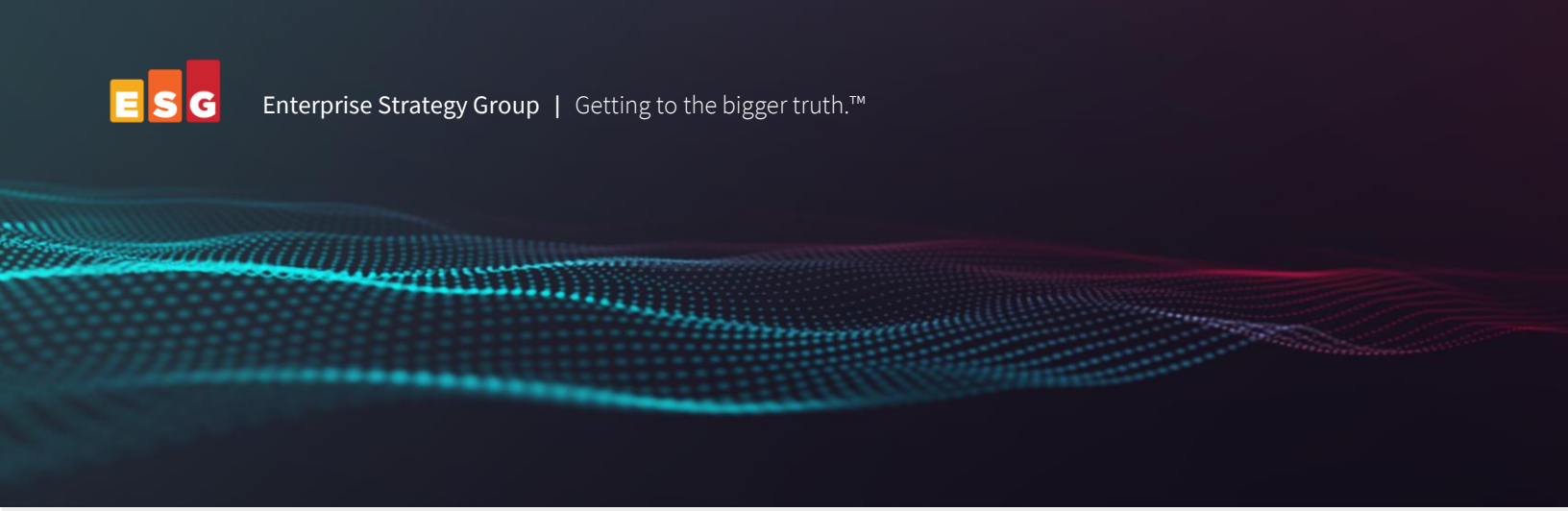


ESG WHITE PAPER

Cymulate: Helping Organizations Create a Threat-informed Cyber Defense

By Jon Oltsik, ESG Senior Principal Analyst and Fellow

November 2021

This ESG White Paper was commissioned by Cymulate and is distributed under license from ESG.

Contents

Executive Summary

The year 2021 has been fraught with costly cybersecurity incidents and data breaches. For example:

- Colonial Pipeline experienced a ransomware attack by a cyber-crime syndicate called DarkSide. This adversary stole nearly 100 gigabytes of data and threated to release the data unless the ransom was paid. In response to this attack, US gas prices rose by as much as six cents per gallon, and many gas stations faced supply shortages. Colonial Pipeline ended up paying $2.3 billion to the criminals to resume business operations.

- In March, Microsoft confirmed a cyber-attack by a Chinese hacking group called Hafnium. The attack utilized an Exchange software vulnerability and ultimately affected over 30,000 organizations across the United States, including local governments, government agencies, and businesses.

- In July, the DarkSide hacking group combined ransomware with a supply chain attack when it hit Kaseya, an IT solution developer for MSPs. The resulting outage not only affected Kaseya, it also affected it's MSPs' customers and subsequently their customers. An estimated 1500 companies in total were affected.

- These and many other notable cybersecurity events uncover a few certainties: 1) Every organization is vulnerable to cyber-attacks, 2) Current cyber-defenses aren't working well, and 3) Organizations should heed the guidelines offered in the US president's executive order of improving the nation's cybersecurity by adopting standards and procedures for pen testing of software and IoT devices.

This reality has led to panic in the boardroom and executive suites, as business leaders wonder if their organizations are vulnerable to similar attacks. Terrified corporate boards demand responses, but CISOs can only speculate in many cases with lukewarm answers like, "I think so but can't be sure."

