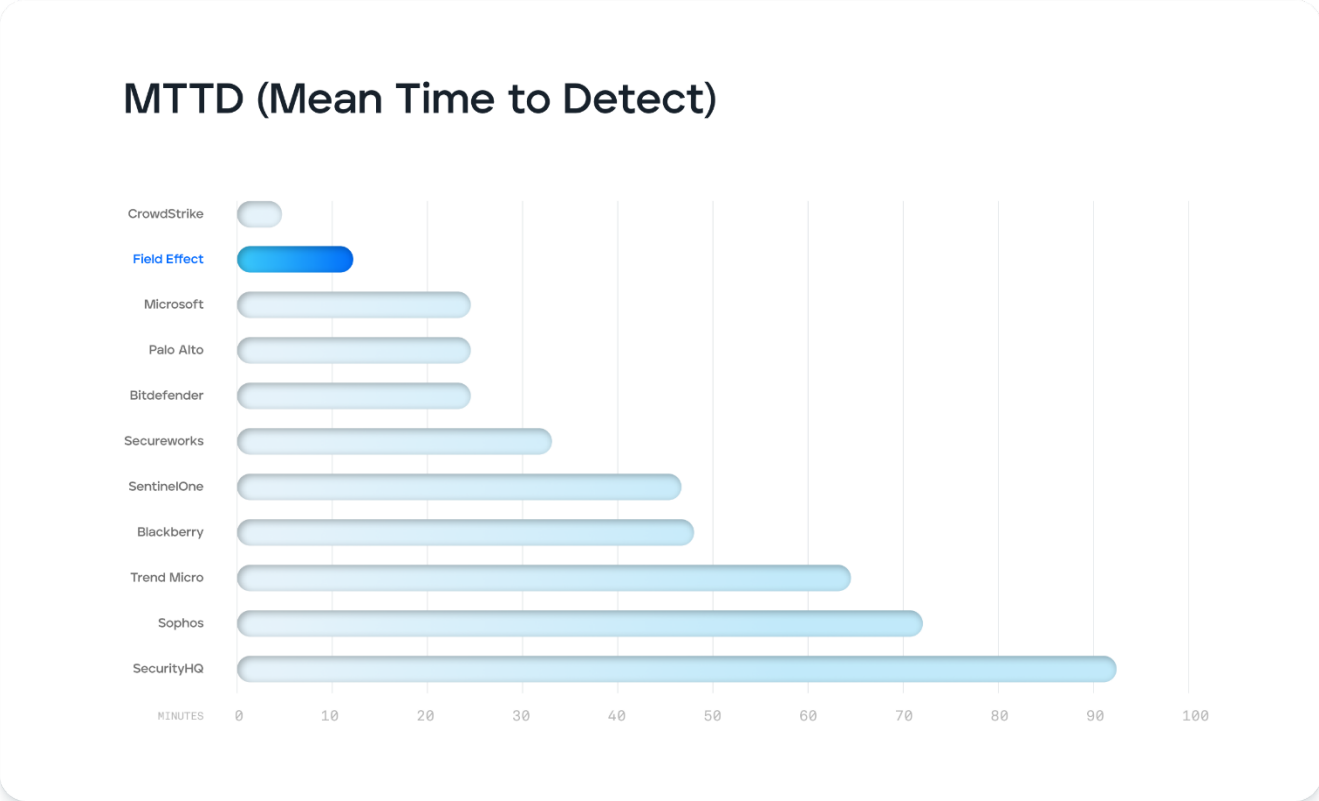
Stage of initial detection



Rapid threat detection

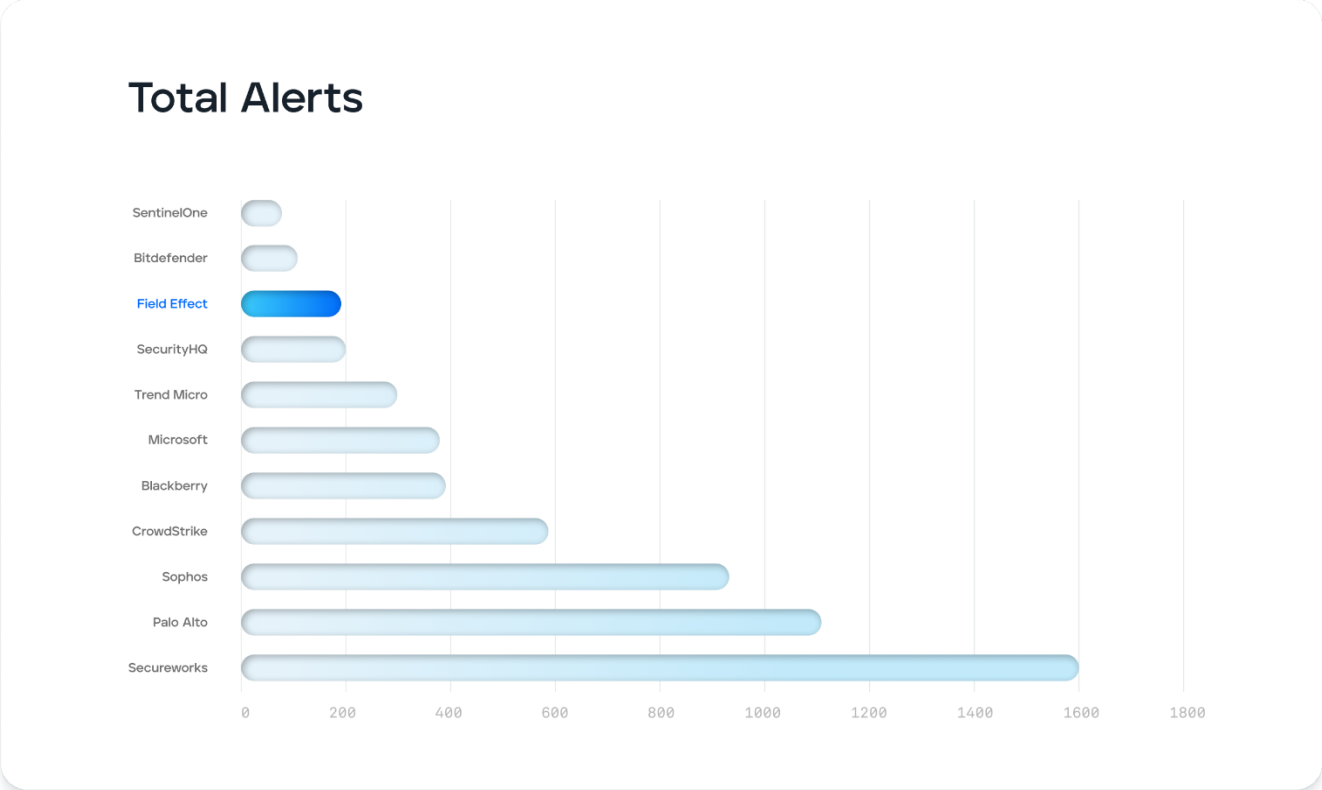
Field Effect MDR detected and reported malicious behavior at the earliest points during each step of the attack with a reported 11-minute MTTD, detecting the first sign of malicious activity in Step 1 in two minutes!

It is an unfortunate reality that any delay in the detection, reporting, and reaction to malicious behavior can lead to significant spread within your environment, increasing damage and operational disruption. Efficient, real-time threat detection capabilities like those exhibited by Field Effect MDR maximizes protection and leaves peace of mind.



Noise-free

Field Effect MDR demonstrated a low volume of alerts throughout the ATT&CK® Evaluations, which is consistent with our approach to cybersecurity.



