Decision Lake SIEM - Product Datasheet

Lakehouse-Native SIEM with 100% OCSF Normalisation, a Dedicated Correlation Engine, and Agentic Parser Generation

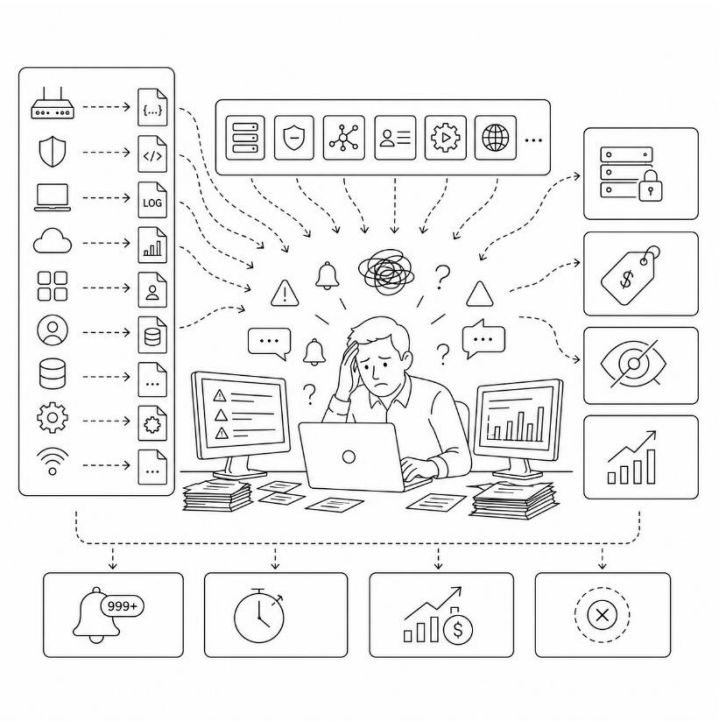
Detect faster. Retain everything. Pay predictably

Current release

The Problem

Security teams face a growing crisis: telemetry arrives in dozens of formats, lives across disconnected tools, and lacks the context needed for fast, effective detection. Traditional SIEMs compound this with rigid architectures, unpredictable licensing, and blind spots that grow as environments scale.

The result: alert fatigue, slow investigations, ballooning costs, and threats that slip through the gaps.



The Decision Lake Approach

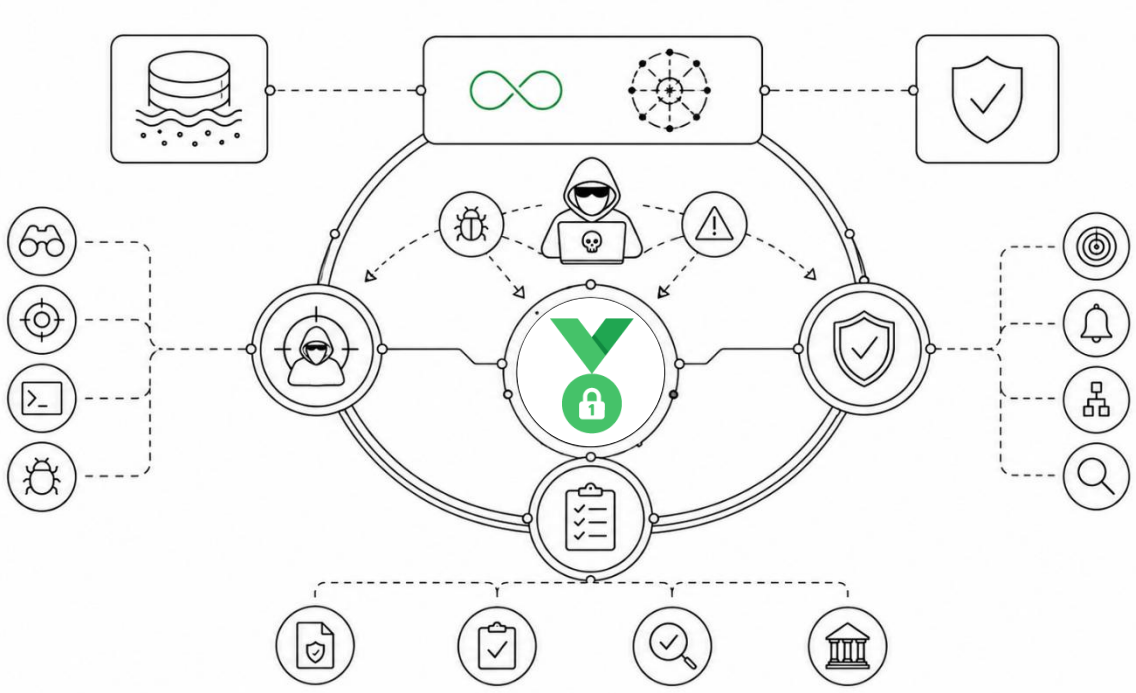
Decision Lake SIEM was built from the ground up to solve these problems. Not patched together from acquisitions, not bolted onto a legacy architecture.

