EOS IT SOLUTIONS

splunk> a CISCO company

Proof of Practice
Splunk Security Stack

Splunk Partnerverse — Premier Level Security Badge

30+	200+	10+	8+
Security Engineers	Splunk Certifications	Years of Practice	Competitor Evaluations

CONFIDENTIAL

Prepared for: Splunk / Cisco Partner Program
Prepared by: EOS IT Solutions
Date: March 2026
Document Version: 1.0

1. Executive Summary

EOS IT Solutions is a premier Splunk professional services partner with over a decade of dedicated practice delivering security solutions built on the Splunk platform. This document serves as our formal Proof of Practice submission for the Splunk Partnerverse Premier Level Security Badge, demonstrating our deep expertise, extensive certifications portfolio, and proven track record of customer success across the full Splunk security stack.

Our security practice is anchored by a team of more than 30 Splunk Certified Core consultants who collectively hold over 200 Splunk certifications spanning every certification track Splunk offers. Our engineers have delivered hundreds of engagements across industries including financial services, healthcare, federal government, defense, energy, and retail. From initial SOC deployments to fully operational SIEM/SOAR environments, our team has the depth of experience to handle the most complex security implementations.

In addition to deployment and optimization expertise, EOS IT Solutions has conducted rigorous competitive evaluations between Splunk and every major SIEM/SOAR competitor in the market, providing our customers with the data-driven confidence to select and commit to the Splunk security platform.

2. Organization Overview

EOS IT Solutions is a global technology services provider that helps organizations automate and accelerate their digital transformation goals. With a strong cloud-first philosophy and deep technical bench, EOS IT Solutions has established itself as a trusted partner for enterprises seeking to modernize their security operations.

Splunk Practice at a Glance

Practice Established	2015 (10+ years of continuous Splunk delivery)
Dedicated Security Engineers	30+ full-time Splunk security professionals
Total Splunk Certifications	200+ across all certification tracks
Security-Specific Certifications	32+ (ES Admin, SOAR Developer, Cybersecurity Defense Analyst)

Industries Served	Financial Services, Healthcare, Federal/Defense, Energy, Retail, Technology
Splunk Products Practiced	Enterprise Security, SOAR, UEBA, Risk Based Alerting, Attack Analyzer, Asset & Risk Intelligence, Intelligence Management

3. Splunk Security Stack Expertise

EOS IT Solutions maintains deep, hands-on expertise across every component of the Splunk security portfolio. Our engineers are not only certified but actively delivering implementations, optimizations, and managed services across the entire stack.

3.1 Splunk Enterprise Security (ES)

Splunk Enterprise Security version 8.X the cornerstone of our security practice. Our team has deployed ES in environments ranging from mid-market organizations to Fortune 100 enterprises and federal agencies. Our capabilities include initial deployment and architecture design, configuration of correlation searches and notable events, Risk-Based Alerting (RBA) implementation and tuning, threat intelligence framework integration, custom dashboard and investigation workflow development, ES performance optimization for high-volume environments, and migration from legacy SIEM platforms to Splunk ES.

3.2 Splunk SOAR (Security Orchestration, Automation and Response)

Our SOAR practice has delivered automation that fundamentally transforms how security operations centers operate. With experience across 50+ third-party integrations and hundreds of automated actions, our team designs and builds playbooks that dramatically reduce response times and analyst fatigue. Key capabilities include custom playbook development and lifecycle management, integration architecture design across security tool ecosystems, automated phishing triage, malware containment, and vulnerability management, case management workflow optimization, and custom app development for proprietary tool integration.

3.3 Splunk User Behavior Analytics (UEBA)

Our UEBA expertise enables customers to detect insider threats, compromised accounts, and advanced zero-day attacks through behavioral modeling and machine learning. Our team has deployed UEBA across critical infrastructure environments, including

OT/ICS networks, building custom anomaly detection models tailored to each customer's unique threat landscape.

3.4 Splunk Attack Analyzer

EOS IT Solutions leverages Splunk Attack Analyzer to provide customers with automated analysis of complex credential phishing and malware threats. Our engineers integrate Attack Analyzer with SOAR workflows to create end-to-end threat analysis and response chains that operate at machine speed.

