Safeguard Your SAP Environment With Splunk

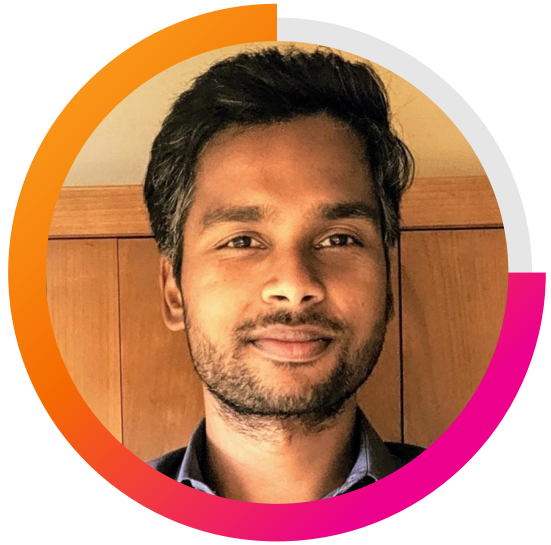
SAP® Endorsed App
Premium Certified

splunk> | SAP®

SAP and Splunk Experts

Dr. Michael Schmitt

SAP ETD Product Manager
SAP



Anush Jayaraman

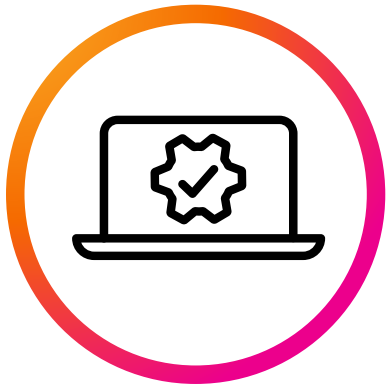
Partner Solutions Engineering Manager
Splunk

splunk>

Securing SAP is not Easy…

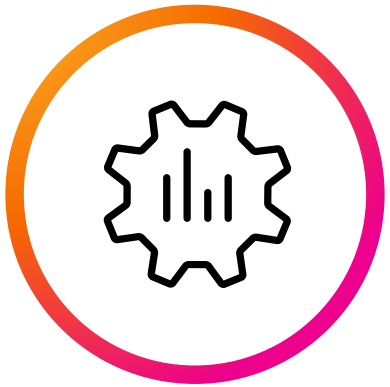
SAP is a “black box” and often left outside of traditional security solutions

Increasingly Complex Systems



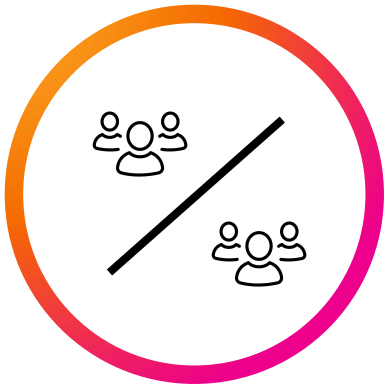
SAP applications write in several different SAP proprietary log files

Lacking Application Level visibility



Application level visibility and correlation with other security data sources isn’t readily available

Separately Managed



Application and Infrastructure security are often separated and stuck in silos

splunk>

Splunk and SAP: A Strategic Partnership

Splunk and SAP are committed to empowering the intelligent enterprise by developing new integrations and joint solutions that enable customers to adapt and respond to change in real time.

