WITH secure | Gold Partner

MEDIALINE

Medialine CyberGuard

Das leistbare Security Operations Center speziell für KMUs

Medialine CyberGuard bietet Unternehmen ein leistungsstarkes Security Operations Center (SOC) zur frühzeitigen Erkennung und effektiven Abwehr von Cyberangriffen. Durch eine Kombination aus modernster Technologie und der Expertise erfahrener Sicherheitsspezialisten wird Ihr Unternehmen rund um die Uhr überwacht, Bedrohungen werden erkannt, analysiert und gezielt entschärft – ohne dass Sie selbst aktiv eingreifen müssen.

Besonders kleine und mittelständische Unternehmen (KMU) stehen vor der Herausforderung, ihre IT-Systeme angemessen zu schützen, ohne über die personellen und finanziellen Ressourcen großer Unternehmen zu verfügen. Daher hat die Medialine AG in Zusammenarbeit mit WithSecure eine leistbare Lösung erarbeitet und bietet mit dem Medialine CyberGuard ein leistungsstarkes und kosteneffizientes Security Operations Center für KMUs. Ein SOC-Team besteht aus ausgebildeten IT Security Spezialisten und überwacht rund um die Uhr - 24/7 - die IT-Systeme Ihres Unternehmens, um Cyberangriffe und Sicherheitsbedrohungen frühzeitig zu erkennen. Bei verdächtigen Aktivitäten analysiert es die Situation, reagiert auf Angriffe und ergreift sofort Gegenmaßnahmen, um Schäden zu minimieren. Zudem sorgt es für die kontinuierliche Verbesserung der IT-Sicherheit durch Prävention und Berichterstattung an die Geschäftsleitung.

Was ist der Medialine CyberGuard?

Der Medialine CyberGuard ist ein Security Operations Center, welches genau für KMUs entwickelt wurde und folgende Vorteile bietet:

- **Rund-um-die-Uhr-Schutz:** Ein SOC überwacht für Sie die IT-Systeme 24/7 und erkennt Angriffe in Echtzeit.
- **Schnelle Reaktion auf Bedrohungen:** 60 Minuten vom Angriff bis zur Gegenmaßnahme - dadurch werden Schäden minimiert und Ausfallzeiten verhindert.
- **Schutz sensibler Daten:** Datendiebstahl und Datenschutzverletzungen, die zu hohen Strafen und Imageverlust führen, können verhindert werden.
- **Unterstützung bei der Einhaltung gesetzlicher Vorschriften:** Viele Branchen müssen IT-Sicherheitsstandards erfüllen (z. B. DSGVO, NIS2, DORA...).
- **Risiko Minimierung:** Ein erfolgreicher Cyberangriff kann sehr teure Folgen haben – ein SOC hilft, diese zu vermeiden.
- **Vertrauen von Kunden und Partnern:** Ein professionelles Sicherheitsmanagement stärkt die Reputation Ihres Unternehmens.

W I T H secure | Gold Partner

MEDIALINE

Welche Leistungen kann ich vom Medialine CyberGuard erwarten?

Der Medialine CyberGuard bietet eine kontinuierliche, kosteneffiziente Überwachung, Erkennung und Reaktion auf Cyberangriffe. Durch ein erfahrenes Analystenteam, fortschrittliche Bedrohungsanalyse und abgesicherte SLAs gewährleistet er umfassenden Schutz rund um die Uhr - zu einem Bruchteil der Kosten eines eigenen SOC.

Die Bestandteile des Medialine CyberGuard sind:

Überwachung: Durch eine Kombination aus modernster Technologie und der Expertise erfahrener Sicherheitsspezialisten wird die IT-Umgebung Ihres Unternehmens rund um die Uhr auf verdächtige Aktivitäten überwacht. Die Bedrohungserkennung basiert auf einem intelligenten System, das verdächtige Aktivitäten identifiziert und in einem zentralen Sicherheits-Dashboard sichtbar macht. Dabei werden zahlreiche Faktoren wie Anomalien im Netzwerkverkehr, unerwartete Systemprozesse und globale Bedrohungsdaten berücksichtigt.

Untersuchung: Bei einer Identifizierung eines potenziellen Sicherheitsvorfalles wird sofort eine Validierung und Analyse von den Spezialisten durchgeführt, um festzustellen, ob es sich um echte Bedrohung handelt welche Maßnahmen erfordern oder ob es sich um Fehlalarm handelt.

Eskalation: Ist die Bedrohung ernst, wird der Eskalationsprozess gestartet. Es werden die entsprechenden Ansprechpartner in Ihrem Unternehmen kontaktiert, um die Abwehrmaßnahmen umzusetzen. Um Verzögerungen im Ernstfall zu vermeiden, können Maßnahmen zur Gefahrenabwehr für Clients z.B. standardmäßig vorab autorisiert werden. Für kritische Systeme wie z.B. Server, erfolgt jede Reaktion ausschließlich nach expliziter Freigabe durch den Kunden, um potenzielle Geschäftsunterbrechungen zu vermeiden.

Reaktion: Im Falle einer bestätigten Bedrohung erfolgt eine detaillierte Untersuchung des betroffenen Systems. Angemessene Maßnahmen zur Eindämmung und Beseitigung der Bedrohung werden nach der Freigabe durch den Ansprechpartners Ihres Unternehmens vom Security-Team selbstständig durchgeführt.

Bereitschaftsdienst: Wenn größere Cyberangriffe und komplexe Bedrohungsszenarien das Unternehmen bedrohen, haben Kunden die Möglichkeit über einen erweiterten Support gezielt tiefere Analysen oder individuelle Sicherheitsbewertungen anzufordern.

