MANDIANT

DATENBLATT: MANDIANT ADVANTAGE

ATTACK SURFACE MANAGEMENT

Betrachten Sie Ihr Unternehmen aus dem Blickwinkel eines Angreifers.

WETTBEWERBSVORTEIL

Attack Surface Management findet und katalogisiert Assets, mindert Risiken und unterstützt somit die sichere Einführung neuer Technologien und Prozesse zur Innovationsbeschleunigung. Es stärkt Ihre Wettbewerbsfähigkeit durch:

- Support für Remote- und hybride Arbeitsmodelle
- Perimeterschutz
- Skalierbarkeit bis hin zu den größten Umgebungen
- Management von Cloud Computing und Schatten-IT
- Einbettung der Governance in die Arbeitsabläufe
- Stärkung der Resilienz der Lieferketten
- Durchsetzung geltender Sicherheitsrichtlinien, auch außerhalb des Unternehmens

IT-Umgebungen sind von Haus aus dynamisch. Sie entwickeln sich organisch, wenn zum Beispiel Cloud-Umgebungen, ungesicherte Netzwerke, SaaS-Implementierungen, Container, Microservices, IoT-Geräte und andere Anwendungen, Infrastrukturen und Daten hinzugefügt und dabei nicht immer alle Sicherheitsrichtlinien des Unternehmens berücksichtigt werden. Weitläufige ältere Systeme, nicht mehr genutzte Infrastrukturen und geografisch immer weiter verteilte Belegschaften verkomplizieren die Situation zusätzlich.

Sogar mit eigens für diesen Zweck entwickelten Tools gelingt es Sicherheitsteams oft nicht, die gesamte, ständig wachsende Angriffsfläche kontinuierlich im Auge zu behalten und neue Herausforderungen sofort zu erkennen und anzugehen. Mandiant Advantage Attack Surface Management, ein Modul der Plattform Mandiant Advantage, kombiniert umfassende Transparenz und kontinuierliches Monitoring mit aktueller Mandiant Advantage Threat Intelligence, damit sämtliche Internet-Assets in den heute üblichen dynamischen, verteilten und gemeinsam genutzten Umgebungen analysiert und etwaige Schwachstellen umgehend erkannt und behoben werden können.

Umfassende, erweiterte Transparenz der Enterprise-Klasse

Attack Surface Management vermittelt Sicherheitsteams eine umfassende, korrekte Sicht auf ihre Umgebung aus der Perspektive eines Angreifers. Das Modul nutzt Angreiferdaten, um Sicherheitsprogramme vom reaktiven in den proaktiven Modus zu überführen.

Attack Surface Management findet und analysiert Internet-Assets in den heute üblichen dynamischen, verteilten und gemeinsam genutzten Umgebungen. Das Modul nutzt graphbasiertes Mapping, um eine umfassende Übersicht über die erweiterte Unternehmensinfrastruktur zu erstellen, in der Assets detailliert dargestellt und Risiken hervorgehoben werden, sodass Sicherheitsteams Threat Intelligence unglaublich schnell und flexibel im Betrieb nutzen können. Attack Surface Management identifiziert professionelle Beziehungen in der gesamten Infrastruktur und wirkt Wildwuchs mit einer umfassenden Übersicht über bekannte und unbekannte Assets entgegen. So können Cybersicherheits-Teams sämtliche Assets katalogisieren und jede erkannte Gefahr umgehend genauer untersuchen.

Ältere Tools werden in statischen Umgebungen und mit einer begrenzten Anzahl an Geräten und Anwendungen hinter einer Netzwerk-Firewall genutzt, da sie mit modernen Infrastrukturen nicht mehr Schritt halten können. Attack Surface Management wurde speziell für dynamische, verteilte IT-Umgebungen und die anspruchsvollsten Sicherheitsteams entwickelt.

Kontinuierliches Schwachstellenmonitoring

Versetzen Sie Ihr Cybersicherheits-Team in die Lage, Assets und Infrastrukturen (darunter auch Softwarestacks und deren Konfigurationen) kontinuierlich zu überwachen und zu bewerten. Attack Surface Management erkennt Änderungen und von außen zugängliche Assets in Echtzeit, identifiziert Schwachstellen, die von Angreifern ausgenutzt werden könnten, und spannt gleichzeitig ein Sicherheitsnetz für die Cloud-Nutzung und die digitale Transformation auf. Das Modul erleichtert Cybersicherheits-Teams das schnelle Verständnis von Bedrohungen und anderen Risiken für die gefundenen Assets, sodass sie richtig eingeschätzt werden können.

Praktische Nutzung von Expertise und Threat Intelligence

Unterstützen Sie Ihre Security Operations bei der Abwehr echter Bedrohungen. Die Expertise und Threat Intelligence von Mandiant werden automatisch auf Ihre Angriffsfläche angewendet, um zu ermitteln, was von außerhalb Ihres Unternehmens erreichbar ist, und um das resultierende Risiko kontinuierlich zu überwachen. Das Modul kann in Ihre vorhandenen Arbeitsabläufe integriert werden. Es benachrichtigt Cybersicherheits-Teams, wenn neue Assets in die Umgebung eingefügt werden, und weist auf alle öffentlich zugänglichen Assets hin.

