ENTHÜLLEN SIE IHRE RISIKEN, NICHT IHRE ASSETS

Exposure Assessment Platform Buyer's Guide

RAPID7

INHALT

Täglich tauchen neue Bedrohungen auf, so dass Sicherheitsteams proaktiv vorgehen müssen, um Schwachstellen zu erkennen und das Risiko einzudämmen. Der Attack Intelligence Report 2024 von Rapid7 hat ergeben, dass zum zweiten Mal innerhalb von drei Jahren mehr Massenkompromittierungen auf Zero-Day-Schwachstellen zurückzuführen sind. Das bedeutet, dass es für Unternehmen immer wichtiger wird, Tools einzusetzen, die Angriffsflächen kontinuierlich überwachen und anpassen.

> **Laut Gartner „identifizieren und priorisieren Exposure Assessment Platforms (EAPs) kontinuierlich Bedrohungen wie Schwachstellen und Fehlkonfigurationen über ein breites Spektrum von Assets hinweg. Sie bieten native Erkennungsfunktionen oder sind in diese integriert, beispielsweise Bewertungstools, die Risiken wie Schwachstellen und Konfigurationsprobleme auflisten, um die Sichtbarkeit zu erhöhen.“**[1]

Darüber hinaus bieten EAPs Unternehmen eine vollständige Sichtbarkeit ihrer gesamten IT-Umgebung in Echtzeit, mit der Folge, dass Risiken proaktiv eingedämmt, Gegenmaßnahmen priorisiert und ihre Sicherheitslage insgesamt verbessert werden kann.

Dieser Buyer’s Guide erläutert, warum eine EAP ein elementarer Baustein des modernen Sicherheits-Stacks ist, und gibt Empfehlungen, wie Sie CTEM nutzen können. Außerdem enthält er die wichtigsten Kriterien, die Sie vor einer Investition berücksichtigen sollten, damit Sie die richtige EAP für Ihr Unternehmen finden. Mit den richtigen Tools können Sie sicherstellen, dass Ihre Organisation darauf vorbereitet ist, seine Assets vor Cybersecurity-Angriffen zu schützen.

1 Gartner®, Hype Cycle™ for Security Operations, 2024; Jonathan Nunex, Andrew Davies; 29. Juli 2024

WIE RAPID7 DEN AUFBAU EINES WIRKSAMEN CTEM-PROGRAMMS SIEHT

Rapid7 ist davon überzeugt, dass ein effektives CTEM-Programm Unternehmen einen strukturierten Ansatz zur Handhabung und Reduzierung von Cyberrisiken bietet.

Da es für Organisationen schwierig sein kann, mit bösartigen Akteuren, Zero-Day-Schwachstellen und anderen Cybersecurity-Bedrohungen Schritt zu halten, konzentriert sich ein gutes CTEM-Programm unserer Meinung nach auf die Reduzierung zukünftiger Gefährdungen durch kontinuierliches Monitoring. Durch die Einführung des CTEM Frameworks können Unternehmen eine proaktive Sicherheitslage schaffen und Risiken eindämmen.

Aus unserer Sicht macht ein CTEM-Programm eine kontinuierliche Verbesserung und Priorisierung möglich, was den Sicherheitsteams ermöglicht, proaktiv Bedrohungen über die gesamte externe Angriffsfläche zu identifizieren, zu bewerten und einzudämmen.

> **Nach Gartner handelt es sich bei einem Continuous Threat Exposure Management (CTEM) Programm um eine „Reihe von Prozessen und Fähigkeiten, die es Unternehmen ermöglichen, die Zugänglichkeit, Gefährdung und Ausnutzbarkeit der digitalen und physischen Assets eines Unternehmens kontinuierlich und einheitlich zu bewerten.“**[2]

Dies geschieht durch einen fünfstufigen Prozess, der in der festgelegten Reihenfolge durchgeführt werden sollte, um Lücken oder übersehene Bedrohungen zu vermeiden. Dieser Prozess ist zyklisch und jeder Schritt muss durchgeführt werden, wenn neue Tools und Technologien eingeführt werden, die Angriffsflächen sich weiterentwickelt oder der Umfang sich wandelt.

Bei effektiver Implementierung reduziert ein CTEM-Programm die Auswirkungen und Gesamtkosten eines Verstoßes, sollte dieser jemals auftreten, schafft eine stärkere, proaktivere Sicherheitslage und erleichtert die Kommunikation und Abstimmung mit wichtigen Stakeholdern. So wird ein klarer Überblick über die Risiken und geplanten Gegenmaßnahmen geschaffen.

2 Gartner „Implement a Continuous Threat ExposureManagement (CTEM) Program“; Jeremy D'Hoinne, Pete Shoard, Mitchell Schneider; 11. Oktober 2023.

RAPID7-LEITFADEN ZU DEN FÜNF PHASEN VON CTEM

Erkennung
Führung eines genauen Inventars aller Assets und ihrer Risikolage

Validierung
Bewertung der potenziellen Auswirkungen von Gefährdungen und Bedrohungen

Scoping
Definieren Sie die Tiefe und die Breite des Zyklus

Priorisierung
Identifizierung der kritischsten Risikosignale

Mobilisierung
Operationalisierung entsprechend den Ergebnissen

DIES SIND DIE FÜNF PHASEN EINES CTEM-PROGRAMMS:

1. **UMFANG:** Bewertung der Angriffsfläche Ihrer Organisation und Erarbeitung eines Aktionsplans.

2. **ERKENNUNG:** Identifizierung sichtbarer oder verdeckter Asset-Schwachstellen oder anderer Risiken.

3. **PRIORISIERUNG:** Ermittlung der Sicherheitsprobleme, die das größte Risiko für Ihre Organisation darstellen, anhand festgelegter Faktoren.

4. **VALIDIERUNG:** Nach Priorisierung der Risiken, Evaluierung der Wahrscheinlichkeit einer Ausnutzung der Schwachstelle durch Bedrohungsakteure, wie ein Angriff erfolgen könnte und ob die aktuelle Abwehr Ihre Organisation schützen kann.

5. **MOBILISIERUNG** Sicherstellen, dass das Sicherheitsteam und die wichtigsten Stakeholder die Pläne und Workflows im Zuge der Gegenmaßnahmen verstehen und ausführen können.

1. UMFANG

Der erste Schritt besteht darin, die Angriffsfläche einer Organisation sowohl intern als auch extern zu untersuchen. Dazu gehört die Untersuchung der Angriffsfläche einer Organisation von außen und die anschließende Erfassung und Inventarisierung interner Assets, die bei externen Scans möglicherweise übersehen werden. Dies umfasst alle Assets, von herkömmlichen Geräten, Apps und Software bis hin zu Unternehmenskonten in sozialen Medien, Online-Code-Repositorys und integrierten Lieferkettensystemen. Bei größeren Organisationen, insbesondere solchen, die durch Fusionen und Übernahmen an Größe gewinnen, geht der Umfang der Angriffsfläche in der Regel über den Fokus herkömmlicher Schwachstellen-Management-Programme hinaus.