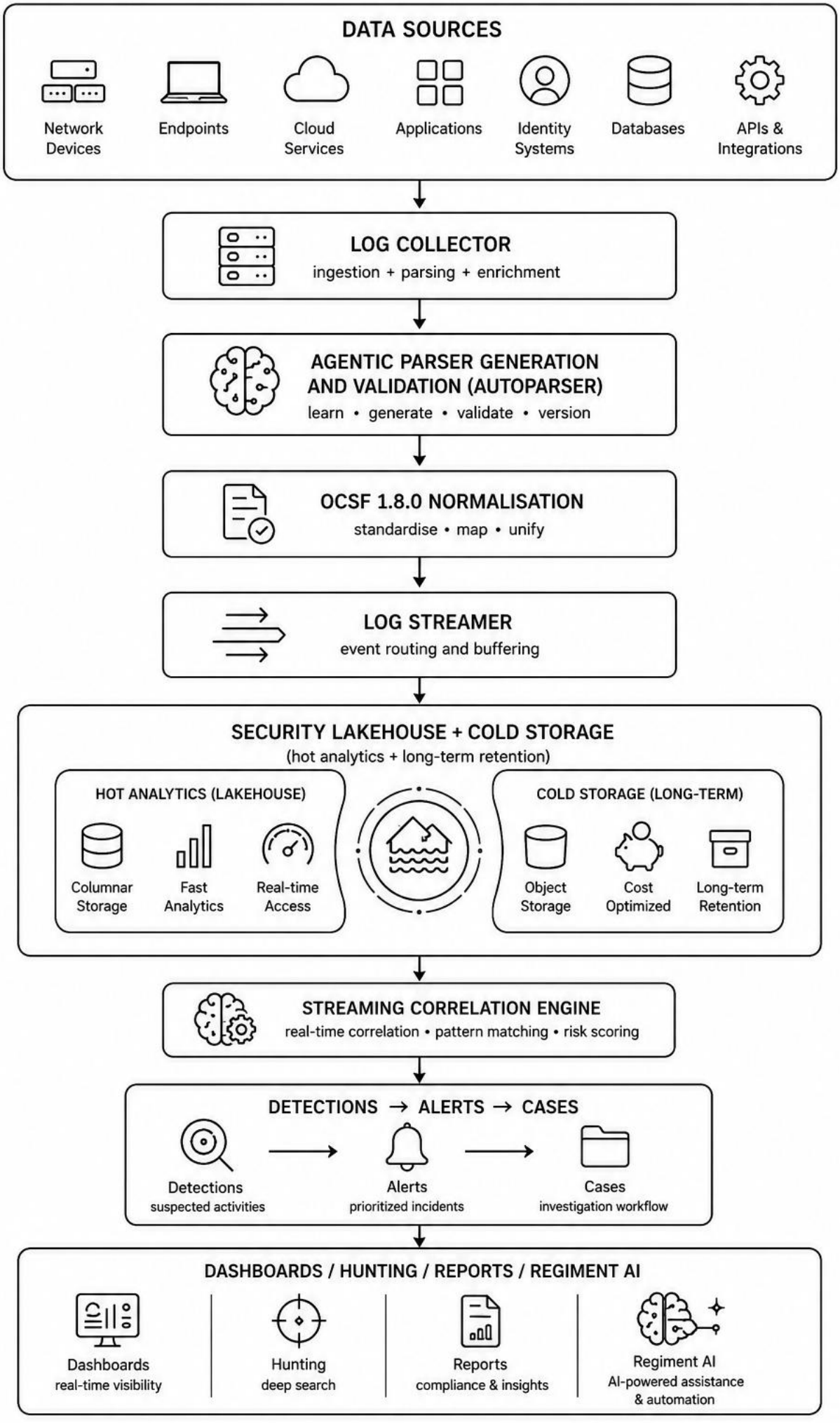
Every event, from every source, is normalised to OCSF 1.8.0 before it enters the Lakehouse. Detections, searches, dashboards, and correlation all operate on a single, consistent data model. No vendor-specific field mapping, no broken queries when sources change, no separate pipeline product to buy and maintain.

