Ontinue

CISO/Board Metrics (Security Scorecard)

Core Security Metrics Library (CISO)

Metric	Strategic / Operational / Tactical	Audience (Board / CISO / Mgmt)	What it measures	How to calculate (summary)	Measurement points (Old / baseline)	Measurement points (New / continuous + AI)
Material incident rate	STRATEGIC	Board, CISO	Frequency of business-impacting security events	count per quarter + trend	incident register, PIRs	automated incident classification + impact tagging (impact_category, loss_estimate, downtime_hours)
Business impact (loss / downtime)	STRATEGIC	Board, CISO	Real-world consequence	sum loss + downtime, by incident class	finance + ops incident records	enriched mapping to services/apps + automated outage correlation
Cyber risk trend (top risks)	STRATEGIC	Board, CISO	Whether risk is rising or falling	top risks with likelihood/impact movement	risk register updates	continuous control scoring feeding risk register + AI-assisted risk narrative
Control effectiveness score (top 10 controls)	STRATEGIC	Board, CISO	Whether key controls work as intended	% passing tests / continuous checks	annual audits, point-in-time testing	continuous control monitoring (CCM): pass/fail + drift over time
Attack surface exposure index	STRATEGIC OPERATIONAL	CISO, Mgmt	How exposed you are to internet-borne attack	weighted count of exposed assets + criticality	CMDB + occasional scans	EASM/ASM feeds + real-time exposure changes + ownership mapping
Crown jewel coverage	STRATEGIC	Board, CISO	Whether critical apps/data have required controls	% crown jewels meeting baseline	spreadsheets + manual reviews	automated policy checks (MFA, logging, EDR, backups) per app/service
Security spend efficiency(optional)	STRATEGIC	Board, CISO	"Are we buying risk reduction?"	cost per avoided/mitigated risk / per incident trend	budget vs incidents (rough)	mapped investments to measurable control improvements and incident reductions

Ontinue

Identity & Access (IAM) – typically the highest ROI set for CISOs

Metric	Strategic / Operational / Tactical	Audience	What it measures	How to calculate	Old measurement points	New measurement points
MFA coverage (workforce)	STRATEGIC OPERATIONAL	CISO, Mgmt	Reduction in account takeover risk	% users with MFA enforced	IAM reports, periodic checks	conditional access policy compliance + "actually used MFA" rate
Phishing-resistant MFA coverage	STRATEGIC	CISO	Strength against modern phishing	% users on FIDO2/WHfB/certs	IAM config review	auth method telemetry + per-role enforcement
Privileged account protection	STRATEGIC	CISO, Mgmt	Safety of admin paths	% privileged identities with MFA + PIM + JIT	manual privileged lists	continuous privileged inventory + JIT usage logs
Privilege sprawl	STRATEGIC OPERATIONAL	CISO, Mgmt	Over-entitlement risk	count/ratio privileged users over time	quarterly access reviews	entitlement graph + "unused privilege" detection
Time to revoke access (joiner/mover/leaver)	STRATEGIC OPERATIONAL	Mgmt	How quickly access is removed/changed	revoke_complete – HR termination_time	ticket timestamps	automated HR-to-IAM workflows + real-time deprovision telemetry
Risky sign-in containment time	OPERATIONAL	Mgmt	Speed to neutralize suspected compromise	containment – detection	SOC/ticket timestamps	identity protection alerts + automated session revoke + device posture tie-in

Endpoint & Device Security

Ontinue

Metric	Strategic/Operational	Audience	What it measures	How to calculate	Old measurement points	New measurement points
EDR coverage	STRATEGIC	CISO, Mgmt	Visibility + detection capability	% endpoints reporting healthy	asset lists + EDR console	continuous heartbeat + "coverage by criticality"
Endpoint health compliance	OPERATIONAL	Mgmt	Whether endpoints are in policy	% meeting baseline (disk, AV, tamper, FW)	occasional audits	continuous posture assessment + drift alerts
Patch compliance (critical)	STRATEGIC OPERATIONAL	CISO, Mgmt	Exposure to known exploitation	% critical patches within SLA	monthly patch reports	real-time patch telemetry + exploitability weighting
Mean time to remediate critical endpoint vuln	OPERATIONAL	Mgmt	Remediation speed	remediated – discovered	scanner timestamps	scanner + EDR + CMDB correlation with ownership
Unsupported OS / EOL footprint	STRATEGIC	CISO	Structural risk	count of EOL assets by criticality	periodic inventory	continuous inventory + network discovery
Device isolation / containment success	OPERATIONAL	Mgmt	Effectiveness of response action	% isolation actions succeed	SOC notes	EDR action logs + automated verification

Vulnerability & Exposure Management

Ontinue

Metric	Strategic	Audience	What it measures	How to calculate	Old measurement points	New measurement points
Critical vuln exposure (internet-facing)	STRATEGIC	Board, CISO	"How close to headline risk are we?"	count of exploitable critical vulns on exposed assets	scanner + manual tagging	EASM + KEV/exploit intel + service criticality weighting
Time-to-remediate by severity	OPERATIONAL	Mgmt	Operational performance	median + p90 remediation time	scan cycles	continuous scanning + ticket automation
KEV / exploited-in-the-wild backlog	STRATEGIC OPERATIONAL	CISO, Mgmt	Risk tied to active threat	count + age of KEV items open	manual KEV crosswalk	automated KEV matching + aging dashboard
Exception rate	OPERATIONAL	CISO, Mgmt	Where policy is being bypassed	exceptions count + duration	spreadsheet exceptions	workflow-based exceptions with expiry + compensating controls tracked
Risk-based vuln score	STRATEGIC	CISO	Prioritization quality	weighted score by exploitability + asset criticality	CVSS-only	EPSS/KEV + business criticality + exposure + control context

