TRANSFORMATION

MICROSOFT SENTINEL

IHRE ERSTE WAHL ALS MODERNER SECURITY-LEADER

Viele Sicherheitsverantwortliche sehen in traditionellen SIEMs und Insellösungen keine zukunftsfähige Option mehr. Bringen Sie Ihr Security Operations Center auf den neuesten Stand – mit intelligenten, KI-gestützten Technologien von Microsoft Sentinel, dem bewährten SIEM der nächsten Generation.

	Einschränkungen bei herkömmlichen und Nischen-SIEM-Lösungen	Erhalten Sie ein vollständiges SIEM mit Microsoft Sentinel
Kritische Fähigkeiten	Komplexität der Lösungen und fehlende Funktionen • Werkzeuge arbeiten isoliert voneinander • Wichtige Funktionen fehlen oder sind unvollständig • Häufige, aufwändige Updates notwendig • Analysten arbeiten ineffizient durch schlechte Usability • Hoher Schulungsaufwand und spezielles Know-how erforderlich	Zentralisierte SOC-Plattform mit entscheidenden Funktionen direkt integriert • Reibungslosere SecOps-Prozesse dank nahtloser XDR-Anbindung – ganz ohne Zusatzmodule oder Spezialwissen • KI-gestützte Erkennung und Reaktion direkt eingebaut • SOAR, UEBA und Threat Intelligence nativ enthalten • Integriertes Fallmanagement für effiziente Abläufe
Schutz vor Cyberbedrohungen	Hohe Alarmflut und aufwändige Vorfallsanalysen • Begrenzte Möglichkeiten zur Weiterentwicklung der Erkennung • Kaum Automatisierung vorhanden • Hohe Zahl an Fehlalarmen führt zu Alarmmüdigkeit • Langsame Erkennungs- und Reaktionszeiten (MTTD/MTTR) • Eingeschränkte Transparenz über Sicherheitsvorfälle • Langwierige, schwer nachvollziehbare Incidents • Zeitintensive Untersuchungen binden Ressourcen	KI-gestützte, präzise Bedrohungserkennung und -analyse • Cyberbedrohungen frühzeitig erkennen – dank intelligenter KI -gestützter Erkennung, Korrelation und Analysefunktionen • Deutlich weniger Fehlalarme, kürzere Reaktionszeiten (MTTR) • Tools zur Entwicklung individueller Erkennungsregeln • Proaktive Bedrohungssuche mit Machine-Learning-optimierten Regeln • Integrierter Security Copilot für KI-gestützte Unterstützung • Umfassende Threat Intelligence und angereicherte Alarme • Fortschrittliche Visualisierungen für tiefere Einblicke • KI-geführte Analysen und automatisierte Reaktionsprozesse

	Einschränkungen bei herkömmlichen und Nischen-SIEM-Lösungen	Erhalten Sie ein vollständiges SIEM mit Microsoft Sentinel
Kapitalrendite (ROI) / Gesamtbetriebskosten (TCO)	Teure und schwer skalierbare Plattform-Betriebsmodelle • Unvorhersehbare Nutzungskosten belasten das Budget • Zusätzliche Module nötig, um wichtige Funktionen abzudecken • Nicht cloud-native – abhängig von lokaler Infrastruktur oder nur eingeschränkt cloudfähig • Hoher manueller Aufwand im täglichen Betrieb	Flexible, cloud-native Architektur mit geringeren Gesamtkosten (TCO) • Planbare und wirtschaftliche Sicherheitslösungen zur Senkung der Gesamtbetriebskosten • Skalierbarkeit durch echte Cloud-Native-Technologie • Höchste Flexibilität für sich verändernde Anforderungen • Effiziente Verwaltung großer Datenmengen • Vereinfachte Betriebsabläufe durch kontextbezogene Empfehlungen direkt im Produkt
Zeit bis zur Wertschöpfung	Komplexe Implementierung mit verzögertem Mehrwert • Mangelnde Unterstützung bei der Migration erschwert den Umstieg • Eingeschränkte Kompatibilität mit bestehenden Tools und Systemen • Hoher Aufwand für individuelle Integration und Bereitstellung • Fehlende vorkonfigurierte Vorlagen, Regeln und Playbooks verlängern die Einführungszeit	Schneller Einstieg dank vorkonfigurierter Lösungen • Schneller Schutz über Clouds, Plattformen und Tools hinweg – mit leistungsstarken Migrationshilfen, einem umfangreichen Content-Katalog, Konfigurationsempfehlungen und sofort einsat bereiten Erkennungsregeln für Cyberbedrohungen • Über 350 sofort nutzbare Konnektoren verfügbar • Codelose Frameworks für individuelle, no-code Konnektoren • Nahtlose Integration in verschiedenste Cloud-Umgebungen und Tools • Große Bibliothek mit mehr als 480 anpassbaren Security-Lösungen

	Einschränkungen bei herkömmlichen und Nischen-SIEM-Lösungen	Erhalten Sie ein vollständiges SIEM mit Microsoft Sentinel
Sicherheitsinnovation	Unklare Produktstrategie und schwache Weiterentwicklung • Eingeschränkte Investitionen in Forschung und Entwicklung • Mangel an KI-Kompetenz und unzureichende KI-Funktionalität • Funktionen wirken unausgereift oder nicht vollständig umgesetzt • Begrenzte Ressourcen im Bereich Threat Intelligence und Sicherheitsforschung	Zukunftsorientierte Roadmap mit Fokus auf KI und Machine Learning • Bleiben Sie Cyberbedrohungen immer einen Schritt voraus – dank einer Produktentwicklung, die kontinuierlich bahnbrechende Innovationen für das SOC liefert • Microsoft setzt kompromisslos auf Sicherheit – gestützt durch langfristige Investitionen und über 10.000 führende Sicherheitsexperten und Ingenieure weltweit • Branchenführend in Bereichen wie generativer KI, SIEM, XDR Cloud-Security und integrierter SecOps • Tiefe, durchgängige Integration von generativer KI, Machine Learning und Automatisierung in allen Sicherheitsfunktionen • Erstklassige Threat Intelligence mit globaler Reichweite und Expertise