LOGMANAGEMENT, SECURITY MONITORING & MANAGED XDR

Während lange Zeit der Schwerpunkt der Cyber Security auf dem Schutz vor Angriffen lag, ist es angesichts der heutigen komplexen Bedrohungslage für Unternehmen unerlässlich, sich für einen Angriff zu wappnen und proaktiv zu handeln. Es gilt nun, ein Verteidigungssystem aufzubauen, um Cyberkriminellen einen Schritt voraus zu sein. Mit unseren indivuduell anpassbaren Cyber Defense Services unterstützen wir Sie dabei, Angriffe nicht nur frühzeitig zu erkennen, sondern auch effektiv zu reagieren, um Schäden zu vermeiden oder eindämmen zu können.

INDEVIS LOGMANAGEMENT – POWERED BY GOOGLE CHRONICLE: KOSTENGÜNSTIGE & SICHERE LOGDATENSPEICHERUNG

Viele Unternehmen übersehen das große Potenzial, das in ihren Logdaten verborgen liegt. Logmanagement spielt eine entscheidende Rolle bei der Bekämpfung von Cyberbedrohungen und bei der Einhaltung von Compliance-Vorschriften.

indevis Logmanagement ermöglicht das präzise Erfassen und sichere Speichern von Daten und Protokollen aus vielfältigen Systemen. Die langfristige Speicherung von Logdaten über volle 12 Monate hinweg erlaubt es Unternehmen, nicht nur die Anforderungen der Compliance- Richtlinien zu erfüllen, sondern auch bei Sicherheitsvorfällen auf historische Daten zuzugreifen, die eine tiefgehende Untersuchung ermöglichen.

indevis Logmanagement bietet darüber hinaus dank Google Chronicle eine herausragende Suchfunktion, die es erlaubt, mehrere Abfragen gleichzeitig durchzuführen und Daten mühelos zu filtern. Durch diesen Ansatz wird das Auffinden relevanter Informationen erleichtert und das Potenzial für Erkenntnisse aus den gesammelten Daten maximiert. Die gesammelten Protokollinformationen können mittels umfangreicher Dashboard- und Berichtsfunktionen in ansprechenden Visualisierungen präsentiert werden, die Einblicke in potenzielle Bedrohungen und die Systemgesundheit bieten.

indevis Logmanagement – Leistungen

- Ein Tenant wird in einem SIEM bereitgestellt und alle ausgewählten Logdaten der Systeme, die daran angebunden sind, auf dem Tenant gespeichert.
- Logdaten werden langfristig gespeichert (im Standard 12 Monate), um Compliance-Anforderungen zu erfüllen oder im Falle einer Untersuchung auf historische Daten zugreifen zu können.

IHRE VORTEILE

INDEVIS LOGMANAGEMENT

+ Bereitstellung eines Tenants in einem marktführenden SIEM
+ Langfristige Speicherung ausgewählter Logdaten (12 Monate)
+ Einfaches und kostengünstiges Lizenzsystem nach TByte
+ Leistungsstarke Suchfunktionalität powered by Google Chronicle

INDEVIS SECURITY MONITORING

+ Bereitstellung eines Tenants in einem marktführenden SIEM
+ Automatisierte Auswertung der Logdaten und Meldung von

INDEVIS MANAGED XDR

+ Schutz vor neuesten Bedrohungen
+ High-Fidelity-Erkennung durch künstliche Intelligenz
+ Automatisierte Ursachenanalyse

cloud services MADE IN GERMANY

SIE WOLLEN MEHR ERFAHREN?

Ihr persönlicher Ansprechpartner berät Sie gerne und findet mit Ihnen heraus, welches Konzept am besten zu Ihnen passt.

+49 (89) 45 24 24-100
sales@indevis.de
www.indevis.de

ÜBER DIE INDEVIS GMBH

Die ISO 27001 zertifizierte indevis GmbH mit Sitz in München bietet seit 1999 IT-Sicherheits-, Datacenter- und Netzwerklösungen, flankiert von professionellen Consulting-, Management- und Support-Dienstleistungen. Dabei erfüllt indevis sowohl die Anforderungen der Wirtschaft als auch die von öffentlichen Behörden und Hochschulen.

Als einer von Deutschlands führenden Managed Security Service Providern ist indevis der Partner für IT Security und Netzwerktechnik für Unternehmen jeder Größe und Branche – denn IT-Sicherheit muss strategisch geplant werden.

Dabei ist indevis nicht nur in München und Umgebung vertreten: Unsere Mitarbeiterinnen und Mitarbeiter sind an Standorten in ganz Deutschland aktiv.

TÜV SÜD ISO 27001

indevis
Sicherheit in einer vernetzten Welt

indevis GmbH
Koppstraße 14
81379 München

Tel. +49 (89) 45 24 24-100
Fax +49 (89) 45 24 24-199

sales@indevis.de
www.indevis.de

INDEVIS SECURITY MONITORING

Die kontinuierliche Überwachung von Systemen, Netzwerken und Anwendungen ist notwendig, um sicherheitsrelevante Ereignisse zeitnah zu identifizieren und handeln zu können.

indevis Security Monitoring basiert auf dem leistungsstarken Tool Google Chronicle SIEM, in dem ein umfangreicher Satz an Erkennungsregeln implementiert ist. Es bietet die Möglichkeit, großzügig Logdaten im Hot Storage zu speichern (12 Monate). So können Unternehmen vor allem im Hinblick auf Kritische Infrastrukturen auch die Anforderungen verschiedener Sicherheitsrichtlinien und Regularien erfüllen.

Durch unsere Partnerschaft mit Google und durch unser hochqualifiziertes Security-Team können wir Ihre Netzwerke ganz nach Ihren individuellen Anforderungen mit den fortschrittlichsten Technologien absichern.

indevis Security Monitoring – Leistungen

- Der Kunde wird unmittelbarunmittelbar automatisiert über erkannte Auffälligkeiten mit den Severities High und Critical per E-Mail informiert.
- Auffälligkeiten mit den Severities Low und Medium werden in einem wöchentlichen Report automatisiert in aggregierter Form zur Verfügung gestellt.
- Der Kunde erhält Lesezugriff auf seine Instanz von Google Chronicle.

INDEVIS MANAGED XDR (NUR ALS TEIL VON INDEVIS MDR*)

Um Bedrohungen frühzeitig zu erkennen, empfiehlt sich die zentrale Erfassung und Korrelation von Daten aus verschiedenen Sicherheitsebenen wie Endpoint, Server und Firewall durch eine XDR-Lösung (Extended Detection and Response). Um das eigene Security-Personal zu entlasten, bietet indevis daher mit seinem *indevis Managed XDR* Service stets aktuellen Schutz vor Angriffen auf dem Endpoint.

Der *indevis Managed XDR* Service basiert auf der Endpoint Schutzlösung von Palo Alto Networks. indevis übernimmt dabei die Implementierung, Konfiguration und Wartung der XDR-Administrationsoberfläche von Cortex XDR Pro oder Cortex XDR Prevent. Wir sorgen mit unserem geballten Know-how für einen reibungslosen Betrieb bei Ihren bestehenden Umgebungen oder unterstützen Sie bei der Migration zur XDR-Lösung von Palo Alto Networks.

indevis Managed XDR – Standardleistungen

- Durchführung von Standard Changes
- Bearbeitung und Lösung von System Incidents. Security Incidents werden im Rahmen von *indevis MDR* bearbeitet
- Durchführung von zwei Reviews pro Jahr

* Der *indevis Managed XDR* Service kann nur in Kombination mit dem indevis Managed Detection and Response Service gebucht werden.