



SOC AS A SERVICE (SOCAAS): IHR SICHERHEITSRADAR IM 24/7-BETRIEB

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 indevis SOC as a Service (SOCaaS) können Sie die entsprechenden Leistungen auch als Service von indevis beziehen. Im Rahmen des indevis SOC as a Service profitieren auch mittelständische Unternehmen von diesen fortschrittlichen Cyber Security Tools zu erschwinglichen Kosten.

INDEVIS SOC AS A SERVICE: AUTOMATISCH AUF DER SICHEREN SEITE

Hackerangriffe werden nicht nur immer ausgefeilter, sondern auch zahlreicher, denn Cyberkriminelle machen sich ebenfalls die Automatisierung zunutze. 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 überprüft werden. Für Unternehmen, v.a. aus dem Mittelstand, die dieses Dilemma überwinden wollen, bietet sich ein optimaler Weg an: indevis SOC as a 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 SOC as a Service profitieren Sie von KI- und Machine Learning unterstützten Schutztechnologien.

IHRE VORTEILE

- + Modernste Schutztechnologien marktführender Hersteller professionell eingesetzt
- + Profitieren von teuren und komplexen Security-Tools (SIEM, SOAR, SecOps) zu erschwinglichen Kosten
- + Verkürzung der MTTD und MTTR
- + Anbindung verschiedener Daten-Quellen
- + KI-gestützte Angriffserkennung in Echtzeit
- + 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



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.



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

FUNKTIONSWEISE INDEVIS SOC AS A SERVICE

indevis SOC as a Service bietet eine automatisierte Bedrohungsüberwachung und -erkennung rund um die Uhr mit einer modernen Security Incident-Analyse. Sicherheitsrelevante System- und Netzwerk-Logs werden vom indevis SOC as a Service um fortschrittliche Analysen und Bedrohungsinformationen aus diversen Quellen angereichert. Die Security-Analysten im indevis SOC untersuchen die anhand der SecOps-Plattform entdeckten Security-Vorfälle. indevis führt eine Vorfalvalidierung durch, informiert die Kunden über den Sicherheitsvorfall und gibt eine passende Handlungsempfehlung.

VERKÜRZTE ANGRIFFSERKENNUNG DANK (TEIL-) AUTOMATISIERTER BEDROHUNGSANALYSE

Mit seiner SOCaaS-Plattform senkt indevis 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. indevis betreibt hierzu in den indevis-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 SOC AS A SERVICE

Standardleistungen

- Die indevis SOCaaS-Plattform wertet gemeldete Security Incidents aus und reichert diese um Informationen aus weiteren Quellen an.
- Durch den Einsatz von fest definierten Playbooks können manuelle Security-Analysen teil- bzw. vollautomatisiert werden.
- Die Plattform ist mandantenfähig ausgelegt mit separierter Datenspeicherung pro Kunde.

Optionale Leistungen

- **Weitere Datenquellen:** indevis kann weitere Datenquellen (z.B. SIEM, Endpoint, Cloud) an die indevis SOCaaS-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:** Dem Kunden wird Zugriff auf den eigenen Tenant der indevis SOCaaS-Plattform zur Verfügung gestellt.

