WHITEPAPER

Back to Back Winner 🏆 2023 & 2024

splunk> AMER Professional Services PARTNER OF THE YEAR

Maximizing Splunk Value:

Solving SIEM Challenges with an Eight-Level Treatment Model

INTRODUCTION

Splunk is a powerful platform that helps organizations gain real-time visibility, enhance security, and drive operational efficiency. However, many companies struggle to extract full value from their Splunk investment due to misconfigurations, poor data management, and inefficient searches and detections.

Our approach follows a progressive "treatment" model—starting from foundational best practices and moving toward advanced analytics and smart detections.

In this article, we'll walk through eight levels of improvement, each tackling a specific pain point, demonstrating the technical and business impact, and showcasing how informed operations transform Splunk into a strategic asset.

Many companies struggle to extract full value from their Splunk investment due to misconfigurations, poor data management, and inefficient searches and detections.

Level 1:

Splunk Best Practices – Building a Strong Foundation

A well-configured Splunk environment is essential for reliability, performance, and scalability. Without following best practices, organizations face frequent crashes, slow searches, and inefficient user management.

CHALLENGE

A global retail company experienced frequent Splunk crashes and slow performance due to misconfigurations in indexing, storage, and user permissions.

CONFIGURATION ISSUES

- **Indexer clustering misconfigured** ▶ led to uneven data distribution
- **Incorrect storage settings** ▶ hot/warm buckets filling up too fast
- **Lack of role-based access control (RBAC)** ▶ unauthorized users modifying pipelines

TECHNICAL IMPACT

- **40% slower searches** due to inefficient bucket management
- **Unplanned outages** due to storage filling up rapidly

BUSINESS IMPACT

- **Delayed sales reports,** impacting real-time decision-making
- **Increased support costs** due to ongoing troubleshooting

SOLUTIONS

✓ **Optimized indexer clustering** to balance data distribution
✓ **Updated storage configurations** to manage hot/warm/cold bucket rollover properly
✓ **Implemented RBAC** to prevent unauthorized changes

☒ **Before:** Splunk crashed weekly, searches were 40% slower, and business reports were often delayed.

✓ **After:** 99.9% uptime, 40% faster searches, and seamless data processing for business teams.

Level 2:

Data Ingestion – Ensuring Smooth and Efficient Data Flow

Efficient data ingestion is crucial for performance and cost control. Poorly configured ingestion leads to high license costs, indexing bottlenecks, and data delays.

CHALLENGE

A financial institution was ingesting multi TB/day, exceeding license limits, and experiencing an unacceptable delay in log availability.

CONFIGURATION ISSUES

- **Too many redundant logs** ▶ (e.g., DEBUG logs included in production)
- **Forwarders were not load-balanced** ▶ causing ingestion bottlenecks
- **No event filtering** ▶ leading to excessive ingestion of irrelevant data

TECHNICAL IMPACT

- **Indexers overloaded,** causing latency in log availability
- **License breaches** led to daily warnings and additional costs

BUSINESS IMPACT

- **Security teams delayed in investigating fraud incidents** due to missing logs
- **High operational costs** from unnecessary ingestion

SOLUTIONS

✓ **Filtered unnecessary logs** (disabled DEBUG logs in production)

✓ **Implemented load balancing** across multiple forwarders

✓ **Used props & transforms.conf** to discard unneeded data at the ingestion level

✗ **Before:** License overages, huge log delays, and bloated storage.

✓ **After:** Noticeable reduction in ingestion, logs available for search in minutes, and great annual savings in licensing costs.

Level 3:

Data Quality – Cleaning the Noise for Actionable Insights

Data quality issues result in incorrect dashboards, false alerts, and compliance risks. Fixing timestamps, field extractions, and event formatting ensures reliable analytics and reporting.

CHALLENGE

A healthcare organization faced incorrect timestamps and missing fields, causing compliance issues.

