G DATA CyberDefense

Allgemeines

Hersteller	G DATA CyberDefense AG
Hauptsitz	Königsallee 178 a, G DATA Campus, 44799 Bochum
Sitz der Softwareentwicklung	Am Hauptsitz
Sitz der Service- und Support-Teams	Am Hauptsitz
Standorte der Rechenzentren	Bochum, Frankfurt am Main, Berlin
Gegründet	1985
Besonderheiten	Erfinder des Antivirus 1987
Betriebssysteme	Windows, Linux

Angriffs-Erkennung (Detection)

- Lokale, graphbasierte Aufzeichnung von Sensordaten
- Übermittlung relevanter Sensordaten an Cloud Backend zur Angriffsbewertung durch Security Analysten
- Lokales Speichern vollständiger Sensordaten, um Fernanalyse eines potentiellen Angriffs zu ermöglichen

Angriffs-Reaktion (Response)

- Auditierte Remoteshell zur Durchführung von Response-Aktionen sowie Fern-Analyse von erkannten Angriffen

Service-Level G5 und G7

Für Ihre gesamte IT-Umgebung

Sie suchen einen MXDR Service, der Ihr gesamtes Netzwerk abdeckt? Dann sind unsere Service-Level G5 und G7 genau richtig für Sie.

Leistungen	G5	G7
	Komfortabler und auf Ihre Bedürfnisse zugeschnittener 24/7 Managed Security Service für kritische Vorfälle	Umfangreicher 24/7 Managed Security Service für ein erhöhtes Schutzlevel und mit direktem Ansprechpartner
Webkonsole	✓	✓
NextGen Endpoint Agent	✓	✓
24/7 Detection & Response Analyst Service	Kritisch eingestufte Vorfälle	Alle Vorfälle
24/7 Support auf Deutsch	✓	✓
Persönliche Betreuung durch Technical Account Management		✓
Onboarding Workshop	✓ (einmalige Kosten)	✓ (inklusive)
Regelmäßige Konfig-Checks		✓
Incident Compromise Check		✓
24/7 Angriffsbenachrichtigung per Telefon		✓
24/7 Angriffsbenachrichtigung per E-Mail	✓	✓
Incident Response Retainer Gold/Platinum	optional	optional
365 Mail Protection	optional	optional
Mobile Device Management	optional	optional
Device Control	optional	optional

Service-Level G3

Speziell für Server

Ein Angriff ist am gefährlichsten, wenn er es schafft, zu Ihren kritischen Servern vorzudringen. Genau hier setzt unser Service-Level G3 an. Indem wir gezielt Ihre Server überwachen, können Sie rechtzeitig die Angriffe eindämmen, die schwerwiegende Folgen für Ihr Unternehmen hätten.