Zu Beginn der Scoping-Phase sollten Sicherheitsteams ihre Angriffsfläche überwachen und ihr Risikoprofil in Bezug auf die Unternehmensziele bewerten. Auf dieser Grundlage kann das Team in Zusammenarbeit mit wichtigen Stakeholdern einen Aktionsplan aufstellen. Mit Scoping können Pläne verfeinert und erweitert werden, während das Programm Zyklen durchläuft und zusätzliche Assets hinzugefügt werden.

2. ERKENNUNG

Bei der Erkennung werden Schwachstellen und Lücken in der Angriffsfläche ermittelt. Eine wirksame Aufdeckung von Risiken geht über Schwachstellen hinaus. Sie erfordert ein umfassendes Verständnis und eine umfassende Sicht auf die Unternehmens- und Infrastrukturdaten eines Unternehmens über alle Standorte und Umgebungen hinweg. Dazu gehört die Bewertung von On-Premise- und Cloud-Umgebungen, sichtbaren und verborgenen Assets, Fehlkonfigurationen und anderen Schwachstellen oder Risiken.

3. PRIORISIEREN

Bei der Priorisierung geht es nicht darum, jede einzelne Schwachstelle zu beheben, sondern die Bedrohungen für das Unternehmen zu identifizieren, die das größte Risiko darstellen könnten. Eine effektive Priorisierung konzentriert sich auf die Bedrohungen mit den größten Auswirkungen durch folgende Bewertung:

- **Geschäftsauswirkungen:** Wie kritisch ist das betroffene Asset oder die betroffene Anwendung für die Betriebsabläufe der Organisation?
- **Zugänglichkeit und Angriffspfade:** Kann ein Angreifer leicht über ein öffentliches Netzwerk auf ein Asset zugreifen oder Benutzerberechtigungen ausnutzen? Welche Angriffspfade könnte ein böswilliger Akteur wählen, um sich seitlich in der Umgebung zu bewegen?
- **Identitätsbezogenes Risiko:** Befolgt Ihre Organisation das Least Privilege-Prinzip? Wie hoch ist die Wahrscheinlichkeit, dass Privilegien missbraucht oder eskaliert werden?
- **Fehlkonfiguration:** Entsprechen die Assets und Anwendungen den Compliance- und Sicherheitsanforderungen? Können sie aufgrund von Fehlkonfigurationen leicht ausgenutzt werden?
- **Aktive und unmittelbare Bedrohungen:** Wurde bösartiges Verhalten identifiziert oder erkannt? Mit welcher Wahrscheinlichkeit tritt dieses auf?
- **Ausnutzung von Schwachstellen:** Gibt es bekannte Schwachstellen, die aktiv ausgenutzt werden? Weisen die Daten auf aktive Exploits oder ein hohes Ausnutzungsrisiko hin?

Nachdem die Risiken identifiziert und kategorisiert wurden, kann sich das Sicherheitsteam darauf konzentrieren, einen Aktionsplan zu erstellen. So wird nicht nur die allgemeine Sicherheit verbessert – das Team kann seinen Fokus verlagern und schnell reagieren, wenn eine Zero-Day-Schwachstelle oder ein anderes kritisches Problem auftritt.

4. VALIDIEREN

In dieser Phase validieren Organisationen, wie eine Schwachstelle ausgenutzt werden kann. Dies geschieht in der Regel mit einem Tool oder einer Technologie, die beurteilen und bestätigen kann, ob ein potenzieller Angriff tatsächlich eine Schwachstelle ausnutzen könnte. Oft testen diese Tools auch, wie Monitoring- und Kontrollsysteme auf diese Ausnutzung reagieren würden. Laut Gartner soll „der Validierungsschritt drei Ziele erreichen:

- Bewerten Sie den wahrscheinlichen „Angriffserfolg“[3] indem Sie bestätigen, dass der Angreifer die zuvor entdeckten und priorisierten Gefährdungen tatsächlich ausnutzen könnten.
- Die „höchsten potenziellen Auswirkungen“ abschätzen[4], die über den anfänglichen Fußabdruck hinausgehen und alle potenziellen Angriffspfade zu einem kritischen geschäftlichen Asset analysieren.
- Identifizieren, ob die Prozesse zur Ergreifung von Gegenmaßnahmen sowohl schnell genug als auch für das Unternehmen angemessen sind.“

5. MOBILISIERUNG

Am Ende eines CTEM-Zyklus besteht das Hauptziel darin, eine Kommunikation über alle relevanten Bedrohungen aufzubauen. Sobald Bedrohungen validiert sind, sollten alle wichtigen Stakeholder benachrichtigt und ein Aktionsplan erstellt werden. Auch wenn die Security in der Regel mit Tools arbeitet, die automatische Gegenmaßnahmen vorsehen, liegt die Gegenmaßnahme nicht allein in ihrer Verantwortung. Jedes Team, das an einem CTEM-Programm beteiligt ist, muss sich dafür einsetzen, die Reibungsverluste bei Genehmigungs- und Implementierungsprozessen sowie bei der Bereitstellung zu verringern.

3, 4 Gartner „Implement a Continuous Threat Exposure Management (CTEM) Program“; Jeremy D'Hoinne, Pete Shoard, Mitchell Schneider; 11. Oktober 2023.

WAS SIND EXPOSURE ASSESSMENT PLATFORMS

Eine grundlegende Komponente eines CTEM-Programms ist eine Exposure Assessment Platform (EAP), die eine breitere Sichtbarkeit der Risiken und einen besseren Schutz bietet als herkömmliche Tools für das Schwachstellen-Management (Vulnerability Management, VM) und das Attack Surface Management (ASM). EAPs sind umfassende Sicherheitslösungen, die Organisationen in Echtzeit und kontinuierlich Einblicke in ihre Umgebung und Angriffsfläche bieten. Die EAP-Abdeckung geht über die Asset-Daten von Erst- und Drittanbietern hinaus und deckt ein breiteres Spektrum an Gefährdungen ab, darunter Identity und Cloud, und bietet Organisationen interne und externe Perspektiven sowie Sichtbarkeit aller IT-Assets.

Im Gegensatz zu herkömmlichen Schwachstellen-Scannern können EAPs potenzielle Gefährdungen auf Basis der Erreichbarkeit und des Verhaltens von Angreifern anhand von simulierten Angriffen und Threat Intelligence validieren und priorisieren. Dies ermöglicht es den Sicherheitsteams, Schwachstellen proaktiv zu erkennen und zu beheben, bevor sie ausgenutzt werden.

EAPs ermöglichen es Sicherheitsteams, einen genauen, umfassenden und kontinuierlichen Überblick über Umgebungen zu erhalten. Die Teams können Assets in Echtzeit nachverfolgen, Risiken aufdecken, kontinuierlich kritische Gefährdungen ermitteln und auf Basis des Unternehmenskontextes Gegenmaßnahmen ergreifen.

