CENOTI
CONNECT SAP® WITH SPLUNK®

EPI-USE LABS
value through innovation

Get complete Splunk visibility. Illuminate your SAP data.

For many large organizations, SAP® is the backbone of their operations. With Cenoti, you can connect SAP with Splunk and get critical security alerts and insights from your SAP system.

As an enterprise security professional, are you concerned about SAP risks, responding to audit information findings and a general lack of insight into your company's SAP environment?

Have you ever had data privacy breaches in your SAP system and struggled with a straightforward strategy to respond to future breaches?

To be proactive in mitigating future security issues, do you need a simpler, more standard way to get insights from SAP?

Cenoti is an innovative solution for maximizing the value of Splunk and for minimizing the risk, outages and cost associated with SAP security breaches.

Available on splunkbase™

SAP® Certified
Integration with SAP NetWeaver®

Unlike other hard-coded solutions, Cenoti is a Splunk- and SAP-certified solution with both out-of-the-box data collectors and visualizations. It's built on a proven, extensible framework, allowing you to get more data from SAP into Splunk easily, without having to write any custom code.

With over 35 years of experience in the SAP space, EPI-USE Labs has a deep understanding of SAP's advanced semantic model which powers our well-established SAP landscape optimization suite for large enterprises, Data Sync Manager™. The Cenoti framework is underpinned by the same technology, and integrates natively into Splunk Enterprise Security and its CIM."

CENOTI
CONNECT SAP® WITH SPLUNK®

EPI-USE LABS
value through innovation

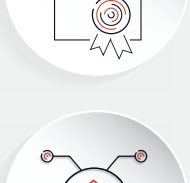
Common challenges of integrating SPLUNK with SAP

- Splunk is your SIEM (Security Information and Event Management) and data analytics platform, but SAP is a black box where enterprise threat may be significant
- Fraudulent activity in SAP is highlighted in your Service Organizational Control (SOC) reports, but you don't know how to address it
- You would like to have Sensitive Data Access (such as recipes) tracked and ingested to Splunk's enterprise-class anomaly detection engine
- You need clear operational visibility of the whole technology stack, not just the SAP & database applications layers, to prevent services issues and mitigate risks to production application uptime
- You are looking for data volume analytics for tracking SAP full-estate data volume growth
- You would like to monitor specific data privacy-related data within Security and Operations dashboards

Why CENOTI?

Benefit from a fully certified and up-to-date solution

- The SAP layer is installed via an SAP-certified Transport, and Cenoti also supports SAP S/4HANA
- The Splunk layer is installed via a certified SplunkBase App that supports Enterprise Security



Get SAP data privacy insights in Splunk

- Robust data access reporting comes as standard
- Compliance standards PCI, HIPAA are supported out of the box
- The SAP data is tagged with compliance metadata as it is being forwarded to Splunk
- Detailed SAP server and instance performance metrics come as standard

Enjoy rapid deployment

- Transport is applied easily and quickly
- Complete end-to-end installation and configuration takes less than ten days
- Cenoti uses existing SAP configuration; minimal client-specific configuration is required
- It's a flexible solution; all SAP collectors are configurable and extensible to suit your business needs

Cenoti quick facts

24+ SAP Data Forwarders powered by our proprietary SAP semantic model

Alerts integrated with Splunk Enterprise Security Models

21+ Splunk Dashboards for enhanced monitoring and reporting

133+ Flexible Splunk Tiles to customize your dashboard

34+ Splunk Searches with Alerts for Security, Operations and Business

CENOTI
CONNECT SAP® WITH SPLUNK®

EPI-USE LABS
value through innovation

Current functionality

SAP Data Forwarders

- ABAP Short-Dump Analysis
- Any database table
- Application log
- User authorization log with buffered data
- User authorization log with long-term persistent data
- Computing Center Management System logs
- Change documents
- Text descriptions for SAP codes
- Database information
- Dialog users' GUI information
- IDOC data
- Background job logs
- Managers and employees
- Operating System Monitor
- Read access logging
- Security audit log
- Self reporting
- System statistics
- System change options
- System log
- Table logging
- Transport logs
- User password status
- Workload summaries

Cenoti Security

Dashboards:

- User Activity Audit
- User Operational Overview
- Alert Feed
- Data Access Report
- Cenoti Change Report
- User Activity Audit
- User Operational Overview
- Alert Feed
- Data Access Report
- Cenoti Change Report

Key features:

- Anomaly Detection of Sensitive Data Access
- Anomaly Detection of Sensitive Data Change
- Review of Jobs Run
- Review of SAP Transactions and Reports Accessed
- Most frequently accessing sensitive data
- Most frequently changing sensitive data
- Report on PII, PCI and HIPAA access/change separately
- System login report
- System failed login report
- Correlate SAP system access with known threat sites
- Correlate SAP system access with known threat signatures
- Track activity by functional team to insure it aligns with job profile
- Review activity of high permission accounts (SAP*, DDIC, FireFighter)
- Review of SAP User Master changes involving high permission Roles/Profiles (SAP_ALL, SAP_NEW, X_REST)

Cenoti Operations

- Environment Overview
- SAP Instance Health
- SAP Jobs Report
- SAP Tcodes Report
- App Server Health
- SAP Buffer Health
- Load Balancing Health
- SAP Client Health
- SAP Error Viewer
- SAP Database Health
- Large Object Viewer
- Slow Statement Viewer

Self Monitoring

- Impact on Splunk license usage (data size)

Learn more at:
www.epiuselabs.com/cenoti-connect-sap-with-splunk

A MEMBER OF groupelephant.com™ BEYOND CORPORATE PURPOSE