Extended Security Posture Management

Die Verwaltung Ihres Cybersicherheitsstatus erscheint Ihnen zu kompliziert?

Jeder Tag bringt Veränderungen für Ihren Sicherheitsstatus. Änderungen an der IT-Architektur verändern die Angriffsfläche, Konfigurationsänderungen an Sicherheitsmaßnahmen führen zu unvorhergesehenen Sicherheitslücken und täglich kommen neue Bedrohungen hinzu, die es zu verhindern gilt.
Es scheint unmöglich zu wissen, wie effektiv Ihre Sicherheitsmaßnahmen im Moment sind, welche digitalen Assets ungeschützt sind, über welche Angriffswege in das Netzwerk eingedrungen werden kann und was in welcher Reihenfolge behoben werden muss.
Penetrationstests sind nicht ausreichend, da die Berichte zu dem Zeitpunkt, zu dem man sie erhält, bereits veraltet und irrelevant sind. Andere Alternativen könnten Ihnen ein aktuelles Bild vermitteln, das aber in der Regel unvollständig ist.
Es gibt eine wirksame und einfache Methode, um zu wissen, dass Sie sicher sind, End-to-End.

Extended Security Posture Management-Plattform

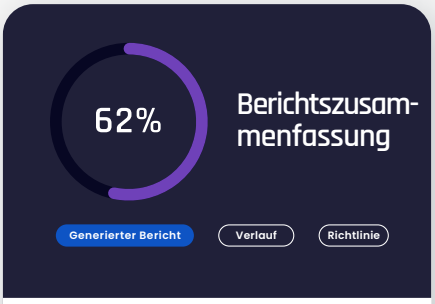
Für Unternehmen, die ihren Sicherheitsstatus im Hinblick auf die sich entwickelnde Bedrohungslandschaft verwalten wollen. Die SaaS-basierte für Extended Security Posture Management (XSPM)-Plattform von Cymulate ist innerhalb weniger Minuten einsatzbereit und versetzt Sicherheitsexperten in die Lage, die Optimierung ihres Cybersicherheitsstatus über das MITRE ATT&CK®-Framework hinweg kontinuierlich zu überprüfen, zu validieren und zu verwalten. Die Plattform umfasst die Breach and Attack Simulation (BAS)-Technologie, die von Frost & Sullivan im Jahr 2021 als innovativste Technologie eingestuft wurde, BAS Radar™, Continuous Automated Red Teaming (CART) und das Advanced Purple Teaming-Framework. Die Cymulate-Plattform bietet sofort einsatzbereite, auf Expertenwissen und Bedrohungsdaten basierende Risikobewertungen, die für alle Reifegrade einfach zu implementieren und zu nutzen sind und ständig aktualisiert werden. Darüber hinaus bietet sie ein offenes Framework zur Erstellung und Automatisierung von Purple und Red Teaming durch die Generierung von Penetrationsszenarien und fortgeschrittenen Angriffskampagnen, die auf die jeweiligen Umgebungen und Sicherheitsrichtlinien zugeschnitten sind. Cymulate ermöglicht es Fachkräften, ihre dynamische Umgebung zu verwalten, zu kennen und zu kontrollieren.

Funktionsweise

Cymulate gewährleistet die Verwaltung Ihres Sicherheitsstatus 24x7x365, innerhalb von Minuten und faktenbasiert mit nur drei einfachen Schritten:

1 Simulieren
Angriffe über verschiedene Vektoren simulieren.

2 Bewerten
Risikoexponierung des Unternehmens erkennen.



3 Korrigieren
Sicherheitslücken schließen.

Zentrale Fähigkeiten

End-to-End-Validierung – Cymulate validiert kontinuierlich Ihren Sicherheitsstatus über die Full-Attack-Kill-Chain: Reconnaissance, Fuß in der Tür, Ausführung, Command and Control, Lateral Movement und Aktion zum Erreichen des Ziels. Es kombiniert Angriffsflächenmanagement (ASM), Breach and Attack Simulation (BAS), Continuous Automated Red Teaming (CART), Advanced Purple Teaming und die Priorisierung von Schwachstellen, um eine Optimierungsbaseline festzulegen - alles in einer Plattform.

