Smarttech
YOUR 24/7 SECURITY PARTNER

+

splunk>
a cisco company

splunk>
Partnerverse
Build
ELITE

Smarttech Premier+
Clearer View of Security

Splunk Enterprise Security Premier

Splunk Enterprise Security Premier is a best-in-class SIEM and AI-powered SecOps platform that helps organisations reduce cyber risk while simplifying security operations across hybrid environments. It delivers unified visibility, detection, and response, enabling faster, more consistent action with lower operational overhead.

Splunk ES Premier aggregates telemetry from endpoints, networks, cloud infrastructure, SaaS platforms, and identity systems, removing data silos and reducing alert fatigue. Correlation, machine learning, and behavioural analytics surface high-confidence threats so teams can focus on what matters.

With UEBA embedded, organisations detect insider threats and compromised accounts earlier, reducing dwell time. Native SOAR sits on top of the SIEM to enable automated, policy-driven response, shortening response times without increasing headcount.

Together, these capabilities support a faster, more predictable security programme.

Smarttech247: Operationalising Splunk

As an elite-level Splunk partner, Smarttech247 delivers a best-in-class MDR service by tuning detections and executing consistent response aligned to business risk. VisionX provides an executive-ready view of security posture and response performance.

Together, Smarttech247 and Splunk deliver measurable improvements:

- Mean Time to Detect (MTTD) reduced by up to 50%
- False positives reduced by up to 70%
- Risk reduced by up to 70%

Smarttech247 Premier+

Smarttech247 Premier+ is designed from the ground up as the first dedicated reporting and insights layer that fully showcases the capabilities of ES Premier, including UEBA and native SOAR. To deliver this, Smarttech247's core MDR service is enhanced through the operational use of behavioural analytics (UEBA) and automated response (SOAR) to deliver faster detection, clearer prioritisation, and more decisive incident handling.

Detection engineering is central to Premier+ and is tailored to each customer's environment, architecture, and industry. Detections are designed, tested, and continuously tuned to reflect how attackers operate within specific sectors, technologies, and identity models. Customer and vertical specific use cases developed by Smarttech247 focus on the threats most likely to impact the organisation, reducing false positives and accelerating investigations.

Within Premier+ operations, UEBA provides behavioural context to surface insider risk, compromised accounts, and subtle misuse earlier. SOAR enables pre-approved, policy-driven response actions to be executed quickly and consistently by the SOC. Visibility into detections, decisions, and response activity is delivered through the VisionX platform.

VisionX: A Trusted View of Cyber Risk and Response

VisionX is Smarttech247's security operations and intelligence platform, designed to maximise the value of existing security investments.

Through a single, unified view, VisionX translates technical security activity into clear, decision-ready insight. Executive dashboards show security posture, risk trends, and response performance, supporting governance, audits, and board-level reporting. Beyond MDR, VisionX provides visibility and access to services such as penetration testing, GRC, and data security from the same platform.

The Role of Splunk SOAR in Smarttech247 Premier+

Smarttech247 Premier+ unifies detections, anomalies, threat intelligence, and SOAR response actions into a single operational and reporting layer. This gives customers clear visibility into how Splunk is driving detection quality, risk reduction, and response effectiveness across SIEM, EDR, CASB, DLP, GRC, and other security tools.

Smarttech247 Premier+ ingests and visualises SOAR data to understand how incidents were handled and what actions were taken:

- Playbook executions
- Automated and manual response actions
- Case activity and investigation steps
- Containment and remediation actions
- Response timelines and outcomes

Making Response Visible

Through the VisionX platform, business leaders and analysts get a clear, simplified view of response activity, showing which actions were taken, when, and why. Automation outcomes are translated into performance insight without exposing underlying technical complexity.

The Result

Splunk SOAR executes response and automation. Smarttech247 Premier+ ensures response is consistent, transparent, and decision-ready.

SOAR: Consistent, Auditable Incident Handling

Once an incident is underway, inconsistency becomes the biggest risk. Different analysts take different approaches, steps are missed under pressure, and managers lack a clear view of what is happening.

Splunk SOAR brings structure to every incident. Splunk SOAR brings structure to every incident. As part of the Smarttech247 Premier+ MDR service, incidents are handled by SOC analysts using enhanced capabilities. Alerts, evidence, actions, and decisions are captured as the incident unfolds, enriched with behavioural analytics and supported by automated, policy-driven response.

Managers no longer need to reconstruct timelines from emails or chat logs. Through the VisionX platform, Smarttech Premier+ provides better, real-time insights into:

- What triggered the incident
- What actions have been taken
- What remains outstanding

Outcome

- Splunk SOAR delivers structured, repeatable response
- Smarttech Premier+ makes response easy to follow, measure, and explain

Key Benefits

- Consistent incident handling under pressure
- All evidence and actions captured in one place
- Analysts guided by clear response steps, not improvisation

The Role of UEBA in Smarttech247 Premier+

Most security alerts indicate something happened, not whether it matters. User and Entity Behaviour Analytics (UEBA) adds behavioural context and risk.

As part of the added service for Smarttech247 Premier+, UEBA learns normal behaviour for users and systems, then highlights meaningful deviations. Instead of treating every alert equally, it focuses attention on activity suggesting misuse, compromise, or abuse of access.

