Cymulate

15 Ways

Cymulate Increases Cybersecurity ROI

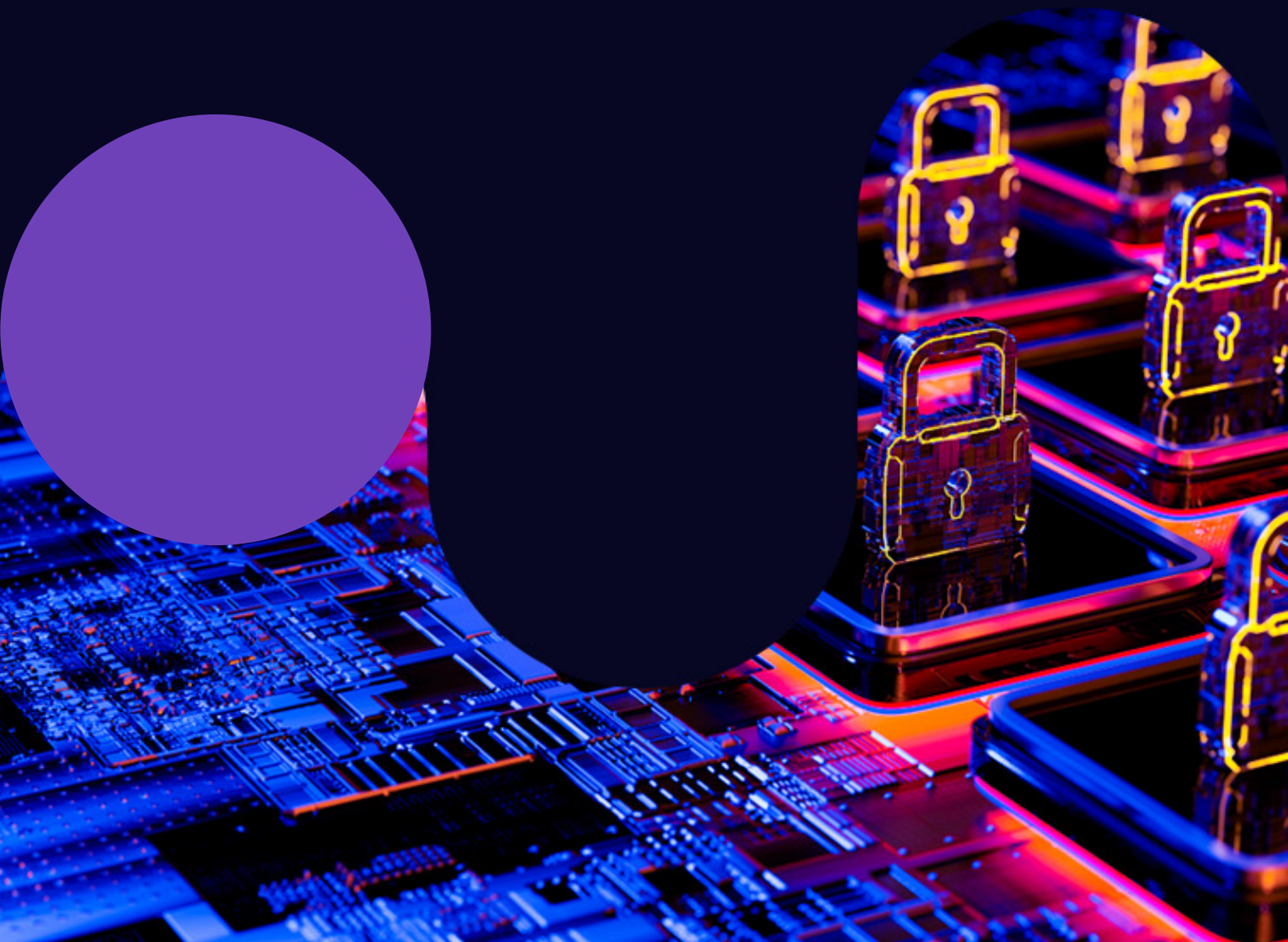


Table of Contents

Introduction

Ransomware and supply-chain attacks are currently the two leading contenders for mainstream news headlines and the number and complexity of cyber-attacks keep growing. Between the militarization of cyber-attacks and the lucrative cyber-crime revenues, their growth is likely to continue in the foreseeable future.

