Bitdefender GravityZone

Mehrstufige Sicherheit für lückenlosen Schutz

Cyberangriffe sind eine sehr ernst zu nehmende Bedrohung für jede Art von Unternehmen. Nahezu jede verwendete Technologie ist zugleich auch ein Einfallstor für einen Hacker-Angriff. Die Bitdefender Security-Plattform GravityZone gewährleistet lückenlosen und mehrstufigen Schutz für die gesamte Infrastruktur. XDR-Sensoren erfassen alle Anomalien, die sich nicht direkt auf den Endpoints ereignen. Ergänzende MDR-Services erkennen ungewollte Aktivitäten im gesamten Netzwerk frühzeitig und schalten diese rechtzeitig

GravityZone XDR

Ermöglicht quellenübergreifende Ereigniskorrelation u. v. m. mit dedizierten Sensoren für Cloud, Produktivitätsanwendungen, Netzwerk und Identität

- **Cloud-Sensor:** Überwacht Aktivitäten, die die Sicherheit von Cloud-Umgebungen wie Amazon Web Services® (AWS) betreffen. Dazu erstellt der Cloud-Sensor eine Baseline als Bezugspunkt für normales Verhalten, anhand derer Abweichungen sofort erkannt werden können
- **Identitätssensor:** Erkennt verdächtige Authentifizierungsaktivitäten für Anwendungen, DevOps-Tools, Datenbanken, Systeme, Cloud-Umgebungen und andere kritische Ressourcen. Stellt Sicherheitsteams Tools zur Verfügung, mit denen sie verdächtige Konten deaktivieren oder das Zurücksetzen von Anmeldeinformationen für diese Konten erzwingen können
- **Produktivitäts-App-Sensor:** Erkennt Angriffe auf oder ausgehend von Office 365-Konten und -E-Mail und ermöglicht es Sicherheitsteams, umgehend einzugreifen, z. B. durch Löschen schädlicher E-Mails
- **Netzwerksensor:** Überwacht den Netzwerkverkehr auf Anzeichen von Angriffen, so z. B. laterale Bewegungen, Versuche der Datenexfiltration, Port-Scans und Brute-Force-Angriffe

Bitdefender Threat Intelligence

Aufbauend auf der Expertise von mehreren Hundert hauseigenen Experten für Data Science, Reverse Engineering, Sicherheitsforschung u. v. m. liefern wir zielführende Bedrohungsdaten aus einem Labor, das täglich über 200.000 Malware-Exemplare ausführt, ergänzt durch Webcrawling, E-Mail-Fallen, Honeypots, überwachte Botnets und Datenaustausch mit Partnern und Strafverfolgungsbehörden

Managementkonsole

Ermöglicht Sicherheitsteams von zentraler Stelle jederzeit die volle Übersicht und Kontrolle über den gesamten Security-Stack

Device Control

Steuert Zugriff und Verwendung von USB- und anderen externen Geräten, damit Sicherheitsteams externe Geräteverbindungen selektiv zulassen oder unterbinden können.

Liefert detaillierte Berichte zu allen Geräten, die mit den verwalteten Endpoints verbunden werden

Full Disk Encryption

Integriert Verschlüsselungsberichte, Schlüsselverwaltung und Wiederherstellung in die zentrale Plattform für den Endpoint-Schutz und reduziert so das Risiko von Datenverlust und -diebstahl und vereinfacht

Patch Management

Sorgt mit lückenloser Transparenz über den Patch-Status Ihrer Windows- und Linux-Systeme für stets aktuelle Betriebssysteme und Anwendungen. Ermöglicht die Konfiguration von Wartungsfenstern, damit Patches ohne Arbeitsunterbrechungen installiert werden können

Network Attack Defense

Setzt auf maschinelles Lernen und Heuristiken, um Verhaltensweisen zu analysieren und Malware-Aktivitäten wie laterale Bewegungen und Brute-Force-Versuche zuverlässig aufzuspüren. Besonders wichtig für Laptops und andere Systeme, die außerhalb Ihres Netzwerks betrieben werden

Risikobewertung für Endpoints und Benutzerverhalten

Sucht nach Risiken im Zusammenhang mit Fehlkonfigurationen, Schwachstellen und Benutzerverhalten. So bleiben Sicherheitsteams immer einen Schritt voraus und können direkt über die GravityZone-Konsole Gegenmaßnahmen ergreifen

Managed Detection & Response (MDR)

Gewährleistet dank 24/7-Überwachung, fortschrittlicher Angriffsprävention, Erkennung und Behebung sowie proaktiver, erkenntnisbasierter Bedrohungssuche durch zertifizierte Experten Ihre Cyberresilienz

Mehr dazu unter **bitdefender.de**