Eine EAP hat die Aufgabe, ein CTEM-Programm zu unterstützen. Sie hilft dabei, große Mengen an Daten und Informationen zu sortieren, um die Angriffsfläche eines Unternehmens zu überwachen und den Teams eine Priorisierung der Maßnahmen zu ermöglichen. Darüber hinaus kann eine EAP zusätzlichen Kontext für das Common Vulnerability Scoring System (CVSS) liefern und einen besseren Einblick in die Schwachstellen gewähren. Dies hat oft Kosteneinsparungen und ein besseres Ressourcenmanagement zur Folge.

RAPID7 ERSPART SEINEN KUNDEN DURCHSCHNITTLICH 96 STUNDEN PRO MONAT AN MANUELLEM DATENABGLEICH UND DEDUPLIZIERUNG.

BEWERTUNG VON EAPS

Die Auswahl der richtigen EAP erfordert eine sorgfältige Abwägung mehrerer wichtiger Kategorien und Kriterien. So wird sichergestellt, dass die von Ihnen gewählte Plattform den spezifischen Anforderungen und Sicherheitszielen Ihrer Organisation sowie jeder Phase eines CTEM-Programms entspricht. Dies stellt auch sicher, dass Sie eine Lösung finden, die als Grundlage für Ihr Programm dient und gleichzeitig die übergreifenden strategischen Anforderungen Ihres Unternehmens erfüllt, was eine proaktivere Sicherheitslage ermöglicht.

Bei der Bewertung von EAPs lassen sich mehrere Schlüsselkategorien differenzieren, denen die Funktionen zugeordnet werden können:

- Sichtbarkeit
- Kontinuierliches Monitoring
- Priorisierung von Schwachstellen
- Threat Intelligence
- Gegenmaßnahmen und Abwehr
- Reporting und Analytics

Bei der Bewertung von EAPs können Sie Ihre Auswahl eingrenzen, indem Sie wissen, welche Kategorien und Schlüsselkriterien für Ihre Organisation am relevantesten sind. Wir haben einige der wichtigsten Merkmale von EAPs entsprechend den einzelnen Phasen eines CTEM-Programms aufgeschlüsselt, um Ihnen die Entscheidung zu erleichtern.

Scoping und Erkennung

Zur Unterstützung der Scoping- und Erkennungsphase eines CTEM-Programms sollte sich eine EAP auf eine umfassende Sichtbarkeit der Assets und Umgebungen konzentrieren. Die wesentlichen Funktionen, die eine EAP zur Unterstützung in dieser Phase anbieten sollte, fallen in diese Kategorien:

- Umfassendes Angriffsflächenmanagement und Sichtbarkeit
- Asset-Inventar- und Topologie-Abbildung
- Erkennung von Lücken in der Sicherheitsabdeckung
- Monitoring der Zugangskontrolle
- Automatisierte Sicherheitstests

Asset-Erkennung und einheitliche Inventarisierung

Dadurch erhalten die Endnutzer ein vollständiges und dynamisches Inventar aller Assets in ihrem gesamten digitalen Besitz mit genauen und aktuellen Informationen.

Warum es wichtig ist

Um Ihre Sicherheitslage zu verstehen, benötigen Sie einen Überblick über alle Assets in Ihren Umgebungen. Man kann nur das schützen, was man auch sehen kann. Viele Unternehmen tun sich schwer damit, immer genau zu wissen, welche Assets gerade wichtig sind und geschützt werden müssen. Dieses Feature ist extrem wichtig und bildet die Basis für die Erfassungs- und Entdeckungsphase. Ohne sie wird es schwierig, ein CTEM-Programm überhaupt weiterzuführen.

WICHTIGSTE FRAGEN UND ÜBERLEGUNGEN

- Für welche Asset-Typen (z. B. Software, Identitäten/Benutzer, Webanwendungen, SaaS) liefert die Plattform Sichtbarkeit?
- Können benutzerdefinierte Asset-Typen zur Lösung hinzugefügt werden?

Sofort einsatzbereite API-Konnektoren

Eine EAP sollte über vorgefertigte Konnektoren verfügen, die von flexiblen APIs gesteuert werden, sowie über eine Vielzahl von bestehenden Sicherheits- und Netzwerk-Tools. Entscheidungsträger sollten nicht nur auf die Anzahl der Konnektoren achten, sondern auch darauf, ob die Plattform über bestehende Konnektoren mit ihrem spezifischen Technologie-Stack verfügt oder nicht.

Warum es wichtig ist

Um Assets und Identitäten in Ihrem gesamten Unternehmen effektiv zu erfassen und kontinuierlich zu entdecken, muss sich eine EAP problemlos in alle vorhandenen Sicherheits- und Netzwerk-Tools integrieren lassen, ohne dass eine umfangreiche Konfiguration erforderlich ist. Ohne die Integration in bestehende Tools können Sie keine umfassende Sichtbarkeit und kein Angriffsflächenmanagement erreichen, was zu Sicherheitslücken durch nicht überwachte Assets führen kann.

WICHTIGSTE FRAGEN UND ÜBERLEGUNGEN

- Wie viele vorgefertigte Konnektoren oder Integrationen bietet die Lösung?
- Verfügt die Lösung über die spezifischen Konnektoren, die Sie für Ihre Umgebung und Ihren Tech-Stack benötigen?
- Welche Informationen müssen Sie bereitstellen, um mit der Erfassung von Daten aus Drittanbieterquellen zu beginnen?
- Wie oft werden die Daten aus Drittanbieterquellen aktualisiert und kann die Frequenz angepasst werden?
- Können Daten aus Quellen erfasst werden, die nicht über einen vordefinierten Konnektor/eine vorgefertigte Integration verfügen? Kann die Datenqualität der verschiedenen Datenquellen beurteilt werden?

Verwaltung und Anpassbarkeit der Plattform

Hier geht es darum, ob Endnutzer Verwaltungsmaßnahmen vornehmen, Konfigurationen aktualisieren und Aspekte der Plattform anpassen können. Dies beinhaltet z. B. die Scanfrequenz, das Hinzufügen von Nutzern und das Erstellen von API-Konnektoren.

Warum es wichtig ist

Benutzer müssen ihre EAP an ihre spezifischen Bedürfnisse anpassen können. Dazu gehört auch die Konfiguration und Instrumentierung ihrer Umgebung im Hinblick auf die Team- und Verwaltungsrichtlinien. Damit Assets in allen Umgebungen und Infrastrukturen richtig erfasst und erkannt werden können, sollte eine EAP anpassbar sein. Unternehmen haben unterschiedliche Bedürfnisse, Anforderungen und Tools, und eine EAP sollte diesen gerecht werden.

WICHTIGSTE FRAGEN UND ÜBERLEGUNGEN

- Können Administratoren mit der Lösung eigene Konnektoren/Integrationen erstellen?
- Wie kann ein Administrator Konfigurationen hinzufügen, ändern oder löschen?
- Für welche Konfigurationen oder Änderungen ist technischer Support erforderlich?
- Wie können Administratoren die Scanfrequenz erhöhen?
- Können die Korrelationsregeln an verschiedene Dateneingaben angepasst werden?

