



AN INTEGRATED APPROACH WITH CYMULATE MITRE FRAMEWORKS

DAVID NEUMAN, SENIOR SECURITY ANALYST, TAG

This joint technical report from TAG and Cymulate explores the benefits of integrating MITRE frameworks and the Cymulate platform for more effective cyber defense and organizational resilience.

INTRODUCTION

In cyber defense, it is essential to continually adapt and refine strategies to address the ever-evolving threat landscape. With over 38 years on the frontline of cybersecurity, I've observed the transformation from basic network defense to advanced threat hunting. The inception of [MITRE ATT&CK](#) and the recently introduced [MITRE Engage](#) framework have further expanded the horizon of defense strategies. The ATT&CK framework, with its adversary-centric approach, has offered unparalleled insights into potential threats. However, with the introduction of Engage, focusing on the defender's perspective, a novel dimension has been added to cyber defense. While some critics argue that the additional layer Engage introduces might complicate cyber defense operations, if employed in the proper context, Engage can be a game-changer. The amalgamation of Engage, ATT&CK, and Attack Surface Management (ASM) ensures an enterprise is hardened, resilient, agile, and primed to counter sophisticated threats. There are several beneficial outcomes of a unified approach:

Defining Success in Cyber Defense Operations: Success in cyber defense is no longer just about preventing breaches; it's about how quickly and efficiently we can detect, contain, and mitigate them. With its defender-centric approach, Engage provides a robust framework for achieving these goals, enhancing our success metrics.

Focus on TTP Countermeasure Development: Adversaries are ever-evolving, and so should our countermeasures. By integrating insights from both ATT&CK and Engage, defenders can develop proactive strategies against specific TTPs, making our defense mechanisms more targeted and effective.

Continuous Training for Defenders: With the complex landscape of tactics and techniques outlined in Engage and ATT&CK, defenders are equipped with a vast knowledge base. It is paramount to invest in continuous training, ensuring they are always at the forefront of understanding and countering threats.

Deep Integration of Engage, ATT&CK, and ASM: These frameworks, when isolated, offer valuable insights. But when integrated, they provide a holistic view of the cyber defense domain. ASM focuses on reducing vulnerabilities by identifying potential threat vectors, ATT&CK offers insights into adversary behaviors, and Engage provides strategies for active defense. The confluence of these three ensures a layered, in-depth defense strategy.

This report will explore a comprehensive cyber defense strategy with the following objectives:

- Understanding the characteristics of MITRE Engage and ATT&CK and the integration with ASM.
- Challenges and opportunities of using MITRE's Engage.
- When and how Engage can be used in conjunction with an ASM platform.
- Final considerations on how to best defend your enterprise.

UNDERSTANDING THE CHARACTERISTICS OF ENGAGE, ATT&CK, AND THE INTEGRATION WITH ASM

In the ever-evolving cybersecurity domain, three primary approaches consistently stand out as cornerstones: MITRE ATT&CK, MITRE Engage, and ASM. To harness the unparalleled potential of their synergy, it's crucial to navigate the intricacies of each.

MITRE's ATT&CK framework operates as a groundbreaking shift in cybersecurity. It functions as a near-exhaustive database, precisely cataloging the tactics, techniques, and procedures (TTPs) cyber adversaries employ. At its core, ATT&CK provides a technical roadmap for analysts, illuminating every stage of a cyber-attack from inception to culmination. It equips the industry with a systematic lens to anticipate and comprehend threat behaviors.

Parallel to this adversary-centric model, MITRE Engage emerges. Engage, in its essence, represents the next phase, pivoting from merely understanding threats to actively countering them. While ATT&CK deciphers the "how" of cyber-attacks, Engage addresses the "how to counter." It outfits defense teams with diverse strategies, allowing them to interact with, redirect, and even confront threats in real time. Through Engage, the traditional defense paradigm transforms, incorporating a layer of active defense. [insert sentence with a few examples of what's in in Engage and how it maps to ATT&CK tactics and techniques.

Concurrently, ASM addresses the vast expanse of vulnerabilities in technology and processes inherent in an organization's digital infrastructure. The ASM model focuses on systematically identifying and analyzing these weak spots. ASM perpetually assesses and strengthens these points by operating across an organization's digital assets, from on-premise systems to cloud integrations, ensuring threat actors encounter minimized entry routes.

In their collective application, the capabilities of ATT&CK, Engage, and ASM establish formidable defensive mechanisms. The integration of Engage into the ASM framework means that vulnerabilities aren't merely identified and patched; they transform into strategic engagement points for understanding and countering adversaries. By harnessing ATT&CK's insights, defense teams actively anticipate potential threat vectors. Using Engage, they strategize to challenge or divert these threats, enhancing their defense depth.

