GENESECURE

GENELLIPSE

SECURITY

Cyber Defense

Security findings connect to business exposure

Core capabilities

The main activities and the information they connect.

Security tool connectors

Normalize signals from the configured tools.

Vulnerability and threat intelligence

Relate exploit context to your asset inventory.

Detection rules and testing

Test and tune detections with retained versions.

SOC case management

Keep alerts, timelines and evidence in an owned case.

From daily work to oversight

Supporting functions keep decisions and evidence current.

Exposure and attack-path graph

Trace exposure toward critical business assets.

Cyber GRC and FAIR analysis

Connect cyber controls to financial risk analysis.

Continuous control evidence

Collect evidence from the configured platform state.

Co-managed SOC and MSSP workflows

Coordinate analyst queues and client oversight.

How the work moves

A proposed operating workflow for your evaluation.

01

Connect

Ingest permitted security and asset signals.

02

Prioritize

Relate exposure to exploit signals and critical assets.

03

Investigate

Build the case timeline and supporting evidence.

04

Respond

An authorized owner approves consequential actions.

A finding gains meaning through context

The relationships that make the workflow understandable.

01

Finding

The vulnerability or detection.

02

Asset

Ownership, identity and business criticality.

03

Path

The relationship to a critical service.

04

Case

The investigation, approved response and proof.

An exposed server has a known exploited weakness

An illustrative finding affects an internet-facing service with access to a critical business system.

Team response

Validate the asset and exposure, check the attack path, and open an owned case. Review containment impact before approving a response.

Decision point

Containment authority remains with the authorized security and service owners.

What changes for your team

The practical value to evaluate against your current process.

More context for triage

Asset criticality and attack paths help analysts assess which findings need attention first.

Less reconstruction after response

The case retains the timeline, approved action and evidence needed for subsequent review.

Where this module connects

Confirm the interfaces and available data for the intended deployment.

Sources	Defender, Sentinel, CrowdStrike, Wiz, Tenable, Qualys or Wazuh where configured.
Connected modules	Cyber Risk Intelligence, Compliance and Risk Management.
Working outputs	Prioritized cases, response records and control evidence.

What to validate in your evaluation

Use a representative case and agree the acceptance evidence before expansion.

Security operations	Validate detections and approve response actions.
Evidence	Retain rule versions, event context and case timelines.
Measure	Track triage time, false positives and overdue material exposures.

A focused walkthrough Cyber Defense

Bring a representative workflow, its source records and the people who own the decision.

Starting point

An exposed server has a known exploited weakness

Working session

Follow the case from input through review to retained evidence.

Genellipse.com

genesecure.ca