For organizations aware of this situation, the expansion of cyber-threats leads to an increase in cyber-security expenses. With both the risk to business as usual and the aggregated costs of successful breaches rise, the board is increasingly interested in obtaining a clear idea of their investment in cyber-security added value.
Yet, the responses they receive from their CISO of SOC head are often sorely lacking in specifics and metrics and, stuck in the middle, the executive leadership that typically lacks cyber expertise struggles to know what to ask and how to get the answer they need.
Even worse, with an average of 45 different security tools under management, organizations' SOCs are drowning in excessive complexity and lack the granular visibility needed to evaluate the efficiency of individual solutions in their tool stack. This often leads to overlapping capabilities generating duplicate, sometimes contradictory data and hides the absence of other needed functionalities, even though those might lead to unmonitored security gaps.
After a short reminder of the inherent issues in evaluating the value of risk reduction, this eBook examines the multiple ways continuous security validation and exposure management enable such an evaluation. Precise measurements also facilitate tool stack rationalization and optimization, resulting in a hardened and stabler security posture and security drift prevention.

Statistics vs. Cost vs. Risk vs. Value – The Quantification Conundrum

Though the cost of a cyber-security defense array – cybersecurity tools and solutions + security teams rising wages + IT team everlasting chase of vulnerability patching - is relatively easy to calculate, calculating defensive solutions value is far more complex. According to a 2021 report from IBM and the Ponemon Institute, the average cost of a data breach for the 500 leading companies surveyed reached $4.24 million per incident in 2021, the highest in 17 years. It seems tempting to use those figures to evaluate the defensive stack value by subtracting its cost from the corresponding estimated data breach cost for similar organizations.

Yet, that would also require knowing exactly how effective the Detect and Respond tools are effective in detecting and preempting attacks. In other words, what percentage of attacks they actually block. The efficacy of SIEM and SOAR arrays depends on selecting and enforcing adequate policies for each solution's security control. Penetration testing lacks the granularity needed to pinpoint which solution stopped what attack and the continuity required to continuously reassess resilience.

Effectively quantifying risk exposure requires continuously measuring the actual defense efficiency against cyberattacks. This requires integrating with a comprehensive security validation suite covering all potential security gaps, from exposed assets and initial foothold entry points to escalation, lateral movement, command execution, and data exfiltration.

How Cymulate Security Posture Management Platform Increases Security ROI

01

It optimizes existing defenses

Cymulate validates the efficacy of each SIEM and SOAR tool by correlating the number of production-safe attacks they detected, preempted, or mitigated. According to IBM's Cyber Resilient Organization Report, an organization uses an average of 45 security solutions from 13 different vendors. Each of these solutions has its own set of configurations, policies, and control settings, making it overly complex to assess whether they perform at their maximum capacity.

02

It maximizes in-depth visibility in a tool stack

Cymulate measures solutions' effectiveness, identifies security gaps and provides actionable remediation recommendations.

03

It rationalizes cybersecurity tool stacks

By comprehensively assessing each tool's effectiveness in detecting, stopping, or mitigating in-context production-safe attacks, Cymulate's platform identifies tools' overlapping capabilities and defines precisely which capabilities are missing.

04

It prioritizes patching and reduces emergency patching loads

Checking active environments' resilience with a comprehensive array of production-safe attacks identifies specifically which vulnerabilities are the most critical to patch. This Attack-Based Vulnerability Management (ABVM) approach prioritizes the patching schedule based on the actual risks to a specific environment. This new approach improves on legacy Vulnerability Management (VM) or even more advanced approaches such as Risk-Based Vulnerability Management (RBVM). RBVM evaluates the risk either exclusively based on risk scores such as CVSS or correlates those scores with other factors based on business context and other generic factors and factors based on statistical-based evaluations. In contrast, the vulnerability patching workload established by ABVM takes into account up-to-date, data-backed inputs such as systems' security controls' ability to compensate for even high-scored vulnerabilities. The streamlined patching schedule lightens the load on the IT team.

05

It preserves business continuity

In addition to strengthening resilience against known threats, the Cymulate platform's Immediate Intelligence Threat module activates the ability to rapidly assess cyber resilience against emerging threats and the continuous nature of the assessments prevents downtime - and waterfall loss of revenue – due to delayed or untested inadequate patching.

06

It prevents security drift

As the environment keeps evolving due to frequent deployments and new threats are emerging daily, a known healthy security posture based on annual or bi-annual validation can slowly or abruptly drift into a worsening condition unless the causes are spotted and addressed in real-time. Continuously running XSPM immediately detects security drift and enables correcting the new security gaps before the security posture shifts from a known good state to a bad state.