Field Effect MDR not only provides a high level of alert fidelity but also eliminates unnecessary noise that—for an SME and MSP audience—may be overwhelming and complex. This means that Field Effect will only share information that is relevant and meaningful to our clients, while our expert-led SOC takes on the role of triaging the full scope of relevant data so we can detect and contain threats on our clients' behalf.

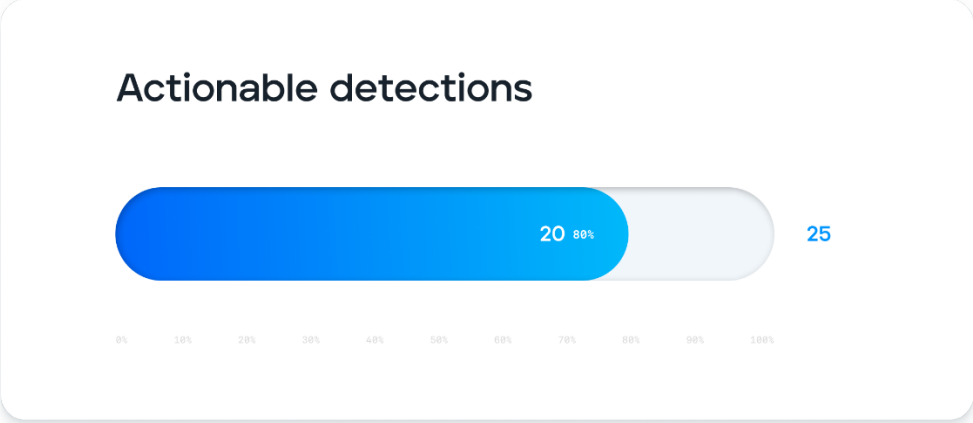
While Field Effect MDR reported one of the lowest levels of alerts in the MITRE evaluation, it was still much higher than our typical deployment. Due to the methodology behind the security simulation, we were not able to access a reliable record of historical activity nor interact with the MITRE team, which is essential to an effective, low-noise, managed service.

