MANDIANT®

DATENBLATT

Security Instrumentation Platform

Ein besserer Überblick dank aussagekräftiger Kennzahlen

HIGHLIGHTS

- **Priorisierung der entscheidenden Bedrohungen** basierend auf aktuellen und relevanten Bedrohungsdaten
- **Bewertung der Effektivität der aktuellen Sicherheitslösungen** bei der Abwehr realer Angriffe
- **Aufdeckung bisher unerkannter Lücken und Überschneidungen** der Funktionsbereiche in der Sicherheitsinfrastruktur
- **Messung der Zeit, die das Team** zur Erkennung und Abwehr von Bedrohungen benötigt
- **Ermittlung der Bereiche** mit dem größten Optimierungspotenzial
- **Quantifizierung der Steigerung** der Abwehrmaßnahmen im Zeitverlauf
- **Rationalisierung des Investitionswerts** mit quantifizierbaren Belegen für Führungskräfte
- **Vereinfachung der Kommunikation** des Sicherheitsstatus im gesamten Unternehmen

In der aktuellen dynamischen Bedrohungslandschaft stellt der Schutz der Unternehmensressourcen CISOs und ihre Teams vor große Herausforderungen. Von ihnen wird erwartet, dass sie den Nutzen der Cybersicherheitslösungen und die Effektivität der Abwehrmaßnahmen bei aktuellen und neuen Angriffsmethoden kennen und auch beweisen können.

Penetrationstests, Red-Team-Übungen und BAS-Lösungen (Breach and Attack Simulations) reichen dazu nicht aus, denn sie liefern keine quantifizierbaren Beweise, die CISOs und andere Führungskräfte zur Einschätzung der Risiken und ihrer Cybersicherheitsstrategie benötigen. Ohne konkrete Nachweise der Leistungsdaten können Sicherheitsteams weder die Abwehrmaßnahmen optimieren noch den Sicherheitsstatus mit Gewissheit bestimmen.

Die Mandiant Security Instrumentation Platform ist eine wichtige Komponente der datengestützten Technologien von Mandiant zur Validierung der Effektivität von Sicherheitslösungen, und liefert die erforderlichen Belege. Sie ist eine Plattform für die Bewertung und das Management von Cybersicherheitsrisiken, mit der Teams den Schutz der wichtigsten Ressourcen sicherstellen können.

Größere Effizienz der Sicherheitslösungen

Die Mandiant Security Instrumentation Platform nutzt globale Bedrohungsdaten und Incident-Response-Daten von Mandiant und bietet damit einen umfassenden Überblick über die Aktivitäten der Angreifer. Mit dieser Kombination aus Bedrohungsdaten und Validierungstechnologie können Sicherheitsteams gezielt eine Strategie für die Angreifer und Angriffstechniken entwickeln, die für ihr Unternehmen relevant sind.

Die datengestützte Validierungstechnologie von Mandiant priorisiert zuerst die relevanten Bedrohungen und erfasst dann in einer sicheren Umgebung einzelne, quantifizierbare Nachweise der Effektivität der gesamten Sicherheitsarchitektur bei der Abwehr realer Angriffe und wertet diese aus. Aus den Ergebnissen lassen sich bestimmte Angriffe und sogar Phasen des Angriffsverlaufs ablesen, die die Sicherheitstechnologien umgehen oder überwinden. Anhand von spezifischen Leistungsdaten und Angaben zu bestimmten Anbietern erkennen Sie, wo und wie sich die Lösungen optimieren lassen. Mithilfe dieser Informationen können Sie dann Ihr gesamtes Sicherheitsprogramm überarbeiten und verbessern.

Mit der Mandiant Security Instrumentation Platform lässt sich die Effektivität der Sicherheitslösungen bei den neuesten und komplexesten globalen Angriffen schnell ermitteln und beweisen. Die Technologie kann in On-Premises-, Cloud- und Hybridarchitekturen eingesetzt werden.

Da die Effektivität konkret gemessen werden kann, lässt sich der Nutzen der Sicherheitsinvestitionen zur Verbesserung der Risikotoleranz des Unternehmens nachweisen.

In der Mandiant Security Instrumentation Platform wird dieser Prozess automatisch und kontinuierlich durchgeführt. So können Sie eine bessere Strategie für Ihr Unternehmen entwickeln, während die Plattform die Effektivität der Sicherheitslösungen überwacht und misst.

Zuverlässiger Sicherheitsstatus
Die Mandiant Security Validation-Experten helfen Ihnen, die Plattform schnell zu konfigurieren, die Actors zu verbinden, Warnmeldungen einzurichten und weitere Funktionen für detailliertere Einblicke auszuwählen. Dank der einfachen Integration können Sie die Leistung des Sicherheits-Stacks visuell nachverfolgen, wenn Angriffsmethoden in einer sicheren Umgebung getestet werden.

