Invinsense by Infopercept

THE BUYERS' GUIDE

Beyond Legacy: The shift to the Integrated SOC.

Why traditional SIEM is buckling under modern threats, data volumes and analyst burnout — and how an AI-driven, cloud-native, data-democracy ISOC changes the economics and outcomes of security operations.

FOR CISOS | FOR SECOPS LEADERS | TDIR STRATEGY | 2026 EDITION

A practical guide to evaluating Integrated Security Operations Center solutions

EXECUTIVE SUMMARY

One definition of SIEM no longer fits.

For two decades, SIEM was the unquestioned center of the SOC: collect logs, write correlation rules, generate alerts. That model is healthy and growing — but it has fractured. As threats, data volumes and cloud estates exploded, buyers split into three distinct approaches to threat detection, investigation and response (TDIR): the extensible **SIEM platform**, the data-centric **Security Data Lake**, and the converged **Integrated SOC (ISOC)**. This guide is about that third path — what it is, why it exists, and how to evaluate it.

80%

of organizations with 2,500+ employees run a SIEM for TDIR today — the incumbent is everywhere, and everywhere strained.

3

competing visions of TDIR have emerged; a single SIEM definition can no longer describe them all.

1

platform, operated as one system, is what the ISOC promises — replacing the stitched-together stack.

THE CORE IDEA

The unit of value has shifted — from "alerts generated" to "incidents resolved." Legacy SIEM optimizes the former. The Integrated SOC is engineered for the latter.

WHAT'S CHANGED

Four forces breaking the legacy model

Everything is security-relevant now

Modern attacks hide indicators anywhere — identity, SaaS, cloud control planes, OT. Teams need to collect far more data than a pay-per-GB SIEM makes affordable.

Complexity has become the top replacement driver

Ongoing configuration, detection-stack dependency management and tuning are now the leading reasons leaders cite for considering a SIEM replacement.

AI moved from assistant to operator

Agentic AI can now perform L1 triage, enrichment and investigation autonomously — making "out-of-the-box" outcomes realistic, not aspirational.

Best-of-breed integration is expensive

Evaluating, integrating and supporting many TDIR vendors raises cost and risk. Buyers increasingly value vendor-delivered convergence over assembling parts.

THE PAIN POINTS

Where traditional SIEM structurally fails.

These are not tuning problems you can configure away — they are architectural limits of the rules-and-index model. Each one is a reason mid-to-large SOCs are actively re-evaluating their platform.

PAIN 01 · INGESTION

It drops the data attackers need you to lose

Agent and server queues are bounded with no guaranteed-delivery caching layer. When event volume spikes, events are dropped rather than durably persisted — and there is no native replay to recover them.

▲ Spikes happen during attacks — you lose your highest-value evidence at the worst moment.

PAIN 02 · DATA MODEL

No schema-first normalization

Events keep vendor-specific field names; normalization is an external bolt-on. Detections, queries and dashboards can't be ported, and ML can't reason consistently across fields.

▲ Content lock-in + AI that can't see straight across your data.

PAIN 03 · STORAGE & COST

No security data lake; the index is the ceiling

Query performance degrades under load, field-mapping conflicts silently fail ingestion, and pay-per-GB pricing forces teams to under-collect. Renewals balloon with data bloat.

▲ You choose between visibility and budget — and lose either way.

PAIN 04 · DETECTION

Rules can't see multi-system attacks

Correlation engines lack true nested, multi-level correlation. A campaign that spans identity, cloud, SaaS and endpoint shows up as disconnected alerts, not one incident.

▲ The most dangerous attacks are exactly the ones that slip between rules.

PAIN 05 · MULTI-TENANCY

Isolation that's only skin-deep

On-prem multi-tenancy is often UI-level only, with global rulesets and no tenant-scoped isolation — forcing MSSPs and shared platforms into fragile architectural workarounds.

▲ Data, detection and response boundaries aren't truly enforced.

PAIN 06 · ECONOMICS

You pay in headcount what you saved in license

The hidden cost is sustained engineering: decoder tuning, rule maintenance, indexer operations and manual scaling. "Free" or open SIEM simply moves the cost to your payroll.

▲ Your best engineers maintain plumbing instead of hunting threats.

THE PATTERN

Every one of these traces to a single root cause: a platform designed to store-and-match logs, retrofitted for a world that demands collect-everything, understand-behavior, and respond-autonomously.

THE BENEFITS OF AN INTEGRATED SOC

What an ISOC does that legacy can't.

An ISOC delivers the core of SIEM — ingestion, normalization, monitoring, investigation, reporting — and extends it with pre-integrated detection, threat intel, automation and AI, operated as one system from a single vendor. It trades open sprawl for ease of use, high out-of-the-box value, and measurable outcomes.

Behavioral detection, not static rules

ML models baseline what's normal for each user and entity and score risk in context — surfacing insider threats, identity abuse, lateral movement and zero-days that signatures miss.

Replaces: brittle, hand-written correlation rules

Agentic AI across the threat lifecycle

AI agents triage, enrich and investigate at machine speed and escalate with full context, while analysts keep decision authority. Mundane L1 work is automated; critical thinking stays human.

Replaces: manual triage and config-file-driven response

Schema-first data, normalized to OCSF on ingest

A normalized, open data model makes detections portable, investigations consistent and the whole dataset AI-ready — no external normalization layer required.

Replaces: vendor-locked fields and bolt-on parsers

Decoupled storage & intelligent data pipelines

Bring your own data lake; route, filter and tier data so you collect everything and still control cost. Hot data stays fast; cold data stays searchable for retention and compliance.

