SentinelOne

DATENBLATT

Vigilance Respond

MDR zur Unterstützung des SOC / Digitale Forensik / Incident Response

Die SentinelOne-Services „Vigilance Respond“ sowie „Vigilance Respond Pro“ für Managed Detection & Response (MDR) ergänzen unsere SaaS-Angebote für Endpunkt-Sicherheit.

Das Vigilance MDR-Team ist die menschliche Seite unserer KI-gestützten Singularity™-Plattform. Das Team besteht zu 100 % aus internen, niemals ausgelagerten Cybersicherheitsexperten der Stufen 1, 2 und 3. Unsere Mitarbeiter überwachen Millionen von Endpunkten und verstärken die Sicherheitsabteilungen unserer Kunden. Damit ermöglichen wir das „Vier-Augen-Prinzip“ für Ihre SentinelOne-Bereitstellung und geeignete Reaktionen zur Bedrohungseindämmung. Da sich Kunden mit Vigilance Respond und Vigilance Respond Pro auf die relevanten Zwischenfälle konzentrieren können, ist das die perfekte Endpunkt-Add-on-Lösung für überlastete IT/SOC-Teams.

ZWISCHENFÄLLE WERDEN IM DURCHSCHNITT IN WENIGER ALS 20 MINUTEN GEKLÄRT.

Dank KI-gestützter Storyline-Automatisierung und Priorisierung, ergänzt um Analysten mehrerer Stufen, erzielt Vigilance MDR eine hervorragende Geschwindigkeit.

BENÖTIGEN SIE WEITERE INFORMATIONEN?

Plattform: s1.ai/platform
Vigilance: s1.ai/services

EXPERTENTEAM
Niemals ausgelagert

VERTRAUENS-WÜRDIG
Von weltweit größten Unternehmen bestätigt

MEHRWERT
MDR und DFIR reduzieren SOC-Belastung

Vigilance Respond

Vigilance Respond MDR bietet Mehrwert, da Sicherheitsabteilungen verstärkt und entlastet werden.

- Übersichtliche Dashboards und zuverlässiger Schutz
- Jede Bedrohung wird überprüft, behandelt und dokumentiert, damit Sie auf dem Laufenden sind
- Eskalationen erfolgen nur in dringenden Fällen

- Täglich rund um die Uhr aktiv
- Triagierung und Priorisierung von Ereignissen
- Weniger Warnungen, mehr Kontext
- Beschleunigte Bedrohungsbehebung
- Übersichtliche Dashboards
- Proaktive Benachrichtigungen
- Managementberichte
- Regelmäßige Telefongespräche zur Abstimmung

Vigilance Respond Pro

Vigilance Respond Pro ergänzt die Respond-Stufe um digitale Forensik und Incident Response.

- Alle Respond MDR-Funktionen plus...
- Direkter Zugang zu Forensik-Experten für Incident-Management, Eindämmung und Beratung
- Retainer-Kontingent für Schadcode-Analysen und Incident Response

- 2x schnellere SLA
- Datengestützte Suche
- Jährliches Retainer-Kontingent
- Digitale Forensik und Malware-Reverse-Engineering
- Fall-Manager für Incident Response
- Eindämmung und Entfernung
- Ursachenanalyse
- Post-Mortem-Beratung

Funktionsweise von Vigilance MDR

Bedrohungen erkannt

KI-Warteschlangen-Mechanismen priorisieren Bedrohungen.

Detaillierte **Analysen**

Bedrohungen werden durch KI/ML, Intelligence, ActiveEDR + Storyline, MITRE® TTPs, Protokolle und das professionelle Urteil eines Analysten klassifiziert.

Einblicke **in Bedrohungen**

Alle Konsolen-Zwischenfälle werden interpretiert und kommentiert, damit Sie auf dem Laufenden bleiben.

Aktion und nächste Schritte

Vigilance behebt und beseitigt Bedrohungen für Sie und startet (falls erforderlich) die proaktive Eskalation.