Nach der Konfiguration stehen Ihnen einzelne Tests oder vordefinierte Sequenzen aus der umfangreichen Angriffsbibliothek von Mandiant zur Verfügung. Die Informationen stammen aus realen Angriffen, von Taktiken, Techniken und Prozessen der Angreifer und diversen Malware-Varianten. Da die Tests in einer sicheren Umgebung ausgeführt werden, können Sie sofort und kontinuierlich feststellen, ob die einzelnen Sicherheitslösungen ordnungsgemäß funktionieren. Die Dashboards werden in Echtzeit aktualisiert, sodass in den Tests erkannte Bedrohungen, Warnmeldungen, übersehene Angriffe und abgewehrte Techniken unmittelbar angezeigt werden.

Außerdem wird sichergestellt, dass die Ereignisse mit Zeitstempeln versehen und korrekt geparst werden. Wenn Sie Korrelationsregeln und Bedrohungsmodelle festgelegt haben, werden auch Warnungen ausgelöst. Berichte zur Effektivität der Sicherheitslösungen im Zeitverlauf können abgerufen und exportiert werden. Mit dieser kontinuierlichen Validierung erhalten Sie die notwendigen Belege, dass das Vertrauen in das Sicherheitsprogramm gerechtfertigt ist. Diese können Sie dann auch der Unternehmensleitung und dem Vorstand vorlegen.

Details zur Plattform
Die Mandiant-Plattform ist offen und lässt sich daher anpassen und ergänzen. Lösungen können automatisch erkannt und reale Angriffe ausgeführt werden, um die Sicherheitslösungen in einer sicheren Umgebung zu testen. Die Plattform umfasst sechs grundlegende Komponenten:

Director
Diese zentrale Steuerungs- und Managementkonsole für die kontinuierliche Validierung in dynamischen Produktionsumgebungen ist als cloudbasierte Plattform (SaaS) oder als virtuelle Appliance oder installierbare Software On-Premises verfügbar.

Actors
Sie führen sichere Tests in Produktionsumgebungen durch, um die Konfigurationen der Infrastruktur zu prüfen und die Effektivität der Sicherheitsfunktionen in Netzwerken, E-Mail- und Cloud-Systemen sowie auf Windows-, MacOS- und Linux-Endpunkten zu validieren.

Integrationen
Durch die problemlose Integration zahlreicher Abwehrtechnologien und Sicherheitsinfrastrukturen können die Sicherheitslösungen noch besser validiert werden.

Angriffsbibliothek
Die Bibliothek umfasst Tausende Angriffstechniken für alle Phasen des Angriffszyklus, einschließlich des gesamten Angriffsverlaufs sowie aktueller und neuer Angriffsmethoden, die aus den globalen Bedrohungsdaten von Mandiant ermittelt wurden.

Frameworks
Die Angriffe werden nach den MITRE™ ATT&CK- und NIST-Frameworks kategorisiert, damit sich die Effektivitätsmaßnahmen einfacher in das Sicherheitsprogramm einbinden lassen. Da Mandiant Security Validation sowohl Informationen zu den relevanten Taktiken der Angriffs-Frameworks als auch zu MITRE ATT&CK-Taktiken liefert, sind umfassende und relevante Tests mit präzisen Ergebnissen möglich.

Dashboards und Berichte
In dieser grafischen Oberfläche werden Testergebnisse aus der Umgebung in Echtzeit angezeigt. Außerdem lassen sich Berichte zur Verbesserung der Effektivität im Zeitverlauf mit realen, quantitativen Daten abrufen, die auch für die Unternehmensleitung nachvollziehbar sind (Abb. 1).

Abbildung 1: Mithilfe der Validierungsergebnisse für den gesamten Angriffszyklus lassen sich im Dashboard die Bereiche mit den größten Risiken erkennen.

Datengestützte Validierung

Die Mandiant Security Instrumentation Platform ermöglicht eine umfassende, kontinuierliche Überwachung, Validierung und Optimierung der Sicherheitslösungen und die automatische Erkennung von Änderungen in der Umgebung. Dieser kontinuierliche Validierungsprozess läuft in fünf Schritten ab und basiert auf Bedrohungsdaten (Abb. 2).

