TAG CYBER

EXTENDED SECURITY POSTURE MANAGEMENT: AN OVERVIEW OF CYMULATE

DR. EDWARD AMOROSO, TAG CYBER

Cymulate

TAGCYBER

EXTENDED SECURITY POSTURE MANAGEMENT: AN OVERVIEW OF CYMULATE

DR. EDWARD AMOROSO

Modern enterprise teams demand continuous views of security posture to address ongoing cyberthreats and prevent enterprise drift, gaps and misconfigurations in today's dynamically changing enterprises. The result is a growing emphasis on extended security posture management—a protection approach exemplified by the commercial Cymulate platform.

INTRODUCTION

The requirement to understand security posture on an ongoing basis has emerged as one of the more challenging aspects of modern enterprise protection initiatives. Specifically, a discipline known as security control validation has emerged as a component of *extended security posture management (XSPM),* which offers detailed technical insights and prescriptive remediation assistance for practitioners, as well as high-level risk guidance for executives.

A key innovation found in most security-control validation systems involves the use of continuous testing and automation to generate accurate visibility and meaningful insights for action. Such automation enables the continuous optimization of controls and IT spending, while minimizing risk and helping assure the operational effectiveness of security systems. It also provides integration with existing cybersecurity components and infrastructure.

In this report, we introduce the concept of extended security posture management, with the goal of helping practitioners understand its relationship to related continuous protections. The commercial Cymulate platform is used to demonstrate the implementation of ongoing security-control validation in an enterprise context. Comprehensiveness, along with the ease of deployment and use, are its top design considerations, making this an attractive extended security posture management solution for working-level experts, senior-level managers and executive staff.

Furthermore, XSPM solutions allow CISOs to measure the effectiveness of security programs and maximize their return on investment, while also providing a clear understanding of enterprise risk levels and, more importantly, a prescriptive and prioritized list of how to further reduce risk. For the cybersecurity practitioner, XSPM solutions offer a clear-cut way to optimize enterprise cybersecurity, while understanding attacker tactics, techniques and procedures, as well as reducing enterprise attack surfaces and threat exposure.

EXTENDED SECURITY POSTURE MANAGEMENT

In the face of evolving threats, increased vulnerabilities and enterprise drift, XSPM solutions use attack simulations and other means to discover misconfigurations, gaps and vulnerabilities in order to establish attack feasibility and prioritize any risks that were found. When done on a continuous basis, enterprises can easily establish security baselines and trends over time, as well as receive automated and prescriptive technical remediation instructions. Executive reporting also includes industry benchmarking for companies that wish to compare their maturity and risk profiles.

A useful, high-level methodology for implementing XSPM includes three basic functional protection objectives: visibility into assets; optimization of posture; and the assurance of continued security. These three high-level management goals provide a helpful view of how XSPM platforms have been developed, and how enterprise teams can implement XSPM to offer the continuous improvement and validation of their deployed protection scheme.

