DATENBLATT

WatchGuard Orion

Proaktive Cyber-Sicherheit. Effiziente Sicherheitsabläufe

Moderne SOC-Herausforderungen

Moderne SOCs sehen sich mit mehreren Herausforderungen konfrontiert, darunter die rasante Entwicklung von Bedrohungen, das hohe Aufkommen an Sicherheitswarnungen und ein erheblicher Mangel an qualifizierten Cyber-Sicherheitsexperten. Die Lücke[1] wird bis 2031 um 35 % wachsen. SOC-Experten müssen diese Probleme angehen, indem sie skalierbare und flexible Lösungen bereitstellen, die die Bedrohungserkennung mit KI- und Machine-Learning-Funktionen verbessern, komplexe Prozesse automatisieren und Echtzeit-Transparenz bieten, was eine effizientere Suche nach Bedrohungen (Threat Hunting) und die Erkennung, Untersuchung und Reaktion auf Bedrohungen ermöglicht. Dies verbessert letztendlich die SOC-Effizienz und das wachsende Ausmaß und die Komplexität von Cyber-Bedrohungen können bewältigt werden.

Was ist WatchGuard Orion?

WatchGuard Orion ist eine mandantenfähige, cloudnative Lösung für SOC zur Bedrohungssuche, Erkennung, Untersuchung und Reaktion auf Vorfälle, die Sicherheitsanalysen, maschinelles Lernen und Automatisierung nutzt, um unbekannte, ausgeklügelte Bedrohungen proaktiv und effizient aufzudecken und darauf zu reagieren.

Vorteile

WatchGuard Orion zielt darauf ab, die Produktivität von SOC-Analysten zu steigern, die Zeit bis zur Erkennung zu verkürzen und die allgemeine Widerstandsfähigkeit der Cyber-Sicherheit der Kunden zu verbessern. Dies ergänzt WatchGuard EDR, EPDR, Advanced EPDR und den Zero-Trust Application Service und erweitert deren Fähigkeiten um Folgendes:

- **Reduzierung der Alarmmeldungen:** 80 % weniger Alarmmeldungen durch automatische IoA-Priorisierung.
- **Zusammenarbeit:** Tools zur effektiven teamübergreifenden Koordination von Alarm- und Vorfallmanagement, Untersuchungen und Reaktionen.
- **Automatisierung:** Erleichtert sich wiederholende Aufgaben wie Aktivitätsüberwachung zur Erkennung verdächtiger Verhaltensweisen, die informations- und analysegestützte Suche und die Untersuchung sich wiederholender Vorfälle. Dadurch werden Analysten für Untersuchungen auf höherer Ebene und das proaktive Threat Hunting entlastet.
- **Benutzerdefiniertes proaktives Threat Hunting:** Umfasst eine informationsbasierte, analysegestützte und hypothesenbasierte Suche, um komplexe Bedrohungen oder unerwünschte Verhaltensweisen aufzudecken. Das Ergebnis kann durch Regeln für das Threat Hunting automatisiert werden.
- **Konsolidierte SOC-Tools in nur einer Konsole:** Optimierte Integration mit sofort einsatzbereiten SOC-Tools, die eine schnelle Triage, Untersuchung und Reaktion ermöglichen.

1. Amt für Arbeitsstatistik

Flexibilität im Vergleich zu vorgefertigten, sofort einsatzbereiten Lösungen

WatchGuard Orion bietet allen SOC-Mitgliedern Flexibilität und Effizienz, indem es leistungsstarke Tools in eine einzige Konsole integriert. Damit können erfahrene Analysten und Threat Hunting-Experten Regeln für das Threat Hunting konfigurieren, Vorfälle frei untersuchen, indem sie auf die 365-Tage-Telemetrie-Speicherung zugreifen, ihre Untersuchungen mit anderen teilen und sie über Jupyter Notebooks an andere weitergeben. Die über 400 vorgefertigten und automatisierten Regeln für die Erkennungsanalyse, die von WatchGuard SOC erstellt und verwaltet werden, die Funktionen der Untersuchungskonsole und die unterstützten Untersuchungen steigern die Effizienz der Analysten. Die Kombination aus Flexibilität und Automatisierung macht Orion zu einer perfekten Lösung für SOC-Teams in jedem Sicherheitsstadium.

