GENESECURE

GENELLIPSE

SECURITY

Cyber Risk Intelligence

An explainable view of cyber posture

Core capabilities

The main activities and the information they connect.

Security rating and trend

Follow posture changes and explain their drivers.

Risk-vector breakdown

Inspect the domains contributing to the rating.

External attack surface discovery

Review public assets within an authorized scope.

Exploit-aware prioritization

Combine exploitation signals with business context.

From daily work to oversight

Supporting functions keep decisions and evidence current.

Vendor cyber profiles

Relate external posture to supplier evidence.

Identity and credential exposure

Route exposed identities and access risks to owners.

Brand and phishing intelligence

Investigate impersonation and phishing signals.

Executive risk reporting

Show exposure, concentration and remediation context.

How the work moves

A proposed operating workflow for your evaluation.

01

Discover

Identify authorized external assets and exposures.

02

Explain

Relate score movements to specific risk drivers.

03

Prioritize

Consider exploit signals and business criticality.

04

Report

Show owners, material exposures and remediation trends.

A rating is the beginning of the explanation

The relationships that make the workflow understandable.

01

Posture

The overall movement over time.

02

Drivers

Exposure, identity, hygiene and control signals.

03

Context

Critical assets and supplier concentration.

04

Action

The investment or remediation decision to review.

A rating improves while one critical exposure remains

Several hygiene issues close, but an important public service still has an unresolved material exposure.

Team response

Review the risk-vector detail and asset criticality. Keep the material exposure visible in the executive report and assign its owner.

Decision point

An aggregate score does not replace review of the underlying findings.

What changes for your team

The practical value to evaluate against your current process.

A more explainable risk conversation

Show why the rating moved and which material exposures remain open.

A clearer investment discussion

Connect remediation priorities to critical services and supplier concentration.

Where this module connects

Confirm the interfaces and available data for the intended deployment.

Sources	Authorized asset discovery, exposure feeds and vendor evidence.
Connected modules	Cyber Defense, Vendor Risk and Trust Center.
Working outputs	Rating explanations, exposure priorities and board reporting.

What to validate in your evaluation

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

Security and vendor owners	Confirm assets and validate exposure context.
Evidence	Retain source timestamps, score drivers and remediation records.
Measure	Track unknown assets, stale findings and time to resolve material exposures.

A focused walkthrough Cyber Risk Intelligence

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

Starting point

A rating improves while one critical exposure remains

Genellipse.com

Working session

Follow the case from input through review to retained evidence.

genesecure.ca