



OSMSTM
ACADEMY

OSMSTM Starter Guide

From zero to working security reporting in 30 days

5 KPIs · 30 days · no new tools

Version 1.0 · July 2026 · opensecuritymetrics.org

Why this guide?

The Open Security Metrics Standard (OSMS™) currently contains 327 KPIs across 39 domains. That is its strength – and, for newcomers, its biggest hurdle. The good news: nobody starts with 327 KPIs. Nobody should.

This guide shows the shortest path from zero to a working security reporting practice: **five KPIs, thirty days, no new tools**. Everything you need, you most likely already have.

OSMS in 60 seconds

What it is: An open, vendor-neutral standard for security metrics. Every KPI comes fully defined – with formula, calculation logic, and guidance on data sources.

How it is structured: KPIs are organised into domains (e.g. SOC – Detection & Response, Vulnerability Management, Human Risk & Security Behavior). Each KPI follows one of six calculation archetypes – such as Ratio, Duration, or Count. Four levels lead from operational detail metrics (L1) to the management and board view (L4).

What it ships with: Ready-made mappings to NIST CSF 2.0, ISO/IEC 27001/27004, CIS Controls v8.1 and MITRE ATT&CK, as well as to DORA, NIS2 and CRA. The entire catalog is machine-readable (osms-catalog.yaml).

The core idea: You no longer have to invent metrics. Definition, formula and compliance mapping are already there. You choose – and measure.

The starter principle: 5, not 300

Every metric you introduce needs three things: a data source, an owner, and a consequence. With five KPIs, that is manageable. With fifty, it fails.

Run every candidate through the **Three-Question Test**:

1. **Available?** Is the data already in a system you run today (EDR, SIEM, scanner, ticketing)?
2. **Influenceable?** Is there a person or team that can actually move the number?
3. **Actionable?** Would a deterioration trigger a concrete response?

Three times yes → a suitable starting KPI. Even one no → later.

The recommended starter set

Five KPIs that pass the Three-Question Test in almost every organisation and together paint a surprisingly complete picture – visibility, detection, response, vulnerabilities, and the human factor. All five carry the catalog's highest priority (P0, MVP-1):

1. Endpoint Protection Coverage · OSMS ID: **END-001** · Archetype: **Ratio**

Share of endpoints, servers and workloads with an installed, activated, and policy-conformant endpoint protection (EPP/EDR/XDR).

Formula: assets with policy-conformant protection ÷ all assets in scope × 100

Data source: EDR/XDR console + inventory (CMDB, AD, MDM)

Why first: Visibility is the foundation of all detection. Every unprotected internet-facing machine is a blind spot of the detection.

2. Mean Time to Detect (MTTD) · OSMS ID: **SOC-002** · Archetype: **Duration**

Time from the event start (or first observable activity) to detection by the SOC.

Formula: median(detection – occurrence) per incident

Data source: SIEM, SOC ticketing

Field tip: Use the median rather than the mean – single outliers distort the picture.

3. Mean Time to Respond (MTTR) · OSMS ID: **SOC-003** · Archetype: **Duration**

Time from detection to full remediation or recovery.

Formula: median(resolution – detection) per incident

Data source: incident ticketing

Field tip: For fine-grained steering, split into MTTA (acknowledgement) and MTTC (containment) – the standard defines all three spans.

4. Internet-facing Critical SLA Compliance · OSMS ID: **STD-016** · Archetype: **Ratio**

Share of critical internet-exposed vulnerabilities that were treated within the defined SLA.

Formula: findings remediated/mitigated within SLA ÷ internet-facing critical findings due × 100

Data source: vulnerability scanner, ticketing

Why: Focuses on the outer shell – where attackers arrive first. An SLA percentage every audience understands and that triggers action immediately.

5. Phishing Report Rate · OSMS ID: **HRM-002** · Archetype: **Ratio**

Share of delivered phishing simulations that were correctly reported via the reporting path.

Formula: reported simulations ÷ delivered simulations × 100

Data source: awareness platform, mail gateway

Why this instead of the click rate: The reporting rate measures the desired behaviour – a stronger signal of security culture than the pure failure rate.