Robuste APIs und Plugins: WatchGuard Orion bietet eine Cloud-Konsole und API-Zugriff für eine einfache SecOps-Integration. Es ermöglicht Aktionen auf Endpoints, Echtzeit- und retrospektive IoC-Suchen, Zugriff auf den Data Lake von WatchGuard, Abrufen von IoCs, IoAs und OSQuery-Daten und vieles mehr. Es unterstützt SIEM (ArcSight, QRadar), Ticketing (ServiceNow) und TIPS (MISP)-Plugins.

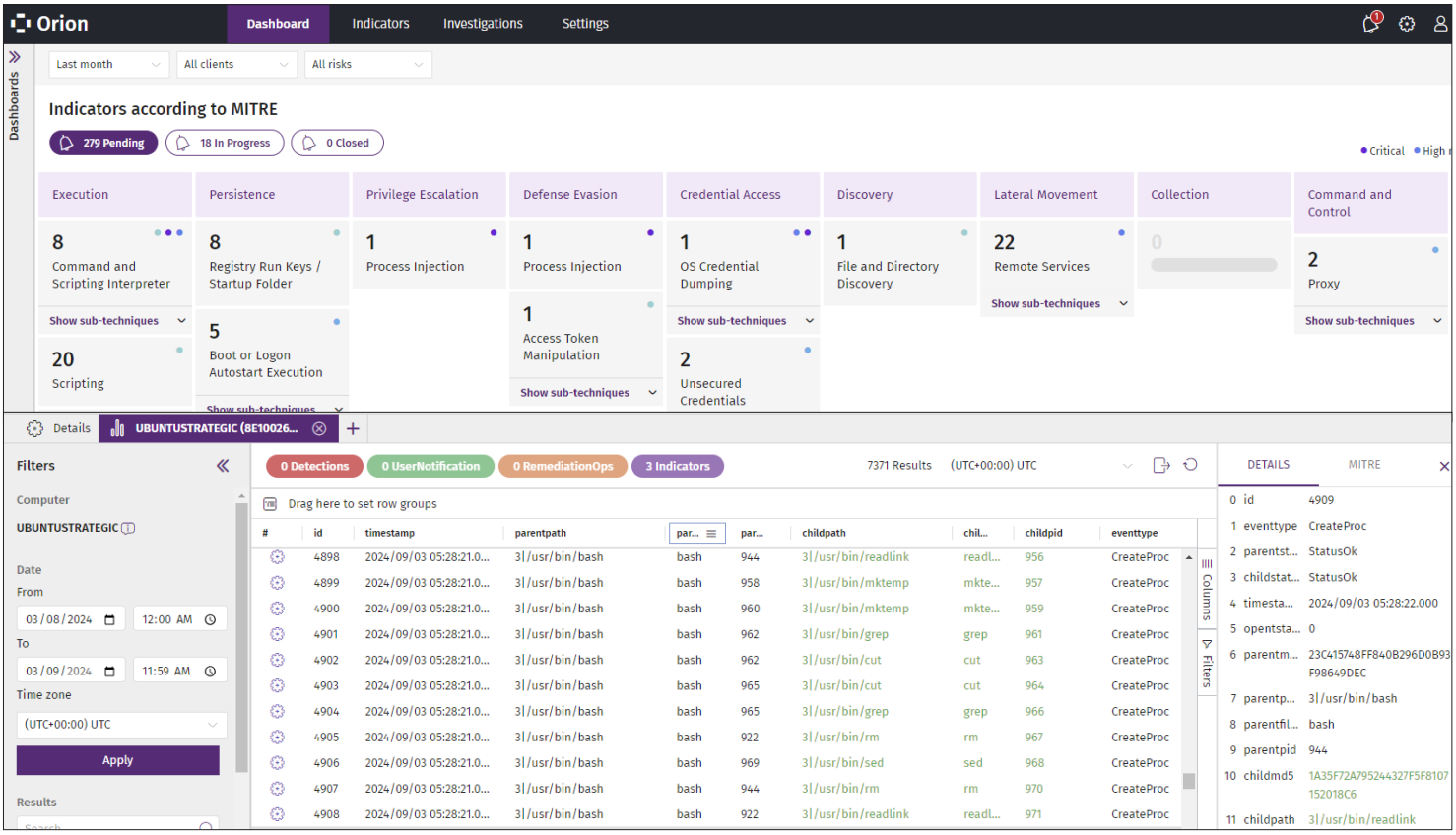

Abbildung 1. WatchGuard Orion und seine Funktionen steigern die Effizienz von Analysten und Threat Hunting-Experten im SOC von WatchGuard sowie in den SOCs von Partnern und Kunden.