Built on a Security Lakehouse architecture with a dedicated streaming Correlation Engine, Decision Lake delivers real-time detection alongside cost-effective, multi-year retention, without compromising on speed, integrity, or investigation depth. With no per-GB ingestion pricing, you never have to choose between visibility and budget.

About Invinsense

Decision Lake SIEM is part of Invinsense, developed by Infopercept. Invinsense is a unified cybersecurity platform built with the mindset of an attacker and the strategy of a defender. It brings defensive, offensive, and compliance-based security into a single operational ecosystem.




DATA SOURCES
Network Devices
Endpoints
Cloud Services
Applications
Identity Systems
Databases
APIs & Integrations
LOG COLLECTOR
ingestion + parsing + enrichment
AGENTIC PARSER GENERATION AND VALIDATION (AUTOPARSER)
learn • generate • validate • version
OCSF 1.8.0 NORMALISATION
standardise • map • unify
LOG STREAMER
event routing and buffering
SECURITY LAKEHOUSE + COLD STORAGE
(hot analytics + long-term retention)
HOT ANALYTICS (LAKEHOUSE)
Columnar Storage
Fast Analytics
Real-time Access
COLD STORAGE (LONG-TERM)
Object Storage
Cost Optimized
Long-term Retention
STREAMING CORRELATION ENGINE
real-time correlation • pattern matching • risk scoring
DETECTIONS → ALERTS → CASES
Detections
suspected activities
Alerts
prioritized incidents
Cases
investigation workflow
DASHBOARDS / HUNTING / REPORTS / REGIMENT AI
Dashboards
real-time visibility
Hunting
deep search
Reports
compliance & insights
Regiment AI
AI-powered assistance & automation

What Makes Decision Lake SIEM Different

1	Security Data Pipeline + SIEM in One Platform	Decision Lake converges two categories the industry has historically treated separately: Security Data Pipeline - ingestion, normalisation, enrichment, routing, and cost-effective storage SIEM - detection, correlation, investigation, and case management While competitors are acquiring data pipeline platforms to bolt onto legacy SIEMs, Decision Lake was built from day one with the pipeline and the analytics on a single, unified architecture.
2	100% OCSF 1.8.0 Normalised Security Data	The ingestion layer performs: • Log collection (agent and agentless) • Parsing and field extraction • Context enrichment (threat intel, asset, identity) • Full normalisation to OCSF 1.8.0 Result: One schema, one query language, one detection foundation across the entire enterprise. No vendor-specific field mapping. No broken dashboards when sources change.
3	Agentic AI Parser Generator (Autoparser)	The biggest operational cost in any SIEM is parser maintenance: new sources, schema drift, vendor updates, and broken mappings consume engineering hours that should go to detection and response. Decision Lake eliminates this with an AI-powered parser generator that autonomously creates, validates, and deploys parsers. What triggers it: • Unknown or new log formats that do not match existing parsers • New fields appearing in previously known formats • Schema drift, vendor updates, or misaligned field mappings • Parsing errors causing incomplete extraction or incorrect mapping How it works (six-gate validation pipeline): • AI generates parsers and maps logs into 100% OCSF 1.8.0 • Every generated parser passes through six validation gates: parser-language syntax, sample execution, OCSF schema conformance, required-field coverage, field-cardinality analysis, and performance benchmarking • Failed gates trigger automatic self-correction with iterative refinement, no human in the loop • Only parsers that pass all gates reach production Outcome: New log sources go from unknown to fully normalised and production-deployed without human intervention. Parser engineering effort drops to near zero while normalisation accuracy stays at 100%.
4	Lakehouse + Cold Storage Architecture	Lakehouse layer for hot analytics: columnar storage with sub-second query performance on structured security data Cold storage layer for economical long-term retention: S3-compatible object storage, Azure Blob, or Google Cloud Storage (on-prem or cloud) Up to 23x data compression - columnar compression dramatically reduces storage costs • Decoupled compute and storage for linear cost scaling • 100% raw log retention - no forced summarisation, no data loss • Configurable lifecycle policies per data source and table: hot retention, hot-to-cold tiering, archive, archive-then-delete, or keep-forever, with an impact preview before any change • Backup and restore - scheduled full or incremental backups with point-in-time restore and a searchable backup catalogue

5

Dedicated Streaming Correlation Engine with 12 Detection Types

A purpose-built streaming engine that evaluates detection logic on events in motion, not after they land in storage.