The real-time collaboration of ATT&CK, Engage, and ASM delivers a multi-layered approach to cybersecurity. By understanding threats, engaging them head-on, and systematically curtailing vulnerabilities through prioritized mitigation, organizations craft an anticipatory and active cyber defense. This multi-faceted defense approach remains crucial for organizations to maintain a resilient digital stance amidst today's dynamic cyber challenges.

CHALLENGES AND OPPORTUNITIES IN THE REALM OF MITRE ENGAGE

In the sprawling panorama of cyber defense, the MITRE Engage framework emerges as a pioneering beacon, simultaneously introducing novel opportunities and intricate challenges. As we navigate this landscape, it becomes imperative to address the dual nature of Engage, dissecting its complexities while also appreciating the potential it unlocks.

At the outset, Engage's emphasis on active defense and adversary engagement diverges from traditional defense mechanisms, thrusting organizations into the relatively uncharted territory of proactive cyber warfare. This shift brings with it inherent challenges. Engage's strategies, by nature, are more aggressive and interactive, urging defense teams to repel adversaries and engage, redirect, and sometimes even ensnare them. While conceptually appealing, this approach necessitates an intricate understanding of the cyber adversary's mindset, capabilities, and intentions. Without this expertise, there's a potential risk of missteps—be it prematurely revealing one's defense strategies or inadvertently amplifying the attack surface.

Furthermore, the complexity of the Engage framework demands a significant upskilling of the cybersecurity workforce. Implementing its techniques requires personnel who are technically proficient and adept in strategy and tactics. Organizations must invest in continuous training and simulations to ensure their teams can harness Engage's full potential.

However, it's within these challenges that Engage's unparalleled opportunities lie. By championing the cause of active defense, Engage allows organizations to shift from a passive, reactive stance to one of anticipation and initiative. Instead of merely waiting for threats to manifest, defenders proactively seek out adversaries, often gaining critical intelligence. This proactive approach provides invaluable insights into an adversary's TTPs and disrupts their operations, reducing their overall efficacy.

Moreover, the very act of adversary engagement acts as a deterrent. When adversaries realize they're contending with an active defense system, they're more likely to reconsider their attack vectors or abandon their campaigns altogether. This psychological edge, paired with the tangible intelligence gained through engagements, can dramatically enhance an organization's security posture.

While the Engage framework introduces complexities that demand careful navigation and a commitment to workforce development, its potential benefits are profound. By embracing the opportunities Engage presents, organizations can transition from mere defense players to strategic cyber warriors, actively shaping the battlefield and redefining the rules of engagement.

INTEGRATING ENGAGE WITH THE CYMULATE PLATFORM: A TECHNICAL BLUEPRINT FOR ENHANCED DEFENSE OPERATIONS

The confluence of MITRE's Engage framework with [Cymulate's](#) platform promises to redefine defense dynamics. As organizations strive to fortify their digital infrastructures, understanding when and how to harness the combined might of Engage and Cymulate becomes critical.

Within cyber defense, Cymulate continually monitors an organization's digital assets, taking the attacker's view to identify weaknesses that could serve as potential entry points for adversaries. Cymulate excels at identifying attack paths and validating attack feasibility. With the integration with Engage and its active defense methodologies, Engage transforms these identified vulnerabilities from mere points of weakness to potential engagement zones—areas where organizations can interact with and gain intelligence on cyber adversaries.

Scenarios Benefiting from the Engage-Cymulate Symbiosis:

- **Threat Hunting in Real-time:** While Cymulate highlights potential weaknesses, Engage can facilitate real-time threat hunting within these areas, actively seeking signs of adversary activity and intent.
- **Deception Operations:** Can create honeypots or decoy systems around the vulnerabilities identified by Cymulate, luring adversaries into controlled environments, thereby protecting genuine assets while gathering intelligence on attacker TTPs.
- **Incident Response Augmentation:** In security breaches, the insights gained from Engage can supplement Cymulate data, offering a more comprehensive understanding of the breach and facilitating quicker, more effective responses.

Seamlessly Integrating Engage within Cymulate: A Step-by-Step Approach:

- **Assessment & Alignment:** Start by cross-referencing the output of Cymulate tools against the components of MITRE Engage most important to the organization.
- **Define Interaction Protocols:** Establish clear protocols dictating how interactions with adversaries will be conducted to avoid potential escalations or unwanted disclosures before active engagement. Test those protocols with Cymulate automated red-teaming.
- **Integrate Data Streams:** Ensure a bidirectional data flow between Engage and Cymulate. Vulnerabilities identified by Cymulate should seamlessly feed into Engage for action, while insights from Engage should inform Cymulate's security assessments.
- **Continuous Training:** Given Engage's active nature, regular training sessions should ensure that defense teams can adeptly handle engagements, making the most of the intelligence gleaned.
- **Automate & Optimize:** Utilize automation tools to ensure that the Engage-Cymulate integration operates in real-time, with immediate actions taken based on the insights from both platforms.
- **Regular Review & Iteration:** Review the combined system's efficacy, updating strategies and tactics based on the evolving threat landscape and the intelligence garnered from engagements.