Why do cyber-defenses remain shrouded in ambiguity, and what can be done to introduce more certainty? This white paper concludes:

- The attack surface is broad and diverse. Organizations are adding new digital transformation applications, connecting to third parties, using DevOps playbooks to push out application changes, supporting growing populations of remote workers, and embracing cloud computing. These initiatives greatly increase their attack surface, making it harder to discover assets, track and remediate vulnerabilities, or monitor "security drift" as enterprise changes occur rapidly. Security teams must be able to do all these things—at scale.

- Cybersecurity remains fraught with too many challenges. Cyber-threat detection and response is constrained by limited visibility, data management challenges, and a state of constant firefighting. In aggregate, these challenges indicate that many organizations are simply unprepared for the tactics, techniques, and procedures (TTPs) used by cyber-adversaries as part of their attack campaigns, so they continue to layer on new defenses and hope for the best. Therefore, CISOs offer educated guesses on whether the organization is vulnerable to the latest sophisticated cyber-attacks.

- Organizations need a threat-informed cyber-defense. Rather than continue with reactive measures, organizations must learn to "think like the enemy" and implement a threat-informed defense. In this model, cyber-defenses are designed as specific countermeasures to adversary TTPs. Additionally, security teams constantly test their defenses against adversary campaigns to validate controls/processes, identify gaps, and then create a plan to fortify their

defenses. A threat-informed defense creates a cycle where organizations gain attack surface visibility, operationalize the MITRE ATT&CK framework as a common language for threats, align adversary offensive tactics with security defenses, adopt processes for continuous security testing, and strive for continuous improvement.

A threat-informed defense can help organizations achieve multiple benefits by giving them the ability to evaluate/optimize security investments, validate defenses against the latest threats, and manage cyber-risks.

CISOs should consider anchoring this transition with breach and attack simulation (BAS) technologies, starting tactically and then moving on to a holistic threat-informed defense over time.

The State of Security Defenses

According to ESG research, 66% of organizations planned to increase cybersecurity spending in 2021, while only 3% claim that their cybersecurity spending will decrease.[1] Where will this spending be focused? Further ESG research indicates that 83% of organizations plan to increase spending on threat detection and response over the next 12 to 18 months.[2] Unfortunately, these spending increases are driven by the fact that existing threat detection and response processes and technologies are fraught with challenges such as (see Figure 1):

- A state of constant firefighting. Nearly one-third of security professionals (31%) admit that their organizations spend most of their time reacting to endless emergencies like DDoS events, ransomware attacks, or even data breaches. Not surprisingly, a perpetual state of emergency can not only burn out the security staff, but also means there's no time for strategic improvements to threat detection and response. In a situation like this, spending increases may provide some small improvements, but they won't alleviate a stressful and tactical "crisis management" cybersecurity approach.

- Limited security monitoring. Twenty-nine percent of organizations say that they have blind spots on their network, precluding the right level of visibility or correct data sources to defend against some advanced attacks. This gives adversaries a distinct advantage to cloak attacks, hide in the shadows, and circumvent controls. Aside from threat management, this lack of visibility can also lead to a state of enterprise drift. Asset configurations constantly change, driven by things like new CVEs, agile development practices, and a DevOps model. In this case, blind spots may lead to SOC teams missing this "drift" from approved configurations, increasing the risk of asset exploitation.

- Combining security data from a variety of sources. Twenty-three percent of organizations report that it is difficult to correlate and combine data from different security controls, which impacts threat detection and response efficiency. In other words, SOC teams are forced to spend hours of time on collecting, normalizing, deduplicating, and processing security data, impacting their ability to analyze and act upon the data. As a result, cyber-adversaries have ample "dwell time" to conduct malicious operations through the kill chain.

- Tracking progress through the lifecycle of a security incident. This challenge was cited by 22% of respondents. Tracking progress requires optimizing alerts for maximum attack visibility, understanding security control responses, and tracking responses with the right automated playbooks and incident response plans. When organizations are challenged in these areas, they miss critical clues or misclassify signals, since these are more prone to human error.

[1] Source: ESG Research Report, *2021 Technology Spending Intentions Survey*, January 2021.
[2] Source: ESG Master Survey Results, *The Impact of XDR in the Modern SOC*, February 2021. All ESG research references and charts in this white paper have been taken from this master survey results set, unless otherwise noted.

