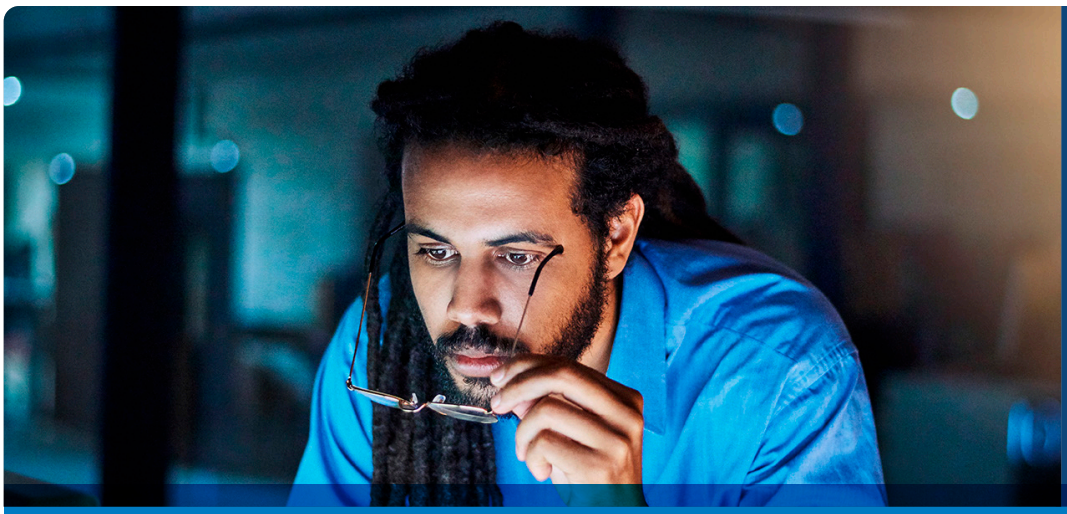
Überprüfung von Sicherheitskontrollen und -richtlinien zur Reduzierung von Angriffsvektoren



Simulieren von Angriffstechniken für den Erstzugriff, die Ausführung bösartiger Dateien, Datendiebstahl und vieles mehr

Pentests und Attack Simulation Management

Dell überprüft Ihre Sicherheitskontrollen und -richtlinien entlang der gesamten Cyber Kill Chain

Unternehmen verfügen über Hunderte von Sicherheitskontrollen, von Endpunkten bis hin zu Web- und E-Mail-Gateways. In vielen Fällen sind diese Kontrollen jedoch komplex und schwierig zu managen, außerdem können minimale Fehlkonfigurationen bereits zu erheblichen Sicherheitsrisiken führen. Defekte oder veraltete Kontrollen werden daher besonders häufig von Bedrohungsagierenden ausgenutzt.

Zur Überprüfung und Validierung der Effektivität Ihrer Sicherheitskontrollen werden die Dell Penetrationstests und das Angriffssimulationsmanagement realen Bedrohungen genau nachempfunden.

In diesem Service ist Folgendes enthalten:

- Monatliche automatisierte Sicherheitsverletzungs- und Angriffssimulationen (kurz „BAS“ für „Breach and Attack Simulation“) zur Bestätigung der ordnungsgemäßen Funktionsweise Ihrer Kontrollen
- Ein jährlicher Penetrationstest, bei dem qualifizierte ExpertInnen versuchen, die Abwehrmaßnahmen für essenzielle Ressourcen und Daten zu überwinden

Prüfung von Sicherheitskontrollen durch Angriffssimulationen

SicherheitsexpertInnen von Dell nutzen die fortschrittliche BAS-Technologie, um verschiedene Angriffsvektoren zu testen, indem sie z. B. versuchen, Malware auf einem Endpunkt zu platzieren oder vertrauliche Informationen von einem Webserver zu erhalten. Die TesterInnen von Dell wenden diese Art der Simulationen an, um Angriffe entlang der gesamten Cyber Kill Chain[1] zu simulieren und so Bedrohungen vorzubeugen. Dazu nutzen sie außerdem die neuesten TTPs[2] der Angreifenden.

Die BAS-Technologie kann bedenkenlos in Produktionsumgebungen eingesetzt werden und wird kontinuierlich mit den neuesten Bedrohungsinformationen, Angriffen und Verhaltensweisen aktualisiert.

Bewertung der Erreichbarkeit wertvoller Ziele durch Pentests

Selbst wenn zuvor eine Angriffssimulation durchgeführt wurde, kann es trotzdem einigen Angreifenden gelingen, Abwehrmaßnahmen zu überwinden und in die Umgebung einzudringen, um an wertvolle Daten zu gelangen. Genau an dieser Stelle kommen Penetrationstests zum Einsatz.

