Splunk Enterprise Dashboard Documentation

By Christopher Contreras

Table of Contents

Project Overview

This project demonstrates enterprise-level SIEM administration through the creation of a comprehensive call center monitoring dashboard in Splunk Enterprise. Using synthetic EventGen data simulating WebServer 1, 2, and 3 access and log control files, the implementation showcases real-world monitoring capabilities essential for cybersecurity operations.

Objectives

- Create an interactive dashboard for real-time call center performance monitoring
- Implement automated alerting for proactive incident detection
- Configure scheduled reporting for executive stakeholder communication
- Establish role-based access control demonstrating security governance
- Document implementation process for knowledge transfer and portfolio development

---

Environment Setup

Splunk Enterprise Configuration

- **Platform:** Splunk Enterprise
- **Data Index:** main
- **Source Type:** eventgen
- **Data Source:** Synthetic telecommunications call data
- **Simulation:** WebServer 1, 2, 3 access and log control files

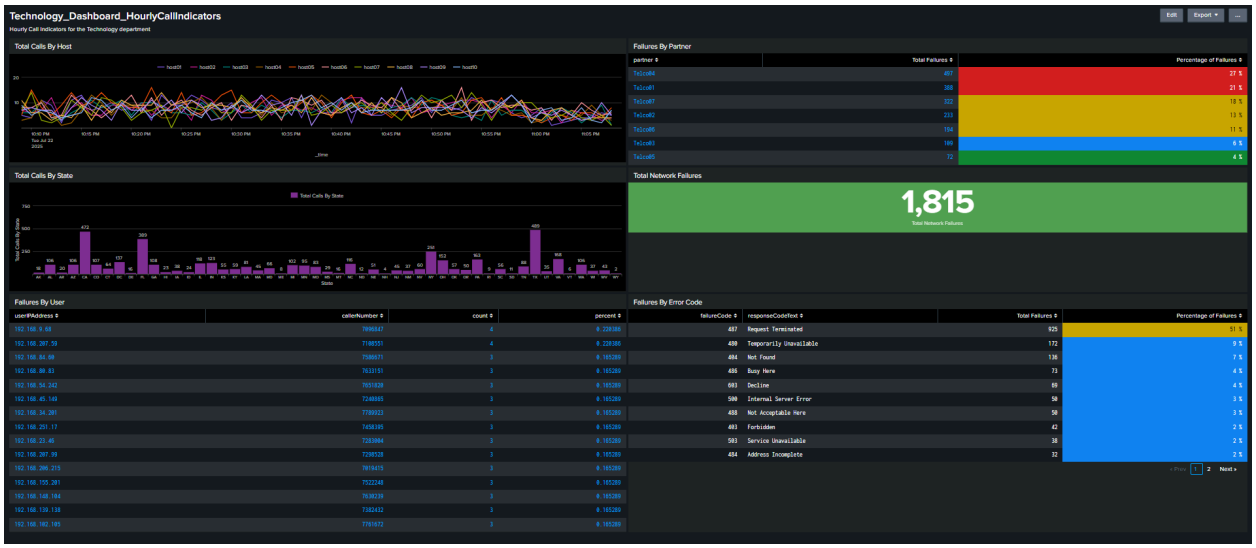
Key Data Fields

- nodeName - Host/server identifier (Host01-Host10)
- partner - Partner organization identifier
- callResult - Success/Failure status
- State - Geographic state information
- userIPAddress - Caller IP address
- callerNumber - Phone number identifier
- failureCode - Technical error classification
- responseCodeText - Human-readable error description

Dashboard Implementation

The dashboard consists of six critical monitoring panels providing comprehensive visibility into call center operations. This integrated approach combines real-time performance metrics, failure analysis, geographic insights, and user experience monitoring to deliver complete operational oversight. Each panel serves specific business functions while contributing to an overall view of system health and performance. The dashboard architecture follows enterprise monitoring best practices, presenting key performance indicators in an intuitive layout that supports both technical teams requiring detailed metrics and executives needing high-level summaries. This comprehensive monitoring enables proactive issue detection, capacity planning, and data-driven decision making across the entire call center infrastructure.

