Three products for security decisions that must survive scrutiny

Secure records the infrastructure. Assure examines the application. SOAR drafts the response. Together they carry one decision from observation to an approved response your team carries out.

Secure

Exposure management
Decision: Record the systems, services and exposure its collector can see on networks you authorize, and the key exchange a service selects in a TLS 1.3 test connection.
Customer keeps: A record of what was seen (not proof the network is complete), imported cloud context, and the questions that still need evidence.

Assure

Code security (engineering candidate)
Decision: Tie application findings to the exact source line, record how far each was checked, and list the cryptography the code calls. Not yet approved for your source code, for installation at your site, or for production use.
Customer keeps: Source references, how far each finding was checked, coverage gaps, and an owner where one is assigned.

SOAR

Detection and response
Decision: Connect supplied evidence to investigation, rehearsal on a rehearsal copy, and a drafted response approved by risk class (automatic with a log for the lowest class; named people above that).
Customer keeps: A reproducible investigation, explicit assumptions and a drafted response. Your team makes the change; SOAR does not re-check your systems afterwards.

One service, three decisions

A maintenance window begins with an unidentified device. Secure records what its collector can see. Assure examines the nominated application source and cryptographic use. SOAR investigates the operational question and drafts a response approved by risk class; your team makes any change. The same service identifier and review window connect the story.

Each product can stand alone

Start with the decision that matters now. Cross-product context depends on explicit asset-to-service-to-repository mapping and configured integrations; a similar name does not establish the relationship.

What the customer keeps

Each stage leaves an inspectable record: accepted input, source and time, evidence or assumption, the decision and how it was approved, the accountable owner, and the next check your team runs.

A business-unit CISO can identify each product, choose the right starting point and ask for the evidence that supports the next decision.

Bring the evidence together without losing its limits

A complete business-unit view depends on agreed scope, identity and time. Buying a product does not establish those relationships automatically.

With or without SOAR

Secure and Assure can be evaluated as separate products. SOAR adds an investigation and response workspace; it should not be described simply as the mandatory backend for both. Supported imports can bring estate evidence into SOAR. Automatic Secure-to-Assure synchronization and a unified group risk dashboard are not established by this overview. Agree installed integrations and commercial scope during pilot design.

Use a common review window

Scans need not start at the same second. Name the BU, site, service, source revision, collector vantage point and evidence timestamps. For an incident, narrow the time window. For migration planning, agree a freshness threshold and refresh changed records. Keep unmatched assets and stale inputs visible.

Keep these questions separate

Origin

Observed, imported, inferred or simulated.
What the label establishes: How the claim was produced. A modeled route remains modeled even if approved.

Review

Confirmed, refuted or unresolved.
What the label establishes: What the available checks support. Refutation rejects a claim; confirmation is limited to the evidence checked.

Action

Proposed, approved by risk class, or changed by your team.
What the label establishes: What happened to the change. Your team makes production changes; a later Secure or Assure run shows the new state, and SOAR does not re-check.

Read only as deeply as the decision needs

Start with each product's executive overview and evaluation brief. Use the four-page manager guide to revisit the workflow and the full product book for screenshots, operating steps and technical detail. Use the separate pilot outline to agree inputs, owners, success measures and the decision about expansion.

Establish the group reporting boundary

Assign a business-unit owner and access boundary, map shared services explicitly, and agree which summaries group reviewers may see. Report coverage, unresolved risks, accepted exceptions and freshness by business unit. Treat the initial group summary as a governed reporting process until automated cross-unit behavior is demonstrated.

The group can ask one coherent question while retaining each product record, evidence boundary and accountable owner.