07

It provides metrics and traceability

Regardless of security programs' effectiveness, cybersecurity strategies are typically based on guesstimates established by statistically evaluating the impact of adherence on best practices and internal pressures, constraints, and politics. Cymulate's algorithm, on the other hand, calculates security scores using industry-recognized standards such as the NIST Risk Management Framework, CSVSS v3.0 Calculator, and Microsoft's DREAD and, most importantly, by correlating these values with the risks incurred in-context based on the percentage of detected and deflected production-safe attacks. The results are quantified based on measurable events, providing a reliable numerical score that can be used as a base to harmonize baselines and KPIs and monitor trending.

08

It optimizes the Security vs. Operability trade-off

An impenetrable security posture can only be achieved through impenetrable walls and total insulation from the external world. Unimpeded operability requires 100% open lines of communication and data transfer. Achieving a state of equilibrium that enables conducting business and provides an acceptable level of risk requires delicate negotiations between the CISO and executive leadership. The precise risk quantification provided by XSPM is a key factor in striking the optimal balance between risk and agility.

09

It reduces dependency on time-consuming and resource-heavy manual methods

Manual security validation methods such as pen testing or red teaming are time and resource-heavy, and costly. In addition, the quality of the testing performed varies according to the pen tester or the red team's skills.
Even worse, even highly skilled pen testers now have to compete with the AI/ML offensive tools available to cyber-attackers and need to be proficient in every one of the hundreds of attacks tactics, techniques, and procedures already listed on MITRE and other repositories and keep up with emerging threats. By operationalizing listed and emerging TTS with both MITRE and NIST matrixes, Cymulate eliminates reliance on manual validation.

