

CORE FUNCTION BRIEF

KPIs and SLAs

A core function of the ClearSkies iISOC platform

Live status, breach risk flagged before the deadline, and metrics that are never read alone.

Contents

1	Executive Summary
----------	--------------------------

2	Why Unmanaged Reporting Falls Short
	A metric that never changes a decision
	Breaches discovered after they happen
	A single metric hides the truth
	The same numbers, retold at the wrong altitude
	The cost of the workaround

3	How KPIs and SLAs Works
	The five stages
	How a prediction is judged

4	KPIs and SLAs in the Platform
	What it draws on, what it writes back, and what it does not do
	A worked example
	Delivery across many tenants

5	Compliance and Reporting Framework Alignment
----------	---

6	Questions Raised in Evaluation
----------	---------------------------------------

7	The Benefits
	At a glance
	What changes, and for whom
	What sets it apart

8	Summary
----------	----------------

SECTION 1

Executive Summary

IN ONE SENTENCE.

KPIs and SLAs is the core function that defines what to measure, tracks every open incident against its live target, predicts a breach before the deadline passes, and reports metrics in pairs so a single green number never hides the whole picture.

A metric nobody acts on is dashboard clutter rather than a control. A monthly spreadsheet reports a breach after it happened rather than flagging it while there is still time to act. A compliance rate on its own can hide an unhappy customer who is technically satisfied. And a report built for an executive rarely serves the analyst who needs a different number at a different moment.

KPIs and SLAs answers this with a five-stage mechanism. Measurement is organized into four layers, executive, service-level, operational and experience, each built for the decision its audience owns. Every open incident carries a live countdown against its applicable target, and a breach-risk model scores tickets before the deadline passes rather than after. The resulting status and risk flags are published into the shared model for other core functions to act on, and metrics are always reported in pairs, delivery against perception, speed against stability, on a cadence matched to each audience.

Because the four layers draw on the same underlying data, an executive and an analyst are never looking at figures reconciled from separate systems. They are looking at the same measurement stack rendered at a different altitude, so a number cited in a board report and a number an analyst investigates trace back to one source rather than two.

THE FUNCTION IS PRECISELY SCOPED.

KPIs and SLAs measures, tracks and reports. It does not decide how urgent an incident is, which is the Risk Scoring Formula. It does not decide who works it or reassign it, which is Intelligent Alert Routing. And it does not escalate or execute a response, which is SOAR and Playbooks. It defines no commercial tier or price: that is a platform commercial decision rather than a measurement one.

Five stages

Define, track, predict, publish, report

Four layers

Executive, service-level, operational, experience

Read in pairs

Never delivery without perception

SECTION 2

Why Unmanaged Reporting Falls Short

Measurement is underinvested relative to the rest of the security operation, and the consequences surface as a number nobody trusted rather than as a single visible failure. Four failure modes explain why, and each is answered by a named stage of the mechanism in section 3.

2.1 A metric that never changes a decision

A dashboard full of numbers nobody acts on is clutter rather than control, and without a defined trigger attached to each one there is no way to tell which numbers matter until someone decides that by convention, inconsistently, each time. The dashboard grows more crowded with every reporting cycle without becoming more useful.

2.2 Breaches discovered after they happen

A spreadsheet compiled monthly reports what already went wrong. By the time a breach appears in a report the window to act pre-emptively has closed, and the report becomes a record of the miss rather than a chance to prevent it.

2.3 A single metric hides the truth

Compliance without customer-experience data hides an unhappy customer who is technically satisfied, and response speed without reliability data hides a service that reacts fast but fails often. Either number alone reads as good news that a paired figure would immediately complicate.

2.4 The same numbers, retold at the wrong altitude

An executive drowning in ticket-level detail and an analyst missing the one number that matters right now are both symptoms of a single report trying to serve every audience at once. Neither gets the number their decision actually needs.

2.5 The cost of the workaround

The usual response is a manually compiled report assembled before each business review, reconciling numbers from several consoles by hand. The cost scales with the number of audiences and cadences a provider has to serve, while the underlying problem, metrics that are not organized by decision and not tracked live, is untouched.

Industry research on service management consistently ties manual, spreadsheet-based reporting to significant analyst and manager time, and separately finds customer churn linked to experience decline that a compliant number alone did not surface, though the specific figures are not yet sourced for this brief.

SECTION 3

How KPIs and SLAs Works

KPIs and SLAs is one continuously operating mechanism native to the TDIR core, not a report compiled before a meeting. Incident activity enters at one end, and a live, paired, audience-matched measurement leaves at the other.

Figure 1. The five-stage measurement mechanism.

3.1 The five stages

Each stage is named once here and referenced by name throughout the rest of this brief, paired with the failure mode from section 2 that it answers.