Leistung	Beschreibung
Webkonsole	In der Webkonsole sehen Sie stets, welche Vorfälle es gab, was wir für Sie getan haben und ob Handlungsempfehlungen vorliegen. Weitere Benutzer können Sie mit verschiedenen Rechten hinzufügen.
NextGen Endpoint Agent	Unsere Software Agents schützen Ihre Endpoints vor Malware-Infektionen und überwachen sie auf auffälliges Verhalten. Dank Graph- und KI-gestützter Event-Korrelation haben wir stets Ihr gesamtes Netzwerk im Blick. Die Software Agents reagieren, falls nötig, automatisch und schlagen direkt bei unseren Analysten Alarm.
24/7 Detection & Response Analyst Service	Unsere Analysten überwachen 24/7 Ihre Endgeräte. Sobald ein Verdacht besteht, analysieren wir den Vorfall tiefgehend. Im Fall eines Angriffs reagieren wir direkt, um die Angreifenden auszusperren – und informieren Sie sofort.
24/7 Support auf Deutsch	Bei Fragen ist unser Support am Bochumer Hauptsitz jederzeit telefonisch für Sie da – rund um die Uhr, an 365 Tagen im Jahr. Per E-Mail stehen wir Ihnen werktags Mo-Fr von 9-16 Uhr zur Verfügung.
Persönliche Betreuung durch Technical Account Management	Direkte Betreuung durch unsere 3rd Level Technical Account Manager. Bei kritischen technischen Fragen helfen wir Ihnen mit Remote Support zum Beispiel via Team Viewer weiter (werktags Mo-Fr von 9 bis 16 Uhr).
Onboarding Workshop	Für einen leichten Start führen wir zusammen einen mehrstufigen Remote Onboarding Workshop durch. Wir besprechen dabei die Konfiguration, wie wir bestimmte Endgeräte behandeln sollen, zum Beispiel ob wir eigenständig Reaktionen ausführen sollen oder nur nach Rücksprache. Gemeinsam wägen wir die Vor- und Nachteile ab.
Regelmäßige Konfig-Checks	Lassen Sie einmal pro Jahr die im Onboarding vorgenommene Konfiguration auf Aktualität prüfen und erhalten Sie Best-Practice-Empfehlungen. Wir passen die Konfiguration für Sie an Ihre aktuellen Bedürfnisse an.
Incident Compromise Check	Sie haben selbst etwas Verdächtiges entdeckt und möchten es prüfen lassen? Wir liefern Ihnen eine Ersteinschätzung inklusive möglicher Handlungsoptionen (werktags Mo-Fr von 9 bis 16 Uhr, 2 Stunden pro Jahr).
24/7 Angriffsbenachrichtigung per Telefon	Bei einem kritischen Vorfall rufen wir Sie umgehend an – rund um die Uhr, an 365 Tagen im Jahr.
24/7 Angriffsbenachrichtigung per E-Mail	Bei einem kritischen Vorfall informieren wir Sie umgehend per E-Mail – rund um die Uhr, an 365 Tagen im Jahr. Weniger kritische Vorfälle teilen wir Ihnen ebenfalls per E-Mail mit, wenn Sie es wünschen.
Incident Response Retainer Gold/Platinum	Ihr Plus an Sicherheit: In Fällen, die den Einsatz eines Incident Response Teams erfordern, stehen Ihnen unsere Fachleute zu garantierten Reaktionszeiten zur Seite. Als BSI-qualifizierter APT-Response-Dienstleister lösen wir IT-Sicherheitsvorfälle jeglicher Komplexität. Zusätzlich beraten wir Sie kontinuierlich, um langfristig gemeinsam Ihre Incident Readiness zu steigern.
365 Mail Protection	Das Zusatzmodul blockiert gefährliche E-Mails und Spam - speziell für Microsoft 365 Exchange Online oder Exchange Online als Einzellösung. Der E-Mail-Schutz fügt sich nahtlos in MXDR ein: Verwalten Sie ihn einfach über dieselbe Webkonsole.
Mobile Device Management	Verwalten Sie zentral die Sicherheit Ihrer iOS- und Android-Mobilgeräte – einfach direkt in Ihrer MXDR Webkonsole. Der Diebstahlschutz sichert Ihre sensiblen Daten: Orten, sperren oder löschen Sie Mobilgeräte aus der Ferne. Unerwünschte Apps können Sie einfach blockieren.
Device Control	Mit der voll integrierten Device Control können Sie steuern, wer im Unternehmen auf welche externen Geräte zugreifen darf, zum Beispiel auf Wechseldatenträger oder optische Laufwerke. Einfach und zentral in Ihrer MXDR Webkonsole.

Deployment

- Kompatibel zu marktüblichen Deploymentsystemen, welche die Ausführung von Executables erlauben
- Minimaler Footprint (Agent wird nur mit Minimalkomponenten ausgeliefert)
- Weitere zum Betrieb benötigte Komponenten lädt der Agent nach der Installation automatisch im Hintergrund nach
- Updates werden im Hintergrund automatisch installiert

Verwendung von Sensordaten

Zweck	Regelbasierte Erkennung von Angriffen Endpointübergreifende Korrelation der Sensordaten für die Bewertung von Angriffswahrscheinlichkeiten
Hosting	Alle in diesem Dokument genannten Daten werden ausschließlich in Rechenzentren gespeichert und verarbeitet, die unter "Allgemeines - Standort der Rechenzentren" aufgelistet sind

MXDR Agents

Malware-Erkennung	Statischer Scanner	Graphbasierte Verhaltensüberwachung	KI-Basierte Erkennung
Funktionalität auch ohne aktive Internetverbindung gewährleistet	✓	✓	✓
Stündliche Updates (benötigt aktive Internetverbindung)	✓	✓	✓
Quarantänisierung infizierter Dateien	✓	✓	✓
On Access Dateiscan	✓	✓	✓
Beenden von schadhaften Prozessbäumen	✓	✓	✓
Entfernung schadhafter Artefakte (Dateien, Registry- und Autostart-Einträge)	✓	✓	✓

Webkonsole

Anmeldung

- Hauptansprechpartner erhält im Onboarding-Workshop Zugangsinformationen zur Webkonsole
- Änderung des Passworts

Profilverwaltung

- Anpassung Kontaktinformationen
- Allgemeine Einstellungen (Theme oder Sprache)

Benutzer- und Rollenverwaltung

- Anlegen zusätzlicher Benutzer und Rollen
- Ändern von Benutzerinformationen und Benutzerrollen
- Ändern von Berechtigungen über Rollenzuweisung
- Sperren von Benutzerkonten
- Löschen von Benutzerkonten und -rollen

Endpoint-Verwaltung

- Listen-Ansicht aller ausgerollten XDR-Agents
- Organisation ausgerollter XDR-Agents in individualisierbare Organizational Units
- Remote-Deinstallation von XDR-Agents
- Festlegung von Zugriffsberechtigungen

Incident-Übersicht

- Listen-Ansicht und Status aller erkannten Angriffe inklusive Handlungsempfehlungen

Hier erfahren Sie mehr:
gdata.de/mxdr