augustschell | splunk> a CISCO company

August Schell's Solutions Engineers deliver tailored Splunk demonstrations, workshops, and technical enablement sessions designed to align with customer operational objectives. Each engagement focuses on platform architecture, data ingestion strategies, correlation logic, and workflow optimization to ensure full alignment with mission requirements and measurable security outcomes.

Splunk Workshops That ASE Provides:

Splunk4Rookies
Introductory, hands-on session for new users. Participants create their first Splunk app, ingest and analyze data, and build basic dashboards—gaining foundational knowledge of Splunk's platform and use cases.

Splunk4Ninjas
Advanced workshop for security admins and analysts. Covers in-depth use of Splunk applications such as the Machine Learning Toolkit, AIOps, ITSI, and SPL best practices. Focuses on solving complex data challenges.

Advanced APT Hunting
Modular, hands-on training exploring Advanced Persistent Threats (APTs). Teaches hypothesis development, hunting techniques, and frameworks like the Lockheed Martin Kill Chain, MITRE ATT&CK, and the Diamond Model.

AWS Security Hands-On
Scenario-based session for Splunk users in AWS environments. Builds familiarity with AWS data sources and applies that knowledge to cloud security monitoring and incident response.

Building Correlation Searches
Guides users through developing custom correlation searches in Splunk Enterprise Security. Introduces data models and tstats commands to optimize searches and improve detection accuracy.

Fraud Investigation
Hands-on workshop for detecting and investigating fraudulent web activity using Splunk Enterprise and Enterprise Security through realistic fraud scenarios.

SOAR (Security Orchestration, Automation, & Response)
Explains incident response automation using Splunk SOAR. Participants manage cases, automate enrichment, and walk through a complete incident workflow from detection to resolution.

Security Operations Suite
Covers Splunk Enterprise, Enterprise Security, UBA, and Phantom in multi-scenario labs. Demonstrates how to investigate, hunt, and orchestrate actions across integrated security tools.

Splunking the Endpoint
Teaches endpoint visibility and logging analysis (Windows Event Logs, Sysmon, PowerShell, osquery, CB, Cisco NVM). Highlights Splunk Security Essentials and ES Content Updates.

User Behavior Analytics (UBA)
Hands-on lab for threat hunting and anomaly detection using UBA's machine-learning models. Participants trace threats, pivot through anomalies, and uncover additional indicators.

Security Lunch & Learn
Compact, interactive session introducing key search commands for analyzing security events in Splunk.

Insider Threat
Focuses on building an Insider Threat Program using Splunk Enterprise, Enterprise Security, and UBA. Includes program fundamentals and hands-on investigations.

Splunk Certifications

- ✓ Splunk Core Certified User
- ✓ Splunk Core Certified Power User
- ✓ Splunk Core Certified Advance Power User
- ✓ Splunk Enterprise Certified Admin
- ✓ Splunk Cloud Certified Admin
- ✓ Splunk Enterprise Certified Architect
- ✓ Splunk Core Certified Consultant
- ✓ Splunk Certified Cybersecurity Defense Engineer