SIEM Migration Services

Modernise Your SIEM. Strengthen Your Security with XDR.

Talanos cybersecurity

The SIEM Migration Imperative

For years, many businesses have relied on legacy SaaS and on-premises SIEM platforms like LogRhythm, ArcSight, and QRadar to detect and respond to cybersecurity threats. But these legacy systems often come with infrastructure overheads,limited scalability, and growing maintenance costs. They also lack the capabilities and features required to detect and respond to modern threats.

Now, many vendors are pushing customers toward cloud-native alternatives — and with good reason. Modern SIEMs like Microsoft Sentinel, LevelBlue USM Anywhere, Exabeam Fusion, and Splunk offer greater scalability, automation, and integration with today's security ecosystems. Broadly these vendors expand beyond traditional SIEM and implement a wide set of capabilities known as Extended Detection and Response (XDR).

However, migrating your SIEM to an XDR shouldn't be just a technical upgrade. It's a strategic inflection point and a potential risk if not done right. Too many migrations fail to deliver value — or worse, leave critical detection gaps during the transition. That's where we come in.

Talanos combines deep SIEM and XDR expertise with real-world security containment and engineering experience. We help organisations like yours to plan, execute, and optimise your migration without disrupting detection or increasing risk.

Regardless of the platform you're migrating to, we help you migrate with confidence and come out stronger on the other side.

Talanos SIEM Migration Services

Expert-led migration with business continuity in mind.

We help mid-sized enterprises and scaleups migrate their SIEM to a modern XDR with minimal disruption and maximum clarity. Whether you're moving from an on-premises platform or consolidating hybrid environments, we help you get it right the first time and deliver value quickly:

Current State Assessment
Understand what your existing SIEM is doing well and where it's falling short - with a clear map of coverage, data ingestion, use cases, and integrations. Validate critical data sources early to avoid blind spots and compliance gaps.

Future State Design
Build an XDR environment that scales with your business and strengthens security based on your unique business context and risks, rather than simply following a vendor's roadmap. With Talanos, outdated rules are retired or consolidated and use cases modernised, so your new XDR delivers clearer, faster insights, benefitting from intelligence feeds that keep rules updated automatically based on the latest threats.

Migration Planning & Execution
Move with confidence with every step planned to minimise disruption and maximise security. Old SIEM and new XDR run in parallel until detections are proven, so you never face blind spots, while noise is reduced and costs contained, ensuring a smooth cutover without compromising coverage.

Detection Engineering & Optimisation
Turn your XDR into a sharper, faster detection engine with rules that are rebuilt around today's risks and proven improvements like reducing false positive rates, balanced alert loads and shortened Mean-Time-To-Detect (MTTD).

Post-Migration Validation & Tuning
Lock in long-term value and confidence from your new XDR from day one with updated playbooks and retrained analysts, as well as ongoing tuning and metrics to deliver continual gains in detection accuracy and response speed.

New XDR. New possibilities.

Modern security operations require more than a new XDR. They require new ways of working. That's why many of our clients use SIEM migration as an opportunity to rethink their operating model - consolidating tooling, improving response times, and even outsourcing SOC capabilities altogether.

Our Managed SOC is built for organisations like yours:

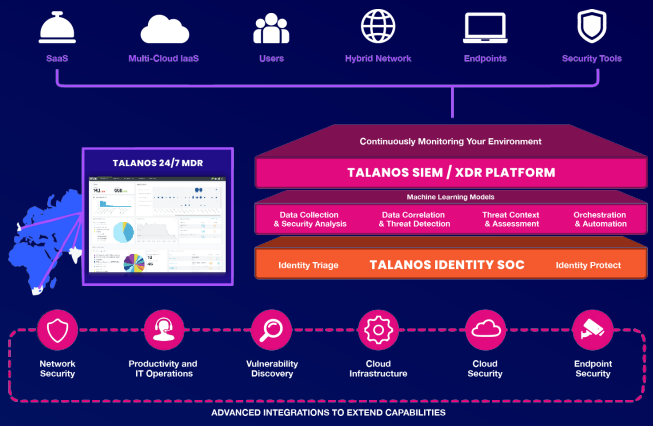
- Fast-moving, security-conscious, and short on bandwidth for 24/7 coverage
- Keen to reduce complexity and operational overhead with built-in SLAs
- Ready for a model that's built around outcomes and improving security maturity - not simply raising alerts

If you're considering a SIEM migration together with an outsourced model, we can help you explore whether a Managed SOC is the right next step.

The modern SIEM/XDR Architecture

A modern SIEM/XDR architecture continuously monitors hybrid IT environments - spanning SaaS, IaaS, endpoints, users and security tools. At the core is the Talanos SIEM/XDR platform, which integrates machine learning, threat detection, and automation to deliver real-time visability and rapid response.

Identity context drives triage and protection through the Talanos Managed SOC, while advanced integrations extend coverage across network, cloud, and endpoint security.



What You Can Expect

Phase	Deliverables
Assessment	Tool, data source and rules inventory, detection gap analysis
Design & Planning	Future state architecture, migration design and roadmap
Implementation	Platform setup, ingestion pipelines, rule migration
Validation & Tuning	Correlation logic, noise reduction, tune out false positives suppression
Ongoing Support	Managed SOC handover or hybrid operations model

Real-World Impact - Multinational SaaS company

- Migrated from **ELK to Microsoft Sentinel**
- Reduced average time to alert triage from **10 hours to 15 minutes**
- Rationalised **300+ detection rules**
- Transitioned to **hybrid SOC model** with Talanos post-migration

Why Choose Talanos?

Tool-Agnostic Expertise
We work across MS Sentinel, LevelBlue, Exabeam, Splunk, and more - with real-world experience of what works.

Security Engineering DNA
This isn't just a data migration. Our engineers are security experts first, helping you preserve and improve threat detection, and environment coverage.

Business-Aligned Delivery
We plan and execute your migration in phases that align with your risk appetite, compliance requirements, and internal capacity.

SOC Readiness & Beyond
Whether you're running your own SOC or looking to migrate operations, we make sure your XDR sets you up for success.

Ready to Talk?

Whether you're early in your planning phases or already under vendor pressure to move, we're happy to help you select the option that works best for you.

Cybersecurity services to protect your organisation and respond to the threats of today and tomorrow.

Talanos cybersecurity

Get in Touch
info@taloscs.com
www.talanoscs.com

UK
14 Upper Church Street,
Bellarmine House,
Chepstow,
NP16 5EX

South Africa
377 Rivonia Boulevard,
Rivonia,
Johannesburg,
2128

India
68, The GranCarmen
Carmelaram, Bangalore,
Karnataka,
560035