LTM

BROCHURE

Splunk Security with LTM

Power the SOC of the Future with Scale, Speed, and Choice

When Security Operations Must Move Faster

Security teams are under growing pressure. Attack surfaces continue to expand, tools remain fragmented, and analysts spend valuable time switching across disconnected systems. At the same time, boards expect stronger digital resilience and faster response to threats.

Splunk Security with LTM helps enterprises unify threat detection, investigation, and response across the SOC. By combining AI-driven security operations with a scalable TDIR framework, organizations can reduce complexity, improve analyst productivity, and strengthen operational resilience. To stay ahead of evolving threats, enterprises must not simply respond faster, but Outcreate with security operations built for scale and adaptability.

Security Operations by the Numbers

***Detect at Scale**
1,500+ ready-to-use detections

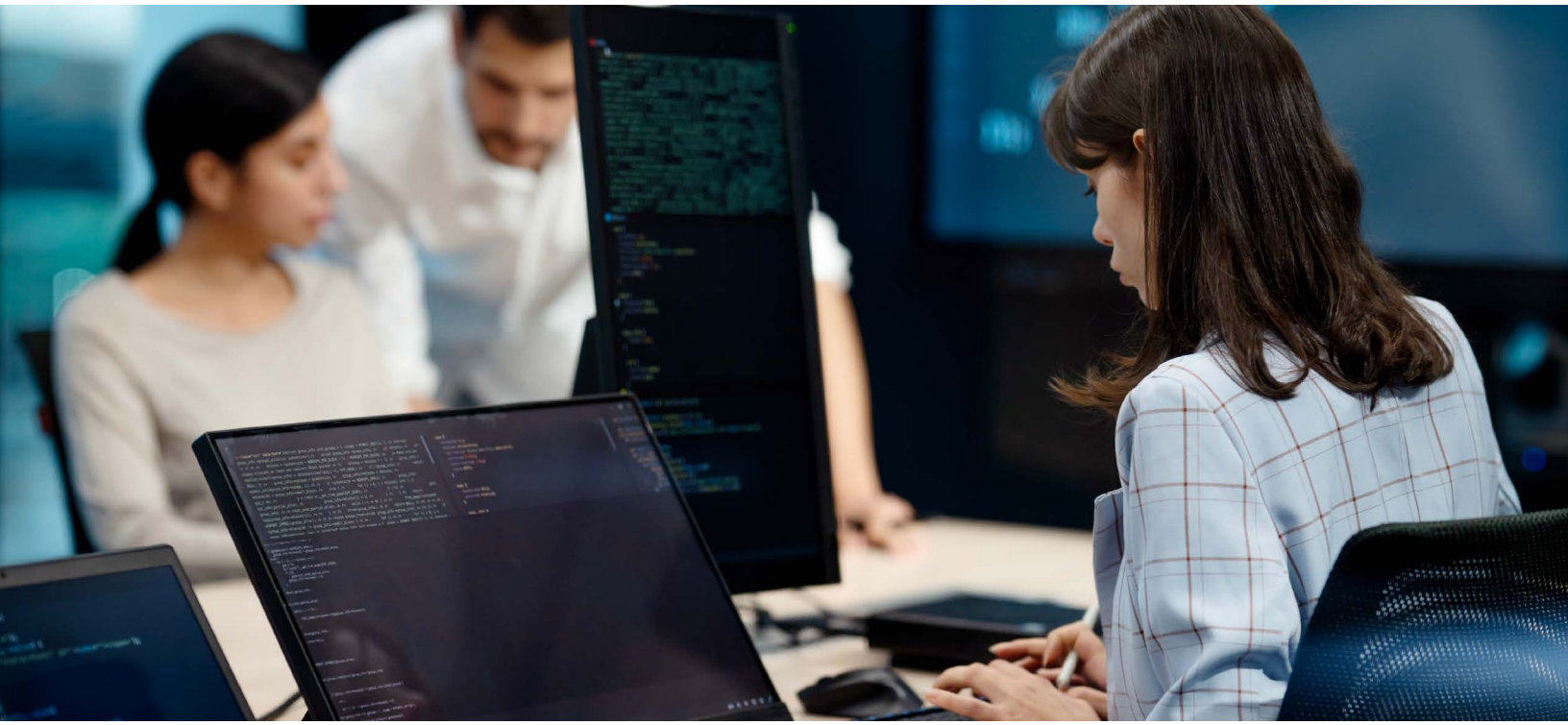
Unify Operations
Single TDIR work surface

