Ontinue

Cyber Defence Metrics Guide

Ontinue Metrics Library: KPI + Measurement Points + Altitude + Audience

Metric	Strategic / Operational / Tactical	Board / CISO / Mgmt	What it measures	How to calculate (sudo measurement entry)	Measurement points (Old / baseline)	Measurement points (New / AI-instrumented)
MTTD (Mean Time to Detect)	STRATEGIC OPERATIONAL TACTICAL	Board, CISO	Speed of detection vs attacker activity	detection_time – incident_start_time (or proxy, could be file creation time in the case of Malware vs detection/incident creation)	incident_start_time (if known), first_detection_time	Same + note if AI influenced correlation time: ai_correlation_start/end
TTD (Time to Detect) per incident	TACTICAL	CISO, Mgmt	Incident-specific detection latency	first_detection_time – incident_start_time	incident_start_time, first_detection_time	Same + ai_assist_flag for detection correlation
MTTQR (Mean Time to Qualified Response)	OPERATIONAL TACTICAL	CISO, Mgmt	Speed from alert to validated conclusion	validated_time – alert_created_time	alert_created_time, validated_time	Add ai_enrichment_start/end, ai_summary_start/end, ai_confidence
MTTI (Mean Time to Investigate)	OPERATIONAL TACTICAL	CISO, Mgmt	Speed from alert to investigation start	updated_time – alert_created_time	alert_created_time, validated_time	Add ai_enrichment_start/end, ai_summary_start/end, ai_confidence
TTN (Time to Notify)	OPERATIONAL TACTICAL	CISO, Mgmt	Speed from validation to customer notification	customer_notified_time – validated_time	validated_time, customer_notified_time(email/Teams/ticket)	Same + ai_draft_start/end (if AI drafts notification)
Containment time (provider-led)	STRATEGIC OPERATIONAL TACTICAL	CISO, Mgmt	Speed to contain when provider can act	containment_complete – validated_time	validated_time, containment_complete	Add automation_exec_start/end, human_approval_time (if gated)
Containment time (customer-led)	STRATEGIC OPERATIONAL	CISO, Mgmt	Speed of handoff when customer must act	handoff_sent – validated_time + track customer completion separately	validated_time, handoff_sent, customer_complete_time	Add ai_recommendation_start/end, ai_confidence, handoff_quality_score
MTTR (Mean Time to Respond/Remediate)	STRATEGIC OPERATIONAL	Board, CISO	End-to-end response speed	remediation_complete – detection_or_validation_time	detection_time or validated_time, remediation_complete	Add automation telemetry + approval gating timestamps

Ontinue

High/Critical SLA attainment	OPERATIONAL TACTICAL	Board, CISO, Mgmt	Reliability against promised response	% cases meeting SLA	sla_target, case_open/notify/contain timestamps	Same + include "AI vs non-AI" split for transparency
Case aging distribution	OPERATIONAL	Mgmt	Backlog health and risk of missed SLAs	bucket open cases by age	case_open_time, current_time, case_status	Same + add "automation queue delay" fields if any
Backlog approaching SLA breach	OPERATIONAL	Mgmt	Near-term service risk	count cases within X% of SLA window	sla_due_time, current_time, case_status	Same
Peak-hour performance (p90 TTN/MTTI/Containment)	OPERATIONAL	CISO, Mgmt	Stability under load	compare p90 during peak vs baseline	all relevant timestamps + peak_window_id	Same + "AI assist rate during peak"
False Positive Rate (FPR)	OPERATIONAL TACTICAL	Mgmt	Signal quality / noise reduction	false_positives / total_alerts	alert_id, disposition=false_positive	Same + flag if AI recommended disposition: ai_disposition, ai_confidence
Alert-to-incident conversion rate	OPERATIONAL TACTICAL	Mgmt	How much alert volume becomes real work	validated_incidents / total_alerts	alert_id, incident_linked, validated=true	Same
Precision by severity (High/Critical)	STRATEGIC OPERATIONAL	CISO, Mgmt	Accuracy where it matters most	true_high / all_high_flagged	initial_severity, final_validated_outcome	Same
Severity accuracy	OPERATIONAL	CISO, Mgmt	Correctness of initial severity calls	initial_severity == final_severity rate	initial_severity, final_severity	Same + if AI suggested severity: ai_severity_suggestion, accepted/rejected
Reopen rate	OPERATIONAL TACTICAL	Mgmt	Quality + completeness of closures	reopened_cases / closed_cases	case_closed_time, case_reopen_time, reopen_reason	Same + "AI-assisted vs not" split
Escalation quality (rework needed)	OPERATIONAL	CISO, Mgmt	Whether escalations are actionable	% escalations needing follow-up due to missing info	escalation_id, rework_flag, missing_fields	Same + AI completeness checks: ai_completeness_score
Evidence completeness rate	OPERATIONAL TACTICAL	Mgmt	Whether cases include artifacts/timeline	% cases meeting evidence checklist	artifact list: logs_attached, timeline_present, ioc_list	Same + ai_evidence_summary_generated
Customer clarity score	STRATEGIC OPERATIONAL	CISO	Whether customer understood impact/next steps	survey score or QC rubric (hard to measure)	survey response, case link	Same
Time-to-actionable summary (TTAS)	OPERATIONAL	CISO, Mgmt	How fast customers get a usable narrative	actionable_summary_sent – validated_time (or alert time)	validated_time, summary_sent_time	Add ai_summary_start/end, human_edit_time