Umsetzbare Analysen – die Ergebnisse jeder Bewertung werden im Management-Dashboard sowie in einem technischen Bericht und einem Bericht für die Geschäftsführung dargestellt. Der Bericht für die Geschäftsführung fasst die Ergebnisse zusammen und enthält einen Score sowie Empfehlungen für Gegenmaßnahmen auf höchster Ebene. Außerdem wird die Punktzahl mit früheren Bewertungen und mit dem Score von Branchenkollegen verglichen. Der technische Bericht enthält eine Beschreibung jedes einzelnen Tests oder Befunds zusammen mit einer Risikostufe und einer umsetzbaren Anleitung für Abhilfemaßnahmen.

Eingehende Validierung – Durch die Nachahmung der unzähligen Strategien und Tools, die Angreifer einsetzen, fordert die Plattform die Sicherheitsmaßnahmen Ihres Unternehmens mit Tausenden von simulierten Angriffen heraus, die das MITRE ATT&CK-Framework eingehend abdecken. Mit dieser umfassenden Validierung wird die tatsächliche Bereitschaft Ihres Unternehmens bewertet, mit Bedrohungen der Cybersicherheit wirksam umzugehen.

Schwachstellenpriorisierung – Integration mit gängigen Schwachstellenmanagementlösungen von Drittanbietern, um Informationen über Schwachstellen mit den Ergebnissen der Validierungsplattform von Cymulate abzugleichen; bietet eine praktische Übersicht über kompensierende Sicherheitsmaßnahmen für ungepatchte Schwachstellen im Netzwerk.

Security Risk Scoring – Cymulate Security Scoring bietet eine Messung des Sicherheitsstatus Ihres Unternehmens und der Effektivität seiner Sicherheitsmaßnahmen.
Dieses Bewertungssystem ermöglicht es Ihnen, den Sicherheitsstatus im Blick zu haben und zu verbessern sowie Ihre Sicherheitsausgaben und die Ressourcenzuweisung zu rationalisieren.
Der Score wird anhand von branchenweit anerkannten Standards berechnet: dem NIST Risk Management Framework, dem CSVSS v3.0 Calculator, Microsoft DREAD und dem MITRE ATT&CK™ Framework.

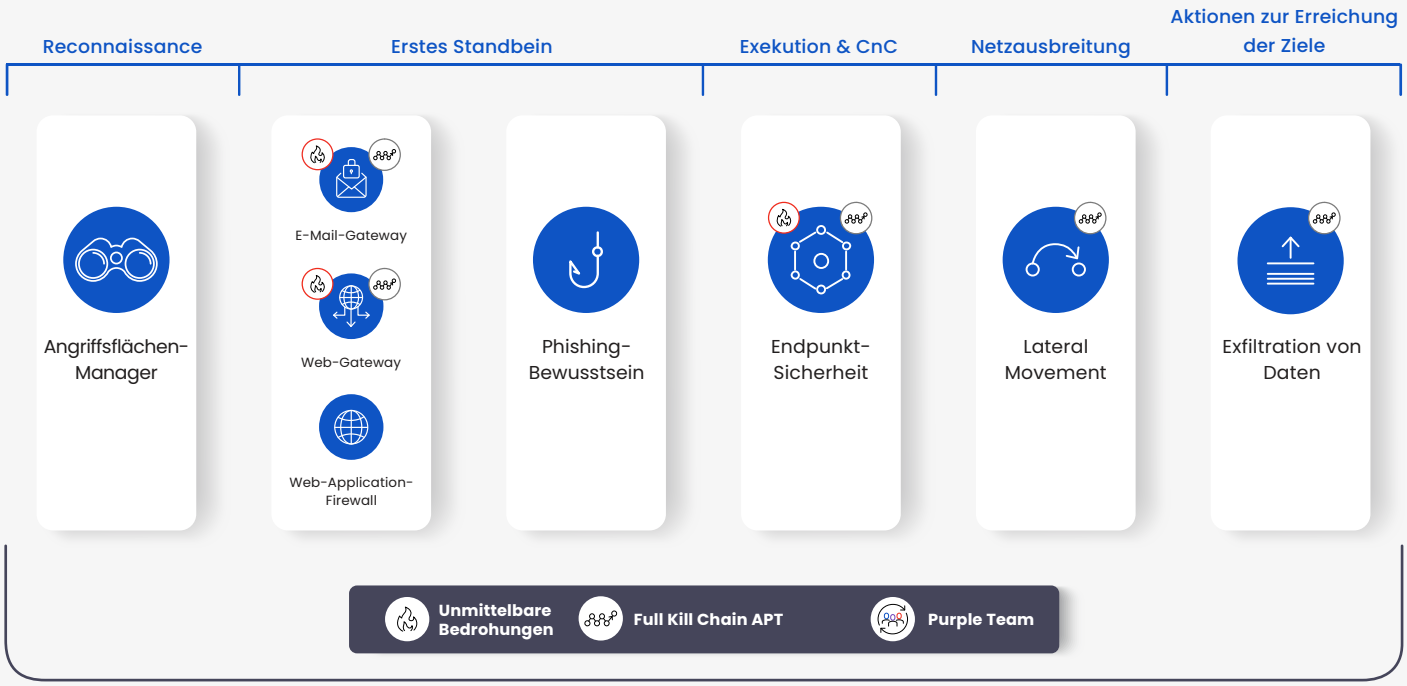
Anpassbar – Erweiterbares, offenes Framework zum Erstellen und Automatisieren von Red/Purple Teaming und zum Automatisieren von Sicherheitsverfahren sowie von Zustandsprüfungen, die auf die jeweilige Umgebung und jeweiligen Richtlinien zugeschnitten sind. Darüber hinaus können Sie bestehende Vorlagen erstellen oder anpassen, um spezifische Anforderungen zu erfüllen.