One of the five doesn't fit? Replace it from this pool: MFA coverage, patch compliance, backup restore success rate, confirmed incidents per month. What matters: it stays at five.

The first 30 days

Week 1 – Select and assign owners

One meeting, 60 minutes, the right people in the room. Pick five KPIs (starter set or your own candidates via the Three-Question Test) and assign **exactly one owner per KPI**. Not two, not “the team” – one person.

Outcome: *A list of 5 KPIs and 5 names.*

Week 2 – Check data sources

For each KPI, clarify: Which system holds the data? Who has access? Can it be exported (CSV is enough)? If a source is missing: swap the KPI from the replacement pool – don't wait for the source to appear someday.

Outcome: *Data-source check for all five KPIs.*

Week 3 – First measurement: manual is allowed

Collect each value once – by hand, via export, in Excel. Automation comes later. Along the way, document a short **fact sheet** per KPI:

KPI name	[from the OSMS catalog]
OSMS ID	e.g. END-001 (see starter set)
Definition / formula	
Data source(s)	
Owner	
Measurement frequency	monthly
Baseline (month 1)	
Thresholds (from M3)	Green ≥ ... Amber ... Red < ...

Outcome: *Five completed fact sheets with first values.*

Week 4 – First report: one page is enough

A one-pager: reporting month, five KPIs with value, trend arrow and RAG status, three sentences of commentary, one decision or need. Present it in an **existing** meeting – no new slot, no new committee.

Outcome: *First report delivered; the repeat for month 2 is in the calendar.*

What you do NOT need at the start

- **No dashboard tool.** Excel or Sheets is fully sufficient for the first months.
- **No automation.** Manual collection is perfectly fine in the first quarter.
- **No perfect data.** An honest 80-percent number beats a perfect number that never arrives.
- **No targets from day 1.** Measure a baseline for three months first, then set RAG thresholds.
- **No new meeting.** Reporting belongs in a meeting that already exists.

Five pitfalls – and how to avoid them

1. **Too many KPIs at once.** Ten half-maintained metrics are worthless; five well-kept ones build trust.
2. **Perfectionism about data quality.** Whoever waits for clean data never starts. Measure, name the gaps, improve.
3. **KPIs without owners.** A metric without a responsible person is orphaned within two months.
4. **Measuring without consequence.** If red triggers no reaction, the RAG status is decoration. Every threshold needs an agreed follow-up.
5. **Tool before question.** First clarify which questions the reporting must answer – then talk about tooling. Never the other way round.

After 30 days: the growth path

Months 2–3: Stabilise the rhythm, complete the baseline, set RAG thresholds. Then add 3–5 more KPIs – every new candidate passes the Three-Question Test.

Months 4–6: Gradually automate data collection (exports, scripts). Introduce first drill-downs: from the aggregated metric to its operational drivers. Use the OSMS mappings to derive NIS2 and DORA evidence directly from existing KPIs – instead of maintaining parallel compliance lists.

From month 6: Build the management and board view (level L4 of the standard). From here on, expand quarterly rather than monthly – stability beats growth.

Checklist

- ☐ 5 KPIs selected via the Three-Question Test
- ☐ Exactly one owner named per KPI
- ☐ Data sources checked (access + exportability)
- ☐ 5 fact sheets completed
- ☐ First measurement done (manual is fine)
- ☐ One-pager created
- ☐ Reporting slot fixed in an existing meeting
- ☐ Month-2 date is scheduled

Resources

Standard & catalog: opensecuritymetrics.org

Machine-readable KPI catalog: osms-catalog.yaml (v0.9.1, YAML/JSON)



OSMS™ is a trademark. All frameworks and standards mentioned (NIST CSF, ISO/IEC 27001/27004, CIS Controls, MITRE ATT&CK) are the property of their respective owners.

Editorial notes – remove before publication

1. Figures and KPI IDs verified against osms-catalog.yaml v0.9.1 (as of 2026-07-05): 327 KPIs, 39 domains. Starter set: END-001, SOC-002, SOC-003, STD-016, HRM-002 – all P0/MVP-1.
2. ™ applies until EUIPO registration; switch to ® afterwards.