In addition to these challenges, recent research from ESG and the Information Systems Security Association (ISSA) indicates that 57% of organizations have been impacted by the cybersecurity skills shortage and 44% believe the skills shortage has gotten worse over the past few years.[3] This indicates that many organizations remain understaffed and lacking advanced security analytics skills, leading to overwhelming workloads, stress, and attrition. Since CISOs won't be able to hire their way out of these challenges, they must consider strategies to bolster staff efficiency and productivity.

Based on the ESG data, it's safe to conclude that threat detection and response is too reactive, haphazard, and resource intensive, leading to increasing cyber-risk and data breaches. Incremental changes won't do, CISOs need an alternative direction.

Figure 1. Threat Detection and Response Challenges

Source: Enterprise Strategy Group

What's Needed? A Threat-informed Defense

Time to 'Think Like the Enemy'

Historically, organizations built their defenses in reaction to periodic different types of threats—email threats, web threats, vulnerable assets, etc. This led to what most organizations have today—security technology silos layered on top of networks that now sprawl across hybrid IT. Regrettably, this leads to a situation where many organizations experience the threat detection and response challenges described above and have no idea whether their security defenses work as they are supposed to.

[3] Source: ESG Research Report, *The Life and Times of Cybersecurity Professionals Volume V*, July 2021.

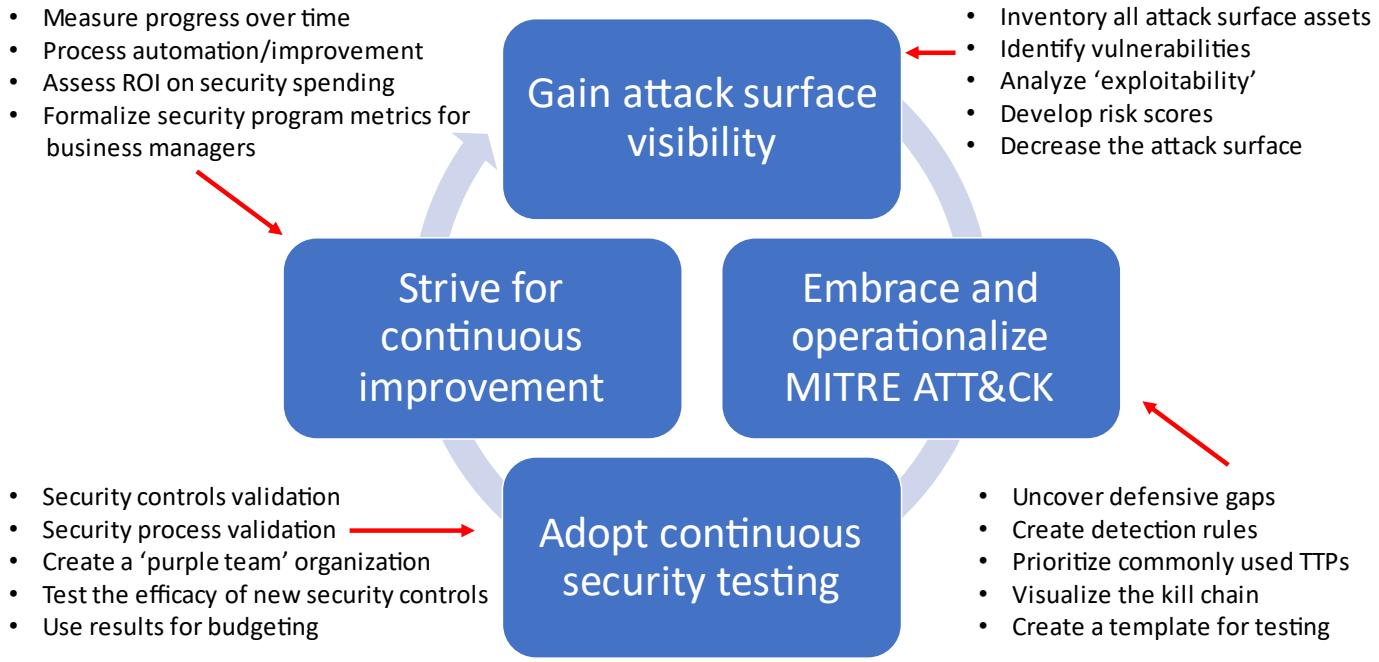
Famed physicist, Albert Einstein, is quoted as saying that the definition of insanity is doing something the same way and expecting different results, but that's exactly what many organizations continue to do with cybersecurity. Rather than layer on additional security tools, organizations need to "think like the enemy" and adopt a threat-informed defense.