CONFIGURATION ISSUES

- **Improper timestamp extraction** ▶ (wrong regex in props.conf)
- **Non-standard field extractions** ▶ making correlation difficult
- **Events missing key metadata** ▶ affecting reporting accuracy

TECHNICAL IMPACT

- **Inconsistent timestamps** resulted in incorrect event ordering
- **Analysts struggled to correlate logs** due to missing fields

BUSINESS IMPACT

- **HIPAA compliance risks** due to incorrect logging
- **Financial penalties** for inaccurate audit logs

SOLUTIONS

✓ **Enforced CIM (Common Information Model)** to standardize logs
✓ **Fixed timestamp extraction** in props.conf using proper regex
✓ **Implemented event normalization** to correct missing fields

☒ **Before:** Many reports were presenting inaccurate insights, leading to regulatory risks.

✓ **After:** Optimal report accuracy, full compliance with audits, and zero fines.

Level 4:

Search Performance – Speeding Up Investigations and Dashboards

Slow searches increase investigation time and reduce productivity. Optimizing searches ensures faster incident detection, better user experience, and improved system efficiency.

CHALLENGE

A cybersecurity team took 15+ minutes to retrieve logs due to inefficient SPL queries.

CONFIGURATION ISSUES

- **Using index=** ▶ * in searches, making them slow
- **No summary indexing** ▶ causing every query to scan raw data
- **Excessive join and transaction commands** ▶ slowing results

TECHNICAL IMPACT

- **High CPU usage** on search heads
- **Searches took 15+ minutes,** delaying response time

BUSINESS IMPACT

- **Delayed breach investigation,** increasing risk of security incidents
- **Analysts wasted time** on inefficient searches

SOLUTIONS

✓ **Used tstats-based searches** for faster retrieval

✓ **Implemented summary indexing** to pre-aggregate data

✓ **Optimized SPL queries** by removing redundant joins

✗ **Before:** Incident investigations took 15+ minutes, delaying response.

✓ **After:** Queries completed in under 30 seconds, leading to real-time threat detection.

Level 5:

Splunk Premium Apps – Enhancing Value with the Right Integrations

Many organizations struggle to enrich their security detections due to a lack of premium apps integration and enrichment like threat intelligence feeds and asset/identity context. Without these integrations, SOC teams operate blindly, leading to false positives, missed threats, and inefficient investigations.

CHALLENGE

A financial services company was experiencing high false positive rates and slow incident triage because Splunk lacked context on assets, identities, and external threats.

CONFIGURATION ISSUES

- **No external threat intelligence (TI) feeds integrated** ▶ into Splunk Enterprise Security (ES)
- **Assets and identities (A&I)** ▶ were missing from correlation searches
- **Detection rules were static** ▶ and lacked contextual enrichment

TECHNICAL IMPACT

- **40% increase in false positives,** overwhelming analysts
- **SOC wasted hours** investigating irrelevant alerts
- **No visibility into high-risk assets** and compromised user accounts

BUSINESS IMPACT

- **Delayed threat response,** exposing the organization to potential breaches
- **Increased SOC workload,** leading to analyst fatigue
- **Regulatory compliance risks** due to incomplete incident documentation

SOLUTIONS

✓ **Integrated external threat intelligence feeds** (e.g., MISP, VirusTotal, Recorded Future) to enrich alerts with real-time threat data

✓ **Onboarded asset and identity data into Splunk ES** to correlate threats to specific users and devices

✓ **Updated detection rules to prioritize high-value assets** and reduce false positives

☒ **Before:** SOC analysts drowned in alerts, struggling to differentiate between real threats and noise.

✓ **After:** Great reduction in false positives, faster investigations, and clearer insight into high-risk users and assets.

Level 6:

Custom Dashboards – Improving Visualization and Decision-Making

Dashboards should provide fast, insightful, and actionable data. Poorly optimized dashboards lead to slow performance, frustrated users, and inefficient decision-making.

CHALLENGE

A manufacturing company's executives struggled with slow, cluttered dashboards.

CONFIGURATION ISSUES

- **Dashboards** ▶ were running expensive real-time searches
- **No base searches** ▶ causing redundant queries

TECHNICAL IMPACT

- **Slow-loading dashboards** lead to frustrating users

BUSINESS IMPACT

- **Executives couldn't make quick decisions** based on real-time data

SOLUTIONS

✓ **Implemented base searches** for optimized performance

✓ **Created executive-friendly dashboards** with key KPIs

☒ **Before:** Slow, complex dashboards with poor visibility.

✓ **After:** Dashboards loaded way faster, enabling data-driven decisions.

