DELL Technologies

Dell SafeGuard and Response

Secureworks® Taegis™ XDR

Management von und Reaktion auf Cybersicherheitsbedrohungen mit automatisierten Funktionen für mehr Sicherheit und Risikominderung

HAUPTMERKMALE

- Umfassender **Schutz der Angriffsfläche**, einschließlich Endpunkt-, Netzwerk- und Cloud-Umgebungen
- **ML- und DL-basierte Analysen der Telemetriedaten und Ereignisse** von mehreren Angriffsvektoren, ergänzt durch umfassende Threat Intelligence
- **Präzisere Warnmeldungen** mit mehr Kontext und Daten, jederzeit und überall verfügbar
- **Reaktionsaktionen mit einem Mausklick** über die Konsole mit automatisierten Playbooks
- **Offene XDR-Lösung** mit zahlreichen vorkonfigurierten und einfach erstellbaren nutzerdefinierten Integrationen mit Sicherheitstools von Drittanbietern

Mit der Cloud-nativen SaaS-Plattform Secureworks Taegis™ XDR verbessern Sie die Effektivität und Effizienz Ihrer Security Operations, da umfassendes Sicherheitswissen in die Bedrohungslandschaft integriert wird.

- Profitieren Sie von ganzheitlicher Sichtbarkeit und Kontrolle über Ihre Endpunkt-, Netzwerk- und Cloud-Umgebungen mit Windows-, macOS- und Linux-Betriebssystemen, indem Sie die Echtzeit-Telemetriedaten aus den IT-Umgebungen Ihres Unternehmens aggregieren.
- Erkennen Sie Taktiken, Techniken und Prozeduren für Advanced Threats und MITRE ATT&CK, die KI-basierte Analysen, Tausende von integrierten automatisierten Gegenmaßnahmen, zahlreiche ML-basierte Bedrohungsdetektoren sowie leistungsstarke Tactic™-Diagramme für die Verknüpfung mit zugehörigen Low-Level-Ereignissen umfassen. Durch maschinelles Lernen und KI kann Taegis Muster in Lower-Level-Ereignissen erkennen und diese bei vorhandenen Gemeinsamkeiten verknüpfen.
- Beschleunigen Sie Ermittlungen, indem Sie sich auf kritische Warnmeldungen konzentrieren. Taegis XDR bietet Ihnen Incident-Response-Daten und Tools für die Bedrohungssuche sowie automatisierte Playbooks in einer nutzerfreundlichen Cloud-Konsole.

Alle Funktionen von Taegis werden kontinuierlich durch umfassende Threat-Intelligence-Erkenntnisse von Secureworks Counter Threat Unit™ und Tausende echter Incident-Response-Projekte, die das Secureworks-Team abgeschlossen hat, ergänzt.

Weitere Informationen finden Sie unter DellEMC.com/endpointsecurity

Secureworks®

DELL Technologies

MAXIMALE SICHERHEIT

Taegis XDR aggregiert Signale aus Ihrem Netzwerk, Ihrer Cloud, Ihren Endpunkten und anderen Sicherheitstools mit Threat Intelligence, damit Sie zentrale Sichtbarkeit und Kontrolle über Ihre Angriffsfläche erhalten.

Die KI-basierten Detektoren von Taegis nutzen hochmoderne Algorithmen für maschinelles Lernen und Analysetechniken, um Ihre Umgebung kontinuierlich auf bösartige Aktivitäten zu überwachen, und können so feindliche Verhaltensweisen frühzeitig erkennen. Die automatischen Playbooks und Reaktionsaktionen mit einem Mausklick von Taegis XDR ermöglichen eine schnelle Reaktion und helfen Ihnen, ausgefeilte Angriffe zu erkennen, zu verstehen und zu stoppen, bevor sie Schaden anrichten können.

Umfassende Threat Intelligence, die kontinuierlich von der Secureworks Counter Threat Unit erstellt wird, bietet eine detaillierte Analyse zu aufkommenden Bedrohungen sowie zur Absicht und zum Verhalten von AngreiferInnen. Die Taegis XDR-Gegenmaßnahmen nutzen dieses Wissen, um Angriffe zu stoppen. Außerdem können Ihre Teams damit verstehen, wer, was, wann, warum und wie eine Bedrohung ist.

EFFIZIENTERE SECURITY OPERATIONS

Ermittlung der wesentlichen Punkte: Taegis kombiniert Threat Intelligence, Protokolle und Ereignisse aus verschiedenen Sicherheitstools, um Warnmeldungen zu validieren und zu priorisieren. Als Folge davon müssen Ihre AnalystInnen nicht mehr so viel Zeit für falsch positive Ergebnisse aufwenden, sondern können sich mehr um die Bewältigung echter Bedrohungen kümmern.

Schnellere Erkennung des Angriffsmusters: Taegis korreliert automatisch zugehörige Ereignisse in Ihren Endpunkt-, Netzwerk- und Cloud-Umgebungen, damit Sie die Ursache eines Angriffs ermitteln können.

Nur eine Plattform für Ermittlungen: Taegis erfasst Daten aus Ihrer gesamten Umgebung und verfügt über ein umfassendes Toolkit für die Bedrohungssuche, einschließlich Taktiken, Techniken und Prozeduren für MITRE ATT&CK. Damit erhalten Ihre AnalystInnen eine ganzheitliche Ansicht Ihrer Sicherheitsinfrastruktur und können Ermittlungen innerhalb der Plattform durchführen, ohne dass sie Daten manuell zusammenfügen oder die Tools wechseln müssen.

Intelligentere und schnellere Zusammenarbeit: Beschleunigen Sie die Ermittlungen durch bessere Zusammenarbeit und schnellere Entscheidungsfindung. Mithilfe der flexiblen Such- und Reportingfunktionen können Ihre AnalystInnen relevante Informationen schnell zusammenstellen und mit anderen teilen, um gemeinsam an den Ermittlungen zu arbeiten: Kommentare ergänzen, zugehörige Daten hinzufügen oder entfernen und den Status ändern.

DELL PROSUPPORT FÜR IHRE SOFTWARE

Ihre Dell Endpoint Security-Softwarelösung umfasst Support von Dell. Mit Dell ProSupport for Software stehen hochqualifizierte, zertifizierte TechnikerInnen 24x7 für umfassenden Softwaresupport zur Verfügung, auf den Sie sich verlassen können.

Wenden Sie sich noch heute unter endpointsecurity@dell.com an Ihren Dell Endpoint Security Specialist, um zu erfahren, wie Sie mit SafeGuard and Response-Produkten Ihren Sicherheitsstatus verbessern können.

Systemanforderungen: Taegis XDR Console – für die Cloud-native Anwendung benötigen Sie einen modernen Browser: Chrome, Edge oder Firefox. Unterstützte Systeme Taegis XDR Agent: Microsoft Windows: Windows 10, 11 sowie Windows Server 2016 und 2019, macOS: MacOS Catalina 10.15, Big Sur 11, Monterey 12 (+M1), sonstige: CentOS 7, Amazon Linux 2, Ubuntu 18.04.

Weitere Informationen finden Sie unter DellEMC.com/endpointsecurity

Secureworks®