Customer involvement rate (CIR)	STRATEGIC OPERATIONAL	CISO	How much work the customer must do	% incidents requiring customer action	customer_action_required_flag, action_count	Same + "AI-resolved vs not"
Self-contained resolution rate	STRATEGIC OPERATIONAL	CISO	% resolved without customer data/actions	resolved_without_customer / total_resolved	customer_action_required_flag=false	Same + if AI performed triage/closure: ai_assist_flag
Detection change failure rate	TACTICAL	Mgmt	Stability of detection engineering	rollbacks / deployments	deployment_id, rollback_flag	Same
Time-to-fix noisy detections	TACTICAL	Mgmt	Responsiveness to noise	fix_deployed – noise_logged	noise_logged_time, fix_deployed_time	Same
Detection coverage growth	STRATEGIC TACTICAL	CISO, Mgmt	Coverage expansion over time	new detections per period + mapped scope	detection_added_time, detection_scope	Same
Telemetry health / ingestion uptime	OPERATIONAL	Mgmt	Whether monitoring has blind spots	% required sources healthy	source_status, last_ingested_time	Same
Playbook success rate	OPERATIONAL TACTICAL	Mgmt	Reliability of response automation	successful_runs / total_runs	playbook_run_id, status	Same + include AI-triggered runs separately
Automation utilization rate	OPERATIONAL TACTICAL	Mgmt	How often automation meaningfully contributes	% cases with successful automation step	automation_step_executed=true	Same + ai_triggered_automation=true
Automation "hours returned"	OPERATIONAL TACTICAL	CISO	Effort reduction (provider + customer)	estimated time saved vs baseline	baseline task timing estimates	Use measured: ai_time_saved_estimate, workflow durations
Utilization rate (internal)	OPERATIONAL	Mgmt	Capacity consumption	consumed_hours / available_hours	staffing schedules + time tracking	Same
Forecast accuracy (case volume)	OPERATIONAL TACTICAL	Mgmt	Predictability of workload	% error / MAPE	forecast_volume, actual_volume	Same
Noise growth rate	OPERATIONAL TACTICAL	CISO, Mgmt	Whether alert fatigue is trending up/down	MoM change in low-value alerts	low_value_alert_count_by_month	Same
Stability index (service variance)	OPERATIONAL TACTICAL	CISO, Mgmt	Whether performance is consistent	variance of TTN/MTTI/MTTR over time	KPI time series	Same
Investigation Quality Score (IQS)	OPERATIONAL TACTICAL	CISO, Mgmt	Quality of investigations (QC sampled)	sampled checklist score	qc_sample_id, qc_checklist_scores	Same + include "AI-assisted" attribute

Severity downgrade/upgrade rate	OPERATIONAL TACTICAL	Mgmt	Triage calibration	% that shift severity materially	initial_severity, final_severity	Same
Root-cause recurrence (30/60/90)	STRATEGIC	Board, CISO	Whether fixes stick	repeats / total	root_cause_tag, incident dates	Same
Time-to-improve (gap → fix deployed)	STRATEGIC OPERATIONAL TACTICAL	CISO, Mgmt	Continuous improvement velocity	fix_deployed – gap_logged	gap_logged_time, fix_deployed_time	Same
Business impact avoided (case-based)	STRATEGIC	Board, CISO	Outcomes tied to business risk	narrative + evidence, count + examples	incident reports + customer confirmation	Same