Level 7:

OTB Detections – Leveraging Splunk's Security Content

Many organizations fail to use Splunk's built-in detection rules, leading to missed threats and slow incident response times. Enabling the right out-of-the-box (OTB) detections can significantly improve security posture.

CHALLENGE

A government agency enabled too many irrelevant built-in use cases from Security Content (ESCU) for threat detection.

CONFIGURATION ISSUES

- **Enabling irrelevant detections** ▶ lead to many false positive alerts
- **Higher priority detections disabled** ▶ lead to missing critical threats

TECHNICAL IMPACT

- **Detecting and responding to the real threats**

SOLUTIONS

✓ **Conducting Security Usecase Workshop** to provide the ideal security posture roadmap

✓ **Enabled prebuilt detections and mapped them** to MITRE ATT&CK for the relevant industry and data sources

☒ **Before:** Detection delay, missed threats.

✓ **After:** Real-time detection, reducing MTTD and MTTR.

Level 8:

Advanced Correlated Detections – The Path to Smart Security Operations

Basic detections identify isolated threats, but correlated detections can reveal complex attack patterns that would otherwise go unnoticed.

CHALLENGE

A bank's SOC team struggled with fraudulent account takeovers but couldn't correlate login patterns, unusual transactions, and new device registrations across different logs.

CONFIGURATION ISSUES

- **Single-rule detections** ▶ missing the full attack chain
- **No correlation** ▶ between user authentication and financial transactions

TECHNICAL IMPACT

- **SOC analysts manually linked logs,** leading to slow investigations
- **Attacks spread across multiple events** were left undetected

BUSINESS IMPACT

- **Revenue loss per quarter** due to undetected fraud
- **Customer trust eroded,** leading to increased churn

SOLUTIONS

✓ **Implemented risk-based alerting (RBA)** to track user behavior across multiple data sources

✓ **Correlated login, device, and transaction logs** to detect fraudulent activity in real-time

✓ **Used machine learning models** to flag high-risk behaviors dynamically

☒ **Before:** Analysts took a lot of time to manually correlate logs, missing real-time fraud attempts.

✓ **After:** Automated detection reduced fraud losses dramatically, with real-time alerts for account takeovers.

SUMMARY

Many organizations face significant challenges in managing, optimizing, and securing their Splunk environments. Without proper configurations, they suffer from slow performance, high costs, security gaps, and inefficient operations.

KEY TAKEAWAYS

- ✓ **Splunk Best Practices: Prevent crashes and performance issues.**
- ✓ **Data Ingestion Optimization: Reduce costs and improve efficiency.**
- ✓ **Data Quality Improvement: Ensure accurate reporting and compliance.**
- ✓ **Search Performance Tuning: Speed up incident investigations.**
- ✓ **Premium App Optimization: Get the best value for the Apps by establishing the best integrations.**
- ✓ **Custom Dashboards: Improve executive decision-making.**
- ✓ **OTB Detections: Enhance threat detection with built-in rules.**
- ✓ **Advanced Correlated Detections: Identify sophisticated attack patterns in real-time.**

HOW SP6 CAN HELP

At SP6, we help clients progress through these eight levels of improvement, from foundational best practices to advanced correlated detections that stop complex threats.

By addressing these areas, we turn Splunk from a challenge into a business-enabling powerhouse. Whether you're struggling with slow performance, high costs, or security blind spots, we have the expertise to optimize your Splunk investment.

Ready to take your Splunk to the next level? Let's talk!

Back to Back Winner
2023 🏆 2024
splunk>
AMER Professional Services
PARTNER OF THE YEAR

About SP6

SP6 is a niche services firm with expertise in both Security Analytics and Cybersecurity Compliance. In Security Analytics, SP6 has one of North America's largest and most competent Splunk services teams in North America. SP6 offers both project-based Professional Services and the Value Acceleration Program for Splunk, a fractional co-management model. In the field of Cybersecurity Compliance, SP6 provides consulting expertise with NIST security frameworks such as NIST CSF, 800-171 and 800-53. These services include security and compliance gap assessments, remediation advisement around missing or failed security controls, outsourced Compliance as a Service, and Continuous Controls Monitoring through our ASCERA software product.