Automatisiertes Purple Teaming – ein Framework, welches das MITRE ATT&CK®-Framework zum Erstellen, Starten und Automatisieren benutzerdefinierter Angriffsszenarien operationalisiert. Zusätzlich zu der umfangreichen und sofort einsatzbereiten Bibliothek kann das Sicherheitspersonal Ausführungen erstellen oder ändern, um sowohl einfache als auch komplexe Szenarien mit atomaren, kombinierten und verketteten Ausführungen zu erstellen. Das Modul ermöglicht APT-Simulationen, Purple Team-Übungen, Übungen zur Reaktion auf Vorfälle, proaktive Bedrohungsjagd und automatisiert Sicherheitsverfahren und Zustandsprüfungen.

Eine Vielzahl von Integrationen – Cymulate-Integrationen ermöglichen Ihnen die Validierung und Verbesserung der SOC-Performance. Integrationen mit xDR/EDR- und SIEM-Systemen korrelieren Angriffssimulationen mit Erkennung, Ereignissen und Warnmeldungen für eine schnelle und einfache Validierung.
Die Integration mit Schwachstellenmanagementsystemen ermöglicht ein risikobasiertes Schwachstellenmanagement. Dieses bietet Angriffskontext zu Schwachstellen und Angriffspfad-Visualisierung von anfälligen Rechnern, um die Priorisierung von Abhilfe- und Patching-Maßnahmen zu unterstützen.

Cymulate

Extended Security Posture Management



Warum Cymulate

- Bereitstellung in Minuten, SaaS-basiert
- Breiteste Abdeckung über die gesamte Kill-Chain
- Anleitung zur Priorisierung von Schwachstellen
- Granulare Analytik
- Simulation neuester Bedrohungen mit wenigen Klicks
- Umfassende vorkonfigurierte Assessments
- Hochgradig anpassbare Red Team-Automatisierung

Über Cymulate

Mit einem Forschungslabor, das mit den neuesten Bedrohungen Schritt hält, hinterfragt Cymulate proaktiv, automatisch und kontinuierlich den Sicherheitsstatus von Anfang bis Ende, so dass hypervernetzte Unternehmen aller Reifegrade Schaden abwenden und sicher bleiben können. Cymulate wurde von einem Elite-Team von Cyber-Forschern gegründet, die über herausragende Erfahrung mit offensiven Cyber-Lösungen verfügen. Hunderte von Unternehmen auf der ganzen Welt vertrauen auf Cymulate, von kleinen Betrieben bis hin zu Großunternehmen, einschließlich führender Banken und Finanzdienstleister. Sie teilen unsere Vision, der Goldstandard für Sicherheitsexperten und Führungskräfte zu sein, um ihren Cybersicherheits-Status zu verwalten, zu kennen und zu kontrollieren. Heute ist es für jeden einfach, sein Unternehmen mit einem Höchstmaß an Sicherheit zu schützen. Denn je einfacher die Cybersicherheit ist, desto sicherer wird Ihr Unternehmen - wird jedes Unternehmen - sein.

Kontaktieren Sie uns für eine Live-Demo oder starten Sie mit einer kostenlosen Testversion

Starten Sie Ihre kostenlose Testversion

Hauptsitz: 2 Nim Blvd., Rishon LeZion, 7546302, Israel | +972 3 9030732 | info@cymulate.com | US Office: +1 212 6522632