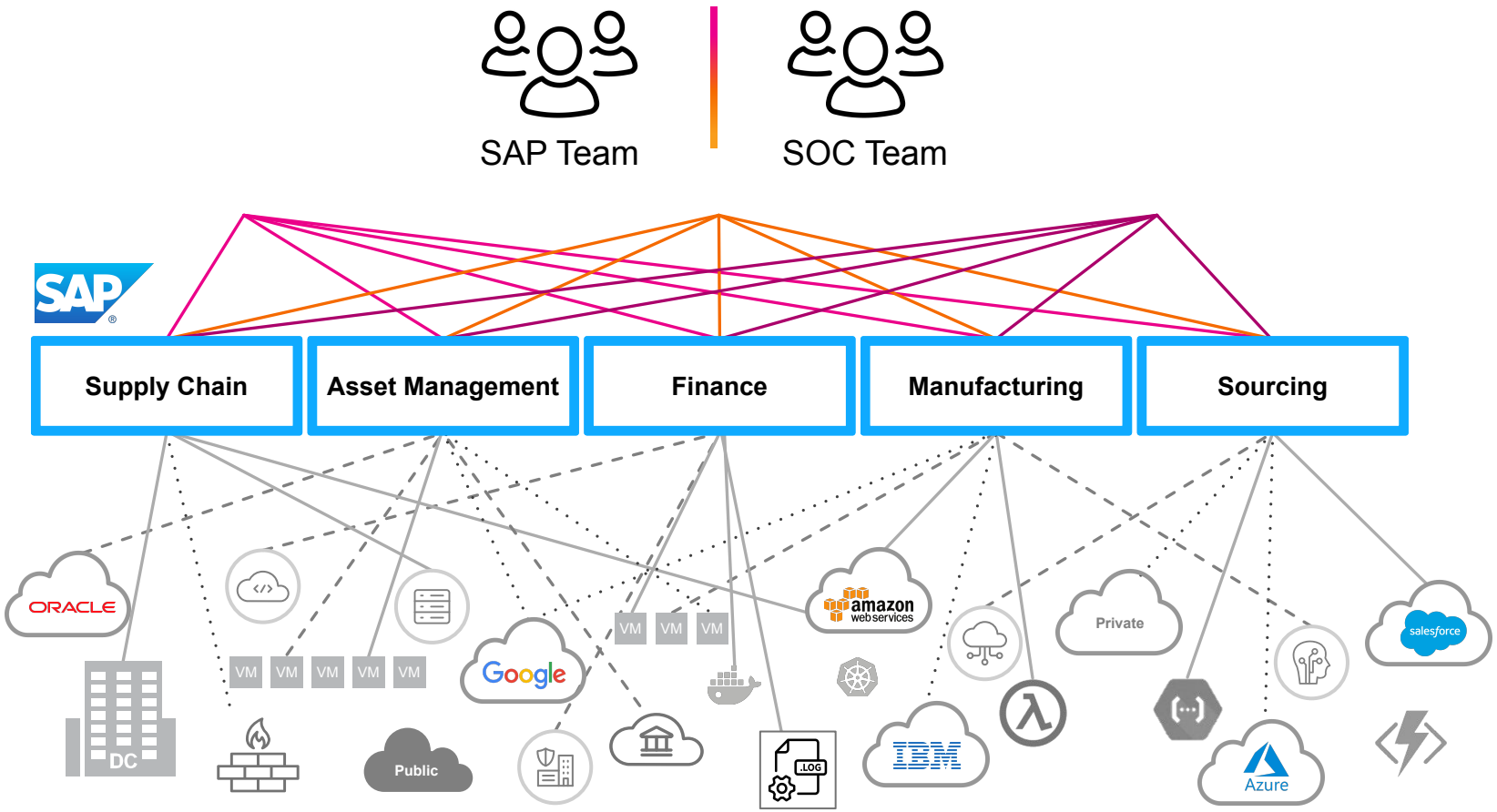
2019
formalized partnership

3,400+
joint enterprise customers

Solution endorsement and commitment to providing value to joint customers

Barriers to SAP® Security & Risk Reduction

1. **Data silos**
2. **Lack of application visibility & correlation**
3. **Lack of security analytics & context**