12 specialised detection and operational types, far beyond the 3 to 4 types offered by most SIEMs:

Type	What It Detects
Pattern Match	Single event matching specific conditions
Threshold	Count-based alerts (e.g., >10 failed logins in 5 min)
Sequence Chain	Ordered or temporal multi-step attack patterns with time constraints (unifies near-in-time event pairs and multi-step sequences)
N-of-M Match	Flexible indicator counting (e.g., 3 of 5 suspicious behaviours)
N-of-M Indicators	Sliding-window indicator accumulation
Wait-State Pattern	Follow-up detection (event A expected but not seen after event B)
Suppression	Deduplication of repeated alerts
Risk Score	Cumulative risk scoring across multiple low-signal events
Beaconing Detection	C2 call back identification (periodic outbound connections)
Diversity Detection	Unique-value counting (e.g., user accessing 50+ distinct hosts)
Data Quality	Pipeline health monitoring (missing fields, parsing failures)
Meta Alert	Alert-on-alert correlation (escalation based on alert combinations)

Key capabilities:

- Multi-source event correlation across endpoints, identity, cloud, and network
- Sequence detection for ordered and temporal attack chains with time constraints
- Hot deployment - deploy, pause, and reactivate detections without pipeline restart
- Detection testing against sample data, plus Retro Scan to run any deployed detection across full history, review every match, and promote real hits into the alert queue (each promoted alert carries a RETRO badge)
- Native SIGMA support - import rules straight from SigmaHQ (paste or GitHub URL) with automatic OCSF field mapping, per-tenant mapping overrides, placeholder expansion, and an import coverage report; export any detection back to SIGMA 2.1 YAML
- Per-rule MITRE ATT&CK and D3FEND mapping
- Rule version history with restore, rule grouping, and active-hours scheduling
- Detection-as-code import/export in native versioned JSON and SIGMA YAML

6

IQL (Decision Lake Query Language)

A purpose-built security query language that lets analysts go from question to answer in seconds. No SQL, no vendor lock-in, no context switching.

Search and Filter:

- Intuitive filter syntax (`severity >= 4 AND src.ip = "10.0.0.1"`); analysts are productive in minutes
- Boolean logic, nested fields, numeric comparisons, wildcards
- Unparsed raw-log search; investigate logs even before normalisation completes

Pipe-based analytics with 40+ commands

- Aggregation, statistics, trend analysis (SMA / WMA / EMA), computed fields, and enrichment
- 22 aggregation functions including percentiles, standard deviation, and time-bucketed analysis
- Inline enrichment (`eventstats`, `streamstats`), GeoIP lookups, and cross-index joins
- Post-aggregation filtering, deduplication, and multi-field sorting
- Anomaly detection (Z-score, IQR) and time-series forecasting built into the query language

Investigation tools

- Field-statistics sidebar: cardinality, top values, distribution per field
- Saved queries with typed, reusable parameters and macro expansion
- Query templates for standardised investigations
- CSV export with streaming support for large result sets (500K+ records, unlimited via async export)
- Dedicated investigation workbench: pivot across events and entities with an interactive entity graph, unified timeline, and one-click PDF report
- Investigation canvas: free-form analysis board that pins log evidence and notes, embeddable on dashboards

<table>
<tr>
<td>7</td>
<td>Regiment AI - The In-Product AI Analyst Assistant</td>
<td>
Regiment AI is the natural-language layer over the entire platform. Analysts ask questions in plain English and Regiment AI runs the right queries on their behalf, then reasons over the results:

Translates questions into IQL, runs searches over events and alerts, and links results straight into Explorer
Summarises incidents and case timelines; explains alerts and detections with full context
Pulls MITRE ATT&CK coverage, threat-intel indicator lookups, datasource and pipeline health, log-streamer lag, and storage metrics on demand
Drafts detection logic and recommends investigative pivots from a plain-language description
Runs long-running analyses as background jobs and notifies you the moment they finish

Built for SOC teams: persistent conversation history, team-shareable conversations, per-user usage and token metering, and admin controls for model and provider (Anthropic or AWS Bedrock), extended-thinking budget, and enable/disable.

