REPORT REPRINT

Cymulate scales red teaming activities with continuous attack simulations

NOVEMBER 18 2019

By Patrick Daly

The company focuses on improving organizations' security postures through continuous testing and validation of security control effectiveness, using simulated attacks mapped to the MITRE ATT&CK framework. Cymulate's breach and attack simulation platform aims to help firms measure the efficacy of their security controls, and evaluate new security investments.

451 Research®

Introduction

Although the security skills shortage has been well documented over the years, it remains a salient problem for the majority of enterprises – 66% of respondents to 451 Research's Voice of the Enterprise: Information Security, Organizational Dynamics 2019 survey still say they do not have enough information security personnel on staff, and 33% specifically cited penetration testing skills as inadequately met in their organization. To fill this gap, companies often outsource penetration tests and other red team activities, though the high cost of these efforts can limit an organization's ability to measure its security posture and the effectiveness of its security tools on a regular basis.

The breach and attack simulation (BAS) market emerged, in part, to reduce organizations' dependence on outsourced security assessments, such as penetration testing and red teaming engagements, with the vision to make it possible for any organization to test its security with the highest levels of offensive technology and know-how. This facilitates remediation actions such as properly configuring security tools, and more efficiently assessing and reducing the organization's exposure to external threats. Cymulate is one such vendor focused on improving organizations' security postures through continuous testing and validation of security control effectiveness using simulated attacks mapped to the MITRE ATT&CK framework.

451 TAKE

BAS may become an important way for organizations to keep pace with evolving IT environments and a rapidly changing threat landscaping by providing security teams with the tools to continuously validate that their security products are functioning as intended against the latest known threats. Cymulate's BAS platform can mimic threat actor tactics such as multistage attacks, and the techniques and procedures of adversaries from pre-exploitation through post-exploitation. It also has a simple deployment model, and a number of pricing options tailored to the needs of SMBs and large enterprises alike. With the platform, the company is aiming to make advanced red teaming accessible to less advanced security teams. However, given the number of higher-priority items on an information security team's budget, the immediate market for BAS tools will be limited to those organizations that already have a mature security program in place with budget dollars to spare on a still-emerging market segment.

Context

Cymulate was founded in 2016 by CEO Eyal Wachsman and CTO Avihai Ben-Yossef. Prior to starting Cymulate, Wachsman held positions as both VP of sales and business development manager at Avnet Cyber and Information Security, a security consulting and professional services firm, after serving as CISO for a national telecom provider. Ben-Yossef also comes from Avnet, having been head of the Cyber Research Team before leaving for Cymulate.

The Israel-based company has raised $26m in venture funding across three rounds, the most recent of which was a $15m series B announced on November 26, 2019. The series B was led by Vertex Ventures with participation from Dell Technologies Capital and Susquehanna Growth Equity. Previous funding rounds included a $3.5m seed round led by Susquehanna Growth Equity in 2017 and a $7.5m series A round led by Vertex Ventures and Dell Technologies Capital with participation from Susquehanna. The series A was announced in March 2019 and was intended to expand operations in the US, fund additional leadership positions, and fuel continued research and development. Cymulate employs over 50 people between its locations in Rishon LeZion, Israel, and New York.

Products

Cymulate's BAS platform enables organizations to measure the effectiveness of their security controls across a range of attack vectors mapped to MITRE's ATT&CK framework. These attack vectors are grouped into pre-exploitation, exploitation and post-exploitation, following the progression that an attacker would go through in achieving their objective.

The pre-exploitation group tests the customer's perimeter defenses and includes email gateway, web gateway and web application firewall simulations. The email gateway vector, for example, sends emails with malicious attachments such as ransomware, worms or malicious URLs to determine whether the company's email gateway is configured to detect or prevent attacks using those techniques.

The exploitation group follows the next step an attacker would take – exploiting a user's device after an initial intrusion. Cymulate places endpoint security simulations and phishing awareness in this group. Endpoint security simulations are used to identify whether a customer's endpoint security controls are capable of detecting common attack techniques using both signature- and behavior-based methods, while the phishing awareness vector measures employees' security awareness.

Following this pattern, the post-exploitation group assesses an organization's ability to prevent attackers from completing their objective, assuming they have gained a foothold on the network. Cymulate includes lateral movement and data exfiltration simulations in this group – lateral movement tests simulate activities an attacker would undertake to move from one section of the network to a higher-value target, while data exfiltration simulations evaluate whether the company's data loss prevention tools are functioning as desired.