Funktionen von WatchGuard Orion

WatchGuard Orion wurde entwickelt, um die Effizienz von SOC-Analysten zu steigern, den Erkennungsprozess zu beschleunigen und die Widerstandsfähigkeit der Cyber-Sicherheit von Kunden zu verbessern. Dabei baut es auf der Grundlage von WatchGuard EDR, EPDR und Advanced EPDR auf. Erreicht wird dies durch die Erweiterung ihrer Fähigkeiten um die folgenden Funktionen:

- **Cloud-native Architektur:** Eine flexible, skalierbare und belastbare Infrastruktur, die eine umfassende Transparenz gewährleistet.
- **Mandantenfähiges Management:** Ermöglicht die zentrale Verwaltung mehrerer Kunden oder „Mandanten“ bei gleichzeitiger Beibehaltung separater, sicherer Umgebungen für die Daten, die Konfiguration und die Verwaltung der einzelnen Mandanten.
- **Flexible Ansichten für rollenbasierten Zugriff der SOC-Mitglieder:** Bietet anpassbare Benutzeroberflächen, die auf die spezifische SOC-Rolle zugeschnitten sind, und stellt sicher, dass sie nur die relevanten Kundendaten und -funktionen gemäß ihren Berechtigungen sehen.
- **Aktivitätsüberwachung in Echtzeit:** Überwacht und analysiert die Endpoint-Aktivität und das Verhalten aller Programme in Echtzeit.
- **Zero-Trust Application Service:** Klassifiziert 100 der laufenden Prozesse auf Endpoints und stellt sicher, dass nur sichere Anwendungen ausgeführt werden. Er nutzt KI/ML und Deep Learning, um die automatische Klassifizierung unbekannter Prozesse zu verbessern.
- **365-Tage Data Lake:** Speichert angereicherte Ereignisse, um retrospektive Aktivitätsanalysen von der ersten Bedrohungsbewegung ab an den Endpoints zu unterstützen. Auf den Data Lake kann über Abfragen über die Threat Hunting API von Jupyter Notebooks, unterstützte Untersuchungen und die Untersuchungskonsole zugegriffen werden.
- **Threat Intelligence:** Zugriff auf globale Bedrohungsdaten für fundierte Erkennungs- und Reaktionsstrategien.
- **Erweiterte Sicherheitsanalysen:** Über 400 vorgefertigte erweiterte Regeln für das Threat Hunting, die MITRE ATT&CK zugeordnet sind, um ausgeklügelte, verborgene Bedrohungen im Strom der Ereignisse sofort aufzudecken und die Entwicklungszeit für die Erkennung erheblich zu reduzieren.
- **Benutzerdefinierte Regeln für die Suche nach Bedrohungen:** Ermöglichen SOC-Teams die Erkennung von abnormalem oder verdächtigem Verhalten zusätzlich zu den vordefinierten Regeln für das Threat Hunting.
- **Verhaltensanalyse-Engine:** Erkennt ungewöhnliches Systemverhalten, löst priorisierte und kontextualisierte Angriffsindikatoren (IoAs) aus und korreliert Verhaltensweisen auf der Grundlage von Regeln für das Threat Hunting.

Funktionen von WatchGuard Orion (Fortsetzung)

- **Störfallmanagement:** Optimierte Zusammenarbeit und Workflows von SOC-Mitgliedern, um Bedrohungen schnell zu erkennen und Vorfälle effizient zu verwalten.
- **Untersuchung mit Jupyter Notebook:** Bietet eine zentralisierte Umgebung für den Austausch von Untersuchungspraktiken und Playbooks. Ermöglicht tiefgreifende Untersuchungen und nutzt Bibliotheken von Drittanbietern.
- **KI-gesteuerte Untersuchung von Bedrohungen:** Notebooks ermöglichen Analysen und Algorithmen für maschinelles Lernen, um ausgeklügelte, versteckte Bedrohungen sofort aufzudecken und auf diese zu reagieren.
- **OSquery-Integration:** Leistungsstarkes Tool für die Überwachung und Analyse von Endpoints, das SQL-basierte Abfragen von Systemdaten ermöglicht.
- **Untersuchungskonsole:** Ermöglicht eine gründliche Untersuchung von Computern, Prozessen und mehr mit verschiedenen Tools für einen detaillierten Blick auf die Aktivitäten im Laufe der Zeit.
- **Untersuchungsdiagramme:** Bieten visuellen Kontext und die Zuordnung von Beziehungen zwischen Einheiten bei Data-Lake-Ereignissen für ein besseres Verständnis und eine bessere Analyse. SOC-Analysten können mit dem Diagramm interagieren, indem sie die Zeitleiste erweitern oder eingehender untersuchen.
- **Werkzeuge zur Eindämmung und Abhilfe**: Dazu gehören die Isolierung, der Neustart, die Verwaltung von Prozessen und Diensten, die Übertragung von Dateien und die Durchführung von Befehlszeilenoperationen durch Fernzugriff auf Endpoints.
- **APIs und Konnektoren:** Erleichtert die Integration mit anderen Systemen für einen optimierten Betrieb.
- **Unterstützte Vorfalluntersuchungen:** Unterstützt Analysten bei der Untersuchung von Cyber-Sicherheitsvorfällen, ohne dass sie Code schreiben und testen müssen, indem sie geführte Schritte, relevante Fragen und umsetzbare Erkenntnisse bereitstellt und so schnellere Untersuchungen, Entscheidungen und Reaktionszeiten ermöglicht.