The synthesis of Engage with Cymulate offers organizations a proactive and enriched defense strategy. By identifying vulnerabilities and then actively leveraging them for engagement and intelligence, organizations can not only defend but also dictate the terms of cyber engagements, establishing a posture of dominance in the digital arena.

CRAFTING A COHESIVE DEFENSE STRATEGY: TAILORING ENTERPRISE PROTECTIONS IN TODAY'S DIGITAL LANDSCAPE

As enterprises navigate the multifaceted challenges of today's cyber environment, a holistic defense strategy—grounded in integrating MITRE's Engage framework, the Cymulate platform, and actionable insights—becomes the linchpin for digital security. Drawing from the intricate tapestry of the previous discussions, it is imperative to synthesize a consolidated approach, ensuring a robust defense posture tailored to the unique attributes of enterprises, irrespective of their scale or sector.

Consolidated Strategy:

Intelligent Integration: The heart of a modern defense strategy lies in the intelligent integration of frameworks. Organizations craft a two-pronged defense by melding the proactive adversarial engagement of Engage with the vulnerability management capabilities of ASM. While ASM continuously identifies potential vulnerabilities, Engage transforms these points from passive weaknesses to prescient engagement zones.

Active Defense Evolution: Traditional defense mechanisms predominantly operating in a reactive mode are no longer sufficient. Instead, organizations should emphasize real-time threat hunting, deception operations, and incident response augmentation—all hallmarks of the Engage approach—to actively confront and confound adversaries.

Continuous Adaptation: In the cyber domain, static strategies are recipes for obsolescence. Defense mechanisms must perpetually evolve, informed by real-time data, emerging threat intelligence, and technological advancements.

Actionable Recommendations Tailored for Diverse Enterprises:

For Small to Medium Enterprises (SMEs):

- **Resource Optimization:** Given typically limited resources, SMEs should prioritize integrating scalable, cloud-based ASM solutions, complemented by select Engage techniques that offer maximum impact, such as deception operations.
- **Outsource when Necessary:** Consider leveraging Managed Security Service Providers (MSSPs) specializing in active defense to bridge the expertise gap without incurring substantial in-house costs.
- **Employee Training:** Human error remains a vulnerability even with the best systems. Regular cybersecurity awareness programs can mitigate this risk.

For Large Enterprises:

- **Holistic Integration:** With more extensive digital landscapes, these entities should aim to seamlessly integrate ASM platforms and the Engage framework, ensuring real-time data flows and automated responses.
- **Dedicated Threat Intelligence Teams:** Establish in-house teams focused exclusively on threat intelligence gathering and adversarial engagement, deriving insights from the Engage-ASM synergy.
- **Sector-specific Customizations:** Given their diverse operations, tailor defense strategies to sector-specific threats, be it financial fraud mechanisms for the finance sector or industrial control system attacks for manufacturing.

For Critical Infrastructure & High-risk Sectors:

- **Red Teaming & Simulations:** Regularly conduct advanced adversarial simulations with platforms like Cymulate to test and improve the defense posture, ensuring readiness against high-stakes attacks.
- **Deep Engagement:** Deploy advanced Engage techniques, such as active engagement zones and high-interaction honeypots, to gain granular insights into adversary TTPs.
- **Regulatory Compliance:** Ensure alignment with sector-specific regulatory guidelines, often more stringent given the elevated risks.

Enterprises must champion an equally dynamic defense approach as cyber threats grow in complexity and sophistication. By cohesively integrating the forward-leaning strategies of Engage with ASM's foundational strength and tailoring the blend to the unique requirements of different enterprise scales and sectors, organizations fortify their digital fortresses, prepared and proactive in the face of evolving digital threats.

CONCLUSION

In the contemporary digital era, the cyber realm is in perpetual flux, marked by relentless advancements and ever-mutating threats. The union of MITRE ATT&CK, MITRE Engage, and Cymulate signifies more than just a strategic collaboration; it epitomizes the forward-thinking mindset that organizations must adopt. As adversaries continue to innovate, so must we – to stay abreast and preemptively counteract emerging threats. By synchronizing the insights from these frameworks and tailoring their application to an enterprise's unique footprint, we don't just strengthen our cyber defenses; we revolutionize them. In this age of digital ubiquity, merely reacting is no longer sufficient; organizations must evolve, anticipate, and actively engage to safeguard their digital frontiers. The synthesis of these tools isn't just a recommendation – it's an imperative for a secure digital future.



(Reprinted from the [TAG Security Annual, 1st Quarter 2024](#).)