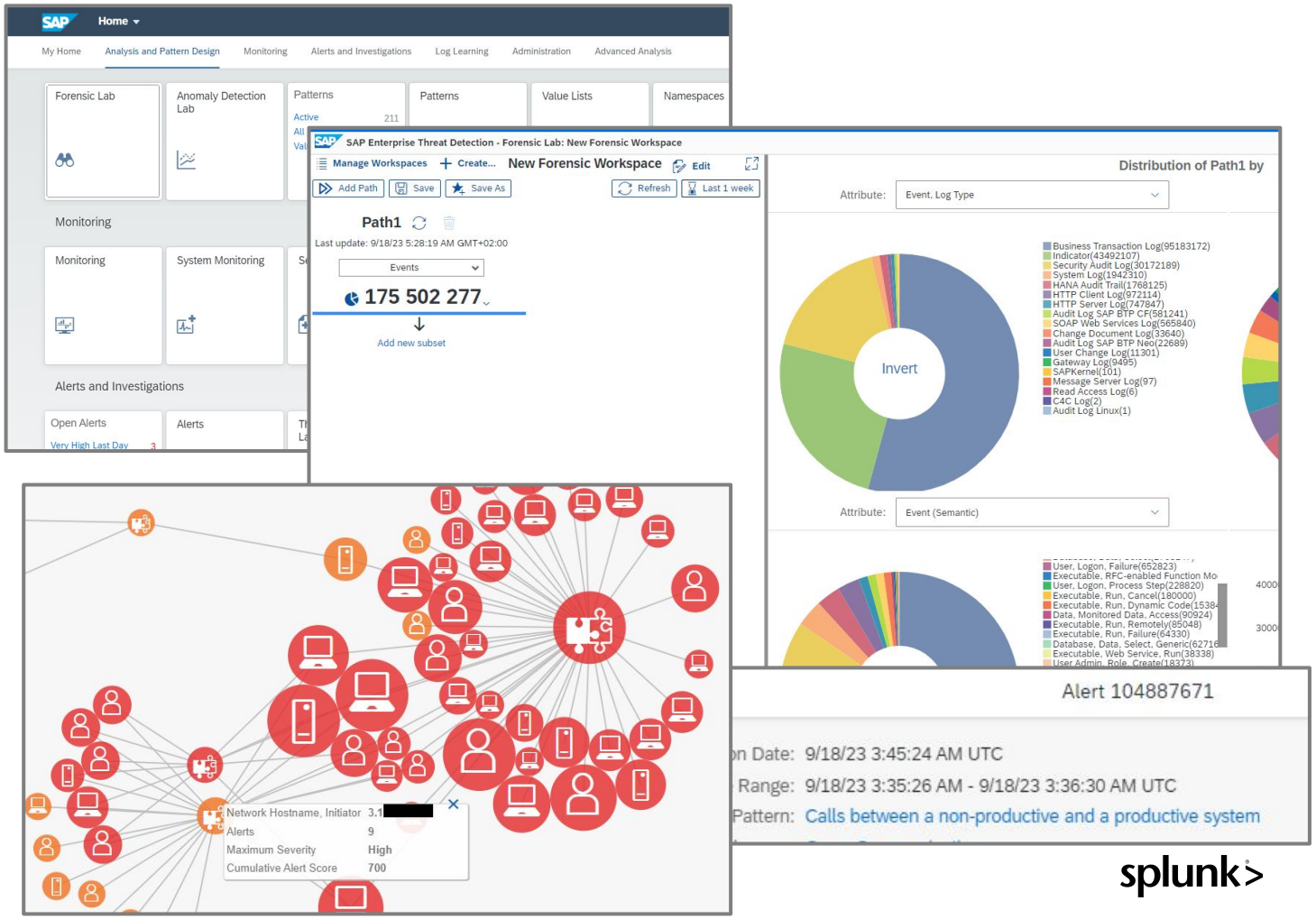


splunk>

SAP Enterprise Threat Detection Overview

Specialized for SAP In-Application Security Monitoring

- Real-time security monitoring and alerting if suspicious activities happen within an SAP system or landscape
- Integrates with hybrid SAP landscapes: (S4/H, S4/H-Cloud, ECC, SAP Java Server, HANA DB, Business Technology Platform, C4C, others on the roadmap 2024/25)
- Provides Use-cases out of the box