3.5 Splunk Asset and Risk Intelligence

Our team implements Splunk Asset and Risk Intelligence to provide customers with continuous asset discovery, compliance monitoring, and proactive risk mitigation. This ensures complete visibility across the attack surface and enables risk-informed security decision-making.

3.6 Intelligence Management

EOS IT Solutions integrates Splunk Intelligence Management (formerly TruSTAR) to accelerate investigations with enriched threat intelligence. Our implementations leverage Cisco Talos intelligence alongside premium threat feeds to enable proactive threat hunting and real-time indicator matching across enterprise environments.

4. Certifications Portfolio

EOS IT Solutions holds certifications across every track in the Splunk certification program. Below we highlight our security-specific certifications, followed by our broader certifications portfolio that supports our security delivery capability.

4.1 Security-Specific Certifications

Certification	Engineers	Competency Areas
Splunk Enterprise Security Certified Admin	14	Administration, configuration, and management of Splunk Enterprise Security deployments
Splunk SOAR Certified Automation Developer	8	Installation, configuration, and playbook development for Splunk SOAR (formerly Phantom)
UEBA Certification	3	Installation and configuration or UEBA
Splunk Certified Cybersecurity Defense Analyst	31	Threat detection, analysis, and response using Splunk Enterprise and Enterprise Security
Total Security Certifications	**56+**	Comprehensive security stack coverage

4.2 Supporting Core & Specialty Certifications

Certification	Engineers	Relevance to Security Practice
Splunk Core Certified User	30	Foundational knowledge of Splunk search, reporting, and dashboards
Splunk Core Certified Power User	30	Advanced searching, reporting, data models, and field extraction
Splunk Core Certified Advanced Power User	30	Expert-level data analysis, optimization, and complex search techniques
Splunk Enterprise Certified Admin	30	Enterprise deployment, configuration, management, and troubleshooting

Splunk Enterprise Certified Architect	30	Large-scale architecture design, clustering, and performance optimization
Splunk Cloud Certified Admin	30	Cloud platform administration and management
Splunk IT Service Intelligence Certified Admin	4	ITSI deployment and service monitoring configuration
Total Core & Specialty Certifications	**184+**	Full platform expertise supporting security delivery

Combined with our 31 security-specific certifications, EOS IT Solutions holds a total of over 200 Splunk certifications, representing one of the most comprehensively certified Splunk security practices in the partner ecosystem.

5. Representative Security Engagements

The following representative engagements demonstrate the breadth and depth of our Splunk security practice. Each engagement showcases our ability to deliver enterprise-grade security solutions across diverse industries and use cases.

SOC Buildout & Optimization

Industry: Fortune 500 Financial Services

Designed and deployed a greenfield Security Operations Center leveraging Splunk Enterprise Security as the core SIEM platform, integrated with SOAR for automated incident response workflows. Reduced mean time to detect (MTTD) from hours to minutes.

SIEM Migration & Consolidation

Industry: Federal Government Agency

Led migration from legacy SIEM to Splunk Enterprise Security, consolidating multiple security tools into a unified platform. Implemented custom correlation searches and risk-based alerting (RBA) across 10,000+ customer correlation searches.

SOAR Playbook Development

Industry: Healthcare Network (Multi-Hospital)

Developed and deployed 60+ automated playbooks in Splunk SOAR to handle phishing triage, malware containment, and vulnerability management workflows, reducing analyst workload by 70%.

Competitive Replacement Program

Industry: Global Retail Enterprise

Conducted a comprehensive technical evaluation of Splunk vs. competing SIEM/SOAR platforms and led the full migration to Splunk security stack, including ES, SOAR, and UEBA integration.

Threat Intelligence Integration

Industry: Defense & Intelligence Sector

Integrated Splunk Intelligence Management with premium threat feeds and Cisco Talos intelligence, enabling proactive threat hunting and real-time indicator matching across classified and unclassified environments.