Cybersecurity thought leader MITRE corporation defines a threat-informed defense as follows:

"'Threat-informed defense' applies a deep understanding of adversary tradecraft and technology to protect against, detect, and mitigate cyber-attacks."

Achieving a threat-informed defense requires organizations to adopt a lifecycle approach to cybersecurity based on 4 phases (see Figure 2):

Figure 2. Phases of a Threat-informed Defense



Source: Enterprise Strategy Group

- Gaining a complete inventory of the attack surface. To paraphrase an old management adage, "You can't secure what you can't measure." In other words, a threat-informed defense starts with an understanding of all assets present, including which ones may be vulnerable to attack and which of these are most likely to be exploited. Rather than analyze this data manually, SOC teams can also benefit from new types of technology that help calculate risks and guide them toward mitigation actions with the highest impact. Finally, security architects can use this input to help them implement least privilege policies and segment their networks, helping them decrease the attack surface.

- Adopting and operationalizing the MITRE ATT&CK framework. Large enterprises are using the MITRE ATT&CK framework as a reference architecture. To fully establish a threat-informed defense, however, organizations need to operationalize MITRE with tools that can analyze data and then present it in a MITRE ATT&CK context. By doing so, SOC teams can visualize the entire cyber-kill chain, uncover gaps (i.e., missing controls and/or data sources), and

create/tune detection rules that align with adversary TTPs targeting their industries. MITRE ATT&CK can also provide a template for ongoing security testing by emulating specific adversary behavior and campaigns.

- Embracing a perpetual testing regimen. Organizations understand that security testing (i.e., pen testing and red teaming) can help to validate security controls, test IR processes, and uncover coverage gaps. So, what's the problem? Many organizations only conduct these tests on a quarterly or biannual basis, the tests are expensive, and they are often outsourced to service providers with their own proprietary methodologies. Furthermore, security test results often present a list of problems but no analysis on which ones to prioritize or guidance on how to remediate them. To reap security testing benefits while addressing these issues, CISOs should strive for a perpetual testing regimen anchored by breach and attack simulation (BAS) technology. The best BAS tools emulate adversary behavior frequently to uncover true vulnerabilities, assess processes, validate controls, and pinpoint needs. Armed with BAS, security analysts can also adopt a "purple team" model where attackers design tests for exercising specific industry-focused attacks for controls validation, while defenders learn more about adversary TTPs and use this knowledge to design focused countermeasures.

- Developing a plan for continuous improvement. Aside from controls validation and fine tuning, organizations should also examine processes and team performance, looking for areas that need improvement. For example, security testing may uncover areas where IT operations teams have misconfigured security controls due to a lack of training or manual processes that act as a bottleneck for threat detection/investigations. CISOs should endeavor to uncover these weaknesses, develop plans for improvement, and then measure progress over time. This can also help pinpoint areas for security investment and measuring ROI on security budgets.

Making Threat-informed Defense Achievable

While a threat-informed defense grows more essential daily, implementing this type of strategy hasn't been easy in the past. Leading organizations with ample skills and resources could deploy and customize technologies for a threat-informed defense objective but most security teams didn't have the expertise or budgets to achieve this objective.

Recognizing impending market requirements, innovative technology vendors have introduced new types of threat-informed defense solutions, especially in areas like attack surface management and continuous security validation. While this progress is promising, the plethora of threat-informed defense options can be confusing for security professionals. To navigate through this confusion, ESG recommends that CISOs seek threat-informed defense solutions offering:

- Comprehensive coverage for multiple use-cases. The best solutions will include functionality for attack surface monitoring, breach and attack simulation, and continuous automated red teaming (CART). In other words, threat-informed defense technologies should support all phases defined above by mapping the entire attack surface, validating security controls, identifying high priority risks uncovered, suggesting the most efficacious remediation actions, and providing guidance through remediation tasks. Solutions should also help organizations operationalize the MITRE ATT&CK framework with the right visualization, reports, and guidelines.

- Rapid time to value for all types of users. Cloud-based solutions can help organizations greatly reduce deployment time and complexity while delivering near-term risk assessments, helping organizations create security baselines and identify high priority areas for remediation. The best solutions can deliver this valuable starting point and immediately assist on prioritization for global enterprises with ample security resources and smaller firms with limited security staff and expertise.