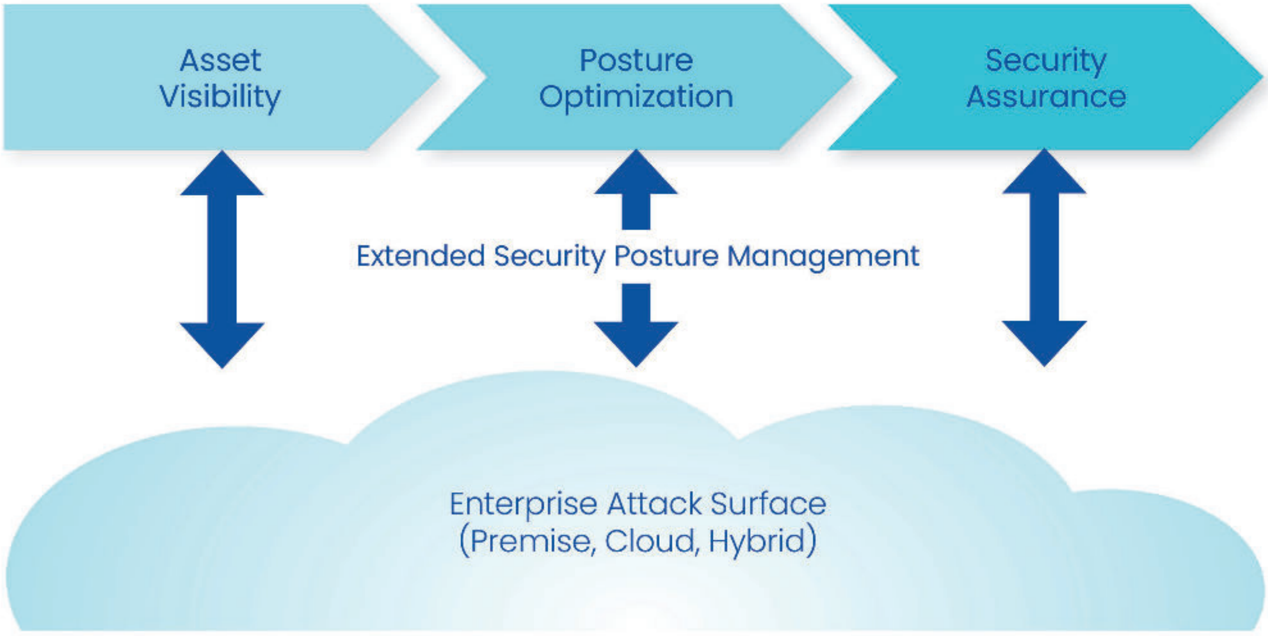

Asset Visibility
Posture Optimization
Security Assurance
Extended Security Posture Management
Enterprise Attack Surface (Premise, Cloud, Hybrid)

Figure 1. High-Level XSPM Objectives

The purpose of XSPM is to provide high confidence that an enterprise is being protected by properly deployed security controls that are configured without vulnerabilities and operating according to expected security parameters. The process is thus related to the emerging attack surface management (ASM) discipline and can easily complement or replace existing or planned security initiatives in this area.

XSPM is a valuable testing solution for Blue and Purple Teams seeking to test and optimize their first- and third-party security controls in order to find and remediate discovered security gaps and vulnerabilities. Advanced-scenario attack testing is a favored tool by Red Teams seeking to automate, scale and customize breach feasibility testing and threat-exposure management. Organizations of all sizes can take advantage of the Jump Start offering, which provides immediate security validation against new and top threats, while its Amplify solution provides a managed service offering an option for organizations that lack the manpower for security validation and ongoing assessment.

OVERVIEW OF CYMULATE

Cybersecurity start-up company Cymulate offers a commercial SaaS-based solution that effectively supports XSPM in accordance with the objectives outlined above. Cymulate security validation combines assessments of outside-in reconnaissance, security awareness, infrastructure resilience and security control validation in one platform.

