KASEWARE

Security Operations Maturity Scorecard

1 — Ad Hoc
Reactive and informal. Siloed and inconsistent.

2 — Developing
Repeatable in places. Processes forming.

3 — Established
Defined and consistent. Measured and managed.

4 — Mature
Optimized and adaptive. Drives business value.

1. DETECTION & AWARENESS

	1	2	3	4
Can you see early signs of risk outside classified channels?	○	○	○	○
Can you connect open-source signals to internal cases?	○	○	○	○
Can you view risk by asset, location, and severity?	○	○	○	○

2. WORKFLOW & RESPONSE

	1	2	3	4
Can your team move from alert to action in one process?	○	○	○	○
Can cyber, physical, and investigations teams work from the same facts?	○	○	○	○
Can you show who acted, when they acted, and why?	○	○	○	○

3. BUSINESS PROOF

	1	2	3	4
Can you show response time trends?	○	○	○	○
Can you show reduced manual work?	○	○	○	○
Can you show risk reduction by site or asset?	○	○	○	○
Can you brief leadership without a manual scramble?	○	○	○	○

4. INVESTMENT DEFENSE

	1	2	3	4
Can you link spend to outcomes?	○	○	○	○
Can you show what risk grows without action?	○	○	○	○
Can you explain the cost of delay?	○	○	○	○

OUTCOME MAPPING

RISK REDUCTION
Average Score: _____
How well you identify, prioritize, and reduce exposure

FASTER RESPONSE
Average Score: _____
How quickly you move from signal to action

OPERATIONAL EFFICIENCY
Average Score: _____
How well your model reduces manual effort and tool friction

DECISION CONFIDENCE
Average Score: _____
How well leadership can see risk, action, and impact

SCORE INTERPRETATION

1.0–1.9	REACTIVE	High risk. Ad hoc and inconsistent.
2.0–2.9	EMERGING	Progress in motion. Not yet consistent.
3.0–3.5	OPERATIONAL	Processes in place. Measured and managed.
3.6–4.0	MATURE	Optimized and adaptive. Delivers measurable value.

EXECUTIVE SUMMARY

OVERALL MATURITY SCORE

(Average of all responses)

SUMMARY

KASEWARE

Scorecard Definitions

Use this with the scorecard to accurately rate each category

Score each statement from 1 to 4 based on your current model.

1 Ad Hoc
Manual effort. Inconsistent process. Limited visibility.

2 Developing
Some parts work. Gaps remain. Teams use workarounds.

3 Established
Process works in a consistent way. Teams can repeat it across most cases.

4 Mature
Connected, measurable, and easy to use. Leaders can act with confidence.

Category	Assessment Question	1	2	3	4	Primary Outcome(s)
Detection & Awareness	Can you see early signs of risk outside classified channels?	Depend on informal monitoring or outside alerts	Monitor some sources; coverage is limited	Track open sources in a repeatable way	Ongoing visibility into external risk signals tied to assets and operations	Risk Reduction; Faster Response
Detection & Awareness	Can you connect open-source signals to internal cases?	Signals stay separate from investigations	Staff connect them by hand when time allows	Teams link external signals to cases in a defined process	External signals flow into casework in a structured, traceable way	Faster Response; Decision Confidence
Detection & Awareness	Can you view risk by asset, location, and severity?	Risk lives in separate files or systems	You can piece it together with manual effort	You can view risk in a consistent format	Clear, shared view of risk by asset, site, and priority	Risk Reduction; Decision Confidence
Workflow & Response	Can your team move from alert to action in one process?	Handoffs are manual and slow	Some steps connect, but gaps remain	Most alerts move through a defined workflow	Alert, assessment, response, and case actions happen in one connected process	Faster Response; Operational Efficiency
Workflow & Response	Can cyber, physical, and investigations teams work from the same facts?	Teams work in silos	Teams share updates by email or meetings	Teams can access common case details	Teams work from a shared operating picture across functions	Faster Response; Decision Confidence
Workflow & Response	Can you show who acted, when they acted, and why?	Actions are hard to trace	Some actions are logged, but not in one place	Most actions are documented in a standard way	Actions, decisions, and rationale are fully traceable	Decision Confidence; Risk Reduction
Business Proof	Can you show response time trends?	You do not track them	You track them for some cases	You report them on a regular basis	You track and use them to improve operations and justify investment	Faster Response; Decision Confidence
Business Proof	Can you show reduced manual work?	You cannot measure it	You have anecdotal proof only	You track some time savings	You can show clear reductions in manual effort and staff burden	Operational Efficiency
Business Proof	Can you show risk reduction by site or asset?	You describe risk in general terms	You can show limited examples	You can measure change for key assets or sites	You can show risk trends by asset, site, and priority level	Risk Reduction; Decision Confidence
Business Proof	Can you brief leadership without a manual scramble?	Briefings require last-minute effort	Briefs are possible, but slow	Briefs follow a repeatable format	Leaders get timely, consistent, decision-ready updates	Operational Efficiency; Decision Confidence
Investment Defense	Can you link spend to outcomes?	Spend and outcomes are not connected	You can describe the link, but not prove it well	You can connect some investments to measurable results	You can show how investment affects risk, speed, efficiency, and leadership visibility	Decision Confidence; Operational Efficiency
Investment Defense	Can you show what risk grows without action?	You cannot show likely exposure	You can describe risk in broad terms	You can explain likely impact in key areas	You can show how delay or inaction increases risk by asset, site, or mission area	Risk Reduction; Decision Confidence
Investment Defense	Can you explain the cost of delay?	You cannot quantify delay	You can describe cost in general terms	You can estimate some cost areas	You can show how delay affects response, disruption, staff time, or recovery cost	Faster Response; Operational Efficiency