STAGE	WHAT HAPPENS	THE FAILURE MODE IT ANSWERS
Define	Metrics are organized into four layers, executive, service-level, operational and experience, each drawing on the same underlying data but built for the decision its audience owns.	The same numbers, retold at the wrong altitude
Track	Every open incident carries a live countdown, continuously compared against its applicable target as elapsed time accrues, with a defined status: on track, approaching, at risk or breached.	A metric that never changes a decision
Predict	A model scores each open incident for breach risk from incident metadata, analyst workload, ticket age and external context, moving a ticket to at risk before its deadline passes rather than after.	Breaches discovered after they happen
Publish	The current status and any at-risk flag are published into the shared model, for Intelligent Alert Routing and SOAR to act on. This function does not itself reprioritize, reassign or escalate.	A metric that never changes a decision
Report	Metrics are always delivered in pairs, delivery against perception, speed against stability, on a cadence matched to each audience.	A single metric hides the truth

Predict hands off at the flag. What happens to an at-risk ticket after that, whether it is reassigned, escalated or accelerated, is a decision Intelligent Alert Routing or SOAR makes, using the flag this function published.

3.2 How a prediction is judged

Quality is measured rather than assumed, on definitions a provider can report and a customer can audit. The measures below are reported natively and per tenant. They are defined here because the same metric name is measured differently by different vendors, and target values are agreed per engagement rather than asserted.

MEASURE	THE DEFINITION USED	WHAT A POOR VALUE TRIGGERS
Prediction accuracy	Breach-risk predictions confirmed correct against the actual outcome, as a share of all predictions.	A retraining review of the model against recent misses.
Lead time	Elapsed time between an at-risk flag and the incident's actual deadline.	A review of whether the flag threshold fires early enough to be useful.
Pairing completeness	Published KPIs presented with their defined paired counter-metric, as a share of all published KPIs.	A review of the report template for the missing pair.
Report timeliness	Scheduled reports delivered on their configured cadence, as a share of all scheduled reports.	Investigation of the cadence or the audience layout that is slipping.
Metric-to-decision rate	Published metrics tied to a named decision or trigger, as a share of the full metric set.	A review of the audience layer carrying metrics nobody acts on.

A flag that does not become a breach is not a false alarm. An at-risk ticket that is reassigned in time and never breaches is Predict and Publish working exactly as intended. Judging the model only by how many predicted breaches actually occurred undercounts every one it helped prevent.

SECTION 4

KPIs and SLAs in the Platform

4.1 What it draws on, what it writes back, and what it does not do

What it draws on. Incident metadata, timing and the score the Risk Scoring Formula publishes; assignment and workload data from Intelligent Alert Routing; action and outcome timestamps from SOAR and Playbooks; and each tenant's configured target for the incident in question. Each is an input to a specific stage rather than a general capability the function generates itself.

What it writes back. Computed KPIs, live status and breach-risk flags, published into the shared model. Intelligent Alert Routing and SOAR consume an at-risk flag to consider reprioritization or escalation, and scheduled reports deliver the paired metrics to each audience. The relationship is one way: nothing returned to this function changes a status or a prediction already published.

What it does not do. It does not decide urgency, assignment or response, and it defines no commercial service tier or price, which is a platform commercial decision rather than a measurement one. It holds no telemetry of its own beyond the incident metadata and timing already present in the shared model.

4.2 A worked example

The chain below is illustrative and technically representative rather than drawn from a named engagement. A critical incident carrying a fast response commitment is assigned to an analyst already holding a heavy ticket load. Track shows the countdown approaching its threshold. Predict combines the analyst's current load, the historical resolution time for this incident type and the elapsed time into a high breach-risk score, moving the ticket to at risk well before the deadline. Publish surfaces the flag. Intelligent Alert Routing reads it and reassigns the ticket to an available analyst at the appropriate tier, and the incident resolves inside its commitment. Report shows the save the next morning: the prediction, the reassignment and the met deadline read together rather than as a bare compliance percentage, so the manager sees why the commitment held rather than only that it did.

4.3 Delivery across many tenants

Targets, report cadence and audience layout are configured per tenant, so the same five-stage mechanism serves every tenant's commitments without a bespoke reporting build. What travels between tenants is the measurement mechanism itself; what never travels is one tenant's incident data or performance history. The layers, the pairing discipline and the breach-risk model are the same framework applied to a different set of targets and a different incident history, so adding a customer does not add a reporting project.

Because the function is switched on with the platform rather than deployed separately, time to value is a matter of configuring targets and layers rather than an onboarding project. In the first week, targets are configured and Track begins carrying a live countdown for every open incident. Through the first month, Predict accumulates enough history for prediction accuracy and lead time to become meaningful per-tenant figures rather than defaults. At steady state, pairing completeness and report timeliness are tracked as ongoing measures.

SECTION 5

Compliance and Reporting Framework Alignment

KPIs and SLAs does not map detection content and does not compute technique relevance, so MITRE ATT&CK plays a minimal role for this subject. The frameworks that matter here are the ones governing outcome reporting and audit evidence, which the function is built to produce.

FRAMEWORK OR STANDARD	ITS ROLE IN KPIS AND SLAS
NIST Cybersecurity Framework 2.0	Outcome language for the executive layer of the measurement stack, used in board and executive reporting on overall security posture rather than on any single incident.
ISO/IEC 27001 and 27002	Control mapping and the audit evidence a compliance report produces, drawn from the same measurement stack an internal audience already reads.
NIS2, DORA and GDPR	European reporting, resilience and privacy obligations the framework evidences, each with its own reporting cadence and audience that the Define stage can accommodate as a layer.