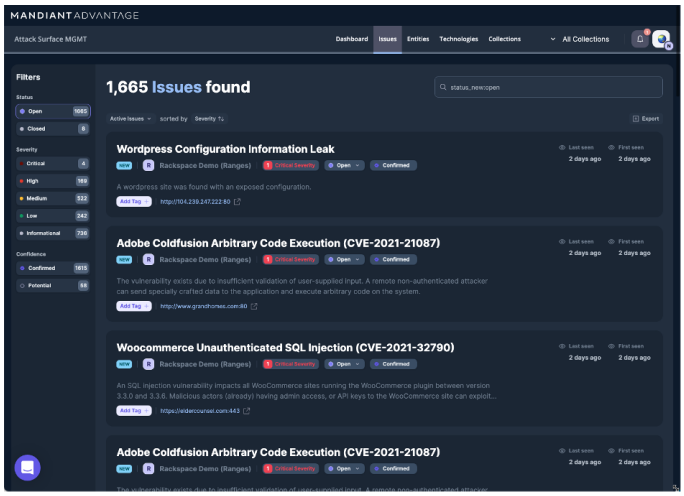

ABBILDUNG 1: Analysieren Sie Assets, um Schwachstellen aufzudecken, von außen zugängliche Assets zu untersuchen und das resultierende Risiko zu mindern.

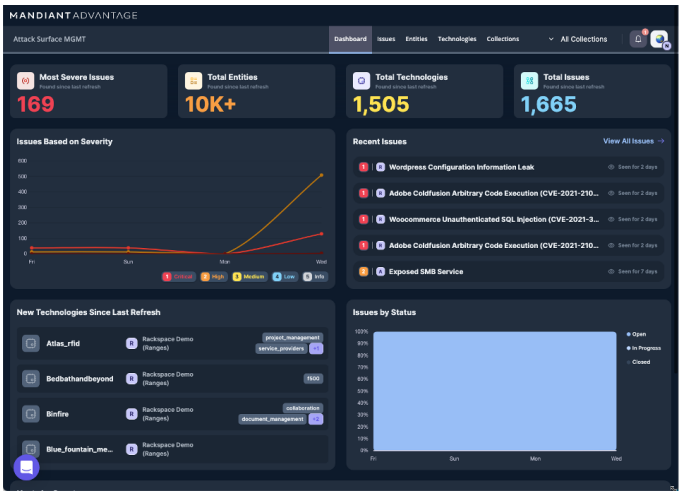

ABBILDUNG 2: Nutzen Sie Threat Intelligence und Expertise von Weltrang, um Änderungen Ihrer Angriffsfläche unter Kontrolle zu halten.

Statistik

Attack Surface Management umfasst:

- **über 250 verfügbare Integrationen:** Integrationen für Datenquellen und Erkennungsmethoden
- **über 30 kategorisierte Asset-Arten:** Umfassende Asset-Transparenz über die gesamte Infrastruktur hinweg
- **über 60 identifizierte Technologien:** Tiefergehende Analyse von Technologien und Konfigurationen
- **über 10.000 abgedeckte Schwachstellen:** Untersuchung von Schwachstellen (sowohl aktive Bedrohungen als auch Fehlkonfigurationen)

Ergebnisse

Kunden mit Attack Surface Management profitieren von:

- **Umfassender, auf graphgestütztem Mapping basierter Transparenz:** Zahlreiche Integrationen und Methoden erleichtern das Inventarisieren von Assets und Cloud-Ressourcen und das Identifizieren von Beziehungen zu Partnern und Dritten. Sie können die Zusammensetzung Ihrer Assets sowie die vorhandenen Technologien und Konfigurationen sofort erkennen.
- **Kontinuierlichem Asset-Monitoring zur proaktiven Bedrohungsabwehr:** Sie können Ihre Infrastruktur in Echtzeit überwachen, um Änderungen und von außen zugängliche Assets zu erkennen, und gleichzeitig ein Sicherheitsnetz für die Cloud-Nutzung und die digitale Transformation aufspannen.
- **Befähigung der Security Operations zur Abwehr echter Bedrohungen:** Die Expertise und Threat Intelligence von Mandiant werden automatisch genutzt, um anfällige Bereiche Ihrer Angriffsfläche zu identifizieren.

Weitere Informationen finden Sie unter **www.mandiant.com/de-landing**

Mandiant
11951 Freedom Dr, 6th Fl, Reston, Virginia 20190, USA
+1 703 935 8012
+1 833 3MANDIANT (362 6342)
info@mandiant.com

Über Mandiant

Seit 2004 ist Mandiant® ein zuverlässiger Partner für sicherheitsbewusste Unternehmen. Heute bilden die branchenführende Threat Intelligence und das Know-how von Mandiant die Basis für dynamische Cyberabwehrlösungen. Diese Produkte ermöglichen die Entwicklung effektiver Programme und stärken das Vertrauen in die Cybersicherheit unserer Unternehmenskunden.

MANDIANT