CENOTI
CONNECT SAP® WITH SPLUNK®

EPI-USE LABS
value through innovation

Erhalten Sie mit Splunk vollständige Transparenz und durchleuchten Sie Ihre SAP Daten.

Für viele große Unternehmen ist SAP® das Rückgrat ihrer Geschäftsabläufe. Cenoti ermöglicht Ihnen, SAP mit Splunk zu verbinden, um kritische Sicherheitswarnungen und Erkenntnisse aus Ihrem SAP-System zu erhalten.

Sind Sie als Sicherheitsexperte Ihres Unternehmens über Risiken in SAP, Reaktionen auf Audit Informationen und einer fehlenden Transparenz der SAP-Umgebung besorgt?

Kam es bereits zu Datenschutzverletzungen in Ihrem SAP-System und ist es Ihnen schwergefallen, mit einer klaren Strategie auf zukünftige Verstöße zu reagieren?

Um zukünftige Sicherheitsprobleme proaktiv zu entschärfen, benötigen Sie einen einfacheren, standardisierten Weg, um tiefere Einblicke aus SAP zu erhalten?

Cenoti ist eine innovative Lösung die den Nutzen von Splunk maximiert und die Risiken, Ausfälle und Kosten minimiert, die mit SAP-Sicherheitsverletzungen verbunden sind.

Available on splunkbase™

SAP® Certified
Integration with SAP NetWeaver®

Im Gegensatz zu anderen hartkodierten Lösungen ist Cenoti eine Splunk- und SAP-zertifizierte Lösung, die sowohl Out-of-the-Box Datensammlungen als auch Visualisierungen bereitstellt. Sie basiert auf einem bewährten, erweiterbaren Konzept, das es Ihnen ermöglicht, mehr Daten aus SAP in Splunk zu integrieren, ohne dass Sie eigenen Code schreiben müssen.

Mit über 35 Jahren Erfahrung im SAP-Bereich verfügt EPI-USE Labs über ein tiefes Verständnis des semantischen Modells von SAP, was die Grundlage für unsere etablierte SAP Suite zur Landschaftsoptimierung, Data Sync Manager™, bildet. Cenoti basiert auf der gleichen Technologie und lässt sich nahtlos in Splunk Enterprise Security und dessen CIM integrieren.

CENOTI
CONNECT SAP® WITH SPLUNK®

EPI-USE LABS
value through innovation

Häufige Herausforderungen bei der Integration von SPLUNK mit SAP

- Splunk ist Ihre SIEM- (Security Information and Event Management) und Datenanalyse-Plattform, aber SAP ist eine Black Box, in der die Bedrohung für Ihr Unternehmen erheblich sein kann.
- Betrügerische Aktivitäten in SAP werden in Ihren SOC-Berichten (Service Organizational Control) hervorgehoben, aber Sie wissen nicht, was Sie dagegen tun sollen.
- Sie möchten den Zugriff auf sensible Daten nachverfolgen und in den Mechanismus von Splunk zur Erkennung von Anomalien aufnehmen.
- Sie möchten Service-Probleme vermeiden und Risiken für die Betriebszeit der Produktion minimieren. Dafür benötigen Sie eine klare, operative Sicht auf den gesamten Technologiebereich, nicht nur auf die Application Layers von SAP und Datenbank.
- Sie sind auf der Suche nach einer Analyse, um das Wachstum Ihres gesamten SAP Datenvolumens zu verfolgen.
- Sie möchten bestimmte sensible Daten innerhalb der Dashboards für Sicherheit und Betrieb überwachen.

Warum Cenoti?

Vollständig zertifizierte und aktuelle Lösung

- Die SAP-Layer wird über einen SAP-zertifizierten Transport installiert, und auch SAP S/4HANA wird von Cenoti unterstützt.
- Die Splunk Layer wird über eine zertifizierte SplunkBase App installiert, die Enterprise Security unterstützt.

Einblicke in den SAP-Datenschutz mit Splunk

- Zuverlässige Berichte über den Datenzugriff gehören zum Standard.
- Compliance-Standards wie PCI, HIPAA werden unterstützt.
- Die SAP-Daten werden mit Compliance-Metadaten versehen, wenn sie an Splunk weitergeleitet werden.
- Detaillierte SAP-Server- und Leistungskennzahlen gehören zum Standard.