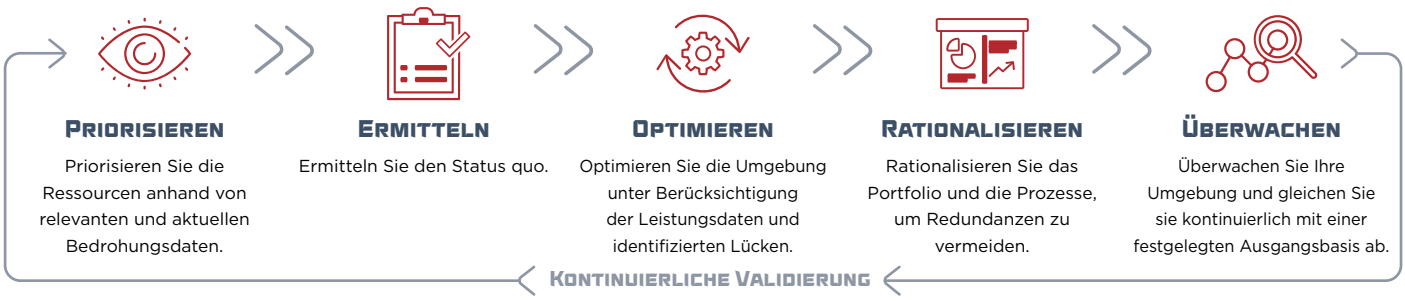

Abbildung 2: Die fünf Schritte der datengestützten Mandiant Security Validation

Erweiterte Funktionen

- **Threat Actor Assurance Module (TAAM):** Damit können Unternehmen ihre Lösungen mit realen Angriffen und den jeweils relevanten Bedrohungsdaten testen. In das TAAM können branchenführende Bedrohungsdatenfeeds von Drittanbietern integriert werden (Abb. 3).
- **Automated Environmental Change/Drift Analysis (AEDA):** Diese Komponente überprüft fortlaufend die IT-Infrastruktur, um Änderungen zu verhindern. Durch diese kontinuierliche Validierung lassen sich eine Regression vermeiden und der Sicherheitsstatus sicherstellen.
- **Protected Theater:** Mit dieser Komponente werden die Sicherheitsfunktionen der Endpunkte getestet. Dazu werden Malware, Ransomware und andere Angriffstechniken in einer sicheren Umgebung ausgeführt, um festzustellen, ob die neuesten Bedrohungen effektiv abgewehrt werden können.
- **Email Theater:** Damit lassen sich die Sicherheitsfunktionen der Lösungen zum Schutz von E-Mail-Systemen testen.

Abbildung 3: Threat Actor Assurance Module (TAAM)

Das Mandiant Security Validation-Portfolio unterstützt diverse Bereitstellungsoptionen:

- **Kundeneigene und verwaltete Lösungen:** Cloudbasiert (SaaS) oder On-Premises-Bereitstellung als virtuelle Appliance
- **Managed oder Co-Managed Service:** In Absprache mit dem Kunden entwickeln Mandiant-Teams ein Validierungsprogramm für spezielle Anwendungsfälle und Ziele und liefern Stakeholdern regelmäßig detaillierte Berichte.
- **Validierung auf Abruf:** Kunden können einen Anwendungsfall auswählen und eine einmalige Prüfung der Effektivität ihrer Sicherheitslösungen in Bezug auf die Prävention oder Abwehr einer bestimmten Angriffsmethode oder eines spezifischen Angreifers erwerben. Außerdem erhalten sie Empfehlungen zu weiteren Untersuchungen, um die Abwehrmaßnahmen zu verbessern und das Risiko zu minimieren.

Security Validation mit Unterstützung von Mandiant Threat Intelligence

Mandiant war bei Untersuchungen, Beratungen und Red-Team-Übungen weltweit im Einsatz und hat in mehr als 15 Jahren ein einzigartiges Portfolio an Bedrohungsdaten zusammengestellt, das kontinuierlich mit neuen Informationen, Erkenntnissen aus Vorfällen und Analyseergebnissen aktualisiert wird. Mandiant gehört inzwischen zu den führenden Anbietern von Bedrohungsdaten mit den folgenden Quellen:

- **Daten von Sicherheitsvorfällen**, die bei Incident-Response-Einsätzen von Mandiant Consulting erfasst werden
- **Daten zu Angreifern**, die von den Mandiant-Analysten zusammengetragen werden
- **Daten von Sensoren** der FireEye-Sicherheitsprodukte
- **Operational-Intelligence-Daten** von den Teams der Mandiant Managed Defense-Services

Weitere Informationen zu Mandiant-Lösungen finden Sie unter:
www.fireeye.de/mandiant/security-validation.html

FireEye, Inc.
601 McCarthy Blvd.
Milpitas, CA 95035, USA
+1 408 321 6300/+1 877 FIREEYE (347 3393)
info-dach@FireEye.com

Über Mandiant
Mandiant-Lösungen kombinieren marktführende Bedrohungsdaten und Daten aus Incident-Response-Einsätzen mit einer kontinuierlichen Sicherheitsevaluierung. So erhalten Unternehmen die notwendigen Informationen, um die Effektivität ihrer Sicherheitsmaßnahmen zu verbessern, geschäftliche Risiken zu minimieren und ihren Ruf und den Unternehmenswert zu schützen.

MANDIANT®