To achieve marks early in the attack lifecycle and accommodate the ATT&CK Evaluation's rules, Field Effect shared AROs that reviewed individual tactics and techniques identified rather than our typical summarized approach.

Field Effect MDR's total of 98 AROs were shared both via email and through our portal, for a total of 196 alerts. Had this scenario been a real-life attack, clients would've received fewer than 20 AROs total.

Actionable alerts

Throughout the ATT&CK Evaluation, Field Effect delivered simple and actionable alerts designed for users of all technical backgrounds. We included jargon-free language to describe malicious tactics and techniques identified within the system and shared actionable recommendations to remediate them.



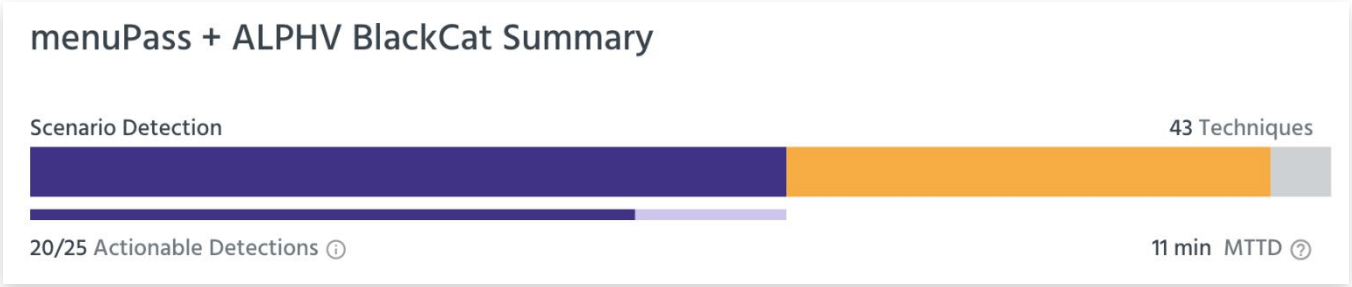
In some cases, the ATT&CK Evaluation team assessed vendors for granular details surrounding the tactic and technique as well as industry terms that Field Effect intentionally excluded due to our policy of jargon-free and straightforward alerting. While this cyber-speak is understood by SOC analysts, it may lead to confusion for our SME audience.

Dissecting our detection rate

Field Effect MDR was built to provide the best level of protection for our clients, which requires a focus on early detection and containment. For our clients, this means preserving business continuity and ensuring that – if they were attacked – they can react as quickly as possible.

As most of the SME market have limited in-house cybersecurity expertise, Field Effect has purpose-built our managed service solution to not only provide a sophisticated level of defense but also deliver it in a way that is noise-free and easy to operate for users of all technical backgrounds.

While we detected critical sub steps in the ATT&CK Evaluation that would be required to neutralize a real-life attack early, our approach to delivering AROs to our clients meant we did not report on all detections evaluated by the MITRE team. Reporting on these tactics and techniques would lead to unnecessary noise and confusion for our target audience and—in some cases—goes against our cybersecurity principles.



Reporting on malicious behavior within Windows processes

In several detections, the MITRE Engenuity ATT&CK Evaluation assessed vendors for their ability to report on malicious behavior happening within Windows processes, which would require vendors to inject code into these processes. Microsoft recommends against this approach as it leads to unexpected business application behavior and operational disruptions for clients.

From Field Effect's perspective, the additional security detections garnered from being in a process do not justify the impact to performance and stability. We ensure that our detections are robust enough to detect malware early in the attack lifecycle, without needing the high-cost security data from user mode processes.

Reporting on behavior, beyond the scope of Field Effect MDR

The ATT&CK Evaluations assessed vendors as if they were reporting to cybersecurity analysts. For some sub steps, this included providing an in-depth analysis of attack behavior at a level of detail that is deliberately excluded from Field Effect client reports as it introduces intense complexity without added benefit to remediation efforts.