Technology_Dashboard_HourlyCallIndicators



1. Total Calls By Host

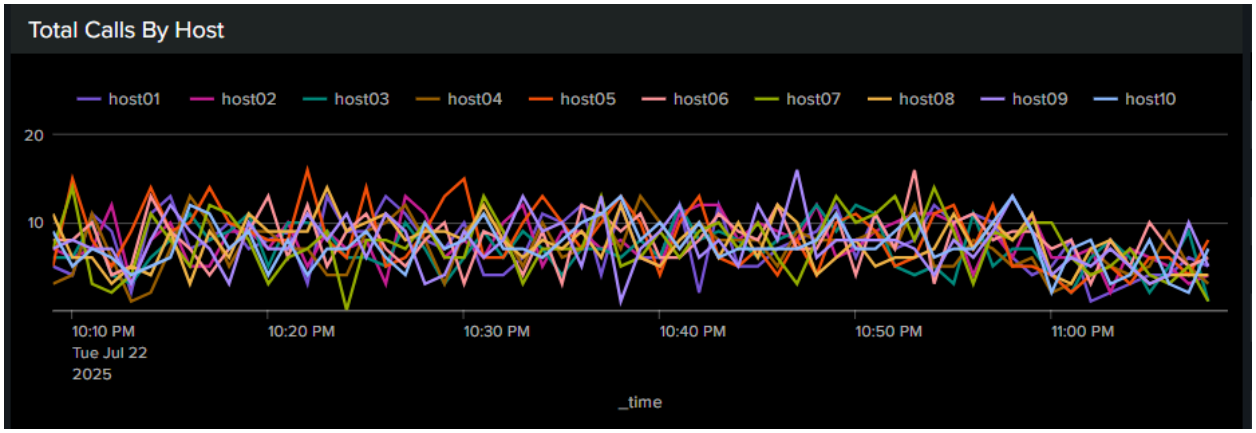
Purpose & Business Value: Monitor call volume distribution across infrastructure hosts to identify traffic patterns, peak usage times, and potential infrastructure bottlenecks. This enables effective load balancing decisions and proactive capacity planning.

Search Query:

```
index=main sourcetype=eventgen

| timechart count by nodeName partial=f
```

Visualization: Multi-series line chart with time-based x-axis showing real-time call distribution trends across all hosts.



---

2. Failures By Partner

Purpose & Business Value: Identify partner organizations experiencing the highest failure rates to enable data-driven partner support prioritization, targeted relationship management, and effective SLA monitoring.

Search Query:

```
index=main sourcetype=eventgen callResult="Failure"
| top partner countfield="Total Failures"
```

Visualization: Table format displaying failure counts and percentage distribution, ranked by total failures for immediate identification of problematic partnerships.

Failures By Partner

partner	Total Failures	Percentage of Failures
Telco04	497	27 %
Telco01	388	21 %
Telco07	322	18 %
Telco02	233	13 %
Telco06	194	11 %
Telco03	109	6 %
Telco05	72	4 %

3. Total Calls By State

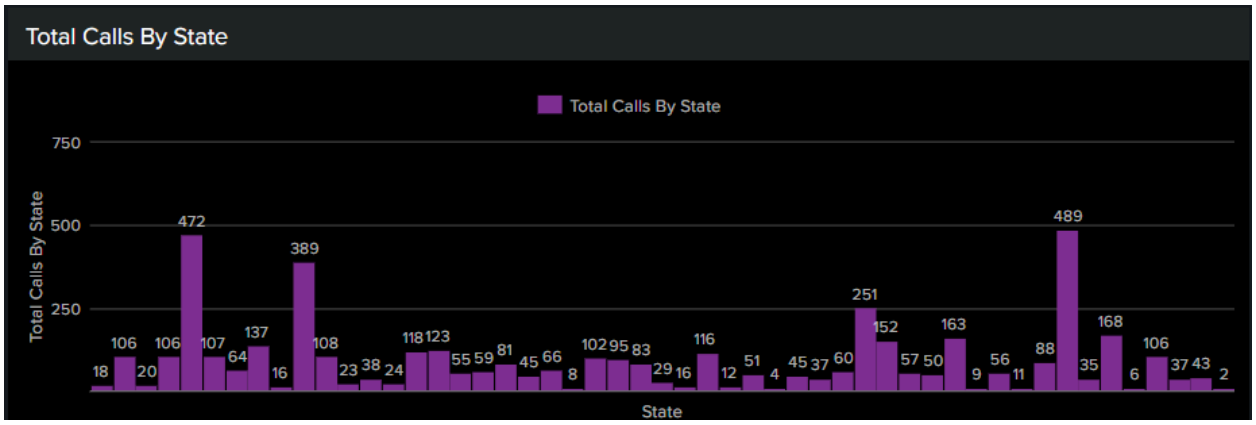
Purpose & Business Value: Geographic analysis of call distribution to provide regional performance insights and guide resource allocation decisions for effective capacity planning across different states.