Speziell entwickeltes, natives Erkennen und Scannen

Die EAP sollte native Scanning- und/oder Harvesting-Funktionen mit einer Vielzahl von Datenerfassungsmechanismen und -ansätzen bieten, um diverse Asset-Typen zu berücksichtigen.

Warum es wichtig ist

Durch ihre nativen Scan-Funktionen ermöglichen EAPs die Konsolidierung Ihres Technologie-Stacks und bieten einen besseren Asset-Kontext. Dazu gehören Asset-Informationen wie Konfigurationen, Abhängigkeiten und Schwachstellen. Die Lösungen müssen Erfassungsmechanismen bieten, die speziell auf die Anforderungen bestimmter Umgebungen und Asset-Typen zugeschnitten sind, wie z. B. Cloud- und Container-Workloads. Bietet eine Lösung diese Funktionen nicht, benötigen Sie wahrscheinlich mehrere verschiedene Tools für die Anpassung an Ihre einzelnen Umgebungen und Assets.

WICHTIGSTE FRAGEN UND ÜBERLEGUNGEN

- Bietet der Anbieter native Funktionen zur Asset-Erkennung, zum Fingerprinting oder zum Scannen von Schwachstellen?

Analyse und Validierung von Sicherheitskontrollen

Die Plattform sollte Ihre Umgebung auf nachgelagerte kompensierende Sicherheitskontrollen, wie z. B. einen Endpoint-Agenten, eine Netzwerk-Firewall oder eine Zugriffsrichtlinie, überprüfen können und die Ausnutzbarkeit und die potenziellen Auswirkungen einer bestimmten Schwachstelle verstehen.

Warum es wichtig ist

Um festzustellen, ob ein kompromittiertes Asset wirklich zugänglich ist oder das Potenzial hat, ausgenutzt zu werden, ist es wichtig zu wissen, welche nachgelagerten kompensierenden Kontrollen vorhanden sind, die den Datenverkehr oder den Zugriff blockieren würden. Diese Sichtbarkeit kann Ihrem Team helfen, das relative Risiko einer bestimmten Schwachstelle oder eines spezifischen Assets zu verstehen und Abwehrmaßnahmen zu priorisieren.

WICHTIGSTE FRAGEN UND ÜBERLEGUNGEN

- Für welche Sicherheitskontrollen führt die Plattform Monitoring durch?
- Bietet die Lösung granulare Sichtbarkeit bzgl. der Konfiguration der Sicherheitskontrolle?
- Wie werden die Endbenutzer über Kontrolllücken informiert?
- Wie oft werden die Kontrollen validiert und können die Benutzer die Häufigkeit anpassen?
- Wie erkennt die Plattform die Abdeckung von Schwachstellen-Scans, EDR, Verschlüsselung und anderen Sicherheitskontrollen?
- Welche Kontrollen bietet der Anbieter selbst an?

Kontextuelle Anreicherung und dynamische Asset-Kennzeichnung

Dynamisches Asset-Tagging und kontextbezogene Anreicherung sind entscheidend für Sicherheitsteams, die ihre Umgebung mehr im Detail verstehen und gleichzeitig effektivere Entscheidungen beim Risikomanagement und der Prioritätensetzung in der gesamten Organisation treffen möchten. EAP-Lösungen sollten Teams in die Lage versetzen, einem überwachten Asset einen relevanten Kontext zuzuordnen, einschließlich der Art des Assets, der mit ihm verbundenen Workloads, der Eigentumsrechte an dem Asset und der Befugnis zur Problemlösung, zum Fingerprinting, zu kompensierenden Kontrollen und zur Bedeutung oder zum Wert des Assets.

Warum es wichtig ist

Mit erweiterten Funktionen zur Aufdeckung können Sie die Sichtbarkeit Ihrer Assets verbessern und die relative Bedeutung und Risikostufe eines gefährdeten Assets nachvollziehen. Bei herkömmlichen Tools für das Schwachstellen-Management sind diese Informationen bei der Durchführung von Untersuchungen oft nicht ohne weiteres bekannt oder verfügbar. Organisationen müssen die Hygiene beim Taggen und Badgen verbessern und Lösungen einführen, die entweder die Assets selbst dynamisch taggen oder Tag-Informationen von anderen Drittsystemen aufnehmen können, um möglichst detaillierte und vollständige Informationen zu erhalten.

WICHTIGSTE FRAGEN UND ÜBERLEGUNGEN

- Welchen Kontext über entdeckte Assets bietet die Plattform?
- Welchen zusätzlichen Umgebungskontext in Bezug auf das Asset, wie z. B. Eigentümer, Fingerprinting, kompensierende Kontrollen und die Kritikalität des Assets, bietet die Plattform?
- Welche Datenquellen kann die Plattform nutzen, um zusätzlichen geschäftlichen und umweltbezogenen Kontext bereitzustellen?
- Wie werden Asset-Tags aus anderen Quellen importiert?
- Sind Tags anpassbar?

Aufdeckung externer Angriffsflächen

Die Plattform sollte native Funktionen für das Scannen von extern zugänglichen Assets mithilfe von internetbasierten Scans sowie für die Integration von Daten aus beliebten Open-Source-Tools wie Shodan bieten.

Warum es wichtig ist

Regelmäßiges und kontinuierliches Monitoring und Erkennen von extern zugänglichen Assets und Systemen hilft Ihnen und Ihrem Team, über das Internet zugängliche Assets zu erkennen, die falsch konfigurierte öffentliche Cloud-Services und Server sowie gefährdete Unternehmensdaten aufweisen. Ohne eine umfassende Sichtbarkeit der Angriffsfläche, wozu auch die internen und externen Assets zählen, setzen Sie Ihre Organisation potenziellen Bedrohungen und Ausnutzungen durch Sicherheitslücken oder eine unklare Asset-Inventur aus.

WICHTIGSTE FRAGEN UND ÜBERLEGUNGEN

- Mit welcher Technologie werden externe Assets erkannt?
- Wie häufig werden Discovery-Scans durchgeführt?
- Welche Open-Source-Komponenten werden für die Erkennung externer Assets verwendet?
- Welche manuellen Eingaben sind vom Endnutzer erforderlich, um externe Scans durchzuführen?
- Welche zusätzlichen Informationen werden den Kunden nach den ersten Eingaben zur Verfügung gestellt (z. B. potenziell eigene IPs oder Tochtergesellschaften)?
- Welche Nachweise für die Asset-Zuordnung werden erbracht?
- Wie werden die Daten der externen Angriffsfläche dem internen Kontext zugeordnet?
- Integriert das Tool Erkenntnisse aus externen und internen Scans?