Empower Innovation
2,200+ partners and 2,800+ apps

90%
lower MTTD and MTTR

80%
faster investigation

267%
ROI from Splunk Security



Why This Matters Now

Why SOC Modernization Cannot Wait

Security leaders are facing four persistent operational pressures:

Expanding Attack Surface

52% of organizations reported a recent data breach as cloud growth, distributed workforces, and connected devices continue to widen exposure

Siloed Tools and Workflows

Analysts pivot across an average of six tools per incident, slowing investigations and increasing operational fatigue

Talent and Skills Shortage

89% of security teams reported that cybersecurity skill shortages are impacting operations, while SOCs manage nearly 25 disconnected tools on average

Compliance and Audit Load

53% of organizations say regulatory compliance has become harder to manage compared to two years ago

Two-thirds of security leaders say stronger security operations could have prevented a recent incident. The SOC is no longer a support function. It sits at the center of digital resilience.*

Our Solution

A Unified Path to the Modern SOC

LTM deploys Splunk Security as the nucleus of the modern SOC, combining unified TDIR operations with AI-driven automation and orchestration.

Four Stages of the Digital Resilience Journey

STAGE 01
Foundational Visibility
See across every environment

STAGE 02
Guided Insights
Detect threats with context and prioritize risk

STAGE 03
Proactive Response
Automate response workflows and reduce analyst effort

STAGE 04
Unified Workflows
Collaborate across the full TDIR cycle

Outcreate Security Operations at Enterprise Scale

The following capabilities help enterprises modernize security operations with greater visibility, faster response, and unified operational control.

SCALE

Detect Threats at Scale

- Search and correlate data across on-prem, cloud, and partner environments
- 1,500+ ready-to-use detections out of the box

60% smaller visibility gap

SPEED

Unify Security Operations

- Single work surface for TDIR operations
- SOAR playbooks automate response in seconds
- Attack Analyzer pulls automated context into every investigation

30% lift in operational efficiency

CHOICE

Empower Security Innovation

- Build for any use case with 2,800+ apps, 2,200+ partners, and a 250K-strong community
- Custom playbooks, custom dashboards, your way

267% ROI from Splunk Security

What You Get

The Splunk Security Portfolio, Delivered by LTM

LTM deploys and operates the four products that power Splunk's unified TDIR experience, bringing together detection, automation, orchestration, and threat intelligence from day one.

Splunk Enterprise Security

The industry-defining SIEM

- Search and analyze data at scale across on-prem and cloud environments
- 1,500+ pre-built detections out of the box
- Risk-based alerting to prioritize imminent threats
- ML-driven detection for anomalies and unknown threats
- Unified work surface across the TDIR lifecycle

Splunk SOAR

Automation and orchestration

- Pre-built playbooks for common containment and response tasks
- Custom playbooks aligned to runbooks and ticketing systems
- Orchestration across security, IT, and third-party tools
- Reduces hours of analyst effort to minutes
- Tight integration with Splunk ES and Attack Analyzer

Splunk User Behavior Analytics

Machine learning for unknown threats

- Multi-entity profiling for users, devices, and applications
- Unsupervised ML correlates anomalies into high-fidelity threats
- Visual threat correlations that accelerate investigations
- Continuous content updates from Splunk
- Native integration with Splunk ES for contextual analysis

Splunk Attack Analyzer

Automated threat analysis

- Automates malware and phishing analysis
- Detonates suspicious files and URLs in isolated environments
- Delivers consistent, high-quality verdicts
- Integrates with Splunk SOAR for end-to-end response
- Returns threat context in minutes, not hours

Backed By Splunk Security Research

SURGe and the Threat Research Team extend intelligence directly into the SOC stack.

1,500+ detection searches • 200+ analytic stories • 68 automation playbooks
• Rapid-response guidance for live incidents

Our Approach

From First Workshop to a Steady-State SOC

LTM's delivery model is led by certified Splunk engineers and SOC architects across global cyber centers. Each phase is designed with clear operational outcomes and measurable exits.

01 Assess

SOC maturity assessment, use-case workshops, and data-source inventory to define the target operating model and phased deployment roadmap.

