

Laufende Sicherheitsvalidierung leicht gemacht

Den Status Ihrer Cybersicherheitslage zu messen erscheint unmöglich?

Jeder Tag bringt Veränderungen Ihrer Sicherheitslage. Änderungen in der IT-Architektur ändern die Angriffsfläche, Konfigurationsänderungen an Sicherheitskontrollen führen zu unvorhergesehenen Sicherheitslücken und die sich entwickelnde Bedrohungslandschaft führt zu neuen Bedrohungen, die vermieden werden müssen. Es scheint unmöglich zu wissen, wie effektiv Ihre Sicherheitskontrollen derzeit sind und was behoben werden muss. Sie haben sicher bereits Penetrationstests und andere Alternativen ausprobiert. Aber bis Sie ihren Bericht erhalten, ist er bereits veraltet und irrelevant. Es muss einen effektiven und einfachen Weg geben, um zu wissen, dass Sie kontinuierlich sicher sind.

Mit Cymulate können Sie Ihre 24/7 Sicherheitslage innerhalb von Minuten in nur drei einfachen Schritten verbessern:



01

Simulation

Von Angriffen entlang der gesamten Kill Chain



02

Evaluierung

Kontrollen um Lücken zu entdecken



03

Beseitigung

Umsetzbare Richtlinien

Wichtige Plattformfunktionen

Eingehende Validierung – Durch die Nachahmung der Vielzahl von Strategien und Tools, die Angreifer einsetzen, fordert die Plattform die Sicherheitskontrollen Ihres Unternehmens mit Tausenden von simulierten Angriffen heraus, die das MITRE ATT&CK-Framework ausführlich abdecken. Diese umfassende Validierung bewertet die tatsächliche Bereitschaft Ihres Unternehmens, mit Cybersicherheitsbedrohungen effektiv umzugehen.

Ende-zu-Ende-Validierung – Cymulate überprüft Ihre Sicherheitslage über die gesamte Angriffskette hinweg: Aufklärung, Ausgangsposition, Ausführung, Befehl und Kontrolle, Seitwärtsbewegung und Zielaktionen. Es vereint Bewertungen von Außenaufklärung, Sicherheitsbewusstsein, Ausfallsicherheit der Infrastruktur und Validierung der Sicherheitskontrolle auf einer Plattform.

Sicherheitsbewertung von Drittanbieter – Cymulate Recon bietet kontinuierliche und quantitative technische Analysen und Bewertungen für öffentlich zugängliche digitale Assets. Außerdem werden organisatorische Informationen und Informationen zu Anmeldeinformationen ermittelt, die ein Hacker bei einem Angriff verwenden kann. Sie können damit die externen Risiken Ihres Unternehmens und die indirekten Risiken, die durch das digitale Geschäftsumfeld entstehen, messen, verfolgen und steuern.

Testen Sie die neuesten Bedrohungen, sobald diese auftreten – Cymulate Research Lab hält sich über die neuesten Bedrohungen auf dem Laufenden und aktualisiert die Plattform täglich mit Immediate Threats Intelligence. Auf diese Weise können Unternehmen ihre Widerstandsfähigkeit gegenüber den neuesten Bedrohungen schnell erkennen.