While detections like these may benefit an enterprise-level SOC responsible for managing the entire threat lifecycle, Field Effect's clients rely on us to detect and neutralize threats at the earliest stages of an attack, triaging and consolidating relevant information, all while providing the level of detail needed to effectively understand and respond to the threat.

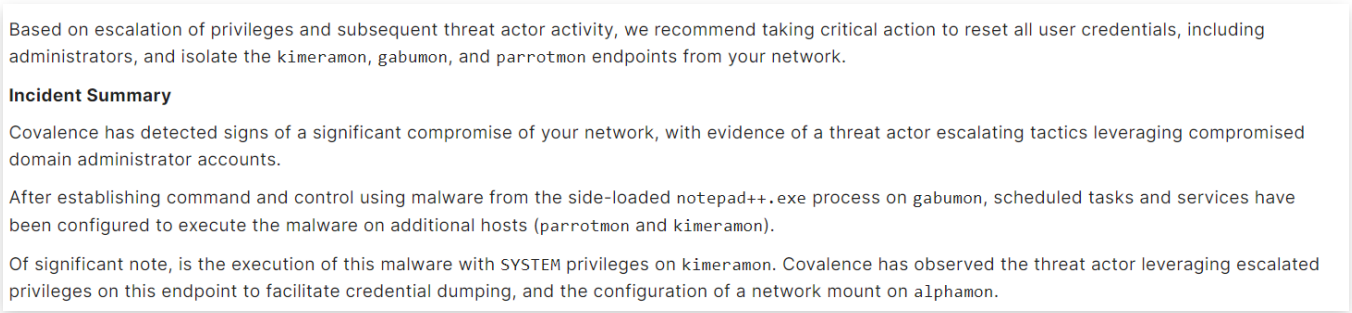
Field Effect clients desiring a deeper level of detail can access an alert dashboard, but this feature is infrequently utilized as our clients tend to leverage our AROs as the primary source of contextualized alerting. Following a cybersecurity incident, clients who require deeper investigation than that which is provided in Field Effect MDR can access Field Effect's Incident Response Services.

Reporting on complex industry jargon

In several detections, MITRE awarded a detection as "reported" only if specific cybersecurity terminology was included, an approach that sits in conflict with Field Effect's policy of jargon-free reporting. While we detected and reported on the activity within several tactics and techniques, we missed out on detections (and actionability) because of this.

For example, in detection 5.a.4 - Exfiltration Over C2 Channel (T1041), MITRE required the term "Exfiltration" to be specified within our AROs to be considered reported.

Field Effect reported that domain credentials were compromised, using clear language that is easy for the SME to understand, sharing a full overview of all sub steps within Step 5 as well as remediation instructions.



Based on escalation of privileges and subsequent threat actor activity, we recommend taking critical action to reset all user credentials, including administrators, and isolate the `kimeramon`, `gabumon`, and `parrotmon` endpoints from your network.

Incident Summary

Covalence has detected signs of a significant compromise of your network, with evidence of a threat actor escalating tactics leveraging compromised domain administrator accounts.

After establishing command and control using malware from the side-loaded `notepad++.exe` process on `gabumon`, scheduled tasks and services have been configured to execute the malware on additional hosts (`parrotmon` and `kimeramon`).

Of significant note, is the execution of this malware with `SYSTEM` privileges on `kimeramon`. Covalence has observed the threat actor leveraging escalated privileges on this endpoint to facilitate credential dumping, and the configuration of a network mount on `alphamon`.

What did we learn?

MITRE Engenuity's ATT&CK Evaluations provided Field Effect a rare opportunity to experience and observe an end-to-end attack in a real-life deployment, guided by MITRE. Instead of cutting off the attack at the earliest stage, the evaluation exposed areas which could provide our internal SOC with greater visibility into in-progress attacks in a way that still best serves our SME market.

Throughout the ATT&CK Evaluation, it was clear that some of the philosophies that make Field Effect MDR ideal for the SME market impacted our ability to be assessed as having "detected" adversarial behavior according to MITRE's criteria (which caters to enterprise-level SOCs.) Having participated in this year's evaluation, we have been able to identify areas where we can alter our service to better align to the evaluation, while keeping our service to SMEs consistent with our approach.