Search Query:

```
index=main sourcetype="eventgen"

| stats count as "Total Calls By State" by State
```

Visualization: Bar chart showing state-based call volume distribution, saved as reusable report for consistent dashboard integration and cross-platform analysis.



4. Total Network Failures

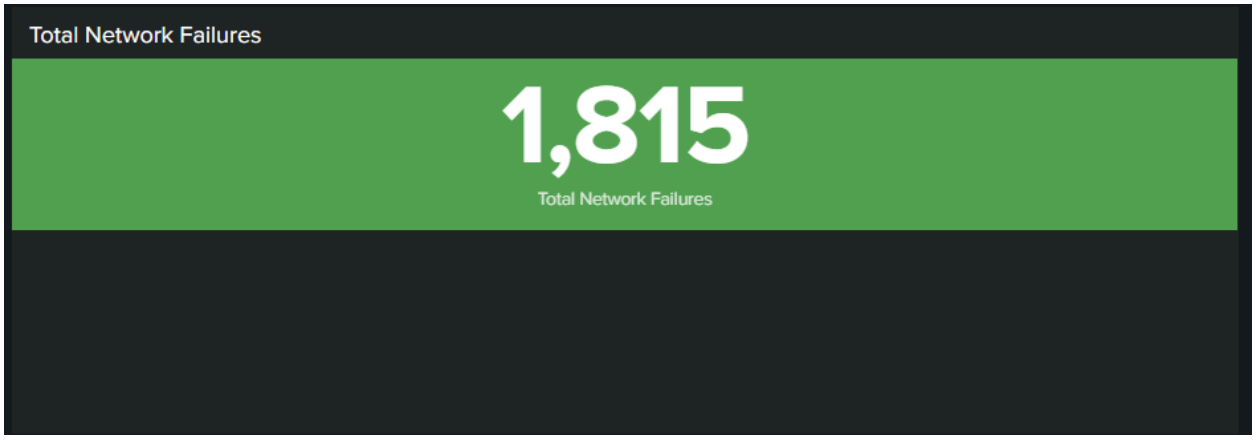
Purpose & Business Value: High-level KPI providing executive visibility into overall system health and reliability, serving as a critical executive dashboard metric for rapid system reliability assessment and strategic decision making.

Search Query:

```
index=main sourcetype=eventgen callResult="Failure"

| stats count
```

Visualization: Single value display with prominent numerical indicator designed for immediate executive comprehension and dashboard prominence.



---

5. Failures By User

Purpose & Business Value: Identify individual users experiencing recurring connection issues to enable proactive user experience management, targeted technical support, and optimization of customer service resources.

Search Query:

```
index=main sourcetype="eventgen" callResult=Failure
| top limit=15 userIPAddress callerNumber
```

Visualization: Table showing top 15 users with highest failure rates, providing actionable data for immediate technical support intervention and user experience improvement.