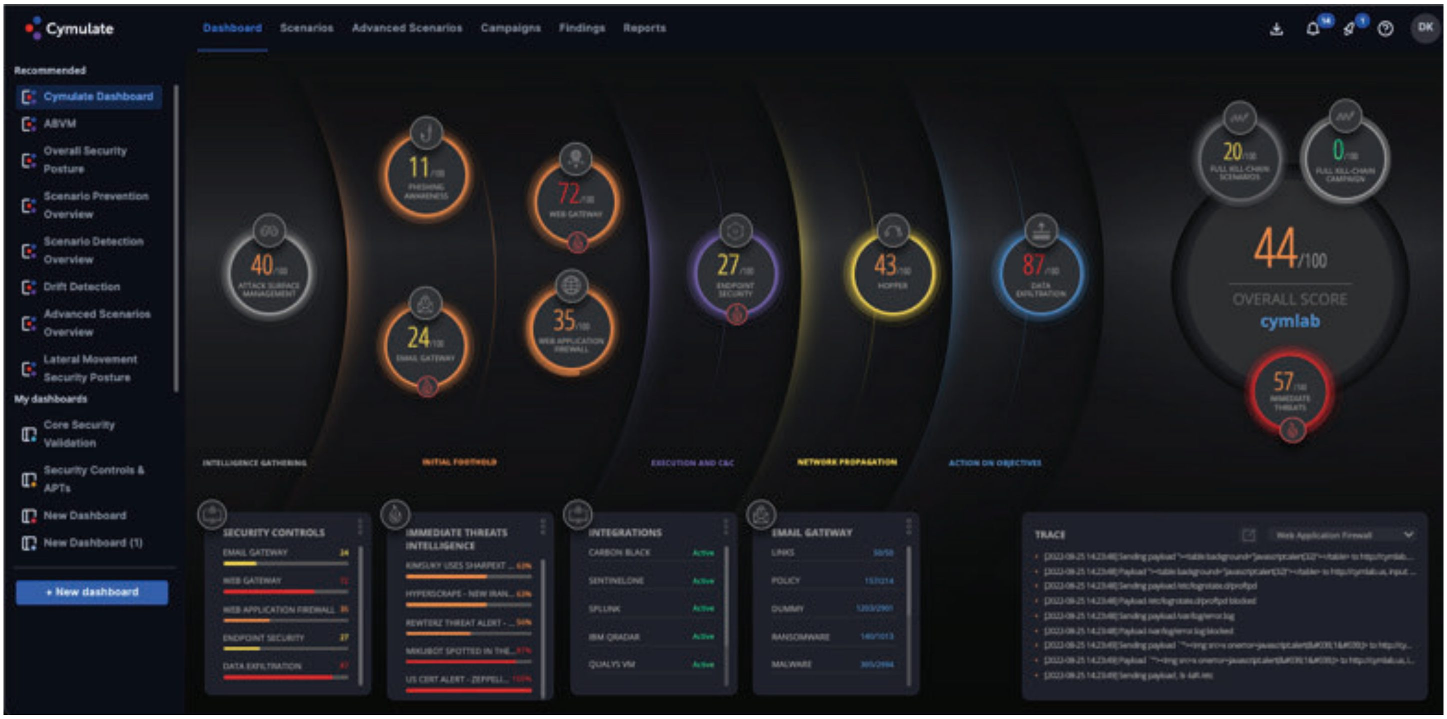
Cymulate provides a range of security scoring, including baselines and trends over time, as well as the possibility to benchmark your scores against those of your peers. It also offers actionable remediation guidance for the following security management and support domains:

Security Control Validation
Cymulate initially provides validation of security controls via carefully designed, advanced attack simulations. This process results in the high confidence that controls for web, web application firewalls, email, applications, endpoints, segmentation and data loss prevention, as well as other resources, are all working as intended. The Cymulate platform receives frequent platform updates to ensure that the most recent adversarial indicators of compromises, attack techniques and procedures are integrated into simulated threat scenarios.

Using the MITRE ATT&CK framework and NIST 800-53, mapping, reporting and explanations ensure a common language that is well understood by the team. Prescriptive technical reporting ensures that any found misconfigurations and gaps are easily remediated. Cymulate has an extensive number of security control categories it can test, and it also incorporates third-party cybersecurity integrations, ensuring in-depth, accurate testing analysis and results.

Phishing Campaigns
Cymulate also allows you to run phishing campaigns to test your employees and provide clear-cut measurements of the risk found, which can lead to important, additional employee education and protection. Tied into Security Controls Validation, you can further see how your email infrastructure, operating systems, email gateways and endpoints handle the testing, as well.

Security Posture Reporting
Cymulate offers a comprehensive user interface for reporting detailed information about security posture. Reporting includes: drilling down into breach and attack simulation (BAS) results; continuous automated Red Team results; and advanced Purple Team data. Numeric scores help provide a rapid visualization of status, so that results can be interpreted not only by security practitioners, but also by management and executive teams (see Figure 2).



SECURITY CONTROLS	
EMAIL GATEWAY	24
WEB GATEWAY	72
WEB APPLICATION FIREWALL	35
ENDPOINT SECURITY	27
DATA EXFILTRATION	87

IMMEDIATE THREATS INTELLIGENCE	
KIMSUKY USES SHARPEXT ...	63%
HYPERSCRAPE - NEW IRAN...	63%
REWTERZ THREAT ALERT - ...	50%
MIKUBOT SPOTTED IN THE...	87%
US CERT ALERT - ZEPPELI...	100%

INTEGRATIONS	
CARBON BLACK	Active
SENTINELONE	Active
SPLUNK	Active
IBM QRADAR	Active
QUALYS VM	Active