Replaces: pay-per-GB indexes and forced under-collection

One investigation surface, one control plane

Cross-product investigations, federated search and unified case management mean analysts stop pivoting between consoles and start closing incidents.

Replaces: a stitched stack of disconnected tools

Native services & MSSP-grade isolation

Vendor-delivered detection content, managed detection & response, and true end-to-end tenant isolation make the ISOC viable for enterprises and service providers alike.

Replaces: UI-only tenancy and partner-dependent services

THE EVALUATION CHECKLIST

Mandatory features of a true ISOC.

Many tools claim to be "next-gen." Use this checklist to separate a genuine Integrated SOC from a legacy SIEM with a new label. A true ISOC should satisfy all of the following.

- ✓ **SIEM core, extended.** Ingestion, normalization, active monitoring, investigation and reporting — including for third-party tools, not just native ones.
- ✓ **One operated ecosystem.** SIEM, EDR, threat intel and AI SOC agents sold and run as a single system, minimum.
- ✓ **Single point of management.** Unified console and control plane for all TDIR operations and response actions.
- ✓ **Native threat intelligence.** Consumable as raw intel, vendor detection content, and cross-product alert enrichment.
- ✓ **Vendor-designed cross-product collaboration.** A control plane (automation/AI) spanning all products, plus shared detection knowledge.
- ✓ **Investigative workbench.** Centralized, enriched, AI-assisted investigations that speed up known-attack response.
- ✓ **Custom monitoring workbench.** Build detections via correlation, behavioral analytics, ML and query building.
- ✓ **Native MDR option.** Managed detection & response from the same provider, on the same technology.
- ✓ **Adjacent coverage.** Identity, cloud/SaaS and exposure management as first-class extensions.
- ✓ **Flexible data management.** Data-lake support and ingestion options that let you control cost by use.
- ✓ **Case management.** Track evidence, communications and collaboration to build an incident.
- ✓ **Open & portable.** OCSF-normalized data and content that isn't trapped in vendor field names.

BUYER FIT

Which path fits which team?

SIEM Platform	Security Data Lake	Integrated SOC ✦
Large, mature teams (20+ operators)	Very high data ingestion	Mid-to-large teams (≤15–20 operators)
Need deep customization & extensibility	Data management is the #1 constraint	Value complexity reduction & outcomes
Many third-party controls	Renewal cost driven by data bloat	Want fastest time-to-value

Note: the three are not mutually exclusive — an ISOC can sit over your data lake and augment or replace a SIEM platform incrementally.

HOW INVINSENSE FLIPS THE NARRATIVE

Built for the changing times.

Invinsense doesn't retrofit a legacy engine — it reframes security operations around three principles the modern SOC actually needs: cloud-native scale, AI-driven operations, and data democracy. Then it adds the one thing legacy SIEM never had: an attacker's mindset.

PRINCIPLE 01

Cloud-Native

Analytics decoupled from storage, federated across globally dispersed, heterogeneous environments.

- SaaS, cloud, on-prem & hybrid — full parity
- Real-time multi-cloud campaign detection
- "Meets you where you are," scales on your terms

PRINCIPLE 02

AI-Driven

Agentic AI and behavioral ML operate across the threat lifecycle — transparent and human-in-the-loop.

- AI triage, threat-hunting & response agents
- Behavioral models over static rules
- OCSF-normalized data that AI can actually reason on

PRINCIPLE 03

Data Democracy

Your data, your lake, your control — open architecture, no vendor lock-in, cost on your terms.

- Bring your own data lake
- Native data pipeline management
- Portable, open OCSF content

◆ The legacy narrative

DATA
Collect less to control cost

DETECTION
Write a rule for every threat

RESPONSE
Humans do the manual work

OWNERSHIP
Data & content locked to the vendor

POSTURE
Detect & respond, after the fact

◆ The Invinsense flip

DATA
Collect everything; route cost intelligently

DETECTION
Model behavior; catch the unknown

RESPONSE
Agents act; humans decide

OWNERSHIP
Open data, open content, your lake

POSTURE
Pre-empt & deceive, before impact

ATTACKER'S MIND · DEFENDER'S BRAIN

Invinsense fuses offense, defense and compliance into one ISOC — CTEM and Automated Moving Target Defense think like the adversary, while UEBA, agentic AI and SOAR defend like a seasoned SOC. Pre-emptive by design, not reactive by patch.

UEBA
Behavioral detection backbone

AI SOC · XDR
Agentic triage & response

OXDR
Exposure & CTEM

OCSF · DPM
Normalization & pipelines

YOUR MOVE

From evaluation to integrated SOC.

You don't have to rip and replace. The fastest path to ISOC value is incremental — augment your current SIEM, prove the outcomes, then consolidate at your pace.

STEP 01

Augment

Layer Invinsense over your existing SIEM and data lake. Normalize to OCSF and light up behavioral detection on data you already have.

STEP 02

Prove

Run a head-to-head: measure MTTR, false-positive rate, data cost and analyst time on real incidents over 4–8 weeks.

STEP 03

Consolidate

Migrate detection content (portable by design), retire redundant tools, and operate the SOC as one integrated system.

BEFORE YOU PUBLISH EXTERNALLY

A note on the numbers

Any outcome figures used alongside this guide (MTTR, false-positive, cost or productivity improvements) should be Infopercept's own validated customer benchmarks. This edition presents the framework; insert verified metrics and named case studies in the final, customer-facing version.

Build your complete AI SOC.

Say goodbye to blind spots, alert overload and data lock-in. See how the Invinsense ISOC reduces risk, gains agility and cuts data cost — across SaaS, cloud, on-prem and hybrid.

Request a Demo →

Talk to a Security Architect

Invinsense ISOC

infopercept.com
gurucul-style ISOC framing
© 2026