- Track trending over time. Once a baseline is established, threat-informed defense technologies should help CISOs monitor progress by aligning with MITRE ATT&CK and providing ample tactical and strategic test suites. For example, early tests should be focused on specific areas, testing configurations and detection rules on technologies like email gateways, web gateways, endpoint security software, and web application firewalls. Over time, SOC teams can move on to testing security controls by emulating adversary TTPs and campaigns. Finally, security teams will grow comfortable with continuous security validation, helping them find technology and process weaknesses on an ongoing basis. In this way, organizations will establish the visibility, reporting, and processes for continuous improvement.

Threat-informed defense technologies should not only improve security efficacy and operational efficiency, but also help organizations rationalize security controls, identify security investment priorities, and measure ROI over time.

Cymulate Supports a Threat-informed Defense

A threat-informed defense reverses the perspective with an outside-in approach to security defenses. As such, it is a new and somewhat confusing area, and many organizations will need guidance from industry experts and technology vendors. Cymulate, a breach and attack simulation vendor based in Israel, may be able to help shepherd through their uncertainty, acting as a threat-informed defense anchor. As a continuous security validation vendor, Cymulate supports the threat-informed defense phases described above, as it:

- Supports a plan for security hygiene and posture management. As part of its continuous security validation suite (which includes Contrinuous Automated Red Teaming), Cymulate performs attack surface management by evaluating external and internal reconnaisance it gathers and providing prescriptive remediation suggestions. Furthermore, Cymulate analyzes assets and determines whether they are vulnerable to attack in a prioritized fashion while providing suggestions for remediation. By doing so, organizations patch just what they need to when first- and third-party security controls can't provide coverage.

- Aligns and supports the MITRE ATT&CK framework for operationalization. Cymulate is designed to analyze and present data in a MITRE ATT&CK context, helping organizations understand adversary TTPs, visualize security controls alignment, validate security defenses, and identify areas of weakness. SOC teams can then operationalize the MITRE ATT&CK framework to bolster security efficacy and streamline security operations.

- Provides continuous testing and additional functionality. Aside from adversary emulation and MITRE ATT&CK synergy, Cymulate provides test suites for email gateways, web gateways, web application firewalls, endpoint security, data exfiltration, phishing, and full kill chain advanced persistent threats (APTs). In this way, Cymulate combines the benefits of BAS, application security monitoring (ASM), continuous automated red teaming (CART), and purple teaming.

- Can be used for continuous improvement for various use cases. As organizations embark on threat-informed defenses using Cymulate, they can introduce standard processes for controls validation, product testing, workflow assessment, etc. These tests can then be used to generate metrics for baselining, goal setting, and continuous improvement. CISOs can then share results with business executives, documenting current security status, future goals, and a roadmap to get there, measuring progress along the way.

It is also worth noting that Cymulate is cloud-based, so organizations can easily evaluate the products, gain insights, use the results to initiate a threat-informed defense program, and gain quick time to value. Furthermore, Cymulate can be utilized by organizations with varying levels of cybersecurity maturity. Beginners get clear explanations and threat-

informed defense as well as prescriptive remediation advice. Organizations with more advanced cybersecurity get detailed visibility into critical risks and controls gaps. This information can be shared with executives and then used as part of a risk mitigation plan.

The Bigger Truth

Cybersecurity is a constant cat and mouse game between cyber-adversaries and defenders. In this dynamic contest, adversaries constantly survey the battlefield, evaluate defenses, and adjust their tactics in response. While most defenders realize this, they are constrained with their countermeasures, often hamstrung by a lack of resources, knowledge, and time. As a result, cyber-defenders tend to simply layer on new defenses and hope for the best. Unfortunately, this leaves them with a growing level of cyber-risk and nearly defenseless against the latest cyber-attack campaigns.

Famed Chinese general and military strategist Sun Tzu is often quoted as saying, "If you know the enemy, and know yourself, you need not fear the results of a hundred battles." With a threat-informed defense, organizations base their defenses on specific TTPs used by cyber-adversaries. How? They do this by emulating adversary campaigns through continuous testing, analyzing the results to identify weaknesses and gaps, and then developing specific plans for fortification. They can then execute these plans as part of a cycle for continuous improvement.

Threat-informed defense may seem like an academic exercise, but organizations can now pursue this strategy through continuous testing with continuous security validation solutions like Cymulate. Given this, CISOs must lead the transition—from traditional security practices and "flying blind" to threat-informed defenses based on adversary behavior, ongoing testing, and a commitment to continuous improvement.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.

 www.esg-global.com

 contact@esg-global.com

 508.482.0188