10

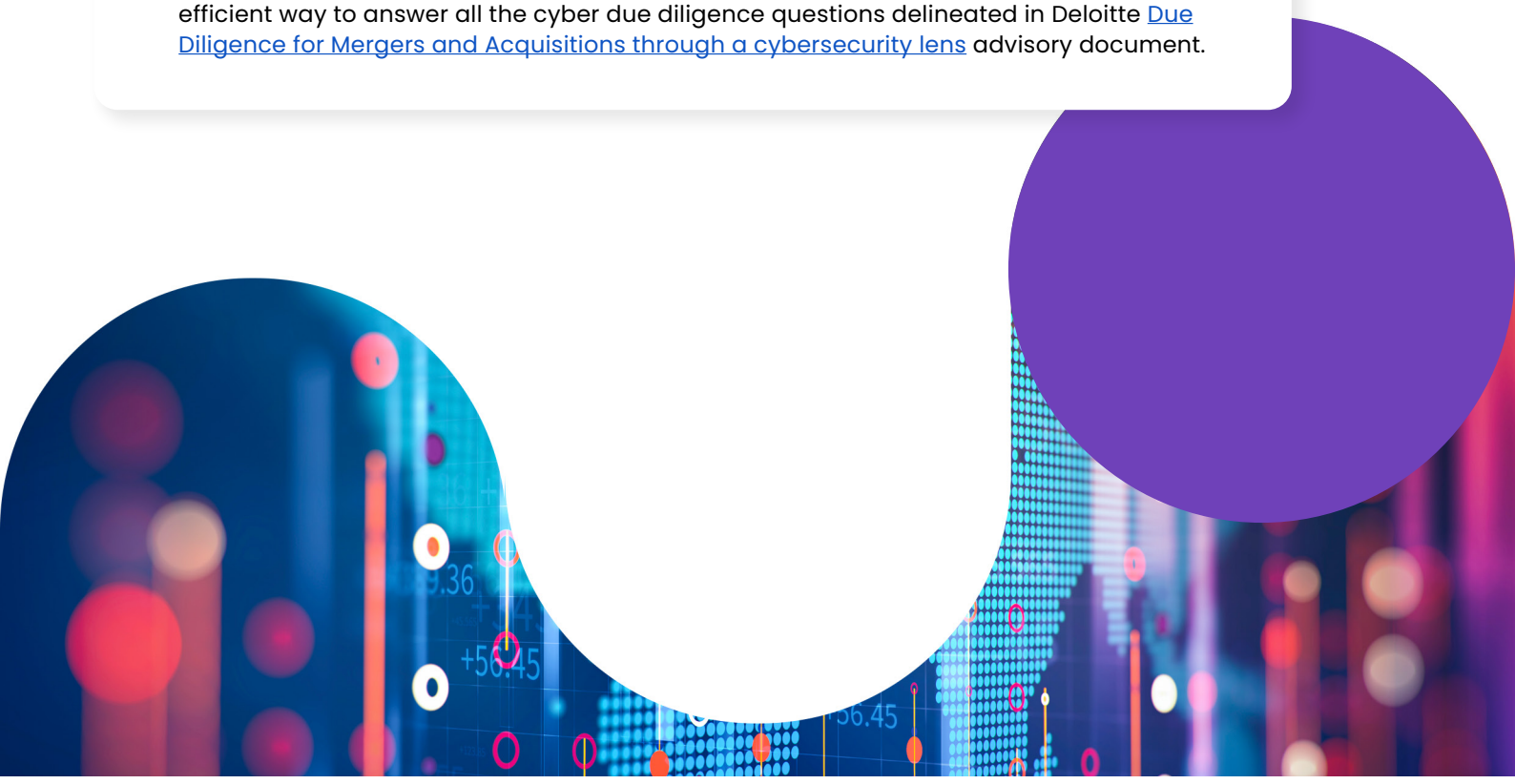
It enables data-driven decision-making

An additional benefit of having access to fact-based, quantified data is the ability to make informed decisions. It answers Jeff Pollard, Forrester's VP and principal analyst, requirements about metrics: "We're always looking at information and making decisions, that's why security leaders need great metrics. If your metrics don't allow you to do that, then you know they're not worthwhile. So, then you need to create metrics that let you make decisions."

11

It facilitates M&A cyber due diligence of prospective acquisition

Aside from past cyber history and HR-related questions, Cymulate platform is a simple and efficient way to answer all the cyber due diligence questions delineated in Deloitte Due Diligence for Mergers and Acquisitions through a cybersecurity lens advisory document.



12

It reduces cyber-insurance costs

Cyber insurance companies are slated to shift their requirements from asking attestation to requiring organizations to document that the controls they claim are in place are indeed installed and effective. Cymulate goes beyond these upcoming requirements and provides documented proof that the controls are indeed in place, continuously tested, and preventing security drift.

13

It helps obtain investments

With cybersecurity ranking second of the top 5 concerns of potential investors, the ability to provide an in-depth, quantified evaluation of cyber resilience, document variance from established baselines and security drift, reassure them about resilience to emerging threats, demonstrate the ability to vet prospective vendors for cyber risk, etc. Cymulate provides and documents all of these and more.

14

It is assessment compliance future-proof

As technologies evolve and regulators attempt to ensure the regulations remain relevant, the extent of risk assessments required by compliance regulators will probably keep widening. Named Innovation Market Leader by Frost Radar™ Breach and Attack Simulation, Cymulate platform covers the most advanced continuous security validation technologies and automatically generates comprehensive risk assessment reports with a level of detail considerably superior to the current - and foreseeable future – regulators' demands. Already today, it generates fully documented updates at any time without needing to divert resources to produce the required information, and the depth of security validation assessment it provides is already far more comprehensive than current requirements, hence ahead of future requirements.

15

It reduces cyber employees' burnout and churns

Aside from chronic understaffing, alert fatigue, increased complexity, and highly repetitive task loads are the main factors behind cyber staff burnout. By shrinking the number of false-positive alerts, rationalizing the tool stack, and automating the majority of repetitive tasks, Cymulate reduces the load of tasks with a negative impact on cybersecurity staff, freeing their time to conduct more high-level risk analysis and improving their job satisfaction level, thus reducing employee turnover.

Aside from providing reliable resilience data to continuously validate organizations' risk exposure assessment and recommend focused mitigation advice to tighten security posture, Cymulate platform provides metrics to effectively measure cyber-security tool stack ROI. It also provides granular quantified data to improve these tools' efficiency and ROI and rationalize the defensive solution stack as a whole.

What are the five pillars of Cymulate Security Posture Management Platform?

01

Attack Surface Management (ASM)

Emulating an attacker during the reconnaissance phase, where they perform a comprehensive analysis on their target organization. ASM tools scan the domains, sub-domains, IPs, ports, etc., for internet-facing vulnerabilities. It is also looking for Open-Source Intelligence (OSINT) that can later be used in a social engineering attack or a phishing campaign. This tool helps organizations understand how hackers might get an initial foothold.

02

Automated Red Teaming

Automated Red Teaming campaigns go beyond just the reconnaissance page to answer the question: "how can an adversary breach my defenses?"
These end-to-end campaigns attempt to penetrate the organization by analyzing exposed vulnerabilities and autonomously deploying attack techniques that penetrate the network. For example, they can trigger the attack with a well-crafted phishing email. After gaining the initial foothold, the attack subsequently propagates within the network in search of critical information or assets.