In addition to testing security controls within individual attack vectors, Cymulate launched a full kill-chain advanced persistent threat (APT) offering in May 2019 that links attack vectors together to test the resiliency of the overall security architecture. In this module, customers choose from a set of templates designed to mimic the techniques of well-known APT groups like Lazarus Group and Fancy Bear. Using a wizard-based template, customers can tailor APT simulations to their needs by selecting from precompiled attack methods, or from a menu of MITRE ATT&CK techniques. In September, the company built on this capability with an agentless APT option.

Customers begin by downloading the Cymulate agent, and selecting attack vectors to test against. Once the simulations have been run, Cymulate reports the results in the form of a risk score for each vector, a report detailing which attacks were detected or blocked and which were able to bypass current security controls, and instructions on how to improve the security posture.

Cymulate can generate two different types of reports: one for management to gain an understanding of the current security posture and where additional investment may be needed, and a technical report for security teams to use as a guide for remediation. Remediation guidance can include installing relevant patches, changing the configuration of individual security controls, closing unnecessary ports or editing security policies.

Cymulate has built technical integrations with security products across several domains, including vulnerability scanners (Qualys, Tenable and Rapid7), SIEM systems (Splunk, IBM QRadar and McAfee), security orchestration and automated response technologies (Demisto), endpoint threat detection and response providers (Microsoft Windows Defender ATP), and governance, risk and compliance offerings (RSA Archer). New integrations are added continually.

Business model and strategy

Cymulate uses a subscription pricing model, charging an annual base price to install the agent and register 10 web application firewall (WAF) domains to target in simulations. Enterprise customers are then charged for each additional attack vector they would like to test against, with separate subscriptions for the APT module, immediate threats and any additional WAF domains or agents.

Each enterprise subscription includes unlimited simulations for the attack vectors the customer subscribes to. In September 2019, Cymulate added a SMB pricing option that allows customers to pay a smaller monthly or annual fee, but specifies the attack vectors that can be used in each bundle. Cymulate offers Basic, Standard and Premium versions of its SMB package. The Basic bundle limits customers to 36 assessments for simulating attacks on the email, web and endpoint vectors. Standard includes simulations of the latest immediate threats, while Premium adds the phishing vector. Both Standard and Premium bundles offer unlimited assessments, and all packages include phone and email support.

Cymulate currently goes to market through a combination of direct sales and partners. The company's partners span VARs, resellers, telecommunications providers, managed security service providers and professional services organizations.

Competition

As the commercial opportunity around BAS developed over the last several years, startups and incumbents alike positioned themselves to take advantage. FireEye was among the earliest incumbent vendors to enter the space (which it refers to as 'security instrumentation') when it acquired Verodin for $250m, a leading startups in the segment at the time.

ReliaQuest, a security services provider, acquired ThreatCare to incorporate the latter's BAS capabilities into its portfolio. The Verodin acquisition left AttackIQ and SafeBreach as Cymulate's largest competitors among BAS-focused startups, along with Picus Security, XM Cyber and Scythe.

Other vendors have come at the BAS market from a different angle – NopSec and RiskSense both primarily focus on automated vulnerability prioritization, but offer BAS as an additional point of validation, while longtime network and security performance testing vendor Spirent recently launched its own service. Organizations also have the option to choose from among several open source BAS tools and services options that map to MITRE ATT&CK, such as Red Canary's Atomic Red Team or Guardicore's Infection Monkey.

SWOT Analysis

STRENGTHS

Ease of deployment, a wizard-based scan tool and reports tailored to specific audiences make Cymulate's BAS platform accessible to organizations without skilled security personnel, while cutting down on the cost of regular penetration tests.

WEAKNESSES

While Cymulate's pricing options may help attract SMBs to its platform, BAS in general is not likely to be a high priority for organizations that do not already have a mature security program in place.

OPPORTUNITIES

Increasing complexity of enterprise IT environments combined with a lack of security resources makes security automation tools such as BAS an interesting consideration for organizations.

THREATS

As the BAS market grows and use cases are further validated by improvements in security posture and reduction in security incidents, we may see a greater number of security incumbents package BAS offerings within a broader security platform, potentially undercutting the value provided by specialists like Cymulate.