Software-Lieferkette und CI/CD-Integration

Die Lösung sollte Risiken über den gesamten Entwicklungs-Lifecycle hinweg bewerten. Sie sollte auch Abhängigkeiten von Drittanbietern, Softwarekomponenten (über die Software-Stückliste) und Infrastructure-as-Code (IaC)-Konfigurationen bewerten, um Schwachstellen und Fehlkonfigurationen vor der Bereitstellung zu erkennen.

Die Plattform sollte automatisierte Sicherheitsprüfungen in CI/CD-Pipelines integrieren, wie statische Software-Testverfahren (Static Application Security Testing, SAST) und dynamische Software-Testverfahren (Dynamic Application Security Testing, DAST), und Build-Artefakte validieren, um die Integrität sicherzustellen. Das Monitoring in Echtzeit auf Anomalien, offengelegte Geheimnisse und die Erkennung von Drifts nach der Bereitstellung sind ebenfalls entscheidend für die Aufrechterhaltung der Sicherheit. Durch die Kombination von Threat Intelligence, Angriffspfad-Analysen und automatisierten Behebungs-Workflows stellt die Plattform sicher, dass Risiken sowohl in der Vorproduktions- als auch in der Produktionsumgebung identifiziert, nach Prioritäten geordnet und effizient behoben werden.

Warum es wichtig ist

Die Integration der Software-Lieferkette und der CI/CD-Pipelines in das Risiko- und Exposure Management-Programm ist entscheidend, um den Entwicklungs-Lifecycle abzusichern und Schwachstellen zu reduzieren, bevor sie die Produktion erreichen. Da immer mehr Unternehmen einen Shift-Left-Ansatz verfolgen, ist es wichtig, über Tools zu verfügen, die sich in die Workflows der Entwickler integrieren lassen. So können Sie sicherstellen, dass Ihr Team sichere Software direkt in der Entwicklungsumgebung erstellt, um das Risiko einzudämmen und eine starke Sicherheitslage in der Produktion aufrechtzuerhalten.

WICHTIGSTE FRAGEN UND ÜBERLEGUNGEN

- **Bietet die Plattform die folgenden Features?**
  - Abdeckung von Code, CI/CD-Pipelines und Produktionsumgebungen.
  - Die Fähigkeit, Software-Abhängigkeiten zu erstellen, zu überwachen und zu bewerten.
  - Nahtlose Sicherheitsintegration mit Tools wie Jenkins, GitHub und GitLab.
  - Unterstützung für SAST-, DAST- und IaC-Scans in den Stufen vor der Bereitstellung.
  - Risikoanalyse für Container-Images und IaC.
- **Welche kontextuellen Einblicke werden geboten, um ausnutzbare Schwachstellen in der Lieferkette zu priorisieren?**
- **Kann die Lösung offengelegte Geheimnisse, Abweichungen und unbefugte Änderungen in Pipelines erkennen?**
- **Welche Optionen gibt es für praxisrelevante, automatisierte Behebungen, die in Entwickler-Tools integriert sind?**
- **Welche vorgefertigten Richtlinienpakete für Frameworks wie NIST, CIS und PCI DSS stehen zur Verfügung?**
- **Kann die Lösung potenzielle Risiken und laterale Bewegungspfade über Systeme hinweg visualisieren?**

Priorisieren

Im Hinblick auf die Priorisierungsphase eines CTEM-Programms sollte eine effektive EAP über Funktionen verfügen, die sowohl das traditionelle Scoring und Management von Schwachstellen als auch kontextbezogene Kriterien zur Risikobewertung nutzen.

Diese Funktionen lassen sich in die folgenden Kategorien einteilen:

- Risikobasiertes Schwachstellenmanagement
- Kontextualisierte Risikobewertung
- Visualisierung und Validierung von Angriffspfaden

Dynamische Analyse der Kritikalität von Assets

Eine EAP sollte die Kritikalität von Assets auf Basis ihrer Rolle und Bedeutung für das Unternehmen bewerten und einstufen, um die Reaktionsmaßnahmen und die Ressourcenzuweisung effektiv zu priorisieren. Dazu gehören Risikofaktoren und aktive Bedrohungslandschaften, die Einfluss auf das digitale Ökosystem einer Organisation haben.

Warum es wichtig ist

Teams müssen die Kritikalität ihrer verschiedenen digitalen Assets verstehen, um bei der Priorisierung und Entscheidungsfindung für Gegenmaßnahmen zu helfen. In Szenarien, in denen mehrere Assets betroffen sind, kann es Ihrem Team helfen, festzulegen, welches Problem zuerst behoben werden muss. Außerdem wird ermittelt, was ein böswilligen Akteur möglicherweise ausnutzen könnte. Dieses Wissen beugt Schwachstellen vor und mindert das Risiko, wodurch Ihr Unternehmen einen Verstoß oder eine Kompromittierung vermeiden kann.

WICHTIGSTE FRAGEN UND ÜBERLEGUNGEN

- Welche betrieblichen Auswirkungen hätte es, wenn das Asset aufgrund einer Kompromittierung offline wäre, einschließlich finanzieller Verluste, Reputationsschäden oder regulatorischer Strafen?
- Wird das Asset derzeit von einem bösartigen Akteur ins Visier genommen (auf Basis von Bedrohungsinformationen)?
- Wird es von bestimmten APT-Gruppen angegriffen?
- Ist das Asset öffentlich zugänglich und/oder erreichbar?
- Bietet diese Ressource Möglichkeiten zur Ausbreitung im Netzwerk, z. B. durch einen aktiven Angriffspfad oder die Möglichkeit einer Privilegienerweiterung?
- Gibt es betriebliche Einschränkungen oder Herausforderungen im Zusammenhang mit dem empfohlenen Patching-Prozess?
- Unterliegt das betreffende Asset Compliance-Verpflichtungen oder einer behördlichen Prüfung?

Anreicherung und Bewertung des Schweregrads einer Schwachstelle

Die Plattform sollte eine native Risikobewertung von Schwachstellen bieten, die durch das CVSS, die proprietäre Risikobewertungsmethode des Anbieters und die Common Vulnerabilities and Exposures (CVE) informiert wird. Neben diesen Bewertungen sollte eine EAP die Informationen aus der Threat Intelligence und dem Kontext Ihrer spezifischen Umgebung und Aktivität berücksichtigen, um Schwachstellen effektiv zu priorisieren.

Warum es wichtig ist

Sicherheitsteams müssen dabei unterstützt werden, den Schweregrad einer bestimmten Schwachstelle zu erkennen, Prioritäten bei der Behebung zu setzen und die Bedeutung und den potenziellen Einfluss einer Schwachstelle im Falle ihres Ausnutzens zu kommunizieren. Zero-Day-Schwachstellen, Sicherheitsvorfälle und Verstöße treten immer häufiger auf, wodurch es schwierig werden kann, die Aufmerksamkeit Ihres Teams zu konzentrieren. Das Scoring hilft Ihnen dabei, das Rauschen zu unterdrücken und sich auf das zu konzentrieren, was wirklich wichtig ist.