splunk>

Introducing Splunk® Security for SAP® Solutions

SAP® Endorsed App
Premium Certified

splunk>

Splunk Security for SAP Solutions

What It Is

- Reduce business risk by carefully monitoring, more accurately detecting and rapidly responding to threats impacting your SAP environments
- Expand attack-surface coverage by including your SAP estate into Splunk security analytics and operations workflows
- Splunk natively integrates with SAP Enterprise Threat Detection

Available on SAP Store

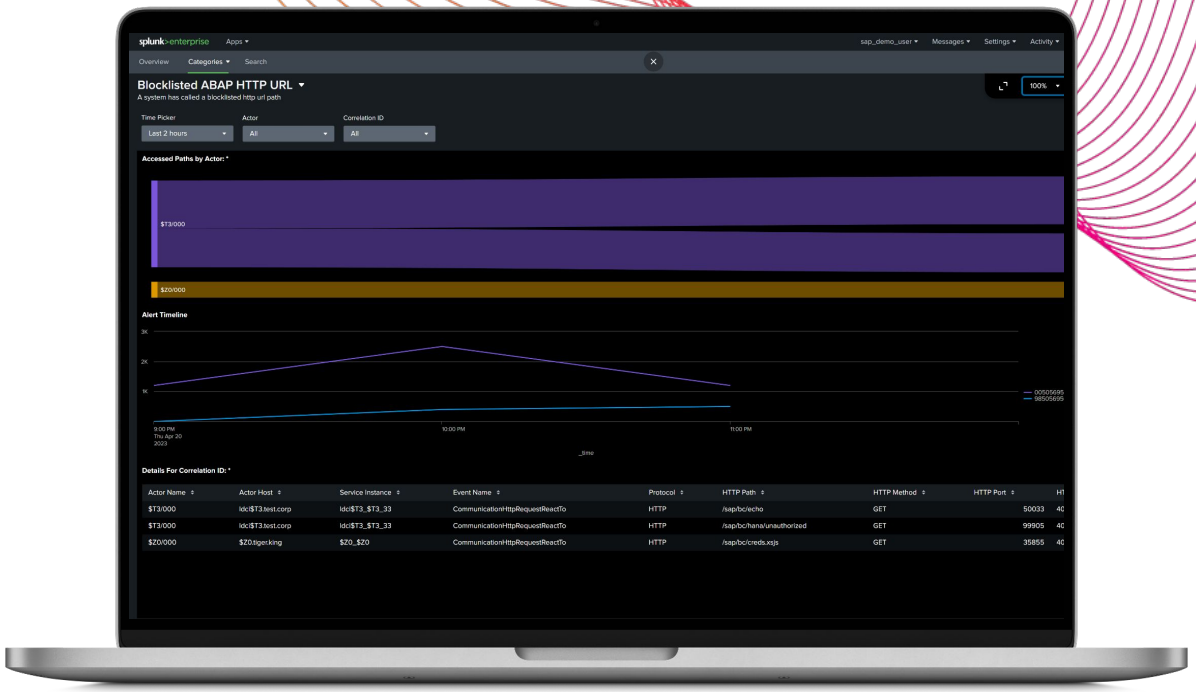
SAP® Endorsed App
Premium Certified

Splunk Security for SAP Solutions

Value It Provides

Delivers immediate value for security and SAP teams by providing:

- Increased security visibility into SAP applications and data
- Correlation and analysis of SAP events and alerts with other security-relevant data in Splunk
- Pre-built, SAP-specific security dashboards, KPIs and correlation searches
- Risk-based alerting consolidating and prioritizing threats by business risk
- Additional capabilities to streamline investigations and threat hunting