02 Design

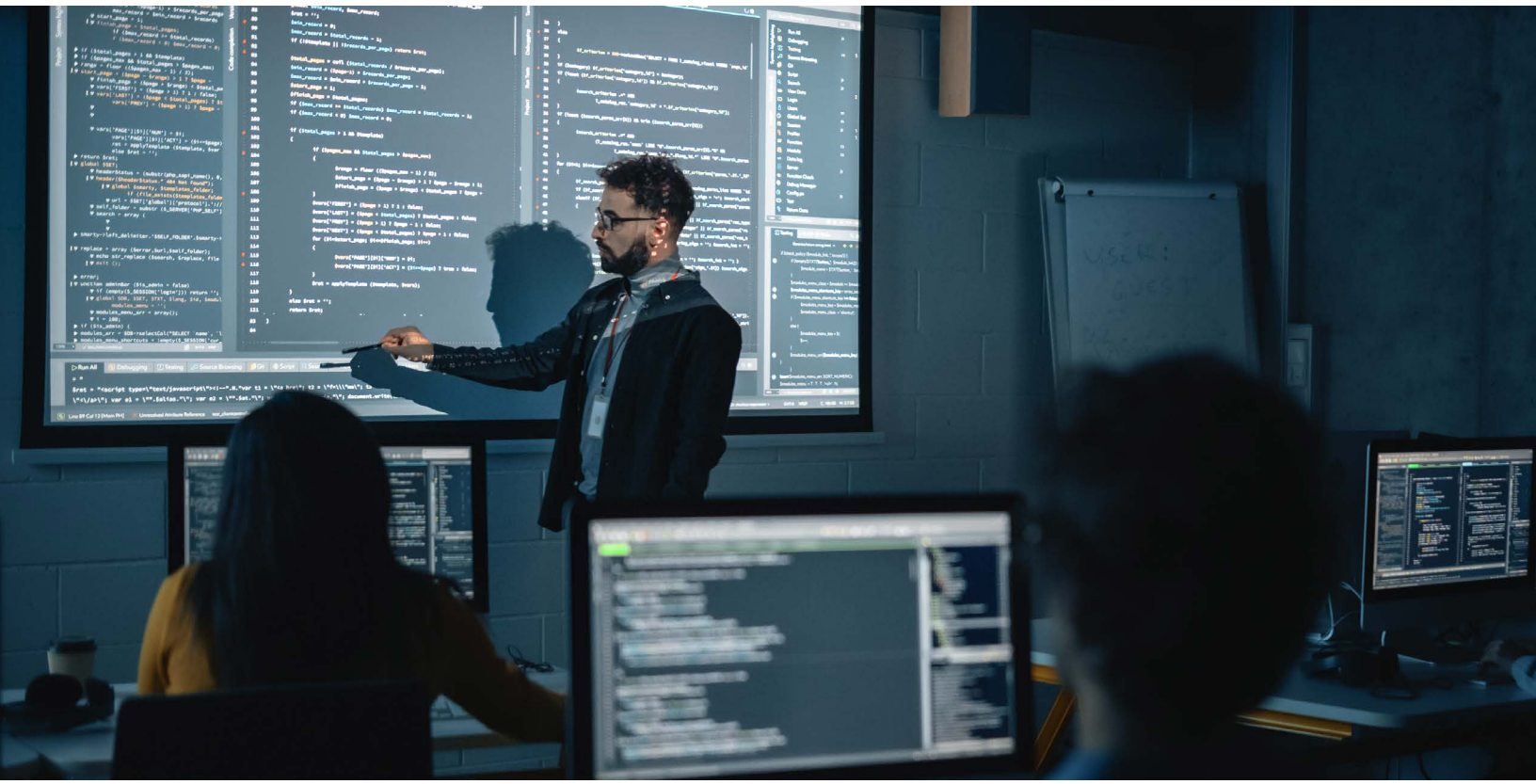
Reference architecture for Splunk ES, SOAR, UBA, and Attack Analyzer, along with onboarding plans and MITRE ATT&CK-aligned detection strategies.

03 Deploy

Platform implementation with log onboarding, detections, dashboards, risk-based alerting, and SOAR playbooks piloted with defined business units.

04 Optimize

24x7 managed SOC operations, content engineering, threat hunting, and continuous tuning tied to MTTD, MTTR, and analyst productivity.



Why Splunk Security With LTM

As a Business Creativity partner, LTM brings human insights and intelligent systems together to help enterprises modernize SOC operations with scale, speed, and operational control. LTM delivers this through:

- Certified Splunk engineers across India, Europe, and the Americas
- Experience building and operating SOCs for Fortune 500 enterprises across BFSI, manufacturing, retail, and pharma
- 24x7 managed detection and response tightly integrated with in-house teams
- Pre-built detections, SOAR playbooks, and dashboards that accelerate go-live
- Outcome-based delivery tied to MTTD, MTTR, and analyst productivity

What's Next

Book a SOC modernization workshop

Half-day session mapped to your detection backlog and data sources.
Reach out to your LTM account team or write to ***cybersecurity.pulse@ltm.com***

Reference

1. *ESG Report: SOC Market Trends, Splunk*: https://www.splunk.com/en_us/form/esg-soc-market-trends-report.html