Mit der Kombination aus reduzierter Angriffsfläche, Prävention und effektiven Erkennungs- und Reaktionsstrategien eröffnen WatchGuard EDR, EPDR oder Advanced EPDR und WatchGuard Orion SOC mit einem robusten Framework für die Cyber-Sicherheit neue Möglichkeiten.

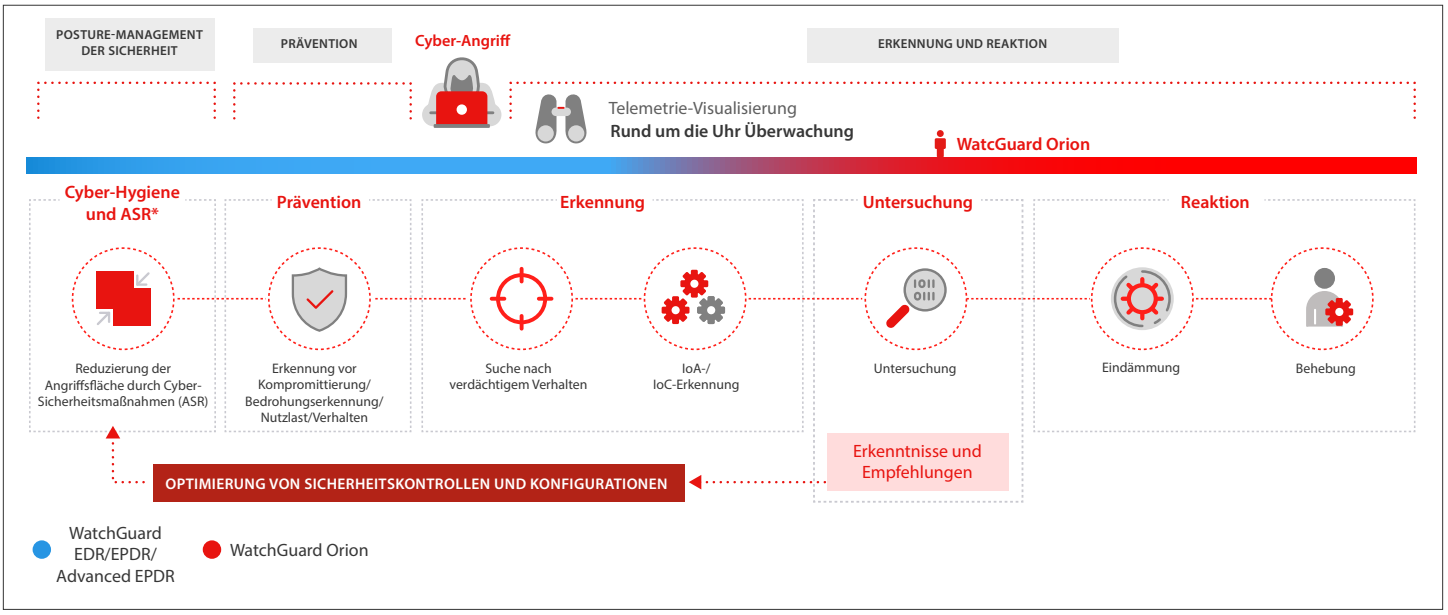

Abbildung 2. Die Lösungen und Module von WatchGuard Endpoint Security arbeiten zusammen, um den gesamten Lebenszyklus von Bedrohungen zu unterstützen, von der Reduzierung der Angriffsfläche und der Prävention bis hin zur Erkennung, Reaktion und Untersuchung, um den Schutz vor zukünftigen Angriffen zu verbessern.