Schnelle Systemeinführung

- Transport wird einfach und schnell durchgeführt.
- Die vollständige End-to-End-Installation und -Konfiguration dauert weniger als zehn Tage.
- Cenoti verwendet bestehende SAP-Konfigurationen; nur minimale kundenspezifische Anpassungen sind erforderlich.
- Die Lösung ist flexibel: alle SAP-Kollektoren sind konfigurierbar und erweiterbar, um Ihren Geschäftsanforderungen gerecht zu werden.

Cenoti Faktencheck

24+ SAP Datenweiterleitungen auf Basis unseres selbst entwickelten semantischen SAP-Modells

Warnungen integriert mit Splunk Enterprise Security Models

21+ Splunk Dashboards für erweiterte Überwachung und Berichterstattung

133+ flexible Möglichkeiten in Splunk, Ihr Dashboard individuell zu gestalten

34+ Splunk-Suchen mit Warnungen zu Sicherheit, Betrieb und Unternehmen

Aktuelle Funktionen

SAP Datenweiterleitungen

- ABAP Short-Dump-Analyse
- Jede Datenbank Tabelle
- Anwendungsprotokoll
- Benutzerberechtigungsprotokoll mit gepufferten Daten
- Benutzerberechtigungsprotokoll mit langzeitpersistenten Daten
- Management-System-Protokolle des Rechenzentrums
- Änderungsbelege
- Textbeschreibungen für SAP Codes
- Datenbank-Informationen
- GUI Informationen der Dialogbenutzer
- IDOC-Daten
- Protokolle von Hintergrundjobs
- Manager und Mitarbeiter
- Operating System Monitor
- Read access logging
- Sicherheits-Audit-Protokoll
- Selbstauskunft
- System-Statistiken
- Systemänderungsoptionen
- Systemprotokoll
- Tabellenprotokollierung
- Transport-Protokolle
- Benutzer Passwort Status
- Workload-Zusammenfassungen

Cenoti Sicherheit

Dashboards:

- Benutzer-Aktivitäts-Audit
- Operative Übersicht der Benutzer
- Alert Feed
- Report über Datenzugriffe
- Cenoti-Änderungsbericht
- Audit der Benutzeraktivität

Hauptmerkmale:

- Anomalie-Erkennung von sensiblen Datenzugriffen
- Anomalie-Erkennung von sensiblen Datenänderung
- Überprüfung der ausgeführten Jobs
- Überprüfung von SAP-Transaktionen und Zugriffe auf Reports
- Häufigste Zugriffe auf sensible Daten
- Häufigste Änderung sensibler Daten
- Separater Bericht über PII, PCI und HIPAA Zugriff/Änderung
- Bericht zur Systemanmeldung
- Bericht über fehlgeschlagene Systemanmeldungen
- SAP-Systemzugriffe mit bekannten Bedrohungsseiten korrelieren
- SAP-Systemzugriffe mit bekannten Bedrohungssignaturen korrelieren
- Verfolgung von Aktivitäten nach Funktionsteams, um sicherzustellen, dass sie mit dem Aufgabenprofil übereinstimmen
- Überprüfung der Aktivität von Konten mit hoher Berechtigung (SAP*, DDIC, FireFighter)
- Überprüfung von SAP-Benutzerstammänderungen, einschl. Rollen/Profile mit hohen Berechtigungen (SAP_ALL, SAP_NEW, X_REST)

Cenoti Betrieb

- Übersicht über die Umgebung
- Zustand der SAP-Instanz
- SAP Job Bericht
- SAP Tcodes Bericht
- Zustand des APP Servers
- Zustand des SAP Puffers
- Zustand des Load Balancing
- Zustand der SAP Mandanten
- SAP Error Viewer
- Zustand der SAP Datenbank
- Large Object Viewer
- Slow Statement Viewer

Selbst Überwachung

- Auswirkungen auf die Splunk-Lizenznutzung (Datengröße)

Erfahren Sie mehr unter **www.epiuselabs.com/de/cenoti-connect-sap-with-splunk** oder kontaktieren Sie uns unter **vertrieb@labs.epiuse.com**