Reporting evidences a duty. It does not discharge one. The platform states which obligations the measurement stack produces evidence for. It never states that reporting alone makes an organization compliant, and control-level mapping is held by the Regulatory Frameworks core function.

SECTION 6

Questions Raised in Evaluation

The questions below recur in buyer evaluations, each answered directly against the mechanism described in section 3.

QUESTION, AS A BUYER ASKS IT	ANSWER
Does KPIs and SLAs decide how to respond to a breach risk?	No. It publishes the at-risk flag. Intelligent Alert Routing and SOAR decide whether to reprioritize, reassign or escalate. The function's role ends at a correctly timed, correctly scoped flag.
Does this framework define commercial service tiers or pricing?	No. Tier and pricing structures are commercial decisions made elsewhere. This function measures and reports against whatever target a tenant is configured with.
How is a breach prediction validated?	Prediction accuracy is tracked against actual outcomes, and lead time, meaning how much warning a flag gives, is reported alongside it, so the model is judged on both correctness and timeliness.
Can a metric be reported without its paired counterpart?	The framework's own discipline is to report metrics in pairs. A metric presented alone is treated as an incomplete picture rather than a valid report, whatever audience is reading it.
Does the same dashboard serve an analyst and an executive?	No. The measurement stack organizes into four layers by audience, and each sees the numbers built for the decision they own rather than a version of someone else's report.
Can reporting cadence be customized per tenant?	Yes. Daily, weekly and monthly cadences are configured per tenant and per audience, though the underlying data is the same regardless of how often a given audience sees it.

SECTION 7

The Benefits

Measurement is where a security operation either proves what it delivered or asks to be believed, and the outcomes are countable: how many commitments were saved rather than reported on, how many numbers tie to a decision, and whether a board figure and an analyst figure come from the same place.

7.1 At a glance

BENEFIT	WHAT PRODUCES IT
A commitment at risk is saved rather than reported on	Predict scores an open incident before the deadline, and Publish surfaces the flag while there is still time to act.
One green number cannot stand in for the picture	Report pairs delivery with perception and speed with stability, every time.
Each audience gets the number its decision needs	Define organizes measurement into four layers drawing on the same underlying data.
A board figure and an analyst figure agree	One measurement stack rendered at different altitudes, rather than two systems reconciled by hand.
A metric that changes nothing does not survive	Metric-to-decision rate, defined in section 3.2, makes an unused metric visible.
Audit evidence is a by-product of operating	The same stack an internal audience reads produces the control mapping a compliance report needs.

7.2 What changes, and for whom

Live, paired measurement changes what each role spends time on, and what each role can act on before it becomes a problem.

ROLE	WHAT CHANGES
SOC analyst	A shift starts with a prioritized queue and a predicted risk rather than a backlog and a breach discovered in a monthly report.
SOC manager	Workload distribution and assurance become visible, real-time numbers, so a staffing decision is informed by the current queue rather than last month's.
CISO and risk	Executive KPIs arrive paired and at the altitude a board needs, with evidence traceable to a defined framework rather than assembled ahead of each review.
Service provider practice lead	The same measurement stack reports consistently across every tenant, without a bespoke build per customer or per cadence.

7.3 What sets it apart

- ▶ **Every metric changes a decision.** A number not tied to a defined trigger does not earn a place in the framework, so the dashboard stays a working tool rather than accumulating figures nobody consults.
- ▶ **Breach risk flagged before the deadline, not after.** Predict surfaces an at-risk ticket while there is still time to act on it, which turns the deadline into a threshold that triggers action rather than a line a report crosses afterwards.
- ▶ **Metrics are read in pairs, never alone.** Delivery is always paired with perception and speed with stability, so one green number cannot hide the whole picture from the audience reading it.

THE VALUE IN ONE LINE.

Retrospective reporting tells an organization what it missed. Live, paired measurement tells it what it is about to miss, in time to do something, and shows the number next to the one that would contradict it.

SECTION 8

Summary

KPIs and SLAs is how the platform proves that the rest of it is working. It is one core function among twelve, scoped to a five-stage measurement mechanism that runs continuously inside the TDIR core rather than as a report compiled before a business review.

- ▶ Define, track, predict, publish and report replace unmanaged, retrospective measurement.
- ▶ Every open incident is tracked continuously against its target, and breach risk is flagged before the deadline passes.
- ▶ The function publishes the at-risk flag. Intelligent Alert Routing and SOAR decide what happens next.
- ▶ Metrics are always read in pairs and delivered at the altitude each audience needs.
- ▶ The function measures, tracks and reports, and leaves urgency, assignment, response and commercial structure to the functions and decisions built for them.

Forward-looking statement: any statement about future capability is forward-looking and non-binding, and capability described in the present tense is capability available at the publication date, subject to the deployment configuration in force. This document describes measurement and reporting capability and does not constitute legal advice on any customer's regulatory obligations.