Failures By User

userIPAddress	callerNumber	count	percent
192.168.9.68	7096847	4	0.220386
192.168.207.59	7108551	4	0.220386
192.168.84.60	7586671	3	0.165289
192.168.80.83	7633151	3	0.165289
192.168.54.242	7651820	3	0.165289
192.168.45.149	7240865	3	0.165289
192.168.34.201	7789923	3	0.165289
192.168.251.17	7458395	3	0.165289
192.168.23.46	7283004	3	0.165289
192.168.207.99	7298528	3	0.165289
192.168.206.215	7019415	3	0.165289
192.168.155.201	7522248	3	0.165289
192.168.148.104	7630239	3	0.165289
192.168.139.138	7382432	3	0.165289
192.168.102.105	7761672	3	0.165289

---

6. Failures By Error Code

Purpose & Business Value: Technical troubleshooting dashboard for root cause analysis and system optimization, enabling technical team prioritization based on error frequency and impact to maximize system reliability improvements.

Search Query:

index=main sourcetype="eventgen"

| top limit=15 failureCode responseCodeText countfield="Total Failures"

percentfield="Percentage of Failures"

Post-Processing Transformation:

| rename percent as "Percentage of Failures"

Visualization: Detailed table with error codes, descriptions, and statistical analysis, saved as reusable report for consistency across dashboards and cross-platform integration.

