SECURITY OPERATIONS

SIEM++ for the Next-Gen SOC

From alert volume to correlated, risk-weighted resilience.

iStreet Network Limited (BSE: 524622)

02 Contents

SECTION 01

In this eBrief

SIEM has moved past being a place to store and search logs. It is now the correlation layer of the SOC: the point where detection, investigation, response, and risk context either come together or stay apart.

What follows covers four pressures shaping security operations today, the capabilities teams now expect from a next-generation platform, and where iStreet SIEM++ fits against each.

SIEM
Security information and event management

SOC
Security operations centre

RBVM
Risk-Based Vulnerability Management

ROC
Resilience Operating Centre

40%

of alerts are never investigated at all.

Coverage keeps expanding across cloud, identity, and endpoint. A single continuous view does not. What arrives is volume without context, and the alert that mattered sits somewhere inside it.

66%
of teams cannot keep pace with daily alert volume

61%
have ignored an alert later found to be critical

46%
of alerts turn out to be false positives

AI SOC Market Landscape 2025; SANS 2025 SOC Survey; Microsoft/Omdia State of the SOC 2026

SECTION 03

Storage is not detection

Roughly a third of what a legacy SIEM holds does any detection work. The rest is archive with a licence fee attached.

Traditional platforms were built to aggregate logs and prove compliance, not to correlate live activity across a distributed footprint. Rules need constant tuning. Ingestion priced by volume turns visibility into a budget decision. The operating burden lands on analysts already stretched thin, and the tooling added to relieve them frequently does the opposite.

35%
of stored SIEM data delivers real detection value

81%
of teams report more workload after adding tools, not less

73%
name false positives their top detection challenge

Red Canary, 2025; SANS 2025 SOC Survey; SANS 2025 Detection & Response Survey

100+

data sources feed a single SIEM, on average.

Cloud, SaaS, identity, endpoint, network, and OT signals each arrive as their own project, with their own connector, cost model, and blind spot. Breadth only becomes an advantage once those sources can be reasoned about as one body of evidence rather than six separate ones.

69%
run 10 or more detection tools

39%
run 20 or more

11
separate consoles managed by the average team

IDC Worldwide Views on SIEM Survey, as reported by Expert Insights, 2026; Vectra AI, 2026; Microsoft/Omdia State of the SOC 2026

Detection, investigation, and response as one workflow

Every handoff between tools is a place where context gets dropped and minutes pass. What teams are asking for is not a faster chain, but fewer links in it — and the reasons they give for bringing AI into the SOC say the same thing.

Reasons cited for adopting, or planning to adopt, AI in security operations. Prophet Security, State of AI in the SOC 2026

What next-gen SOC teams look for

The capability set has shifted from search and storage to correlation, context, and action inside one interface. When buyers rank what matters most in a platform, a real-time detection engine leads, followed by breadth of connectors and freedom over deployment.

Real-time detection

An engine that keeps pace with the speed of the threats it watches for, rather than a scheduled query over yesterday's logs.

Open ingestion

Connectors for every source already running, without a cost curve that turns coverage into a budget argument.

Deployment freedom

On-premises, sovereign, or hybrid, decided by data residency requirements rather than by vendor architecture.

Behavioural analytics

User and entity behaviour analysis that surfaces slow, low-volume activity trending over weeks.

Built-in automation

Correlation, enrichment, and response inside the platform, with no pivot into a second tool to finish the job.

Risk-weighted priority

Alerts ordered by what they could actually reach in this environment, not by a generic severity score.

Feature ranking: IDC Worldwide Views on SIEM Survey, as reported by Expert Insights, 2026

SECTION 07

Essential guidance

01 Automate what is mechanical

There are more alerts than any team can clear. Automation should decide what reaches an analyst, and group related alerts before it does.

02 Ingest for coverage, not for licence economics

Bringing in another source should be an architectural decision rather than a budget one. Gaps in ingestion become gaps in detection.

03 Prioritise by exploitability

A severity score describes a vulnerability. Risk context describes what it could actually reach here. The second should order the queue.

04 Unify the workflow, not just the console

Detection, investigation, response, and case management in one interface is what brings down time to detect and time to resolve. Everything short of that is a dashboard.

Inside iStreet SIEM++

SIEM++ is the correlation layer of the iStreet security portfolio: detection, investigation, response, and risk context operating as one system rather than four integrations.

Cross-domain correlation

Cloud, identity, endpoint, network, and OT telemetry reasoned about as one body of evidence, not one console at a time.

RBVM risk context

Risk-Based Vulnerability Management weights every detection by what it could actually reach, so the queue orders itself by exposure rather than by score.

No pivot to investigate

Enrichment, case management, and response actions inside the same interface that raised the alert.

Sovereign by architecture

On-premises and data-resident deployment as a design property, not a compliance retrofit after the fact.

Behavioural analytics

User and entity behaviour analysis surfacing the slow, low-volume activity that rule-based detection misses.

Continuous compliance evidence

DPDP, RBI, SEBI, and CERT-In alignment produced as an operating output rather than reconstructed for each audit.

How SIEM++ answers each reality

Each pressure in this brief has a specific counterpart in the platform, delivered through the Resilience Operating Centre as one continuous view.

Visibility stops at the edges of each tool.	**One correlated view.** Every connected source contributes to the same evidence set, so a chain of activity reads as one story rather than five fragments.
Legacy SIEM stores far more than it detects on.	**Detection-first ingestion.** Sources are onboarded for the detection value they carry, with cost modelled on architecture rather than on ingest volume alone.
Alert volume exceeds what any team can clear.	**RBVM-weighted prioritisation.** Related alerts are grouped and ranked by exploitability in the environment, so analyst time goes to genuine exposure.
Handoffs between tools cost context and time.	**One workflow through the ROC.** Detection, investigation, response, and compliance reporting sit in a single operating view across AIOps and security operations.

Ready to power your next-gen SOC with SIEM++?

In modern security operations, resilience depends on how quickly a team can separate the signal that matters from everything else arriving alongside it. SIEM++ strengthens that by correlating telemetry across cloud, identity, endpoint, network, and OT, weighting every detection by the risk it actually carries, and closing the gap between an alert and the action it needs. This helps regulated enterprises reduce dwell time, contain incidents earlier, and hold continuous compliance evidence across critical digital services.

Learn more about how iStreet SIEM++ and the Resilience Operating Centre help regulated enterprises strengthen resilience across critical digital services.

Learn More