EMAIL GATEWAY	
LINKS	50/50
POLICY	157/214
DUMMY	1203/2901
RANSOMWARE	140/1013
MALWARE	305/2994

TRACE

Web Application Firewall

```
[2022-08-25 14:23:48] Sending payload "><table background="javascript:alert(32)"></table> to http://cymlab...
[2022-08-25 14:23:48] Payload "><table background="javascript:alert(32)"></table> to http://cymlab.us, input ...
[2022-08-25 14:23:48] Sending payload /etc/logrotate.d/proftpd
[2022-08-25 14:23:48] Payload /etc/logrotate.d/proftpd blocked
[2022-08-25 14:23:48] Sending payload /var/log/error.log
[2022-08-25 14:23:48] Payload /var/log/error.log blocked
[2022-08-25 14:23:49] Sending payload "'><img src=x onerror=javascript:alert(&#039;1&#039;)> to http://cy...
[2022-08-25 14:23:49] Payload "'><img src=x onerror=javascript:alert(&#039;1&#039;)> to http://cymlab.us, i...
[2022-08-25 14:23:49] Sending payload [illegible]
```

Figure 2. Cymulate XSPM Solution Dashboard
Showing Cybersecurity Posture Scoring Baselines and Trends

Attack Surface Management

The Cymulate platform identifies and prioritizes external-facing corporate assets, including web applications, exposed servers and other resources in order to expose the presence of exploitable vulnerabilities. Such attack surface management (ASM) is supported by the Cymulate Attack Surface Manager; it is valuable for complex environments that include a wide range of external assets, including shadow IT. An internal phishing awareness function provides complementary support.

Infrastructure Resilience

The Cymulate Lateral Movement component involves simulation of the East-West, lateral traversal, which is common in modern advanced persistent threat (APT) campaigns. The goal is to simulate the threat actions that result after an initial connection has been made to the target enterprise infrastructure. Misconfigurations and vulnerabilities are exposed via this traversal process, and support for risk measurement is included.

Continuous Testing

The Cymulate Continuous Automated Red Teaming solution involves support for attack campaigns against target enterprise infrastructure. The goal is to discover and expose vulnerabilities, weaknesses and soft spots in an enterprise, thus complementing the overall ASM solution. The testing process can be tailored to attack specific resources and can include tactics such as phishing to create initial access to target resources.

ABOUT TAG CYBER

TAG Cyber is a trusted cyber security research analyst firm, providing unbiased industry insights and recommendations to security solution providers and Fortune 100 enterprises. Founded in 2016 by Dr. Edward Amoroso, former SVP/CSO of AT&T, the company bucks the trend of pay-for-play research by offering in-depth research, market analysis, consulting, and personalized content based on hundreds of engagements with clients and non-clients alike—all from a former practitioner perspective.

IMPORTANT INFORMATION ABOUT THIS PAPER

Contributor: Dr. Edward Amoroso

Publisher: TAG Cyber LLC. ("TAG Cyber"), TAG Cyber, LLC, 45 Broadway, Suite 1250, New York, NY 10006.

Inquiries: Please contact Lester Goodman, (lgoodman@tag-cyber.com), if you'd like to discuss this report. We will respond promptly.

Citations: This paper can be cited by accredited press and analysts but must be cited in context, displaying the author's name, author's title, and "TAG Cyber". Non-press and non-analysts must receive prior written permission from TAG Cyber for any citations.

Disclosures: This paper was commissioned by Cymulate Ltd. TAG Cyber provides research, analysis, and advisory services to many cybersecurity firms mentioned in this paper. No employees at the firm hold any equity positions with any companies cited in this document.

Disclaimer: The information presented in this document is for informational purposes only and may contain technical inaccuracies, omissions, and typographical errors. TAG Cyber disclaims all warranties as to the accuracy, completeness, or adequacy of such information and shall have no liability for errors, omissions, or inadequacies in such information. This document consists of the opinions of TAG Cyber's analysts and should not be construed as statements of fact. The opinions expressed herein are subject to change without notice.

TAG Cyber may provide forecasts and forward-looking statements as directional indicators and not as precise predictions of future events. While our forecasts and forward-looking statements represent our current judgment and opinion on what the future holds, they are subject to risks and uncertainties that could cause actual results to differ materially. You are cautioned not to place undue reliance on these forecasts and forward-looking statements, which reflect our opinions only as of the date of publication for this document. Please keep in mind that we are not obligating ourselves to revise or publicly release the results of any revision to these forecasts and forward-looking statements considering new information or future events.