

Ihre Vorteile

- KI-gestützte Angriffserkennung in Echtzeit
- Modernste Schutztechnologien marktführender Hersteller professionell eingesetzt
- Anbindung verschiedener Daten-Quellen
- Profitieren von teuren und komplexen Security-Tools (SIEM, SOAR) zu erschwinglichen Kosten
- Dt. Rechenzentrum, deutschsprachige Ansprechpartner in eigenem indevis SOC
- Full Service durch das indevis SOC gemäß gewähltem Leistungsumfang



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

INDEVIS MANAGED DETECTION AND RESPONSE

SIEM, SOAR UND SOC: DIE EVOLUTION VON PROTECTION ZU DETECTION HEISST MDR

Selbst die besten Schutzmaßnahmen bieten keine Garantie, von Hackerangriffen verschont zu bleiben. Wer Security ernst nimmt, muss sich darüber im Klaren sein, dass Protection-Tools keine 100%ige Sicherheit bieten und auch ein Augenmerk auf Detection gelegt werden muss. Um Schaden durch Cyberangriffe zu vermeiden, ist es für Unternehmen wichtig, Bedrohungen schnell zu ermitteln und zu beseitigen.

Das Zusammenwirken moderner Security-Tools wie SIEM und SOAR (Security Orchestration, Automation and Response) als Unterstützung für ein SOC (Security Operations Center) ermöglicht es, Angriffe und deren Vektoren in Echtzeit aufzudecken und zu stoppen. Sparen Sie sich den komplexen und kostenintensiven Eigenbetrieb dieser Lösungen und vergeuden Sie in Zeiten von Fachkräftemangel keine Ressourcen für die mühselige Suche nach den benötigten Security-Mitarbeitern. Dank Managed Detection and Response (MDR) können Sie die entsprechenden Leistungen auch als Service von indevis beziehen. Im Rahmen des *indevis Managed Detection and Response Services* profitieren auch mittelständische Unternehmen von diesen fortschrittlichen Cyber Security Tools zu erschwinglichen Kosten.

INDEVIS MDR: AUTOMATISCH AUF DER SICHEREN SEITE

Hackerangriffe werden nicht nur immer ausgefeilter, sondern auch zahlreicher, denn Cyberkriminelle machen sich ebenfalls die Automatisierung zu Nutzen. Von Menschenhand kann dem kaum etwas entgegengesetzt werden, denn die Datenmengen, die auf verdächtige Inhalte hin untersucht werden müssen, nehmen rasant zu. Außerdem müssen alle potenziellen Einfallstore auf Malware hin überprüft werden. Für Unternehmen, v.a. aus dem Mittelstand, die dieses Dilemma überwinden wollen, bietet sich ein optimaler Weg an: *indevis Managed Detection and Response* als Service.

KI-GESTÜTZTE ANGRIFFSERKENNUNG – AUCH FÜR DEN MITTELSTAND

Der Aufbau eines eigenen SOC sowie der Betrieb von SIEM und SOAR Lösungen ist nicht nur teuer, sondern erfordert auch ein hohes Maß an personellen Ressourcen. Darüber hinaus haben solche Lösungen hohe Hardware-Anforderungen, sind komplex zu bedienen und bieten oft nur mit der Integration von kostenpflichtigen Threat Intelligence-Feeds einen entscheidenden Mehrwert. Das immer aufwendigere Security-Management und die Masse an Security Alerts führen dazu, dass Incidents nicht schnell genug ausgewertet werden und Bedrohungen zu lange unbemerkt bleiben. Mit *indevis Managed Detection and Response* profitieren Sie von KI- und Machine Learning unterstützten Schutztechnologien im Rahmen eines kosteneffizienten MDR-Services.

VORTEILE DES INDEVIS MANAGED DETECTION & RESPONSE SERVICES:

- Modernste Schutztechnologien marktführender Hersteller professionell eingesetzt
- Entlastung der IT-Abteilung, kein umfangreicher eigener Know-how-Aufbau bei verschärftem Fachkräftemangel notwendig
- Anbindung verschiedener Datenquellen
- KI-gestützte Angriffserkennung in Echtzeit
- Verkürzung der MTTD und MTTR
- Angepasste Handlungsempfehlungen



FUNKTIONSWEISE INDEVIS MANAGED DETECTION & RESPONSE

Der Service *indevi*s Managed Detection and Response bietet eine automatisierte Bedrohungsüberwachung und -erkennung rund um die Uhr mit einer modernen Security Incident-Analyse. Sicherheitsrelevante System- und Netzwerk-Logs werden vom *indevi*s Managed Detection and Response Service um fortschrittliche Analysen und Bedrohungs-Informationen aus diversen Quellen angereichert. Die Security-Analysten im *indevi*s SOC untersuchen die anhand der MDR-Plattform entdeckten Security-Vorfälle. *indevi*s führt eine Vorfalvalidierung durch, informiert die Kunden über den Sicherheitsvorfall und gibt eine passende Handlungsempfehlung.