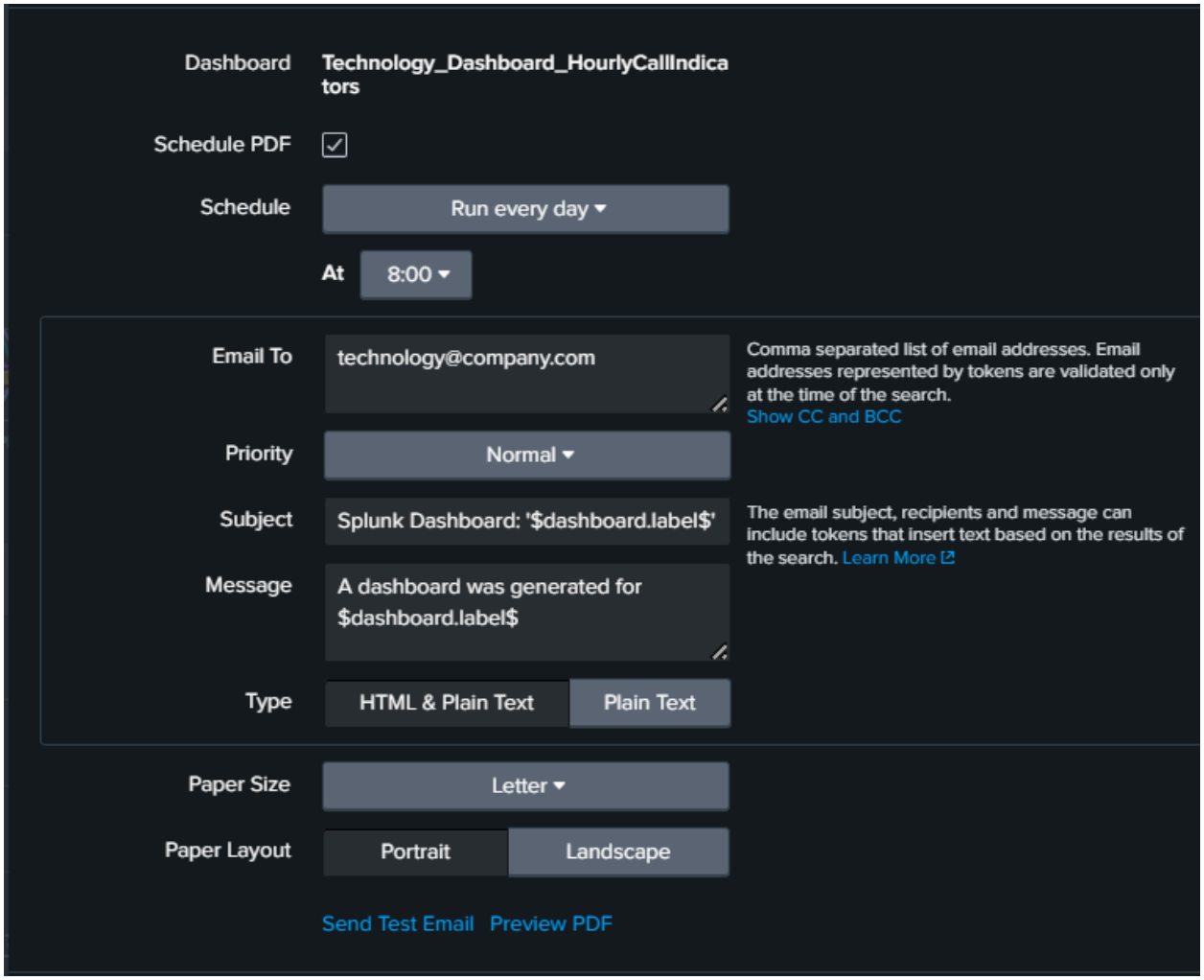
Failures By Error Code

failureCode	responseCodeText	Total Failures	Percentage of Failures
487	Request Terminated	925	51 %
480	Temporarily Unavailable	172	9 %
404	Not Found	136	7 %
486	Busy Here	73	4 %
603	Decline	69	4 %
500	Internal Server Error	50	3 %
488	Not Acceptable Here	50	3 %
403	Forbidden	42	2 %
503	Service Unavailable	38	2 %
484	Address Incomplete	32	2 %

Scheduled Report: Technology Dashboard PDF Export

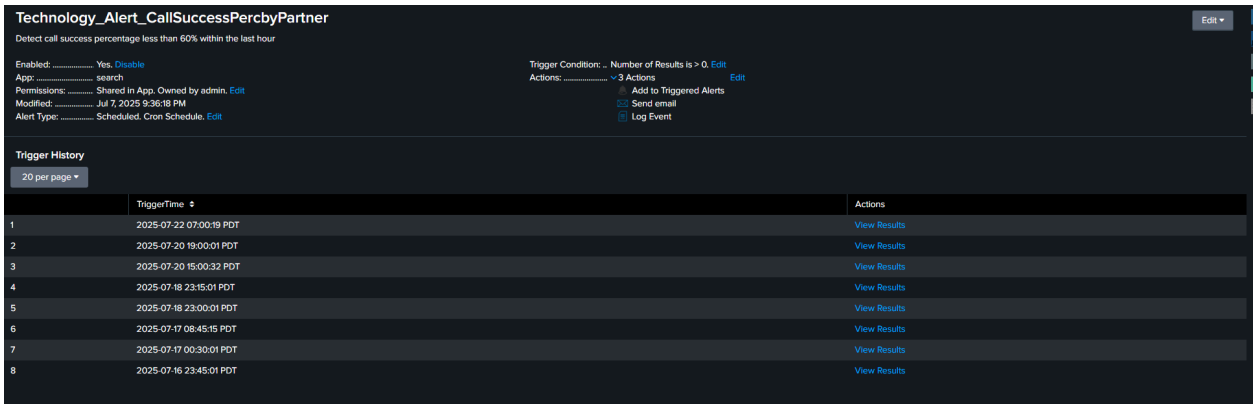
Configuration & Distribution: Daily automated PDF report (Technology_Dashboard_HourlyCallIndicators_PDF) scheduled for 8:00 AM delivery to executive management and operations teams via email attachment, providing complete dashboard snapshot with executive summary.

Professional Use Case & Business Value: Supports executive oversight without requiring direct Splunk access, enabling data-driven decision making while maintaining operational transparency. Provides historical trend documentation for strategic planning, compliance audit requirements, and stakeholder communication independent of technical platform access.



Alert Configuration

Technology_Alert_CallSuccessRateByPartner



Purpose: Proactive monitoring to detect when call success percentage falls below acceptable thresholds.