Get a complete defense with Field Effect MDR

While Field Effect MDR provided complete coverage as well as fast and purposeful alerting on the endpoint through the ATT&CK® Evaluations: Managed Services, our endpoint coverage only represents a small component of our overall solution, purpose-built for SMEs and the service providers that protect them.

Holistic defense

Detect, respond, and recover from threats while proactively reducing risk across endpoint, network, and cloud. Replace 15+ tools and services with one natively built solution, delivering better and faster cybersecurity.

Actionable alerting

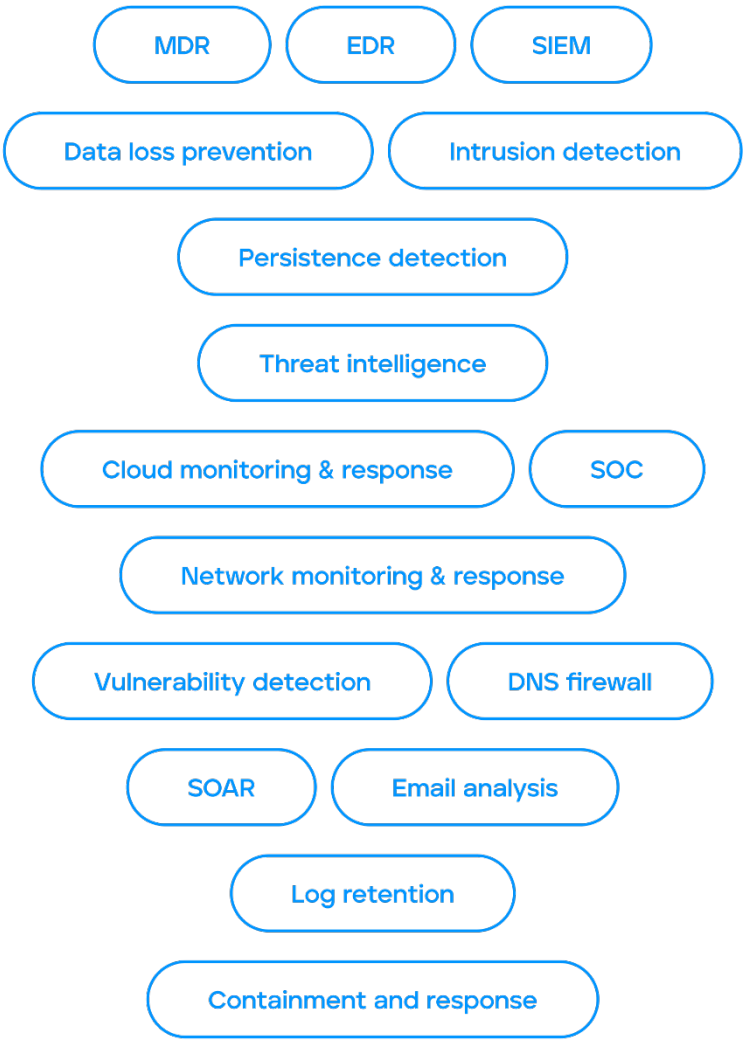
Cut through the alert noise with Field Effect's Actions, Recommendations, and Observations (AROs), telling you in simple terms what threat is present, how you can remediate, and where you need to focus first.

24/7 monitoring and support

Extend your team with world-class experts that will monitor your environment around the clock, responding to threats on your behalf and providing support with the click of a button.

Real-time response

Automatically neutralize threats, according to your unique preferences. With several options, from automated to manually verified, you can balance business continuity and risk management effectively.



Profound simplicity, powerful cybersecurity.

Field Effect MDR is an advanced cybersecurity solution that monitors and protects your entire threat surface—endpoints, networks, and cloud services—all from a single platform. No add-ons, no modules, and no gaps in your security. Field Effect MDR not only monitors every aspect of a business's threat surface, but reduces alert fatigue and false positives by aggregating data from multiple security events into simple, actionable remediation steps.

FIELD EFFECT / MDR

About Field Effect

Field Effect believes that businesses of all sizes deserve powerful cybersecurity solution.

Our threat detection, monitoring, training, and compliance products and services are the result of years of research and development by the brightest talents in the cybersecurity industry. Our solutions are purpose-built for SMBs and deliver sophisticated, easy-to-use and manage technology with actionable insights to keep you safe from cyber threats.

Contact our team today.

Email:
letschat@fieldeffect.com

Phone:

CANADA + UNITED STATES
+1 (800) 299-8986

UNITED KINGDOM
+44 (0) 800 086 9176

AUSTRALIA
+61 1800 431418