Enterprise UEBA Deployment

Industry: Energy & Utilities Provider

Deployed Splunk User Behavior Analytics to detect insider threats and compromised credentials across critical infrastructure environments. Built custom machine learning models for anomaly detection specific to OT/ICS networks.

6. Competitive Analysis Capability

A distinguishing strength of the EOS IT Solutions Splunk practice is our extensive experience conducting rigorous, data-driven competitive evaluations between Splunk and every major SIEM/SOAR platform on the market. These evaluations enable our customers to make informed platform decisions based on objective technical assessment, total cost of ownership, and alignment with their specific security requirements.

Our competitive analysis methodology encompasses feature parity evaluation across detection, investigation, and response capabilities; performance benchmarking including ingestion rates, search speed, and scalability; total cost of ownership modeling across licensing, infrastructure, and personnel; integration ecosystem assessment; and operational workflow comparison.

Platforms Evaluated Against Splunk

Competitor Platform	Evaluation Focus Areas
Microsoft Sentinel	Cloud-native SIEM and SOAR integration, cost modeling, KQL vs SPL comparison, hybrid deployment architecture
IBM QRadar	On-premises SIEM migration, offense management comparison, data normalization, log source integration
Google Chronicle / SecOps	Cloud-scale SIEM, YARA-L detection rules comparison, data lake architecture, cost-per-GB analysis
CrowdStrike Falcon LogScale	High-volume log management, real-time search performance, endpoint telemetry integration
Elastic Security	Open-source SIEM comparison, detection rules framework, Elasticsearch performance vs Splunk indexing
Palo Alto Cortex XSIAM	Autonomous SOC capabilities, XDR integration, automated investigation and response comparison
Exabeam	UEBA capabilities comparison, behavioral analytics models, TDIR workflow efficiency
Securonix	Cloud-native SIEM, UEBA feature parity, threat model comparison, multi-tenancy architecture

In every competitive evaluation conducted, our team has provided customers with comprehensive, vendor-neutral findings that ultimately demonstrated the strength of the Splunk security platform. This unique capability ensures that EOS IT Solutions customers deploy Splunk with complete confidence in their platform selection.

7. Service Delivery Model

EOS IT Solutions delivers Splunk security services through a structured engagement model designed to ensure consistent quality and measurable outcomes at every stage of the customer lifecycle.

Assessment & Discovery

Every engagement begins with a security workshops of the customer's current security posture, existing tooling, data sources, and operational requirements. Our engineers conduct gap analyses against industry frameworks such as MITRE ATT&CK and NIST CSF to identify priorities and build a tailored implementation.

Architecture & Design

Our certified Splunk architects design scalable, resilient security architectures that align with each customer's performance requirements, data volume projections, and compliance mandates. Designs account for hybrid and multi-cloud environments, high availability, and disaster recovery.

Implementation & Deployment

Our implementation teams follow proven deployment methodologies that minimize disruption while maximizing time to value. From initial data onboarding through correlation search tuning and SOAR playbook deployment, our engineers deliver fully operational security environments on schedule and within scope.

Optimization & Enablement

Post-deployment, EOS IT Solutions provides ongoing optimization services to ensure customers realize the full potential of their Splunk security investment. This includes detection content development, alert tuning to reduce false positives, performance optimization, and comprehensive knowledge transfer to empower customer security teams.

8. Conclusion

EOS IT Solutions has built one of the most experienced, deeply certified, and broadly capable Splunk security practices in the partner ecosystem. With over a decade of dedicated Splunk professional services delivery, a team of 30+ engineers holding 200+ certifications, and a proven track record spanning every component of the Splunk

security stack, we have consistently demonstrated our ability to help customers achieve the most modern and effective security operations possible.

Our unique combination of deployment expertise, competitive analysis capability, and deep product knowledge across Enterprise Security, SOAR, UEBA, Attack Analyzer, Asset & Risk Intelligence, and Intelligence Management positions EOS IT Solutions as a partner that can deliver the full spectrum of Splunk security outcomes. We respectfully submit this Proof of Practice in support of our application for the Splunk Partnerverse Premier Level Security Badge.

EOS IT Solutions

eosits.com

Empowering Digital Transformation Through Security Excellence