Regiment AI uses your existing role-based access controls and tenant scope - it can only see what you can see, and every action is authorised server-side on each call.
</td>
</tr>
<tr>
<td>8</td>
<td>Comprehensive Case Management with Alert-to-Case Automation</td>
<td>
Full incident lifecycle management built into the platform:

Alert-to-case automation - case templates and template mappings auto-create cases from matching alerts, eliminating manual triage for known patterns

Case creation - manual or auto-generated from templates
Status workflow - Open -> In Progress -> Resolved / Closed
Priority and severity - P1 to P4 priority with OCSF severity mapping
SLA tracking with configurable targets per priority:

P1 (Critical): 30 min response, 4 hr resolution
P2 (High): 1 hr response, 8 hr resolution
P3 (Medium): 4 hr response, 1 day resolution
P4 (Low): 8 hr response, 3 day resolution

Investigation tabs per case: Timeline, IOC tracking, discussion threads, task checklists, file attachments, related alerts, attack graph, MITRE technique mapping, metadata and audit trail

Analytics dashboard - MTTA, MTTI, MTTR, SLA compliance, resolution trends, analyst workload, case ageing
</td>
</tr>
<tr>
<td>9</td>
<td>OCSF Transformer Wizard - Visual Parser Creation</td>
<td>
A six-step visual wizard for creating and editing OCSF field mappings:
<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>1</td><td>Log Input - Paste sample logs or search existing events</td></tr>
<tr><td>2</td><td>Parse Log - Extract fields from raw log format</td></tr>
<tr><td>3</td><td>OCSF Mapping - Select event class, map extracted fields to OCSF schema</td></tr>
<tr><td>4</td><td>JSON Preview - Side-by-side validation of input vs OCSF output</td></tr>
<tr><td>5</td><td>OCSF Builder - Conditional mappings, computed variables, observable extraction</td></tr>
<tr><td>6</td><td>Review - Auto-generated transform code, ready for deployment</td></tr>
</table>
Supports conditional mappings, observable extraction (IPs, domains, hashes), and type validation against the OCSF 1.8.0 schema.
</td>
</tr>
<tr>
<td>10</td>
<td>MITRE ATT&CK and D3FEND Mapping</td>
<td>
MITRE ATT&CK Enterprise (v19.1, April 2026):

Interactive tactic-by-technique coverage matrix across all 15 Enterprise tactics
Colour-coded detection coverage (events detected vs gaps)
Sub-technique support with platform filtering (Windows, Linux, macOS, Cloud, Network)
Time-range scoped coverage analysis

MITRE D3FEND (v1.4.0):

Defence-in-depth technique framework
Maps detections to defensive techniques
Complementary view: ATT&CK shows attacker perspective, D3FEND shows defender perspective

</td>
</tr>
</table>

11	Alert Management and Fatigue Reduction	• Alert lifecycle - New -> Open -> In Progress -> Resolved -> Closed • Canonical resolution verdicts - true positive, false positive, benign, duplicate, no action required (one consistent set across the verdict filter and both close actions) • Alert grouping - correlate related alerts into groups • IOC extraction - attach indicators to alerts • Alert fatigue analysis - identify noisy detections, suppression recommendations, trend analysis • Suppression - field-based, time-windowed alert suppression with enable/disable controls • Escalation workflows - auto-escalation based on severity, time, or conditions
12	Threat Intelligence Integration	Built-in threat intelligence with MISP integration and real-time IOC matching: Feed Management: • MISP integration with configurable sync intervals • Multi-feed support with priority-based deduplication • Feed health monitoring and connectivity testing Real-Time IOC Matching: • Automatic matching of incoming events against threat indicators • Support for IPs, domains, file hashes (MD5, SHA1, SHA256), URLs, and email addresses • Events tagged with threat context (threat level, feed source, campaign info) Retro Hunting: • Scan historical event data against current threat intelligence • Identify past compromises that were unknown at ingestion time • Configurable scan ranges and indicator-type filtering Investigation Tools: • IOC lookup for ad-hoc indicator checks • Bulk indicator lookup for rapid triage • Dashboard with match trends, top IOCs, and feed statistics
13	Dashboards, Visualisations, and Reporting	Build the dashboards your SOC actually needs. 18 widget types, no compromises. 15 chart types: Line, Bar, Area, Pie, Metric, Gauge, Histogram, Scatter, Heatmap, Sankey, Funnel, Treemap, Word Cloud, Geo Map, and Data Table. 3 specialised widgets: Text Box (markdown annotations), Investigation Canvas, and Saved Visualisation Reference. Every dashboard supports drag-and-drop layout, live auto-refresh, time range controls, team sharing with permissions, full import/export, and dark/light themes. Reporting: • Automated PDF generation - turn any dashboard or visualisation into a branded, distributable report • Flexible scheduling - daily, weekly, or monthly delivery • Configurable distribution - recipients, custom subject lines, and report scope per schedule • Full report history - status tracking, version history, one-click re-download • Pre-built report templates - SLA compliance, case summary, alert fatigue analysis, executive overview
14	Data Source Onboarding at Scale	Connect any source (cloud, endpoint, identity, network) and start ingesting in minutes, not weeks. • Agent and agentless ingestion - collect from any environment without forcing architectural changes • Multi-protocol support - syslog (TCP/UDP), HTTP, API polling, file collection, custom protocols • Shared-port listener routing - consolidate multiple sources on a single port, intelligently routed by source IP • Zero-downtime configuration - hot-reload on any change, no pipeline restart required • Fault isolation - per-source collection processes ensure one failing source never impacts another Endpoint Agent Management: • Centralised deployment and monitoring of log-collection agents • Real-time health tracking with automatic offline detection • Agent grouping for fleet-wide configuration management • Secure enrolment tokens for zero-touch agent registration • Cross-platform: Linux (DEB/RPM), Windows (MSI), macOS, Docker