Trigger Condition:

- **Search:** Detects call success rate below 60% within the last hour
- **Condition:** Number of Results is > 0
- **Schedule:** Continuous monitoring with real-time evaluation

Alert Actions:

1. **Add to Triggered Alerts** - Dashboard visibility and alert management
2. **Send Email** - Immediate notification to operations team
3. **Log Event** - Audit trail creation for compliance and analysis

Email Configuration:

- **Recipients:** Operations team and management stakeholders
- **Subject:** ALERT: Call Success Rate Below Threshold
- **Message Template:** Professional notification with incident details and recommended actions

Trigger History Maintenance:

- Complete log of alert activations with timestamps
- Performance metrics for alert effectiveness
- Historical trend analysis for threshold optimization

Role-Based Access Control

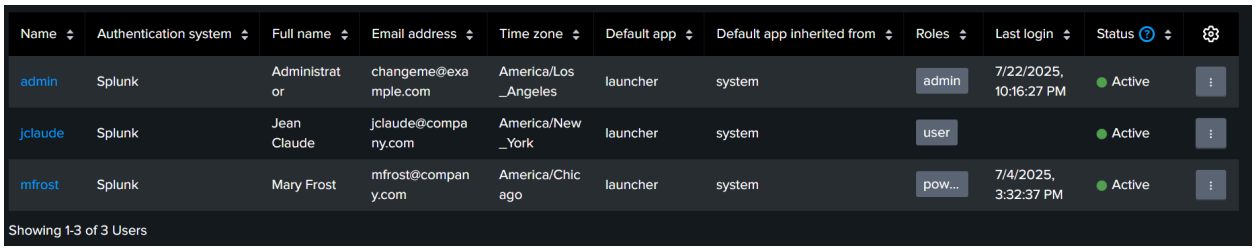
Three-Tier Access Model Implementation

Admin Role (admin): Complete platform control including dashboard creation, alert management, user administration, and system configuration. Provides full read/write access to all indexes and unrestricted search capabilities for IT administrators and security team leads**.**

Power User Role (mfrost): Operational management access with dashboard viewing, limited editing permissions, report creation within assigned areas, and advanced search functionality. Enables operations managers and senior analysts to perform their duties with restricted administrative functions.

User Role (jclaude): Read-only dashboard access with basic search functionality, report viewing without modification permissions, and alert notification viewing. Designed for end users, junior analysts, and stakeholders requiring information access without modification capabilities.

Security Implementation: Demonstrates principle of least privilege by ensuring users access only functionality required for their role, maintaining audit compliance, and supporting enterprise security governance requirements.



Name	Authentication system	Full name	Email address	Time zone	Default app	Default app inherited from	Roles	Last login	Status
admin	Splunk	Administrator	changeme@example.com	America/Los_Angeles	launcher	system	admin	7/22/2025, 10:16:27 PM	Active
jclaude	Splunk	Jean Claude	jclaude@company.com	America/New_York	launcher	system	user		Active
mfrost	Splunk	Mary Frost	mfrost@company.com	America/Chicago	launcher	system	pow...	7/4/2025, 3:32:37 PM	Active

Showing 1-3 of 3 Users

Summary and Future Enhancements

Project Success Metrics

- **Dashboard Functionality:** All six monitoring panels operational with real-time data
- **Alert System:** Automated monitoring with email notification confirmed operational
- **Report Scheduling:** Daily PDF generation and distribution successfully configured
- **Access Control:** Three-tier role model implemented with appropriate permission restrictions
- **Documentation:** Comprehensive technical documentation completed for knowledge transfer

Lessons Learned

- **SPL Optimization:** Query efficiency directly impacts dashboard performance and user experience
- **Alert Tuning:** Threshold configuration requires a balance between sensitivity and false positive reduction
- **User Experience:** Dashboard design must consider both technical accuracy and business usability
- **Security Governance:** Role-based access control requires careful planning and ongoing maintenance

Future Enhancement Opportunities

- **Advanced Analytics:** Integration of machine learning capabilities for predictive analysis
- **Threat Intelligence:** Incorporation of external threat feeds for security context
- **API Integration:** Automated response capabilities through external system integration
- **Scalability Planning:** Enterprise-scale implementation with distributed architecture

Professional Development Next Steps

- **Advanced Splunk Certification:** Pursuit of Splunk Enterprise Security and ITSI certifications
- **Security Framework Integration:** Application of NIST, ISO 27001, and other frameworks
- **Cloud Security Monitoring:** Extension of skills to cloud-native security monitoring platforms
- **Leadership Development:** Team management and strategic security planning capabilities