Hauptvorteile:

- Erkennen falsch konfigurierter Sicherheitskontrollen durch umfassende Sicherheitsverletzungs- und Angriffssimulationen, um Ausnutzung vorzubeugen
- Erfassen neu auftretender Probleme und Sicherheitslücken durch monatliche Simulationen
- Eingehende Überprüfung besonders gefährdeter Pfade zu wertvollen Ressourcen oder Daten mit jährlichen Pentests
- Berichte zu Testergebnissen, vierteljährlichen Entwicklungen und auffälligen Aktivitäten zur Verbesserung des Sicherheitsstatus
- Schnelle Einblicke in neuartige Gefahrenquellen mit Ad-hoc-Tests

Penetrationstests werden ergänzend zur BAS durchgeführt – statt einzelne oder kombinierte Kontrollen zu testen, werden bei Pentests besonders gefährdete oder ungeschützte Pfade in eine Umgebung ermittelt. Dell PentesterInnen können unterschiedliche Techniken von Bedrohungsagierenden und sogar verschiedene Payloads emulieren, um ein bestimmtes Ziel zu erreichen, z. B. das Eindringen in ein System mit wertvollen Daten oder das Stehlen bzw. Sperren bestimmter Dateien. Genau wie bei einem echten Angriff können erfahrene PentesterInnen auf andere Techniken umschwenken oder diese anpassen, um das Ziel zu erreichen.

Nutzen von Testergebnissen zur Verbesserung des Sicherheitsstatus

Dell Technologies Services bietet basierend auf den Ergebnissen der BAS ein monatliches Reporting zu den Problemen in Bezug auf Sicherheitskontrollen, die behoben werden müssen. Alle drei Monate wertet Dell zusätzlich die Entwicklung der verschiedenen Angriffssimulationen aus, meldet auffällige Aktivitäten innerhalb Ihrer IT-Umgebung und berät Sie hinsichtlich der Verbesserung Ihres Sicherheitsstatus.

Hauptmerkmale

Sicherheitsverletzungs- und Angriffssimulation (BAS)

- Monatliche Durchführung automatisierter Sicherheitsverletzungs- und Angriffssimulationen – angepasst an die Umgebung des Kunden
- Überprüfung von Sicherheitskontrollen für Perimeter und interne Infrastrukturkomponenten, einschließlich Webgateway, E-Mail-Gateway und Endpunkte
- Kontinuierliche Aktualisierung des BAS-Tools mit den neuesten Bedrohungsinformationen, Angriffen und Verhaltensweisen
- Vornehmen von Änderungen am Simulationsworkflow basierend auf vorherigen Simulationen und Faktoren der Sicherheitsumgebung
- Durchführung von Ad-hoc-Simulationen für neu erkannte Sicherheitsprobleme basierend auf Threat Intelligence und der Bewertung von Dell

Penetrationstests

- Durchführung von jährlichen Penetrationstests für eine definierte Teilmenge von Webgateways, APIs, Mobilgeräten, externen und internen IP-Adressen und Cloud-Konfigurationen
- Erneute Durchführung eines Pentests nach der Problembehebung des ersten Tests (optional)

Reporting und Überprüfung

- Monatliches Reporting zu durchgeführten Sicherheitsverletzungs- und Angriffssimulationen
- Bereitstellung eines vierteljährlichen Berichts zur Auswertung von Entwicklungen und Meldung von auffälligen Aktivitäten innerhalb der IT-Umgebung des Kunden
- Empfehlungen zur Verbesserung des allgemeinen Sicherheitsstatus

Onboarding

- Durchführung eines Meetings zur Initiierung des Service
- Prüfung der vom Kunden ausgefüllten Checkliste vor dem Engagement
- Überprüfung der kundenseitigen IT-Umgebung
- Aktivierung der BAS-Anwendung für den Kunden
- Bereitstellung von Unterstützung beim Agent-Rollout

Wenden Sie sich noch heute an Ihre Ansprechperson im Vertrieb.

[1] „Gesamte Cyber Kill Chain“ – umfasst unter anderem externe Bedrohungen wie Phishing, Webgateways usw., Datenausschleusung oder die Gefährdung von Endpunkten und der daraus folgende Zugriff auf weitere Elemente im Netzwerk, um Anmeldedaten zu erhalten oder den Angriff auszuweiten.
[2] „TTPs“ – Taktiken, Techniken und Prozesse

Copyright © 2023 Dell Inc. oder deren Tochtergesellschaften. Alle Rechte vorbehalten. Dell Technologies, Dell, EMC, Dell EMC und andere Marken sind Marken von Dell Inc. oder deren Tochtergesellschaften. Alle anderen Marken können Marken ihrer jeweiligen Inhaber sein. Die Verfügbarkeit und die Bedingungen von Services sind je nach Region und Produkt unterschiedlich. Februar 2023-LC | Pentests und Attack Simulation Management DS

DELL Technologies