		Pipeline Health Monitoring: • Per-source status dashboards with independent Raw and Events liveness, plus a plain-language diagnosis (parsing issue, collection down, raw only) • End-to-end throughput visibility with per-stage and per-source event accounting and data-loss attribution (filtered vs parse errors), peak EPS, and compression economics • Configurable silence thresholds and automated error detection and alerting on collection failures • Built-in connectivity diagnostics per source: TCP port, DNS, TLS certificate, ICMP latency, HTTP probe, and live event sampling
15	Real-Time Alert Delivery and Escalation	Analysts never have to refresh or poll. Critical alerts arrive the instant they fire. • Push-based delivery - alerts stream to the UI in real time, not on a refresh cycle • In-app notification centre - centralised feed with read/unread state and priority filtering • Automated escalation - severity-based, time-based, and condition-based triggers • Email notifications - configurable email alerts for critical and high-severity events
16	Secure Operations and Access Control	Authentication: • Local credentials with password policies • SSO/OIDC support (Google, Azure AD, Okta, Keycloak, generic OIDC providers) • Multi-factor authentication with backup codes • Account lockout and session-idle timeout Authorisation: • Role-based access control with fine-grained permissions • Default roles: Admin, Analyst, Reader • Custom roles with granular permission sets • API key authentication for programmatic access Audit and Compliance: • Complete, tamper-evident audit trail of every user action • Searchable by user, action, resource type, and date range • One-click CSV export for compliance evidence and regulatory audits
17	Outbound Integration Engine	Extend Decision Lake into your existing security stack. Forward alerts and enriched events to any downstream system: • OCSF-aware event filtering - trigger integrations on specific event conditions, not just alert severity • Extensible by design - add new integrations (webhook, SOAR, ticketing, messaging) without core platform changes • Secure credential management - secrets injected at runtime, never stored in integration logic • Test before deploy - execution logging and dry-run mode for validation • Per-integration health monitoring - track delivery success, latency, and failure rates
18	Cloud-Native, Flexible Deployment	Decision Lake SIEM is designed as a cloud-native platform that deploys, scales, and self-heals without manual infrastructure management. • One-command deployment - the entire SIEM stack installs in a single step, fully configured and production-ready • Rolling upgrades - the platform stays available during version upgrades and maintenance windows • Self-healing infrastructure - if any component fails, the platform automatically restarts it and recovers state • Elastic scaling - scale ingestion, storage, and detection independently based on demand • ARM/Graviton support - runs natively on ARM64 processors for up to 40% better price-performance on AWS Graviton instances • Built-in platform monitoring - pre-configured dashboards and alerts for infrastructure health ship out of the box • Multi-protocol log ingestion - accepts logs over syslog (TCP/UDP), Fluent, OTLP, HTTP, and custom protocols on standard ports

Deployment Models:

Model	Description
On-Premises	Full platform in your own data centre or private cloud
Bring Your Own Cloud (BYOC)	Your cloud account (AWS, Azure, GCP) with Infopercept managing the platform
SaaS	Fully managed by Infopercept, zero infrastructure overhead

Capability Snapshot

Core SIEM Capabilities

Capability	Status	Details
Unified security data ingestion	Yes	Agent and agentless, structured and unstructured
Schema normalisation	Yes	100% OCSF 1.8.0
High-fidelity data storage	Yes	Lakehouse (hot) + cold storage (long-term), multi-year retention
Real-time detection	Yes	Streaming Correlation Engine with sub-minute evaluation
Query and analytics engine	Yes	IQL with sub-second Lakehouse queries
Correlation and alerting	Yes	Multi-source joins, windowed aggregation, sequence detection
Investigation workflows	Yes	Case management with timeline, IOCs, tasks, discussions
Detection content	Yes	12 detection types with MITRE ATT&CK mapping, SIGMA import/export, and detection-as-code