WICHTIGSTE FRAGEN UND ÜBERLEGUNGEN

- Welche CVSS-Scoring-Version(en) unterstützt die Lösung?
- Welche zusätzlichen Bewertungsmethoden sind neben CVSS verfügbar oder werden unterstützt?
- Welche kontextbezogenen Informationen stehen zur Verfügung bzw. werden verwendet, um Scoring-Entscheidungen zu beeinflussen?
- Unterstützt die Lösung Open-Source-Quellen für Informationen über Schwachstellen (wie CISA, FIRST und NIST)?

Bewertung der Sicherheitskontrolle

Die Plattform sollte in der Lage sein, die Wirksamkeit von Sicherheitskontrollen, wie z. B. einer Firewall oder einer Endpoint Protection Platform (EPP), kontinuierlich zu bewerten, während diese in Ihrer gesamten digitalen Umgebung implementiert werden. Dies stellt sicher, dass sie wie vorgesehen funktionieren und die Sicherheitsanforderungen für das System angemessen erfüllt werden.

Warum es wichtig ist

Um Gefährdungen richtig einschätzen und priorisieren zu können, muss Ihr Team genau wissen, wie wirksam die vorhandenen Kontrollen sind. Durch die kontinuierliche Bewertung der Kontrollen kann eine EAP die Performance aller Kontrollen beurteilen und sie nach Risiko kategorisieren, anstatt davon auszugehen, dass alle potenziell gefährdeten Assets die gleiche Risikostufe haben.

WICHTIGSTE FRAGEN UND ÜBERLEGUNGEN

- Wie gut setzt die Lösung Prioritäten bei der Beseitigung von Gefährdungen?
- Wie werden Funktionen wie Bedrohungsdaten, geschäftliche Auswirkungen, Angriffspfadmodellierung, kontinuierliche Sicherheitstests und kompensierende Kontrollen bei Priorisierungsentscheidungen berücksichtigt?
- Wie transparent ist die Berechnung/der Ansatz, mit der/dem die Gefährdungen priorisiert werden?
- Wie reagiert die Lösung auf prominente und neu auftretende Schwachstellen?
- Berücksichtigt die Plattform aktiv ausgenutzte Schwachstellen innerhalb und außerhalb der Kundenumgebung?
- Wie aggregiert und dedupliziert die Plattform Gefährdungsdaten aus verschiedenen Quellen?

Scannen auf Codeebene

Beim Scannen auf Codeebene werden der Quellcode von Anwendungen, Konfigurationsdateien und IaC-Vorlagen analysiert, um Schwachstellen, Fehlkonfigurationen und unsichere Codierungspraktiken frühzeitig im Lifecycle der Entwicklung zu erkennen. Durch die Integration in CI/CD-Pipelines stellt dieser Ansatz sicher, dass sowohl der Anwendungscode als auch die Infrastrukturdefinitionen sicher sind, bevor sie in die Produktion ausgerollt werden.

Warum es wichtig ist

In modernen Entwicklungsumgebungen kann die Sicherheit kein nachträglicher Gedanke sein. Scannen auf Codeebene, einschließlich IaC, hilft Organisationen, einen Shift-Left-Ansatz zu verfolgen, indem es Schwachstellen bereits in den frühesten Stufen der Entwicklung identifiziert und behebt. Die frühzeitige Integration von Sicherheitsmaßnahmen stellt sicher, dass sich eine Schwachstelle oder ein Sicherheitsproblem nicht im gesamten Code ausbreitet oder in die Produktion gelangt. Dadurch können Unternehmen Risiken minimieren, ohne Workflows zu unterbrechen.

WICHTIGSTE FRAGEN UND ÜBERLEGUNGEN

- Unterstützt die Lösung das Scannen über moderne Frameworks, Sprachen und IaC-Tools wie Terraform, AWS CloudFormation und Kubernetes-Manifeste hinweg?
- Wie gut lässt sich die Lösung in bestehende CI/CD-Pipelines integrieren (z. B. Jenkins, GitHub Actions)?
- Kann das Tool hart kodierte Geheimnisse oder sensible Informationen erkennen und deren Weitergabe verhindern? Bietet es den Entwicklern praxisrelevante Anleitungen, um erkannte Probleme effizient zu beheben?
- Wie effektiv analysiert die Lösung Drittanbieter-Bibliotheken und -Abhängigkeiten auf bekannte Schwachstellen?
- Unterstützt es die Durchsetzung von Richtlinien für Programmierungsstandards, Sicherheits-Benchmarks (z. B. CIS) und Compliance-Frameworks?

Analyse des Angriffspfads

Die Plattform bietet eine klare und umfassende Methode, mit der sich abbilden lässt, wie Angreifer Schwachstellen ausnutzen können, um sich durch On-Premises- und Cloud-Umgebungen zu bewegen.

Warum es wichtig ist

Um Prioritäten bei den Abwehrmaßnahmen zu setzen, müssen Sie verstehen, wie Angreifer sich in Ihrer Umgebung bewegen, sei es On-Premises oder in der Cloud. Durch die Kartierung von Angriffspfaden kann Ihr Team Schwachstellen identifizieren, die Angreifer ausnutzen könnten, um ihre Berechtigungen zu erweitern oder sich systemübergreifend zu bewegen. Dank dieser Einblicke können Sie Ihre Ressourcen auf die am meisten gefährdeten Bereiche konzentrieren und das Risiko verringern, bevor ein Angriff erfolgt.

WICHTIGSTE FRAGEN UND ÜBERLEGUNGEN

- Bietet die Plattform eine detaillierte Kartierung der Eintrittspunkte und Ausbreitungswege von Angreifern im Netzwerk?
- Wie oft werden diese Angriffspfade aktualisiert, um Änderungen der Infrastruktur in Echtzeit zu berücksichtigen?
- Kann das Tool erkannte Angriffspfade auf Basis aktiver Bedrohungen, Fehlkonfigurationen oder spezifischer Angriffsszenarien automatisch synthetisch testen und validieren?

Validieren

Für die Validierungsphase eines CTEM-Programms sollte eine EAP Funktionen zur Simulation von Angriffen und zum Testen der Wirksamkeit von Sicherheitskontrollen bieten, um potenzielle Schwachstellen aufzudecken. Automatisierte Sicherheitstests und kontinuierliche Validierung sind zwei wichtige Kategorien, in die EAP-Funktionen in dieser Phase fallen.

Dynamic application security testing (DAST)

Die Plattform verfügt über eine automatisierte Testfunktion, die Scanner einsetzt, um Schwachstellen in Live- oder Vorproduktions-Webanwendungen und APIs zu identifizieren, indem sie reale Angriffsszenarien simulier

Warum es wichtig ist

Moderne Anwendungen sind aufgrund ihrer Komplexität und Gefährdung durch das Internet häufig das Ziel von Angreifern. DAST ermöglicht es Organisationen, Schwachstellen in der Entwicklungs- und Vorproduktionsphase zu identifizieren und so das Risiko vor der Bereitstellung erheblich zu verringern. Durch frühzeitiges Erkennen solcher Vorfälle werden kostspielige Abhilfemaßnahmen in der Produktion minimiert und die Sicherheitslage kritischer Anwendungen insgesamt verbessert.