Smarttech247 Premier+ ingests and visualises UEBA data to understand who or what is behaving abnormally and why:

- Behavioural anomalies
- User and entity risk scores
- Behaviour deviations from established baselines
- Risk trends over time
- Indicators of insider risk or compromised accounts

Clearer Decisions

- Analysts investigate patterns over time, not isolated alerts
- Subtle threats surface earlier
- Managers prioritise cases based on risk

Key Benefits

- Highlights genuinely unusual behaviour
- Reduces false positives and alert fatigue
- Surfaces high-risk activity earlier
- Prioritises investigations using risk scores
- Provides clear justification and audit visibility

Technical Integration

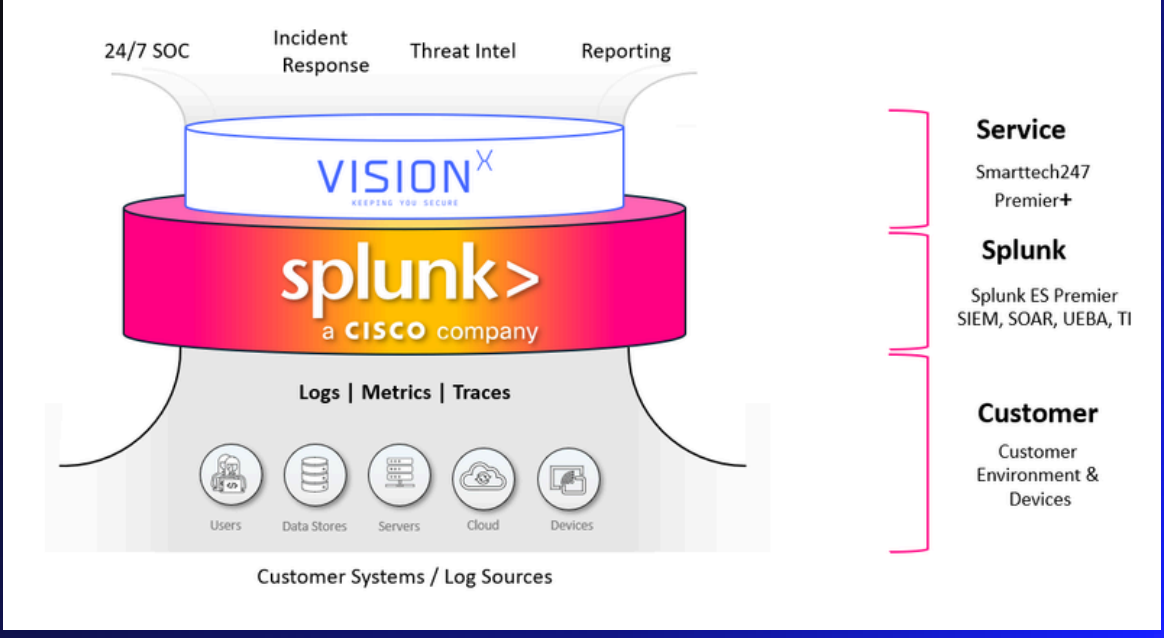
Smarttech247 Premier+ integrates with Splunk ES Premier to act as the operational and reporting layer that brings detection, behavioural, and response activity into a single, clear view.

Integration Method

- Retrieve detection, notable event, risk, and KPI data from Splunk ES Premier via APIs
- Retrieve UEBA anomaly outputs and entity risk scores
- Ingest threat intelligence correlation outcomes generated within Splunk
- Synchronise SOAR case activity, playbook executions, and response metrics
- Normalise and correlate all inputs within Smarttech247 Premier+ for operational visibility and reporting

Outcome

This combined view enables a human-led, machine-assisted security operating model, combining Splunk's analytics and automation with Smarttech247's 24/7 MDR analyst expertise.



Customer Benefits

✓ **Full Value from Splunk ES Premier**
Deeper insight from ES Premier, UEBA, threat intel, and SOAR in a single reporting layer.

✓ **Unified Security Visibility**
Consolidates SIEM, UEBA, EDR, GRC, CASB, DLP, and more into one operational view.

✓ **Faster, More Accurate Response**
UEBA, threat intelligence, and SOAR enable quicker, better-informed decisions.

✓ **Measurable Security Performance**
Executive dashboards show posture trends, KPIs, and response metrics for reporting and audits.

✓ **Reduced Operational Complexity**
Smarttech247 manages data normalisation, correlation, and dashboards.

✓ **Improved Analyst Efficiency**
Consolidated anomalies, risk scores, and response data reduce triage effort.

✓ **Stronger Return on Investment**
Maximises existing Splunk spend by operationalising underused UEBA and SOAR.

✓ **Continuous MDR-Led Improvement**
Ongoing threat hunting, playbook optimisation, and proactive improvement using Splunk analytics.

About Us

Smarttech YOUR 24/7 SECURITY PARTNER

Smarttech247 is a Gartner-recognised MDR provider with proven expertise in SIEM transformation. Validated by Forrester for driving up to 319% ROI, Smarttech247 is trusted by global enterprises to deliver high-touch, high-impact managed detection and response services.

Enterprise teams across highly regulated industries rely on Smarttech247 to simplify migration, reduce operational overhead, and strengthen outcomes in complex environments.

www.smarttech247.com

splunk> Partnerverse Build ELITE

Gartner 4.7

CERTIFICATION BODY CYBER ESSENTIALS PLUS

Tech EXCELLENCE AWARDS

CERTIFIED ISO COMPANY