AI and Investigation Capabilities

Capability	Status	Details
AI-powered parser generation	Yes	Autoparser with six-gate validation and self-correction
Visual OCSF mapping wizard	Yes	Six-step wizard with preview and code generation
Regiment AI assistant	Yes	Plain-English queries, incident summaries, rule drafting
Real-time detection	Yes	Built in: normalisation, enrichment, routing, filtering
Security data pipeline	Yes	Built in: normalisation, enrichment, routing, filtering |
Context enrichment	Yes	Threat intel, lookup tables, asset context
Threat hunting	Yes	IQL + field stats + saved queries + investigation canvas

Enterprise and Operations Capabilities

Capability	Status	Details
MITRE ATT&CK mapping	Yes	ATT&CK v19.1 (15 Enterprise tactics) with interactive coverage matrix
MITRE D3FEND mapping	Yes	D3FEND v1.4.0 defensive-technique framework

SIGMA rule support	Yes	Bidirectional import (SigmaHQ paste/URL) and SIGMA 2.1 export with OCSF mapping and coverage report
Case management	Yes	Full lifecycle with SLA tracking and analytics
Custom dashboards	Yes	18 widget types, drag-drop, auto-refresh
Reporting	Yes	Scheduled PDF generation, branded templates, history
Alerting integrations	Yes	Escalation, notifications, real-time push
Access control	Yes	RBAC + MFA + SSO/OIDC + audit logging
Alert fatigue management	Yes	Analysis, suppression, trend detection
Alert-to-case automation	Yes	Template mappings auto-create cases from alerts
Real-time push notifications	Yes	Push-based, not polling
Detection types	Yes	12 specialised types
IQL pipe commands	Yes	40+ commands
Investigation workbench	Yes	Entity graph, timeline, pivots, PDF report
Backup and restore	Yes	Scheduled full/incremental with point-in-time restore
Data forwarding (sinks)	Yes	Route raw and normalised streams to object storage, message brokers, and search backends
Connectivity diagnostics	Yes	Per-source TCP/DNS/TLS/ICMP/HTTP and event-sample checks
Outbound integrations	Yes	Webhook, SOAR, custom scripts with OCSF-aware filtering
API access	Yes	RESTful API with OpenAPI docs and API-key auth
Cloud-native deployment	Yes	One-command install, self-healing, rolling upgrades
Multi-deployment	Yes	On-prem, BYOC, SaaS
MSSP multi-tenancy	Yes	Tenant isolation, cross-tenant administration, unified dashboards
Endpoint agent management	Yes	Deploy, monitor, group agents with health tracking
Retro hunting	Yes	Scan historical data against current threat intelligence

Architecture Advantages

Advantage	How It Helps
Streaming Detection	Detections evaluate on events in motion. Minutes, not the hours typical of batch SIEMs
Cross-Source Correlation	Multi-source joins reduce false positives by correlating endpoints, identity, cloud, and network in one detection
Unified Investigation	Single query language across all normalised data: no tool-switching between log search, alert triage, and case management
Extended Retention	Lakehouse (hot) + cold storage architecture enables multi-year retention at a fraction of traditional index-based storage costs
No Per-GB Licensing	Decoupled compute and storage, no per-GB ingestion penalty: costs scale with infrastructure, not data volume
Storage Efficiency	Up to 23x data compression: columnar storage dramatically reduces disk and cloud storage costs
Forensic Depth	100% raw log retention: no forced summarisation, no data loss
Always-On Audit Trail	All telemetry is searchable at any time: compliance evidence and audit data are always accessible, not archived

Capability Snapshot

vs Traditional SIEMs

Dimension	Traditional SIEM	Decision Lake SIEM
Data normalisation	Partial, vendor-specific	100% OCSF 1.8.0
Storage architecture	Monolithic, index-heavy	Lakehouse (hot) + cold storage
Detection model	Batch / scheduled queries	Streaming correlation on events in motion
Parser maintenance	Manual, brittle	Agentic AI with validation
Cost model	Per-GB ingestion pricing	Decoupled compute / storage, predictable
Data retention	30 to 90 days typical	Multi-year with query access
Pipeline integration	Requires add-on	Built-in

vs Next-Gen SIEMs

Capability	Typical Next-Gen SIEM	Decision Lake
Schema normalisation	Partial (ECS or custom)	OCSF 1.8.0 (100%)
Data pipeline	Acquired or bolt-on	Native, built-in
AI parser generation	Not available	Yes (agentic, multi-stage validation)
Visual OCSF mapping wizard	Not available	Yes (six-step)
SIGMA interoperability	Import-only or none	Bidirectional (import from SigmaHQ + export to SIGMA 2.1)
Detection types	Basic	12 specialised types
Streaming correlation	Varies	Yes (dedicated engine)
MITRE ATT&CK + D3FEND	ATT&CK only	Both
Case management	Basic or via separate product	Full lifecycle with SLA
In-product AI assistant	Limited or none	Regiment AI
Query language	Vendor-specific	IQL (pipe-based analytics)
Lakehouse architecture	Varies	Columnar Lakehouse + S3
Deployment options	Typically SaaS-only	On-prem / BYOC / SaaS