DFIR geht weiter ins Detail

Respond Pro-Kunden können detaillierte forensische Untersuchungen, gezieltes Threat Hunting und Incident Response durchführen.

	RESPOND	RESPOND PRO	SERVICE-UMFANG
MDR 24x7	✓	✓	• Jede in der Konsole angezeigte Bedrohung wird überprüft, behandelt und dokumentiert • Umfassende Reaktionsmaßnahmen • Proaktive Benachrichtigungen
THREAT RESPONSE SLA	**Standard** 2 Stunden/ 4 Stunden Lösung/ Untersuchung	**Premium 1 Stunden/ 2 Stunden Lösung/ Untersuchung**	• Der weltweit schnellste MDR-Service • Triagierung, Klassifizierung und erste Aktionen durch Analyst
DIGITALE FORENSISCHE ANALYSE	Triagierung	**Umfassende Untersuchung**	• Umfassende Untersuchung: RCA-Infektionsvektor, Feststellung Exfiltration/ Breach, datengestützte Suche, Anreicherung von Bedrohungsdaten/Kontext, Malware-Reverse-Engineering, Speicheranalyse und Code-Extraktion, Entschleierung von Schadcode • Triagierung: Konsolenindikator und dynamische Analyse
RETAINER FÜR INCIDENT RESPONSE		✓	• Vorab festgelegtes Retainer-Kontingent (verfällt nach Fristablauf) • Untersuchung → aktive Eindämmung → Entfernung → Reporting • Zugewiesene Fall-Manager für Incident Response • Mindestkontingent pro Zwischenfall: 8 Stunden
VIERTEL-JÄHRLICHE SICHERHEITS-PRÜFUNG		✓	• Beratung zu langfristigen Wiederherstellungsmaßnahmen und zur Optimierung der Sicherheitsarchitektur • Abstimmung der Agentenversion und Prüfung von Ausschlüssen • Trends bei Bedrohungen/Akteuren

Gartner peerinsights

"Durchgehend erstklassige Erfahrung"

★★★★★

Verantwortlicher für Sicherheit und Risikomanagement
Energie- und Versorgungsunternehmen, 500 Mio. bis 1 Mrd. USD

Gartner peerinsights

"Sehr proaktives, unterstützendes und professionelles Team"

★★★★★

Verantwortlicher für Infrastruktur und Betrieb
Medienunternehmen, 500 Mio. bis 1 Mrd. USD

Gartner peerinsights

"Kompetentes und professionelles Team"

★★★★★

Verantwortlicher für Sicherheit und Risikomanagement
Gesundheitswesen, 1 Mrd. bis 3 Mrd. USD

Gartner peerinsights

"Sehr nützlicher Add-on-Dienst"

★★★★★

Verantwortlicher für Sicherheit und Risikomanagement
Fertigungsunternehmen, 1 Mrd. bis 3 Mrd. USD

Bei SentinelOne haben Kunden höchste Priorität

Durch kontinuierliche Auswertung und Verbesserung können wir die Erwartungen unserer Kunden übertreffen.

Gartner peerinsights customers' choice™

97 %
der Gartner Peer Insights™ „Voice of the Customer"-Bewerter empfehlen SentinelOne

97 %
Kundenzufriedenheit (CSAT)

FedRAMP

ISO 27001 CERTIFIED by schellman

EU GDPR COMPLIANT

SE Labs AAA

TEVORA
PCI DSS-Bestätigung
HIPAA-Bestätigung

Gartner peerinsights 4,9 ★★★★★

Informationen zu SentinelOne

Mehr Funktionen, weniger Komplexität: SentinelOne ist ein innovativer Anbieter für Cybersicherheit mit autonomer, verteilter Endpunkt-Threat Intelligence, der das Sicherheitskonzept vereinfacht, ohne Kompromisse zu verlangen. Unsere Technologie lässt sich automatisieren und ermöglicht die reibungslose Behebung von Bedrohungen. Sind Sie bereit?

sentinelone.com
sales@sentinelone.com
+ 1 855 868 3733