Available on SAP Store

SAP® Endorsed App
Premium Certified

Splunk Security for SAP® Solutions

Common Use Cases

Compromised Credentials/ Accounts

Ex. unusual use of credentials to move laterally throughout the SAP systems

Insider Threats

Ex. suspicious use of access to change configs or exfiltrate data

Data Loss Prevention

Ex. Protect sensitive data from internal as well as external threats

Compliance & Auditing

Ex. Report on change requests & user activity

Risk Assessment

Ex. System vulnerability & attack surface assessment

splunk>

Solutions Overview

SAP Enterprise Threat Detection

- Collect security-related information from your system landscape
- Normalize original data to the semantic data model of SAP ETD
- Enrich the log data with context information
- Pseudonymize the user data

DATA SOURCES (Log Providers)

- SAP Netweaver
- SAP HANA
- SAP BTP
- SAP Commerce
- SAP Commerce
- SAP Sales & Service Cloud
- SAP S/4HANA Cloud
- Third Party Systems

LOG TYPES

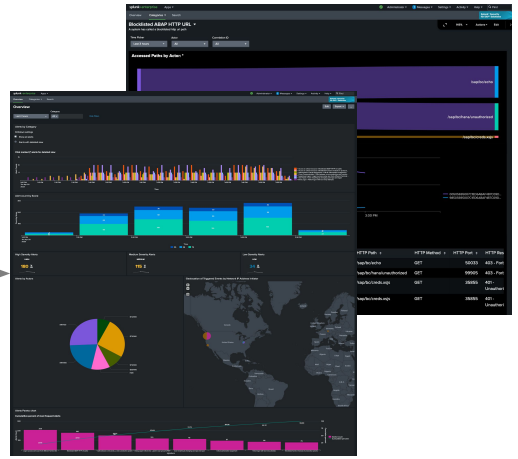
- Security Audit Logs
- System Logs
- Business Transaction Logs
- HTTP Server Logs
- RFC Gateway Logs
- User Change Logs
- Change Document Logs
- SOAP Based Web Services Logs
- Read Access Logs / UI Logs
- HTTP Access Logs (Java)
- Security Audit Logs (Java)
- Security Log (Java)
- HANA Audit Trail
- SAP Cloud Platform Audit Logs

