LOG MANAGEMENT & SIEM

Logdefence Edge

Your signals.
A clearer security picture.

Turn logs from your infrastructure into a shared view for security monitoring, investigation and response.

AT A GLANCE

01 Central log collection

02 Parsing & normalization

03 Detection & investigation

04 Raw-data integrity

Deployment size and integration scope are assessed against source formats, event volume, retention needs and infrastructure.

CAPABILITIES & WORKFLOW

From raw events to usable security context.

01 Collect across your infrastructure

Bring server, network, security and application events to a common collection point.

02 Make formats usable

Normalize known formats and investigate unfamiliar ones through Parser Studio and a controlled learning process.

03 Investigate with context

Search by source, device, user, time and event fields; evaluate normalized events against security rules.

04 Preserve the evidence

Keep original logs traceable and support integrity checks alongside role-based central administration.

Log sources

Collection

Parsing & normalization

Detection & investigation

USE CASES & DEPLOYMENT

Scope collection around your infrastructure.

Security operations

Bring events, alarms and source health into a shared investigation workflow.

Data control

Keep security logs in infrastructure selected by your organisation.

Unfamiliar log formats

Review unknown formats and develop parser candidates in a controlled process.

Integration areas: Windows & Linux · Network & firewall logs · Security products · Application logs

Source compatibility is checked during discovery. Parsing, collection method and capacity depend on the actual source and deployment profile.

info@softbytlabs.com