Fortschrittliche Endpoint-Sicherheit von WatchGuard für SOCs

ENDPOINT-SICHERHEIT UND MANAGEMENT	WatchGuard Orion	Orion-Advanced EPDR
Direkter Zugriff auf 365-Tage-Endpoint-Telemetrie – Vorab erstellte und benutzerdefinierten Abfragen	✓	✓
Verhaltensanalysen – Vorab erstellte und benutzerdefinierte Threat Hunting-Regeln	✓	✓
Untersuchungskonsole and Diagramme zu Angriffen	✓	✓
Vorab erstellte und benutzerdefinierte Notebooks (automatische Untersuchung) und Playbooks	✓	✓
OSQuery und Remote-Shell für tiefergreifende Untersuchungen	✓	✓
Antwort: Isolierung, Neustart und Remote-Shell zum Abbrechen von Prozessen, Ausführen von Skripten usw.	✓	✓
Orion-APIs - Suche durch IoCs 365 Tage rückwirkend, OSQuery, Abfragen usw.	✓	✓
Suche anhand von STIX IOC- und Yara-Regeln in Echtzeit an den Endpoints		✓
Threat Hunting Service: Deterministische High-Fidelity-IoA-Erkennung		✓
Erweiterte Sicherheitsrichtlinien zur Verringerung der Angriffsoberfläche		✓
Remote-Shell zur Verwaltung von Prozessen, Dateien, Diensten, Befehlszeilen, Dumps, pcap usw.		✓
Ressourcensparender cloudbasierter Agent		✓
Suchen in Echtzeit im Rahmen der Schwarmintelligenz		✓
Zero-Trust Application Service: Vor der Ausführung, während der Ausführung, nach der Ausführung		✓
Anti-Exploit-Technologie für Arbeitsspeicher		✓
Decoy-Dateien und Schattenkopien		✓
Erkennung permanenter Malware Suchen in Echtzeit im Rahmen der Schwarmintelligenz		✓
IDS, Firewall und Gerätesteuerung		✓
Web-Browsing- und E-Mail-Schutz		✓
Kategoriebasiertes URL Filtering		✓
Endpoint Access Enforcement Fähigkeit, Verbindungen zu verweigern		✓

ENDPOINT-SICHERHEIT UND MANAGEMENT	WatchGuard EPDR	WatchGuard Advanced EPDR
Direkter Zugriff auf 7-Tage-Endpoint-Telemetrie – Vorab erstellte und benutzerdefinierten Abfragen		
Graphen zu Angriffen und eine Konsole zur Analyse		✓
IoAs und Ereignisse, die Taktiken und Techniken von MITRE ATT&CK zugeordnet sind		
CAPA-Tool-Informationen für Dateien (Verhaltensweisen, Strings, Importe, Exporte)		✓
Suche anhand von STIX IOC- und Yara-Regeln in Echtzeit an den Endpoints		✓
Erweiterte Sicherheitsrichtlinien zur Verringerung der Angriffsoberfläche		✓
Remote-Shell zur Verwaltung von Prozessen, Dateien, Diensten, Befehlszeilen, Dumps, pcap usw.		✓
Threat Hunting Service: Nicht-deterministische IoA-Erkennung mit kontextualisierter Telemetrie		✓
Ressourcensparender cloudbasierter Agent	✓	✓
Suchen in Echtzeit im Rahmen der Schwarmintelligenz	✓	✓
Zero-Trust Application Service: vor der Ausführung, während der Ausführung, nach der Ausführung	✓	✓
Anti-Exploit-Technologie für Arbeitsspeicher	✓	✓
Decoy-Dateien und Schattenkopien	✓	✓
Schutz von Systemen bei der Erstellung von Dateien	✓	✓
Threat Hunting Service: Deterministische High-Fidelity-IoA-Erkennung	✓	✓
IDS, Firewall und Gerätesteuerung	✓	✓
Web-Browsing- und E-Mail-Schutz	✓	✓
Kategoriebasiertes URL Filtering	✓	✓
WatchGuard Unified Security Platform-Funktionen: WatchGuard Cloud, ThreatSync – XDR	✓	✓

Deutschland, Österreich, Schweiz: +49 700 92229333 INTERNATIONALER VERTRIEB: +1 206 613 0895 WEB: www.watchguard.de