Kiteworks

LÖSUNGSBESCHREIBUNG

Beschleunigte Erkennung und Reaktion auf Bedrohungen

Integriertes MDR (Embedded Managed Detection and Response)

MDR ermöglicht eine beschleunigte Reaktion auf Bedrohungen, ohne die Mitarbeiter zu belasten

Für Unternehmen wird es immer schwieriger, auf die wachsende Zahl ausgeklügelter Cyberangriffe zu reagieren, da die Budgets stagnieren und der Markt für Cybersicherheitsexperten knapp ist. Häufig füllen sie diese Lücke, mit einem schlüsselfertigen MDR-Dienst, der den gesamten Zyklus von der Erkennung der Bedrohung bis zur Remote-Reaktion abdeckt.

Bei Kiteworks betreiben wir eine spezielle MDR-Untergruppe, die sich ausschließlich auf Kiteworks Enterprise-Produktinstallationen konzentriert und in Ihrem Abonnement enthalten ist. Dadurch wird die Integration mit Ihrem IT-Sicherheits-Stack, Ihren Prozessen und denen Ihrer Enterprise MDR-Anbieter ermöglicht.

Schlüsselfertige Erfassung, Telemetrie und Reaktion

Ihr System wird bei der ersten Installation automatisch in den Kiteworks Embedded MDR Service integriert, wenn Sie die Verbindung der virtuellen Appliance mit dem Cloud-basierten MDR/Update Server aktivieren.

Wir haben eine umfassende Bedrohungserkennung in die gehärtete virtuelle Appliance integriert und die Telemetrie alarmiert automatisch das Kiteworks Security Operations Center (SOC) mit den Indikatoren für Bedrohungen (Indicators of Compromise, IOCs) und dem wesentlichen Kontext.

- Erkennt Regelverstöße im Vergleich zu den Referenzwerten
- Überwacht Dateien, Ports, Dienste, Prozesse, Webschnittstellen, Anwender usw.
- Anonymisiert Compliance-sensible Informationen
- Lokale automatische Abhilfemaßnahmen, wie IP-Adresssperrung

Kontinuierliche Überwachung und Bedrohungsdaten

Das hochqualifizierte und erfahrene SOC-Team von Kiteworks überwacht kontinuierlich die Telemetrie aller Kiteworks-Systeme weltweit, rund um die Uhr, jeden Tag. Es verfügt über fundierte Kenntnisse der Produkteigenschaften und Erkennungsmethoden und ist in der Lage, individuelle Bedrohungen, Trends und koordinierte Angriffe schnell zu erkennen und zu analysieren.

Highlights der Lösung

Integrierte Erkennung und Telemetrie

24/7 SOC und Sicherheits-technik

Gezielte Bedrohungs-analyse

Remote Auto-Patching

Enge Kopplung von Produktentwicklung und SOC beschleunigt Reaktionen

Die Sicherheitsentwickler von Kiteworks arbeiten eng mit den SOC-Ingenieuren zusammen, um jede wahrgenommene Bedrohung oder Schwachstelle zu untersuchen. Sie bewerten den Schweregrad und die Gefährdung und überwachen andere Feeds, um zusätzliche Bedrohungen und Schwachstellen zu identifizieren:

- Externe Informationen über Bedrohungen
- Bounty Hunter-Schwachstellenberichte (Blackbox und Whitebox)
- Resultate der Penetrationstests externer Parteien
- Schwachstellen-Scans

Automatische Übermittlung der Reaktionen an alle Kiteworks-Systeme weltweit

Ein Markenzeichen von MDR für Unternehmen ist die Fähigkeit, per Fernsteuerung eine Reaktion auf einen einzelnen Angriff zu orchestrieren. Das in Kiteworks eingebettete MDR kann ebenfalls remote eine Reaktion orchestrieren, da jedoch alle gehärteten virtuellen Appliances identisch sind, kann es für die gesamte installierte Produktbasis und nicht nur für jeweils einen Kunden eingesetzt werden. Die Techniker von Kiteworks analysieren Bedrohungsdaten aus der gesamten installierten Produktbasis und anderen Feeds, identifizieren Bedrohungen, entwickeln Abhilfemaßnahmen und wenden diese dann per Fernzugriff auf alle angeschlossenen Kundensysteme an. Kiteworks wendet eine Vielzahl von Abhilfemethoden an:

- **Aktualisierungen der eingebetteten WAF-Regeln** – identifiziert und blockiert neue Web- und REST-API-Bedrohungen
- **Code-Patches** – behebt Sicherheitslücken im Betriebssystem, in Open Source und in von Kiteworks geschriebenem Code.*
- **Benachrichtigungen der Verwaltungskonsole** – informiert Ihre Administratoren, damit sie spezifische Maßnahmen zur Schadensbegrenzung ergreifen können

Beachten Sie, dass Aktualisierungen der WAF-Regeln und des WAF-Codes sofort und automatisch wirksam werden, ohne dass Ihre Mitarbeiter daran beteiligt sein müssen.

Das Kiteworks-Produkt stellt auch sicher, dass die Kontaktinformationen Ihres Unternehmens regelmäßig aktualisiert werden, so dass unser SOC-Team im Falle einer kritischen Bedrohung direkt mit Ihrem Administrationsteam kommunizieren kann.

Kiteworks Embedded MDR reduziert Cyberrisiken

Das schlüsselfertige, integrierte MDR-System von Kiteworks nutzt integrierte Erkennungs-, Telemetrie- und Systemaktualisierungssoftware in Kombination mit den Dienstleistungen hochqualifizierter und erfahrener SOC- und Sicherheitsentwickler, um die Zeit von der Erkennung bis zur Reaktion zu verkürzen. Dies verringert das Risiko von Cyberbedrohungen, die sensible Daten gefährden und das Geschäft und den Ruf Ihres Unternehmens schädigen und erleichtert gleichzeitig das Leben Ihres IT-Sicherheitspersonals.

*Remote Code Patching ist für Ende 2024 geplant. Alle Pläne können ohne Vorankündigung geändert werden.