SAP S/4 HANA · SAP NetWeaver · SAP ERP

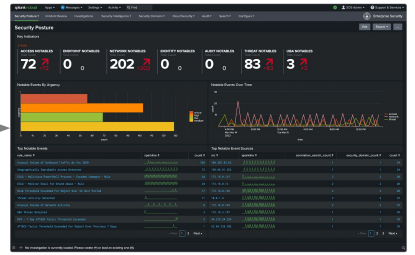
splunk>

Additional Security Data Sources

Splunk Security for SAP Solutions

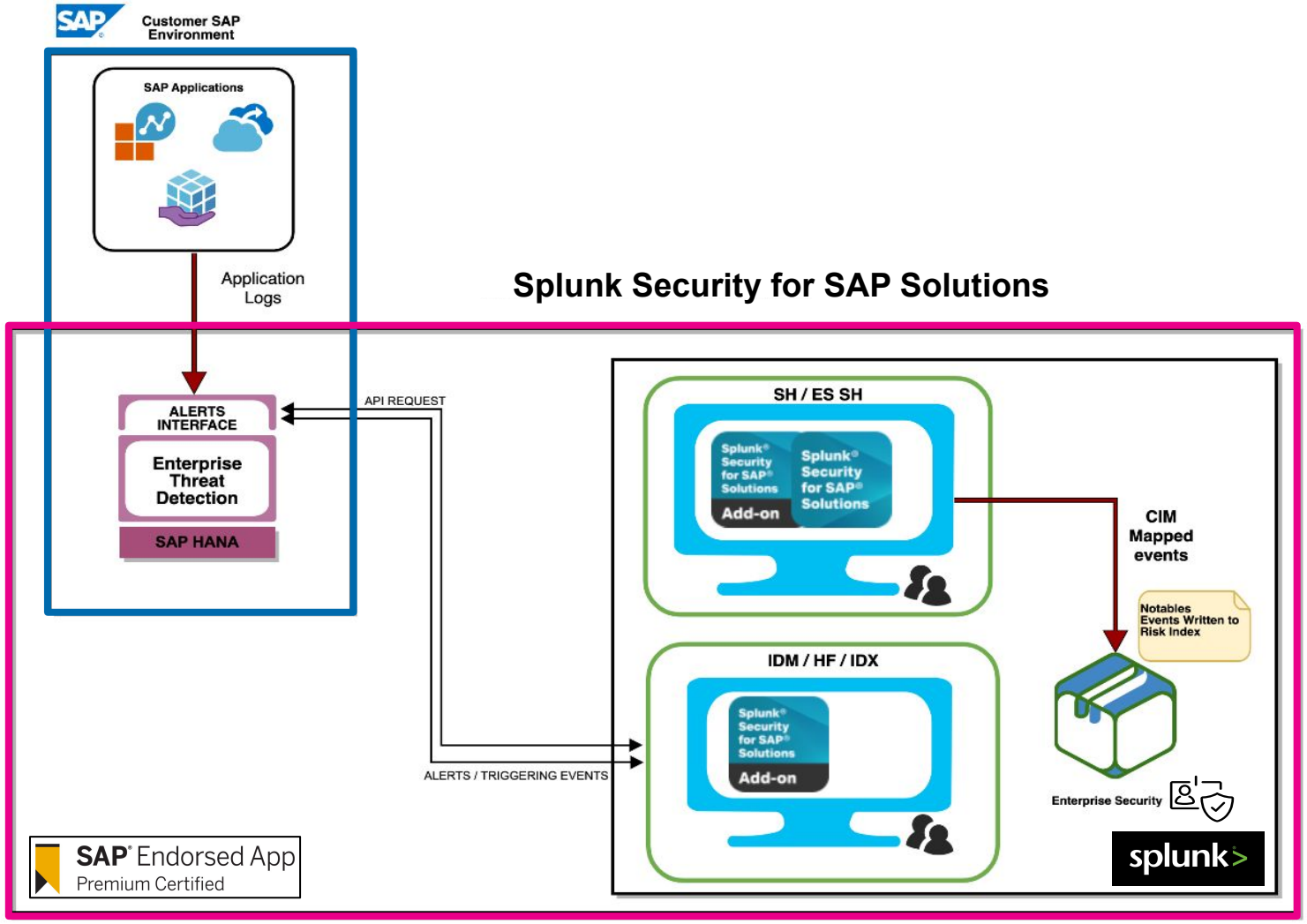


Splunk Enterprise Security



splunk>

System Architecture



Solution Demo

Overview

Category

Last 4 hours

All

Alerts by Category

Drilldown settings

Show all alerts

Alerts with detailed view

Click marked (*) alerts for detailed view

Alert count by Score

High Severity Alerts

HIGH

57

Medium Severity Alerts

MEDIUM

55

Low Severity Alerts

LOW

44

Alerts by Actors

Geolocation of Triggered Events by Network IP Address Initator

Recap

Proactive in Threat Analysis

Complimented with the goodness of Enterprise Security

Reduced MTTD and MTTR

Reduced mean time to detect and respond to threats with our out of the box risk analysis built into Enterprise Security

Enriched alerts with ETD's foundational data

Combined with 800+ security relevant use cases and content from Splunk, Splunk enhances the data

Key Takeaways

Secure the “Black Box”

Splunk’s industry leading data analytics & security platform now extends to the SAP application.

Bring application and infrastructure security data & telemetry together

Use Splunk to see and act on SAP detections, correlated with other security telemetry and conduct deep, end to end investigations

Secure SAP with Splunk today!

Contact your Splunk Account Manager. Learn how to modernize SAP security monitoring and protection

splunk>

Thank You!

splunk>