60 Minuten vom Vorfall bis zum Einschreiten...

Ein wesentlicher Bestandteil von Medialine CyberGuard ist die garantierte Reaktionszeit auf sicherheitskritische Vorfälle. Durch definierte Service-Level-Agreements (SLAs) wird sichergestellt, dass erkannte Bedrohungen innerhalb eines festgelegten Zeitraums analysiert und bearbeitet werden. Kritische Vorfälle werden innerhalb von maximal 60 Minuten eskaliert, sodass eine schnelle Reaktion möglich ist. Unabhängig von Zeit und Ort stehen Experten rund um die Uhr zur Verfügung, um Sicherheitsvorfälle zu bewerten und geeignete Maßnahmen einzuleiten.

Durch diese klar definierten SLAs erhalten Unternehmen nicht nur eine zuverlässige Sicherheitslösung, sondern auch die Gewissheit, dass im Notfall schnelle Hilfe verfügbar ist. Zudem bietet Medialine CyberGuard flexible Eskalationsstufen, sodass Unternehmen je nach Schweregrad einer Bedrohung angemessen informiert und unterstützt werden.

Warum Medialine CyberGuard?

Cyberangriffe betreffen längst nicht mehr nur Großunternehmen – auch kleine und mittelständische Unternehmen (KMUs) rücken zunehmend ins Visier von Cyberkriminellen. Doch während Konzerne über eigene Security Operations Center (SOC) verfügen, die oft mehrere zehntausend Euro pro Jahr kosten, fehlte KMUs bislang der Zugang zu professionellem Schutz auf diesem Niveau. Mit dem Medialine CyberGuard schließen wir genau diese Lücke. Durch unsere Initiative ermöglichen wir es nun auch kleineren Unternehmen, sich auf Enterprise-Niveau zu schützen – ohne hohe Investitionen oder eigene Sicherheitsteams aufbauen zu müssen.

Unsere Lösung kombiniert modernste Technologie mit der Expertise erfahrener Sicherheitsspezialisten und einer schnellen Incident-Response. Dies bedeutet für Unternehmen maximale Sicherheit bei minimalem Aufwand: kontinuierliche Bedrohungserkennung, automatisierte Gegenmaßnahmen und die enge Zusammenarbeit mit einem spezialisierten Security-Team sorgen für effektiven Schutz gegen Cyberangriffe – zu einem Bruchteil der Kosten eines eigenen SOC.

Wie gut ist Ihr Unternehmen vorbereitet?

Vergleichen Sie, wie viel Zeit ohne und mit Medialine CyberGuard vergeht, wenn ein Sicherheitsvorfall eintritt.

Beispiel: Ein Sicherheitsvorfall tritt außerhalb der Bürozeiten bei Ihnen im Unternehmen auf.

Stunde 0

Ein Angreifer verschafft sich Zugang zum Unternehmensnetzwerk.

In Unternehmen beträgt die durchschnittliche Zeit zur Erkennung eines Angriffs 10 Tage.

Stunde 1

Der Angreifer versucht, in das Unternehmensnetzwerk einzudringen, doch das 24/7-Monitoring von Medialine CyberGuard erkennt die verdächtige Aktivität nahezu in Echtzeit.

Die Expert*innen beginnen eine detaillierte Untersuchung, um die Art der Bedrohung zu analysieren und zu bestätigen.

Stunde 1-2

Das Medialine/WithSecure-Team identifiziert die Aktivität als echten Sicherheitsverstoß und leitet den Vorfall mit detaillierten Informationen und Handlungsempfehlungen an die Ansprechpartner des Kunden weiter.

Die Behebungsmaßnahmen starten sofort, wobei Spezialisten die betroffenen Systeme isolieren und den Zugriff des Angreifers blockieren.

Stunde 3

Die Experten arbeiten gemeinsam mit dem Kunden daran, die möglichen Auswirkungen zu bewerten und die Behebungsmaßnahmen vorzubereiten.

Stunde 4

Der Vorfall wird vollständig eingedämmt, wodurch größerer Schaden oder Datenverlust vermieden wird.

Unternehmen, das Medialine CyberGuard zur Erkennung und Reaktion auf Sicherheitsvorfälle einsetzt.

Tag 10

Ein Mitarbeitender des Unternehmens beginnt mit der Untersuchung der verdächtigen Aktivität. Doch aufgrund begrenzter Ressourcen sowie fehlender Expertise und Ausbildung im Bereich Cybersecurity verläuft der Prozess langsamer als ursprünglich angenommen.

Tag 11

Die Untersuchung deutet darauf hin, dass es sich um einen Sicherheitsverstoß handeln könnte. Ein Fehlalarm kann jedoch nicht ausgeschlossen werden. Zu diesem Zeitpunkt hat der Angreifer bereits Zugriff auf sensible Daten erlangt und sie möglicherweise kopiert oder verschlüsselt.

Das Unternehmen ergreift Behebungsmaßnahmen, isoliert betroffene sowie kritische Systeme und beginnt mit der Analyse der Sicherheitslücken, die es zu schließen gibt. Diese Verzögerung hat dem Angreifer ermöglicht, erheblichen Schaden anzurichten und möglicherweise Hintertüren für zukünftige Zugriffe zu hinterlassen.

Tag 12

Der Sicherheitsverstoß wird eingedämmt, indem mehr Systeme als nötig heruntergefahren werden - um Zeit zu gewinnen. Dennoch hat das Unternehmen bereits Datenverlust erlitten. Der tägliche Geschäftsbetrieb des Unternehmens ist stark eingeschränkt. Der Vorfall muss gemeldet werden und es drohen potenzielle regulatorische Strafen sowie Reputationsschäden.

Stand: 03/2025