WICHTIGSTE FRAGEN UND ÜBERLEGUNGEN

- Wie viele Scan-Engines sind enthalten?
- Sind diese Open Source oder kostenpflichtig?
- Wie hoch ist der Prozentsatz der identifizierten falsch-positiven Ergebnisse?
- Wie viele Angriffs-Frameworks unterstützt die Lösung standardmäßig?
- Welche Integrationen stehen zur Verfügung, um Anwendungsscans in die CI/CD-Pipeline zu integrieren?

Kontinuierliche Gefährdungsvalidierung

Eine Plattform, die über einen Service zur kontinuierlichen Gefährdungsvalidierung verfügt, stellt sicher, dass Sie stets wissen, wo Schatten-IT oder unbekannte Unternehmen-Assets vorhanden sein könnten. Dazu gehören exponierte Webdienste, Remote-Verwaltungsdienste, potenzielle Remote-Zugriffsrisiken und riskante oder unverschlüsselte Services.

Warum es wichtig ist

Die Bedrohungslandschaft entwickelt sich ständig weiter, und statische Sicherheitsanalysen werden neuen Angriffstechniken oft nicht gerecht. Eine kontinuierliche Gefährdungsvalidierung stellt sicher, dass die Sicherheitskontrollen im Laufe der Zeit wirksam bleiben, indem Umgebungen auf reale Verhaltensweisen von Angreifern getestet werden. Dieser fortlaufende Validierungsprozess hilft Teams, Schwachstellen zu erkennen und zu beheben, bevor sie ausgenutzt werden können.

WICHTIGSTE FRAGEN UND ÜBERLEGUNGEN

- Wie oft überprüft der Service die Gefährdungspunkte der Angriffsoberfläche?
- Erstattet er detailliert Bericht über die Ergebnisse der Validierung und die Fortschritte bei der Risikominderung?
- Wie gut simuliert die Lösung das Verhalten von Angreifern, um sich entwickelnde Schwachstellen und Fehlkonfigurationen zu testen?

Mobilisieren

In der letzten Phase sollte sich eine EAP problemlos in die Workflows von Entwicklern und in vorhandene Tools integrieren lassen, damit die Teams Vorfälle leichter kommunizieren und beheben können. EAP-Funktionen in dieser Phase fallen typischerweise unter diese Kategorien:

- Compliance- und Richtlinienmanagement und -durchsetzung
- Integration mit der CI/CD-Pipeline und Entwickler-Tools
- Anpassbare Dashboards und Reporting

Integrierte Automatisierung und Durchsetzung von Richtlinien

Diese Funktion einer EAP ermöglicht Ihrer Organisation die Automatisierung von Sicherheitsmaßnahmen und die Durchsetzung von Richtlinien in allen Umgebungen. Durch den Einsatz vorgefertigter Automatisierungsworkflows und Funktionen zur Richtliniendurchsetzung können Teams in Ihrem Unternehmen die einheitliche Einhaltung von Sicherheitsstandards und Compliance-Frameworks gewährleisten.

Warum es wichtig ist

Eine manuelle Verwaltung der Sicherheit ist sowohl zeitaufwändig als auch fehleranfällig. Integrierte Automatisierung und Richtliniendurchsetzung sind entscheidend für Organisationen, die ihre Sicherheitsprogramme skalieren möchten, ohne ihre Teams zu überfordern. Wenn die EAP beispielsweise einen Richtlinienverstoß feststellt, kann sie den Vorfall automatisch angehen und beheben. Das Sicherheitsteam muss die Bewertung nicht mehr manuell vornehmen und die EAP kann potenziell Zeit sparen, indem sie eine nicht genehmigte Änderung rückgängig macht oder stattdessen eine genehmigte Konfiguration anwendet.

WICHTIGSTE FRAGEN UND ÜBERLEGUNGEN

- Wie behebt die Lösung automatisch Lücken in den Sicherheitskontrollen?
- Welche nativen Automatisierungsfunktionen bietet die Plattform im Vergleich zu Workflows über Drittanbieterintegrationen?
- Welche Maßnahmen können über bestehende Integrationen mit Datenquellen und Werkzeugen von Drittanbietern ergriffen werden?

Anpassbare Live Dashboards und Reporting

Plattformen mit anpassbaren, zentralisierten Dashboards und Live-Berichten bieten Sicherheitsteams einen gezielten Überblick über ihre Umgebung, Schwachstellen und laufenden Aktivitäten. Mit einer EAP können Benutzer dynamische Echtzeit-Visualisierungen erstellen, um wichtige Performance-Metriken zu überwachen und die Sicherheitslage gegenüber den Stakeholdern zu demonstrieren.

Warum es wichtig ist

Effektive Berichterstattung und Sichtbarkeit sind für die Kommunikation von Risiken und Fortschritten in der gesamten Organisation unerlässlich. Ein zentrales Dashboard erleichtert die Entscheidungsfindung durch Sichtbarkeit in Echtzeit und ermöglicht es Führungskräften, fundierte, datengestützte Entscheidungen zu treffen, insbesondere bei einem kritischen Vorfall oder einer Entwicklung, die möglicherweise Ihre sofortige Aufmerksamkeit erfordern. Außerdem verbessert es die Zusammenarbeit, da Dashboards von verschiedenen Teams gemeinsam genutzt werden können, um eine Abstimmung hinsichtlich Zielen, Prioritäten und Verantwortlichkeiten zu gewährleisten.

WICHTIGSTE FRAGEN UND ÜBERLEGUNGEN

- Welche Berichte gibt es, die auf die Bedürfnisse von Führungskräften zugeschnitten sind, inklusive Benchmarking, Risikostatus und Fortschrittskontrolle auf Teamebene?
- Inwieweit unterstützt die Lösung Berichte, die neu erkannte Assets, ihren Status und ihre Sicherheitslage einschließlich der Compliance mit Kontrollen aufzeigen?
- Inwieweit unterstützt die Lösung Stakeholder-Berichte, die den Status der Abhilfemaßnahmen bei Gefährdungen aufzeigen, die an die relevanten Stakeholder weitergeleitet wurden?
- Wie gut ermöglicht die Lösung den Benutzern, Berichte mit benutzerdefiniertem Format zu erstellen?

Remediation Workflows

Remediation Workflows rationalisieren den Prozess der Behebung identifizierter Risiken und Schwachstellen durch die Zuweisung von Aufgaben, die Verfolgung des Fortschritts und die Integration in den IT-Betrieb. Dank einer EAP muss ein Event nicht mehr von einer Person ausgelöst werden, sondern kann sofort in einen Remediation Workflow überführt werden, der sicherstellt, dass es entweder automatisch bearbeitet oder an das richtige Teammitglied weitergeleitet wird.