VERKÜRZTE ANGRIFFSERKENNUNG DANK (TEIL-) AUTOMATISIERTER BEDROHUNGSANALYSE

Mit seiner MDR-Plattform senkt *indevi*s die MTTD (Mean Time To Detect) und die MTTR (Mean Time To Response). Durch die Automatisierung verschiedener Aktivitäten kann ein Großteil der auftretenden Security Incidents sofort und automatisch bearbeitet werden. *indevi*s betreibt hierzu in den *indevi*s-Rechenzentren eine SOAR Plattform. Diese stellt Software und Verfahren zur Verfügung, mit denen sich Informationen über Sicherheitsbedrohungen sammeln und mögliche Reaktionen automatisieren lassen. Die Analyse der Bedrohungslage basiert auf Daten aus Quellen wie Firewalls, EDR-Lösungen und anderen Datensammlungen (z.B. Palo Alto Networks Data Lake).

LEISTUNGSUMFANG INDEVIS MANAGED DETECTION & RESPONSE

Standardleistungen

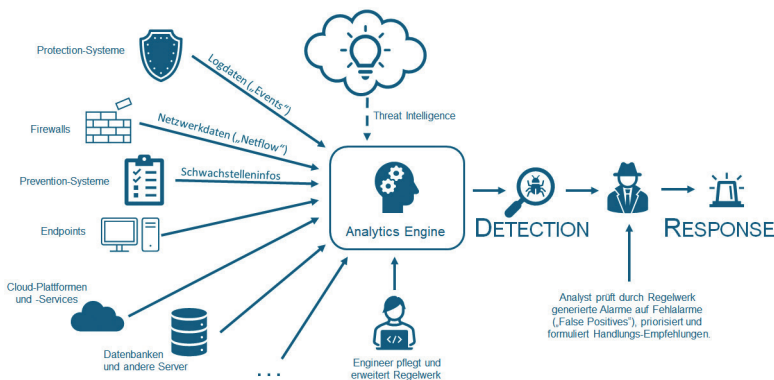
- Die *indevi*s MDR-Plattform wertet die gemeldeten Security Incidents der MDR-Plattform aus und reichert diese um Informationen aus weiteren Quellen an.
- Durch den Einsatz von fest definierten Playbooks in SOAR können manuelle Security-Analysen teil- bzw. vollautomatisiert werden.
- Die Plattform ist mandantenfähig ausgelegt mit separierter Datenspeicherung pro Kunde.

Optionale Leistungen

- **Weitere Datenquellen:** *indevi*s kann weitere Datenquellen (z.B. SIEM, Endpoint, Cloud) an die *indevi*s MDR-Plattform anschließen, soweit die Anbindung unterstützt wird.
- **Kundenspezifische Use Cases:** Entwicklung von kundenspezifischen Use Cases zur Erkennung von Security Incidents, insbesondere im Kontext von zusätzlichen Datenquellen.

Weitere Leistungen

- **Co-Managed SOAR:** Dem Kunden wird Zugriff auf den eigenen Tenant der *indevi*s MDR-Plattform zur Verfügung gestellt.



indevis GmbH

Irschenhauser Straße 10
81379 München

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

sales@indevi

www.indevi

Über die *indevi*s GmbH

Die ISO 27001 zertifizierte *indevi*s GmbH bietet seit 1999 IT-Sicherheits-, Data-center- und Netzwerklösungen, flankiert von professionellen Consulting-, Management- und Support-Dienstleistungen. Dabei erfüllt *indevi*s sowohl die Anforderungen der Wirtschaft als auch die von öffentlichen Behörden und Hochschulen.

Als einer von Deutschlands führenden Managed Security Service Providern ist *indevi*s der Partner für IT-Sicherheit und Netzwerktechnik für Unternehmen jeder Größe und Branche – denn IT Sicherheit passiert nicht von alleine, sondern muss strategisch geplant werden.

*indevi*s betreibt zwei Niederlassungen: in München und Hamburg. Weitere Mitarbeiter agieren von mehreren Standorten über Deutschland verteilt aus.



Sie wollen *indevi*s Managed Detection and Response kennenlernen? Auf Wunsch stellen wir Ihnen den Service gerne in einer Demo-Session vor – und Sie erfahren die Vorteile eines modernen und kosteneffizienten MDR-Services für Ihr Unternehmen.