Platform Ecosystem

Decision Lake SIEM is not a point product. It is a unified security operations platform where every capability works together natively:

	Case Workflows	Integrated incident management with SLA enforcement and analyst workload tracking
	Threat Intelligence	MISP integration, real-time IOC matching, retro hunts, multi-feed management
	Detection Engineering	streaming detections with MITRE ATT&CK + D3FEND mapping, SIGMA import/export, Retro Scan over history, and detection-as-code workflows
	Compliance and Audit	always-on evidence collection, full audit trails, compliance-ready reporting
	Scheduled Reporting	automated PDF generation with flexible scheduling and full history
	Endpoint Management	centralised agent deployment, health monitoring, fleet configuration
	Outbound Integrations	webhook, SOAR, and custom-script actions triggered by OCSF event conditions
	MSSP Operations	multi-tenant isolation with cross-tenant administration and unified dashboards
	Regiment AI	natural-language assistant covering search, summarisation, and rule authoring
	API-First Architecture	RESTful API with OpenAPI documentation for full automation
	Multi-Protocol Ingestion	syslog (TCP/UDP), Fluent, OTLP, HTTP, and custom protocols via managed ingress

OCSF 1.8.0 Schema Coverage: 83 Event Classes Across 9 Categories

Decision Lake normalises every ingested event into the Open Cybersecurity Schema Framework (OCSF) 1.8.0 before it enters the Lakehouse. All 83 event classes are supported natively with no per-class configuration required.

	System Activity	File System Activity, Kernel Extension Activity, Kernel Activity, Memory Activity, Module Activity, Scheduled Job Activity, Process Activity, Event Log Activity, Script Activity, Peripheral Activity, Registry Key Activity, Registry Value Activity, Windows Resource Activity, Windows Service Activity
	Findings	Security Finding, Vulnerability Finding, Compliance Finding, Detection Finding, Incident Finding, Data Security Finding, Application Security Posture Finding, IAM Analysis Finding
	Identity & Access Management	Account Change, Authentication, Authorize Session, Entity Management, User Access Management, Group Management
	Network Activity	Network Activity, HTTP Activity, DNS Activity, DHCP Activity, RDP Activity, SMB Activity, SSH Activity, FTP Activity, Email Activity, Network File Activity, Email File Activity, Email URL Activity, NTP Activity, Tunnel Activity
	Discovery	Device Inventory Info, Device Config State, User Inventory Info, OS Patch State, Kernel Object Query, File Query, Folder Query, Admin Group Query, Job Query, Module Query, Network Connection Query, Networks Query, Peripheral Device Query, Process Query, Service Query, User Session Query, User Query, Device Config State Change, Software Inventory Info, OSINT Inventory Info, Startup Item Query, Cloud Resources Inventory Info, Live Evidence Info, Registry Key Query, Registry Value Query, Prefetch Query
	Application Activity	Web Resources Activity, Application Lifecycle, API Activity, Web Resource Access Activity, Datastore Activity, File Hosting Activity, Scan Activity, Application Error
	Remediation	Remediation Activity, File Remediation Activity, Process Remediation Activity, Network Remediation Activity
	Unmanned Systems	Drone Flights Activity, Airborne Broadcast Activity
	Base	Base Event (universal fallback for any telemetry type)

About Infopercept - Infopercept is one of the fastest-growing comprehensive cybersecurity companies in India, serving global clients. It provides platform led managed security services that covers all areas of cybersecurity, including defensive, offensive, detection and response, and security compliance. Infopercept has its own cybersecurity platform, 'Invinsense,' which integrates tools such as SIEM, SOAR, EDR, deception, offensive security, and compliance tools. Its cybersecurity and MDR services include dedicated teams of experts, ensuring that organizations have 24x7 cybersecurity operations support.

Imprint

Publisher

3rd floor, Optionz Complex, CG Rd, Opp. Regenta Hotel, Navrangpura, Ahmedabad, Gujarat 380009, INDIA

Contact

sos@infopercept.com

www.infopercept.com