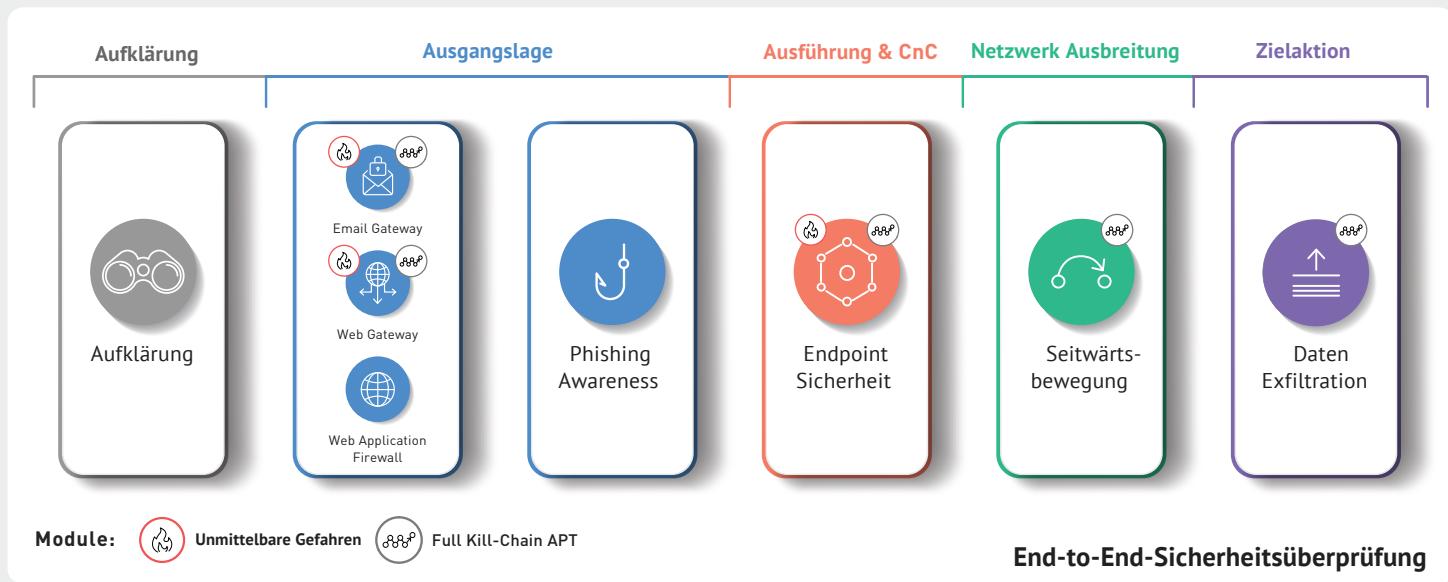
Ergebnisse und Berichte – Nach jeder Bewertung wird ein Executive Report erstellt. Er bewertet und fasst Ergebnisse zusammen und gibt hoch professionelle Empfehlungen für Gegenmaßnahmen. Der Executive Report vergleicht die Punktzahl auch mit früheren Bewertungen und Mitbewerbern. Der technische Bericht enthält eine Beschreibung jedes einzelnen Tests oder Befundes sowie die Risikostufe und umsetzbare Richtlinien zur Behebung des Misstands.

Security Scoring - Cymulate Security Scoring bietet eine Messung der Sicherheitslage Ihres Unternehmens und der Wirksamkeit seiner Sicherheitskontrollen. Das Bewertungssystem ermöglicht es Ihnen, Ihre Sicherheitslage zu verfolgen und zu verbessern sowie die Sicherheitsausgaben zu rationalisieren und Ressourcen zuzuweisen.

Die Punktzahl wird nach branchenweit anerkannten Standards berechnet: NIST Risk Management Framework, CSVSS v3.0 Calculator, Microsoft DREAD und das MITRE ATT&CK™ Framework.

Angriffsanpassung – Sie können Ihre eigenen Angriffsszenarien mit einfach zu verwendenden Vorlagen erstellen und starten, die die umfangreiche Bibliothek an Angriffsbefehlen, Malware und gegnerischen Taktiken und Techniken des MITRE ATT&CK-Framework nutzen.

Integrationspartner - Cymulate lässt sich in Lösungen anderer Technologiepartner integrieren, um vorhandene Sicherheitstestprogramme zu erweitern, indem simulierte Angriffe mit ihren Ergebnissen korreliert werden. Mit diesen Integrationen können Sie die Funktionen zur Erkennung und Reaktion von EDR und SOC validieren und verbessern sowie die Korrektur- und Patch-Bemühungen priorisieren, indem Sie Angriffe mit den Ergebnissen des Schwachstellenmanagementsystems korrelieren.



Warum Cymulate

 Ausrollung in Minuten	 Einfach zu bedienen	 Einzelagent, unbegrenzte Angriffe	 SaaS-basierte Plattform	 Automatisiert oder on demand	 Neueste Bedrohungen mit wenigen Klicks simuliert	 Deckt die gesamte Angriffskette ab
--	--	--	--	---	---	---

Wer ist Cymulate?

Mit einem Forschungslabor, das sich über die neuesten Bedrohungen auf dem Laufenden hält, fordert Cymulate Sicherheitskontrollen proaktiv heraus und schützt exponierte Organisationen nachhaltig vor Schäden. Cymulate wurde von einem Elite-Team von Cyber-Forschern mit erstklassiger Erfahrung in offensiven Cyber-Lösungen gegründet und wird von Unternehmen weltweit, von kleinen bis zu großen Unternehmen, einschließlich führender Banken und Finanzdienstleister, als vertrauenswürdig eingestuft. Sie teilen unsere Vision, es jedem einfach zu machen, sein Unternehmen mit einem Höchstmaß an Sicherheit zu schützen. Denn je einfacher die Cybersicherheit ist, desto sicherer wird Ihr Unternehmen.

Kontaktieren Sie unseren Partner für eine Live-Demo oder kostenlose Testversion www.softprom.com