Fortschrittliche Endpoint-Sicherheit von WatchGuard für SOCs. Die Jagd nach unbekannten Bedrohungen

Möchten Sie warten und zum Opfer werden?
Oder auf den Angreifer reagieren?

Threat Hunting Services

Erkennung, Untersuchung und Reaktion

Cyber-Widerstandsfähigkeit

Was ist die fortschrittliche Endpoint-Sicherheit von WatchGuard für SOCs?

WatchGuards Werteversprechen für SOCs basiert auf einer Kombination aus fortgeschrittenen Sicherheitslösungen und Managed Services für die effiziente Suche und Erkennung von und Reaktion auf Bedrohungen, die es geschafft haben, andere Schutzmaßnahmen auf Computern, Servern, virtuellen Umgebungen und mobilen Geräten zu umgehen.

WatchGuard setzt sich für die Unterstützung von Organisationen ein, die ein fortschrittliches Sicherheitsprogramm implementieren möchten – unabhängig davon, ob sie eigene Teams für die Sicherheit und Reaktion auf Vorfälle verwenden oder diese Aufgaben einem Security Service Provider überlassen (MSSP, SOC, MDR und CSIRT).

WatchGuard begleitet diese spezialisierten Anbieter außerdem aktiv und stellt eine einzigartige Plattform und Tools für umfassendes EDR und das Threat Hunting bereit. Somit können sie ihr Portfolio um schnellere Dienste für das Threat Hunting und die Erkennung und Reaktion auf Vorfälle erweitern.

Diese Plattform für EDR und das Threat Hunting verwendet ein Zero-Trust-Sicherheitsmodell, das Cyberangriffe (Malware, Exploits oder anomales Verhalten auf Endpoints) proaktiv neutralisiert. Hiermit wird ein Framework von Lösungen und Diensten geboten, die die folgenden Schwerpunkte haben:

- **Entdeckung von Angreifern, die „living-of-the-land"-Techniken ohne Malware verwenden**, um zu versuchen, bestehende Kontrollen zu umgehen und die Organisation zu gefährden

- **Beschleunigung der Prozesse der Endpoint-Untersuchung, -Risikominderung und -Reaktion** Maßnahmen, die der SOC normalerweise im Notfall manuell, ineffizient, mit hohem Kostenaufwand und ohne Anleitung durchführen müsste.

Werteversprechen

Höhere SOC-Effizienz, niedrigerer MTTD- und MTTR-Aufwand („Mean Time To Detect“ und „Mean Time To Respond“)

- Echtzeit-Monitoring und -Transparenz
- 365 Tage Transparenz und umfassende Telemetrie
- Keine Kompromisse bei Malware-Angriffen, dank dem Zero-Trust Application Service
- Threat Hunting Service im Produktumfang enthalten
- Erkennung von anomalen Verhaltensweisen
- Exploit-basierte Angriffe werden blockiert
- Rückblickende und Echtzeit-IoC und Suche für Yara Rules
- Fortschrittliche Warnmeldungen werden priorisiert und dem MITRE ATT&CK Framework zugeordnet
- Tools für Threat Hunting und Anomalie-Erkennung und -Untersuchung mit vorerstellten und benutzerdefinierten Abfragen, Notebooks und Analysen
- Eindämmung und Abhilfe per Fernzugriff und im großen Ausmaß

Unterstützung für das Technologie-Stack des SOCs

- API-fokussierte Architektur, die Folgendes ermöglicht:
  - Integration im Stack des SOCs
  - Automatisierung von Anwendungsfällen der Endpoint-Abhilfe
- **Untersuchung im SIEM oder Delegierung der Untersuchung an die Orion-Plattform,** die auf skalierbare Endpoint-Analysen spezialisiert ist.
- Integrierte Reaktion auf Vorfälle vom SOC Der Zugriff auf die Endpoints ist über Orion oder über jedes Element im Stack verfügbar.

Einfacher Rollout-Prozess

- Einzelne Cloud-basierte Plattform Einzelner, ressourcensparender Agent
- Keine Server oder Wartungspersonal
- Rollout innerhalb von Sekunden Kostengünstige Implementierung
- Kosteneinsparung bei der Bekämpfung von Cyberkriminalität, indem die Effizienz von Prävention, Erkennung, Eindämmung und Wiederherstellung bei Vorfällen erhöht wird.
- Unterstützt die Ursachenanalyse und die kontinuierliche Verbesserung des Sicherheitsniveaus

Proaktive Erkennung/Threat Hunting

- Im Produktumfang standardmäßig enthaltene Dienste:
  - Zero-Trust Application Service
  - Threat Hunting Service
- Außerdem verwaltete Threat Hunting Services
- Telemetrie-Dienst auf dem Unternehmens-SIEM

DEUTSCHLAND, ÖSTERREICH, SCHWEIZ **+49 700 92229333** INTERNATIONALER VERTRIEB: **+1 206 613 0895** WEB **www.watchguard.com/de**

Kontaktieren Sie uns
strategic.accounts@watchguard.com