03

Breach Attack Simulation (BAS)

Breach and Attack Simulation tools answer the question: "how well are my security controls and processes performing?"
It launches simulated attack scenarios out-of-the-box and correlates findings to security controls (email and web gateways, WAF, Endpoint, etc.) to provide mitigation guidance. These are primarily used by the blue team to perform security control optimization.

04

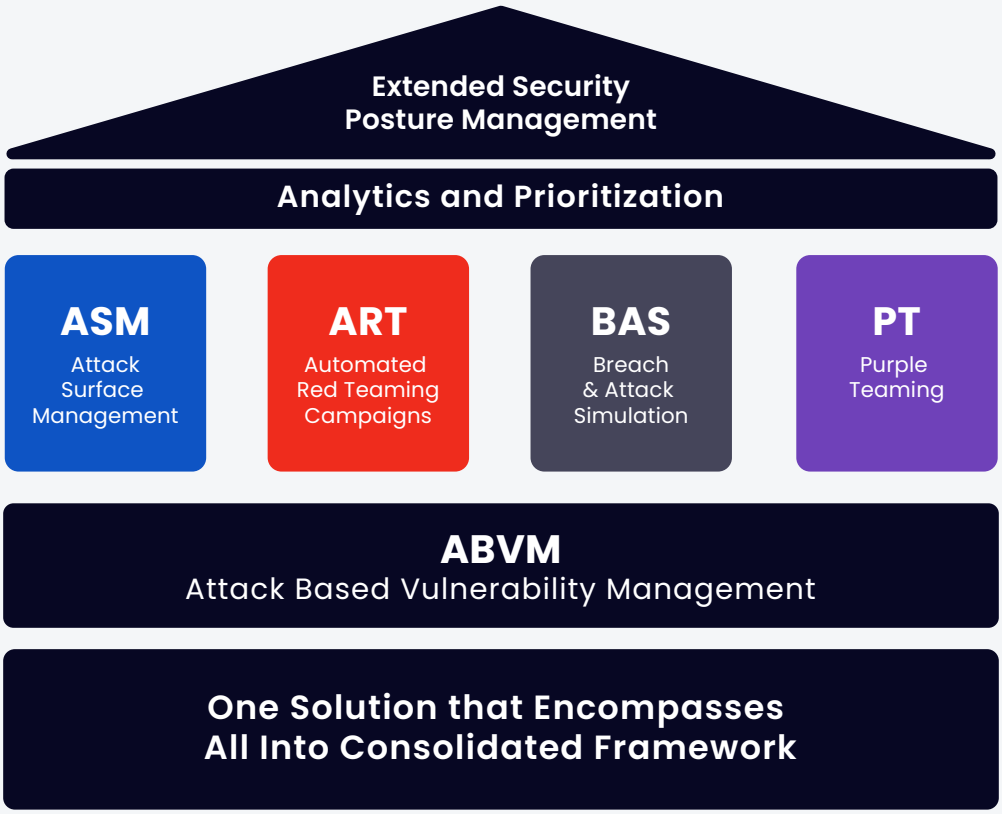
Advanced Purple Teaming

Purple teams expand BAS into the creation and automation of custom advanced attack scenarios. These tools usually extensively leverage the MITRE ATT&CK® framework, enabling advanced security teams to create complex scenarios from predefined resources and custom binaries and executions. Custom scenarios can be used to exercise incident response playbooks, pro-active threat hunting, and automate security assurance procedures and health checks.

05

Attack-Based Vulnerability Management (ABVM)

Relieve the chronic vulnerability patching overload chronically afflicting IT teams by drastically reducing the number of critical patches required. ABVM checks which vulnerabilities are effectively compensated for by the defensive array and deprioritizes them, focusing the patching effort on vulnerabilities that effectively endanger an organization's infrastructure.



About Cymulate

The Cymulate SaaS-based Security Posture Validation Platform provides security professionals with the ability to continuously challenge, validate and optimize their on-premises and cloud cyber-security posture with end-to-end visualization across the MITRE ATT&CK® framework. The platform provides automated, expert, and threat intelligence-led risk assessments that are simple to deploy, and easy for organizations of all cybersecurity maturity levels to use. It also provides an open framework for creating and automating red and purple teaming by generating tailored penetration scenarios and advanced attack campaigns for their unique environments and security policies.

Contact us for a live demo, or get started with a free trial

Start Your Free Trial

info@cymulate.com | www.cymulate.com