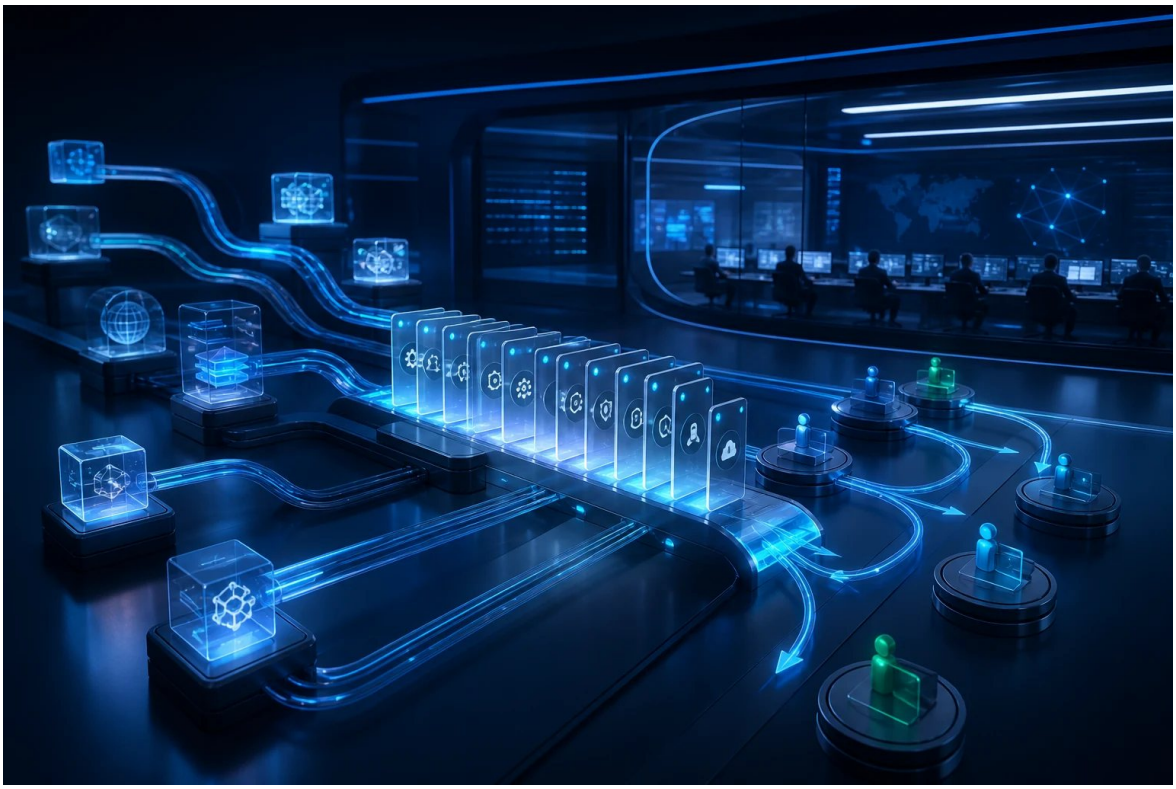
OPERATIONAL SECURITY VISIBILITY

Security Operations

Bring security findings and assurance signals into one operational queue

Help authorised teams triage findings, follow ownership and connect assurance activity to day-to-day security operations.



The value for your team

01

One work queue

Bring approved findings and assurance events into a focused view.

02

Source transparency

Keep connector state and evidence origin visible to operators.

03

Operational follow-through

Track priority, ownership and status without losing technical context.

Product overview

Security Operations provides a protected operating view for findings and assurance signals from approved sources. It is designed to keep connector status truthful, preserve source context and help teams move work forward without relabelling synthetic or disconnected data as live production telemetry.

Security Operations is designed for security operations and assurance teams that need a focused queue across approved customer data sources. It connects finding intake and normalisation, source and connector status and audit-friendly activity history so teams can move from input to accountable action without losing the decision trail.

The product supports the operating workflow; it does not remove professional judgement, statutory responsibility or customer ownership. Final controls, integrations and commercial scope are confirmed during discovery and recorded in the implementation plan.

Customer challenges it addresses

01 Information about finding intake and normalisation, priority and ownership queues and source and connector status often lives in separate tools, inboxes or spreadsheets, making the operating picture difficult to trust.

02 When teams need to triage findings with source context, manual hand-offs can hide ownership, delay decisions and make exceptions harder to resolve.