Warum es wichtig ist

Diese Workflows bieten klare Schritte und Verantwortlichkeiten in Bezug auf Abhilfemaßnahmen und sorgen so für eine zeitgerechte Lösung von Vorfällen. Ihr Team muss keine Zeit mehr mit einfachen Aufgaben verbringen, da diese in der Regel automatisch erledigt werden können. So bleibt ihm mehr Zeit, sich auf anspruchsvollere und wertvollere Aufgaben zu konzentrieren. Da die Workflows anpassbar sind, können Sie außerdem sicherstellen, dass jeder Workflow mit allen anderen Tools und Systemen integriert wird, die Ihr Team derzeit verwendet.

WICHTIGSTE FRAGEN UND ÜBERLEGUNGEN

- Wie können Endbenutzer Lücken in der Sicherheitskontrolle und Fortschritte bei der Beseitigung von Gefährdungen verfolgen und koordinieren?
- Welche Integrationen in Gegenmaßnahmen-Orchestrierungssysteme von Drittanbietern werden unterstützt?
- Wie wird der Korrekturstatus von Drittanbietersystemen, wie IT Service Management, verfolgt und verwaltet?
- Wie identifiziert die Lösung die für die Gegenmaßnahmen Verantwortlichen?
- Wie gut unterstützt der Anbieter die Funktionen zur Automatisierung der Gegenmaßnahmen?
- Bietet die Lösung eine praxisrelevante Anleitung zur Behebung von Gefährdungen, die nicht durch Automatisierung behoben werden können?
- Wie interagieren Teams außerhalb der Security, wie zum Beispiel Entwickler, mit den Daten?

Es ist von entscheidender Bedeutung, dass Sie Ihre EAP-Bewertungskriterien auf die spezifischen Bedürfnisse Ihres Unternehmens abstimmen. Ein guter Anfang ist die Überprüfung der Kriterien durch Ihr Security Operations Center (SOC), das dann die wichtigsten Funktionen priorisieren und mit den Zielen Ihrer Organisation in Einklang bringen sollte. Wenn Ihr Sicherheitsteam zum Beispiel eher klein ist, werden Sie wahrscheinlich eine EAP mit robusten Automatisierungsfunktionen bevorzugen, um Ihre Abläufe zu optimieren und Ressourcenverschwendung zu vermeiden. Durch die aktive Einbeziehung Ihres SOC können Sie sicherstellen, dass die EAP mit der Risikobereitschaft und dem übergreifenden strategischen Plan Ihrer Organisation in Einklang steht.

AUSWAHL DER RICHTIGEN EAP

Es ist von entscheidender Bedeutung, Wege zu finden, um Unternehmen vor neuen Bedrohungen zu schützen. Die Einführung und Implementierung des richtigen EAP als Grundkomponente eines CTEM-Programms ist eine Möglichkeit, das Risiko proaktiv zu mindern. Aber eine erfolgreiche Implementierung geht über die Auswahl der richtigen Lösung hinaus. Für eine effektive Implementierung und um Ihre Angriffsfläche wirksam abzusichern, benötigen Sie einen zuverlässigen Anbieter. Ein guter Partner kann Anleitung zur Implementierung geben, bei der Integration helfen und fortlaufendes Training sowie Support bieten, um die Plattform und Ihre Nutzung zu optimieren.

Mit der Einführung einer EAP durch einen vertrauenswürdigen Partner kann Ihr Unternehmen seine Sicherheitslage verbessern, seine Ressourcen optimieren und Risiken und Bedrohungen kontinuierlich eindämmen.

Gefährdungen mit Rapid7 Exposure Command lokalisieren und priorisieren

Laut Gartner® können „nur 17 % der Organisationen die Mehrheit (95 % oder mehr) ihrer Assets eindeutig identifizieren und inventarisieren“.[5] Dieser Mangel an Sichtbarkeit führt zu erheblichen Sicherheitslücken, die Bedrohungsakteure ausnutzen können. Um die vollständige Kontrolle und Sichtbarkeit Ihrer gesamten Angriffsfläche zu erhalten, ist ein Tool wie Exposure Command von Rapid7 unerlässlich.

Rapid7 Exposure Command bietet nicht nur vollständige Transparenz über die Angriffsfläche, sondern auch einen hochpräzisen Risikokontext und Einblicke in die Sicherheitslage Ihres Unternehmens. Dabei werden die Ergebnisse sowohl unserer nativen Funktionen zur Erkennung von Schwachstellen als auch von bereits vorhandenen Schwachstellen- und Anreicherungsquellen von Drittanbietern zusammengeführt. Durch dieses Situationsbewusstsein können sich die Teams gezielt auf die Gefährdungen und Schwachstellen konzentrieren, die Angreifer im Visier haben – mit dem bedrohungsbezogenen Risikokontext, der für eine effizientere und effektivere Priorisierung erforderlich ist.

Indem Sie Rapid7 Exposure Command in Ihr CTEM-Programm einbinden, stellen Sie sicher, dass Sie über den besten Schutz und die besten Einblicke verfügen, um Schwachstellen zu identifizieren, zu priorisieren und zu beheben, sobald sie auftreten. So hat Ihr Team mehr Zeit und Ressourcen, um sich auf erfolgsentscheidende Aufgaben zu konzentrieren.

ERHALTEN SIE EINE KONTINUIERLICHE 360°-ANSICHT IHRER ANGRIFFSFLÄCHE

Kostenlose Testversion

ENTDECKEN SIE EXPOSURE COMMAND

Sehen Sie unsere Produkte in Aktion

5 Gartner; Innovation Insight: Attack Surface Management; Mitchell Schneider, Pete Shoard, John Watts; 9. April 2024

Über Rapid7

Rapid7 schafft eine sicherere digitale Zukunft für alle, indem es Unternehmen dabei hilft, ihre Sicherheitsprogramme vor dem Hintergrund des sich beschleunigenden digitalen Wandels zu stärken. Unser Portfolio erstklassiger Lösungen versetzt Sicherheitsexperten in die Lage, Risiken zu managen und Bedrohungen über die gesamte Bedrohungslandschaft hinweg zu beseitigen – von Apps über die Cloud bis hin zur traditionellen Infrastruktur und dem Dark Web. Wir fördern Open-Source-Communities und innovative Forschung und nutzen diese Einblicke zur Optimierung unserer Produkte und zur Aufklärung der globalen Sicherheits-Community über die neuesten Angriffsmethoden. Weltweit vertrauen mehr als 11.000 Kunden auf unsere branchenführenden Lösungen und Services, mit denen sie Angreifern und der Konkurrenz immer einen Schritt voraus und für die Zukunft gerüstet sind.

RAPID7

PRODUKTE

Cloud Security
XDR und SIEM
Threat Intelligence
Vulnerability Risk Management
Application Security
Orchestrierung & Automatisierung
Managed Services

KONTAKT

rapid7.com/de/contact

Hier erfahren Sie mehr und können eine kostenlose Testversion anfordern:
rapid7.com/de/trial/insight