Email & Collaboration Security (high-frequency breach vector)

Ontinue

Metric	Strategic/Operational	Audience	What it measures	How to calculate	Old measurement points	New measurement points
DMARC enforcement	STRATEGIC	CISO	Brand + spoofing protection	DMARC policy level + % passing	DNS checks	continuous monitoring + aggregate report trends
Phish click rate / report rate	STRATEGIC OPERATIONAL	CISO, Mgmt	User resilience	clicks per campaign; reports per 1,000 users	periodic simulations	continuous campaign telemetry + real phish reporting
Mailbox takeover rate	STRATEGIC	Board, CISO	Outcome: compromise frequency	count per month/quarter	incident tickets	identity + email telemetry correlation
Time to contain BEC	OPERATIONAL	Mgmt	Speed to stop financial fraud	detection → revoke sessions/rules reset	manual steps tracked	automated playbooks + time-stamped actions

Cloud & SaaS Security Posture

Metric	Strategic	Audience	What it measures	How to calculate	Old measurement points	New measurement points
Cloud misconfiguration exposure	STRATEGIC	CISO, Mgmt	Preventable cloud risk	count of critical findings open	CSPM periodic scans	continuous CSPM + IaC policy-as-code gating
Public storage exposure	STRATEGIC	Board, CISO	High-impact data risk	count of public buckets/containers	occasional audits	continuous discovery + auto-remediation evidence
Cloud identity posture	STRATEGIC OPERATIONAL	CISO, Mgmt	Privilege and auth strength in cloud	% privileged roles w/ JIT + MFA	manual role reviews	continuous role graph + drift alerts
Logging coverage for cloud control plane	OPERATIONAL	Mgmt	Forensics and detection readiness	% subscriptions/accounts with required logs on	config review	continuous policy compliance + “last event received”

Data Security & Privacy

Ontinue

Metric	Strategic	Audience	What it measures	How to calculate	Old measurement points	New measurement points
Sensitive data discovery coverage	STRATEGIC	CISO	Where sensitive data lives	% repositories scanned/classified	manual classification	continuous DLP/classification + discovery scanning
Data exfiltration detection time	STRATEGIC OPERATIONAL	CISO, Mgmt	How fast you detect major leakage	detection – exfil start (or proxy)	incident review estimates	network + endpoint + SaaS telemetry correlation + AI-assisted triage
DLP policy effectiveness	OPERATIONAL	Mgmt	Whether DLP is tuned	true blocks vs noise; override rate	manual sampling	continuous DLP outcomes + false positive labeling
Key management / encryption coverage	STRATEGIC	CISO	Baseline data protection	% critical systems encrypted + keys managed	audit checks	continuous config compliance + key rotation telemetry
Privacy incident rate	STRATEGIC	Board, CISO	Regulatory risk	count and severity	privacy incident log	integrated security+privacy classification + response timelines

Resilience (Ransomware readiness, recovery, continuity)

Ontinue

Metric	Strategic	Audience	What it measures	How to calculate	Old measurement points	New measurement points
Backup coverage for crown jewels	STRATEGIC	Board, CISO	Ability to recover critical services	% crown jewels backed up to policy	manual mapping	continuous backup policy compliance
Restore success rate (tested)	STRATEGIC OPERATIONAL	Board, CISO	"Backups that restore" reality	successful restore tests / tests run	occasional tabletop claims	automated restore tests + evidence artifacts
RPO/RTO attainment (tested)	STRATEGIC	Board, CISO	Business continuity capability	% services meeting targets	annual DR exercises	continuous DR evidence + recovery telemetry
Ransomware containment time	STRATEGIC OPERATIONAL	Board, CISO	Whether you can stop spread fast	detection → isolate/contain	incident timestamps	EDR action logs + network segmentation events + approval gates
Immutable backup adoption	STRATEGIC	CISO	Protection against backup wiping	% critical backups immutable	policy review	continuous configuration evidence

Third-Party & Supply Chain

Metric	Strategic	Audience	What it measures	How to calculate	Old measurement points	New measurement points
Critical vendor coverage	STRATEGIC	CISO	Whether key vendors are assessed/monitored	% critical vendors reviewed	annual questionnaires	continuous monitoring + attestation freshness
Vendor risk remediation time	OPERATIONAL	Mgmt	Speed to fix vendor findings	close time – finding date	email chains	workflow timestamps + SLA
Concentration risk	STRATEGIC	Board, CISO	Single points of vendor failure	count of crown jewels per vendor	manual mapping	dependency mapping + service criticality

Governance & Program Health

Ontinue

Metric	Strategic	Audience	Board, CISO	How to calculate	Old measurement points	New measurement points
Policy compliance (top policies)	STRATEGIC OPERATIONAL	CISO, Mgmt	Whether key security policies are followed	% compliant controls	audits	continuous policy-as-code checks
Security training completion + effectiveness	OPERATIONAL	Mgmt	Whether people are improving	completion + phish performance shift	LMS stats	role-based training + behavioral telemetry
Security debt index	STRATEGIC	CISO	Accumulated risk from known gaps	weighted backlog (EOL, KEV, misconfigs)	manual aggregation	automated scoring from vuln/CSPM/ASM sources
Time-to-close audit findings	OPERATIONAL	Board, CISO	Governance execution	close date – finding date	audit tracker	workflow + evidence attachments
Security OKR delivery	STRATEGIC	Board, CISO	Execution against plan	% OKRs on track	quarterly updates	automated evidence from control telemetry
Budget	OPERATIONAL	Board, CISO	Execution against plan	% of budget allocated % of budget overspend	Accounts	