03 Leaders need a clearer way to achieve operational follow-through while preserving human approval, role boundaries and an understandable record of what happened.

Value created in practice

One work queue

Bring approved findings and assurance events into a focused view.

Source transparency

Keep connector state and evidence origin visible to operators.

Operational follow-through

Track priority, ownership and status without losing technical context.

Detailed capabilities

Six connected capabilities shape the core Security Operations operating experience.

01 Finding intake and normalisation

Keep validated observations connected to supporting evidence, scope and review status throughout the assurance lifecycle.

02 Priority and ownership queues

Organise security work by priority, responsible owner and status so the queue supports action rather than noise.

03 Source and connector status

Keep connector health and source state visible so disconnected or synthetic information is never presented as live telemetry.

04 Assurance event visibility

Make relevant assurance events visible to operations teams without erasing their original engagement context.

05 Operational dashboards

Provide a focused security-operations view of workload and exceptions drawn only from approved sources.

06 Audit-friendly activity history

Preserve a chronological record of significant actions and status changes for operational follow-through and review.

Connected operating model

The capabilities are designed to work together. Finding intake and normalisation establishes context, source and connector status moves the work forward, and audit-friendly activity history supports review and accountability.

How teams use the product

The workflow is intentionally simple to understand, while retaining visible owners, review points and evidence.

01

Connect an approved read-only source

Authorised users combine finding intake and normalisation and priority and ownership queues to connect an approved read-only source. The workflow keeps the responsible owner, review point and resulting action visible.

02

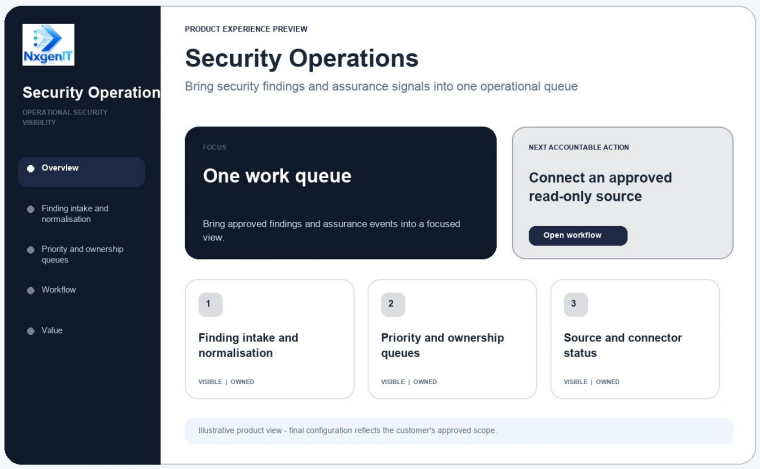
Triage findings with source context

Authorised users combine source and connector status and assurance event visibility to triage findings with source context. The workflow keeps the responsible owner, review point and resulting action visible.

03

Track ownership and operational response

Authorised users combine operational dashboards and audit-friendly activity history to track ownership and operational response. The workflow keeps the responsible owner, review point and resulting action visible.



Illustrative product preview. Final screens and configuration reflect the customer's approved scope.

Rollout, governance and success

A controlled rollout keeps the product aligned to customer ownership, real operating roles and measurable outcomes.

PHASE 01

Discover and scope

Confirm the users, operating boundaries, source data and decisions that Security Operations must support.

PHASE 02

Configure roles and controls

Define authorised roles, approval points, protected information and escalation paths before customer data is introduced.

PHASE 03

Prepare data and connections

Map the required inputs for finding intake and normalisation and priority and ownership queues, including migration or integration needs.

PHASE 04

Pilot, validate and scale

Run a controlled pilot, review outcomes with responsible users, adjust the workflow and expand only after acceptance.

Roles, ownership and control

Security Operations is configured around named users, authorised roles and explicit approval points. Customer data remains customer-owned, protected information is limited to appropriate roles, and important actions retain an understandable history.

What success can look like

- Shorter cycle time across 'Connect an approved read-only source'.
- Fewer unresolved exceptions around source and connector status.
- Clearer ownership of approvals, follow-ups and closure evidence.
- Stronger adoption among the intended users and responsible reviewers.

Best for

Security operations and assurance teams that need a focused queue across approved customer data sources.

See how this product fits your operation

www.nxgenit.co.za/products/security-operations | info@nxgenit.co.za