Claranet Threat Detection for SAP® Technology

SAP-Systeme sind das Rückgrat Ihres Unternehmens, sie beinhalten die Daten ihrer sensibelsten Geschäftsprozesse, Finanzdaten und Kundeninformationen. Genau das macht sie zu einem bevorzugten Ziel für Cyberangriffe. Gleichzeitig steigen die regulatorischen Anforderungen und verlangen nach nachweisbaren Sicherheitsmaßnahmen, während die persönliche Haftung der Geschäftsführung zunimmt.

Claranet Threat Detection wurde entwickelt, um genau diese Lücke zu schließen: Eine Plattform, die speziell für SAP-Umgebungen konzipiert ist und Ihnen zeigt, was in Ihren Systemen passiert. Von verdächtigen Zugriffen über ungewöhnliche Verhaltensmuster bis hin zu konkreten Sicherheitsvorfällen. Vier aufeinander abgestimmte Module sorgen dafür, dass Sie Bedrohungen nicht nur erkennen, sondern gezielt darauf reagieren können.

Ihre Vorteile auf einen Blick

- **Transparenz:** Jederzeit Überblick über Aktivitäten und priorisierte Warnmeldungen in SAP-Systemen.
- **Speziell für SAP:** Erkennt SAP-spezifische Risiken und Angriffsmuster, die Standardlösungen übersehen.
- **Compliance:** Automatisierte Nachweise für NIS-2, DORA und ISO 27001, weniger manueller Auditaufwand.
- **Nahtlose Integration:** Einbindung in bestehende Sicherheitsarchitektur (SIEM)
- **Geringeres Ausfallrisiko:** Früherkennung ermöglicht schnelle Reaktion und minimiert Betriebsunterbrechungen.

ThreatDetect Collect

Daten sicher erfassen

Das Fundament der Plattform: Über 15 spezialisierte SAP-Datenextraktoren erfassen sämtliche sicherheitsrelevanten Protokolle direkt aus Ihren SAP-Systemen. Die Daten werden normalisiert und einem SIEM (anbieterunabhängig) bereitgestellt. Ohne SAP-Add-on und kompatibel mit RISE with SAP.

ThreatDetect Rules

Bedrohungen erkennen

Über 500 SAP-spezifische Erkennungsregeln versetzen ein angebundenes SIEM in die Lage, SAP-spezifische Logdaten zu analysieren und priorisierte, nachvollziehbar begründete Alarme zu erzeugen. Alles auf Basis einer nahtlosen Anbindung an bestehende SIEM-Lösungen.

ThreatDetect Behave

Verhalten verstehen

Behave erkennt, was regelbasierte Systeme übersehen: Auf Basis individueller Verhaltensprofile identifiziert das Modul Abweichungen vom normalen Nutzungsverhalten. Wie etwa kompromittierte Konten oder Insider-Bedrohungen. Zukünftig mit Drift Detection und einer Risikobewertung pro Nutzer und Peer-Group-Vergleichen.

ThreatDetect Respond

Automatisch reagieren

Respond wird die Plattform um automatisierte Reaktionsfähigkeiten ergänzen: Playbooks, die bei Sicherheitsvorfällen automatisiert greifen (z.B. durch Sperren kompromittierter Konten, dem Berechtigungsentzug oder einer automatischen Ticket-Erstellung). Das Modul wird voraussichtlich ab Q4 2026 als eigenständige Erweiterung verfügbar sein.

claranet | Make modern happen®

Service-Stufen – Von der Erkennung zum vollständigen Managed Service

Claranet Threat Detection lässt sich schrittweise ausbauen. Je mehr Module Sie kombinieren, desto umfassender wird Ihr Schutz, bis hin zum vollständig von Claranet betriebenen Managed Service, der maximale Sicherheit bei minimalem Eigenauf-

Collect & Rules

Unsere SAP-Datenextraktoren erfassen sämtliche sicherheitsrelevanten Protokolle. Über 500 Erkennungsregeln ermöglichen die kontinuierliche Analyse dieser Daten basierend auf dem eingesetzten SIEM und liefern priorisierte Alarme. Sie erhalten Transparenz darüber, was in Ihren SAP-Systemen passiert – die Grundlage für gezielte Sicherheitsentscheidungen.

Collect & Rules & Behave

Regelbasierte Erkennung allein findet nur bekannte Muster. Mit Behave kommt eine entscheidende Dimension hinzu: Das Modul erstellt individuelle Verhaltensprofile Ihrer SAP-Anwender und erkennt automatisch, wenn jemand von seinem normalen Nutzungsverhalten abweicht. So werden Insider-Bedrohungen, kompromittierte Konten und schleichende Berechtigungsausweitungen sichtbar, die klassische Regeln nicht erfassen.

Managed SAP Security

Claranet übernimmt den vollständigen Betrieb Ihrer SAP-Sicherheit. Unser SAP Security SOC überwacht und analysiert rund um die Uhr und reagiert auf Verdachtsfälle mit Maßnahmen, die von der automatisierten Sperrung kompromittierter Konten bis zur kontinuierlichen Optimierung Ihrer Sicherheitslage gehen. Das verspricht maximale Sicherheit bei minimalem Eigenaufwand.

Für wen ist Claranet ThreatDetect geeignet?

Unternehmen, deren Wertschöpfung auf SAP-Systemen basiert

IT-Sicherheitsteams, die SAP-spezifische Bedrohungen gezielt adressieren wollen

Compliance-Verantwortliche mit Nachweispflichten (NIS-2, DORA, ISO 27001)

Managed-Service-Kunden, die SAP-Sicherheit in professionelle Hände geben möchten

claranet®

Weitere Informationen: claranet.com/de
Bei Fragen zu unseren Services und für Terminvereinbarungen:
Telefon: 069 40 80 18 450 - E-Mail: de-info@claranet.com