



OSMSTM
ACADEMY

OSMSTM Starter Guide

In 30 Tagen zum funktionierenden Security-Reporting

5 KPIs · 30 Tage · keine neuen Tools

Version 1.0 · Juli 2026 · opensecuritymetrics.org

Warum dieser Guide?

Der Open Security Metrics Standard (OSMS™) umfasst derzeit 327 KPIs in 39 Domänen. Das ist seine Stärke – und für Einsteiger die größte Hürde. Die gute Nachricht: Niemand startet mit 327 KPIs. Niemand sollte es.

Dieser Guide zeigt den kürzesten Weg von null zu einem funktionierenden Security-Reporting: **fünf KPIs, dreißig Tage, keine neuen Tools**. Alles, was Sie brauchen, haben Sie vermutlich schon.

OSMS in 60 Sekunden

Was es ist: Ein offener, herstellerneutraler Standard für Security-Kennzahlen. Jeder KPI ist fertig definiert – mit Formel, Berechnungslogik und Hinweisen zu Datenquellen.

Wie es aufgebaut ist: Die KPIs sind in Domänen organisiert (z. B. SOC – Detection & Response, Vulnerability Management, Human Risk & Security Behavior). Jeder KPI folgt einem von sechs Berechnungs-Archetypen – etwa Ratio (Anteil), Duration (Zeitdauer) oder Count (Anzahl). Vier Ebenen führen von operativen Detail-Metriken (L1) bis zur Management- und Board-Sicht (L4).

Was es mitbringt: Fertige Mappings zu NIST CSF 2.0, ISO/IEC 27001/27004, CIS Controls v8.1, MITRE ATT&CK sowie zu DORA, NIS2 und CRA. Der gesamte Katalog liegt maschinenlesbar vor (osms-catalog.yaml).

Der Kern: Sie müssen keine Metriken mehr erfinden. Definition, Formel und Compliance-Bezug sind bereits da. Sie wählen aus – und messen.

Das Starter-Prinzip: 5 statt 300

Jede Kennzahl, die Sie einführen, braucht drei Dinge: eine Datenquelle, einen Verantwortlichen und eine Konsequenz. Bei fünf KPIs ist das leistbar. Bei fünfzig scheitert es.

Nutzen Sie für die Auswahl den **3-Fragen-Test**:

- 1. Verfügbar?** Liegen die Daten heute schon in einem vorhandenen System vor (EDR, SIEM, Scanner, Ticketing)?
- 2. Beeinflussbar?** Gibt es eine Person oder ein Team, das den Wert tatsächlich verändern kann?
- 3. Handlungsrelevant?** Würde eine Verschlechterung eine konkrete Reaktion auslösen?

Dreimal Ja → geeigneter Start-KPI. Auch nur einmal Nein → später.

Das empfohlene Starter-Set

Fünf KPIs, die in fast jeder Organisation den 3-Fragen-Test bestehen und zusammen ein erstaunlich vollständiges Bild ergeben – Sichtbarkeit, Erkennung, Reaktion, Schwachstellen und Faktor Mensch. Alle fünf tragen im Katalog die höchste Priorität (PO, MVP-1):

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

Anteil der Endpunkte, Server und Workloads mit installiertem, aktiviertem und richtlinienkonformem Endpoint-Schutz (EPP/EDR/XDR).

Formel: Assets mit richtlinienkonformem Schutz ÷ alle Assets im Scope × 100

Datenquelle: EDR-/XDR-Konsole + Inventar (CMDB, AD, MDM)

Warum zuerst: Sichtbarkeit ist die Grundlage jeder Erkennung. Jede ungeschützte internetexponierte Maschine ist ein blinder Fleck der Detektion.

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

Zeit vom Ereignisbeginn (bzw. der ersten beobachtbaren Aktivität) bis zur Erkennung durch das SOC.

Formel: Median(Erkennung – Auftreten) je Vorfall

Datenquelle: SIEM, SOC-Ticketing

Praxistipp: Median statt Durchschnitt verwenden – einzelne Ausreißer verzerren sonst das Bild.

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

Zeit von der Erkennung bis zur vollständigen Behebung bzw. Wiederherstellung.

Formel: Median(Behebung – Erkennung) je Vorfall

Datenquelle: Incident-Ticketing

Praxistipp: Für die Feinsteuerung nach MTTA (Annahme) und MTTC (Eindämmung) trennen – der Standard definiert alle drei Spannen.

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

Anteil der kritischen, internetexponierten Schwachstellen, die innerhalb des definierten SLA behandelt wurden.

Formel: innerhalb SLA behobene/mitigierte Findings ÷ fällige internetexponierte kritische Findings × 100

Datenquelle: Vulnerability Scanner, Ticketing

Warum: Fokussiert die Außenhaut – dort, wo Angreifer zuerst ankommen. Ein SLA-Prozentwert, den jedes Gremium versteht und der unmittelbar Handlung auslöst.

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

Anteil der zugestellten Phishing-Simulationen, die über den Meldeweg korrekt gemeldet wurden.

Formel: gemeldete Simulationen ÷ zugestellte Simulationen × 100

Datenquelle: Awareness-Plattform, Mail-Gateway

Warum diese statt der Klickrate: Die Meldequote misst das erwünschte Verhalten – ein stärkeres Signal für die Sicherheitskultur als die reine Fehlerquote.

Passt einer der fünf nicht? Ersetzen Sie ihn aus diesem Pool: MFA-Abdeckung, Patch-Compliance, Backup-Restore-Erfolgsquote, bestätigte Incidents pro Monat. Wichtig ist nur: Es bleiben fünf.

Die ersten 30 Tage

Woche 1 – Auswählen und Verantwortliche benennen

Ein Termin, 60 Minuten, die richtigen Leute im Raum. Wählen Sie fünf KPIs (Starter-Set oder eigene Kandidaten per 3-Fragen-Test) und benennen Sie **pro KPI genau einen Owner**. Nicht zwei, nicht „das Team“ – eine Person.

Ergebnis: Liste mit 5 KPIs und 5 Namen.

Woche 2 – Datenquellen prüfen

Für jeden KPI klären: In welchem System liegen die Daten? Wer hat Zugriff? Lassen sie sich exportieren (CSV genügt)? Wenn eine Quelle fehlt: KPI aus dem Ersatz-Pool tauschen – nicht warten, bis die Quelle irgendwann existiert.

Ergebnis: Datenquellen-Check für alle fünf KPIs.

Woche 3 – Erste Messung: manuell ist erlaubt

Erheben Sie jeden Wert einmal – von Hand, per Export, in Excel. Automatisierung kommt später. Dokumentieren Sie dabei pro KPI einen kurzen **Steckbrief**:

KPI-Name	[aus dem OSMS-Katalog]
OSMS-ID	z. B. END-001 (siehe Starter-Set)
Definition / Formel	
Datenquelle(n)	
Owner	
Messfrequenz	monatlich
Baseline (Monat 1)	
Schwellen (ab M3)	Grün ≥ ... Gelb ... Rot < ...

Ergebnis: Fünf ausgefüllte Steckbriefe mit ersten Werten.

Woche 4 – Erstes Reporting: eine Seite genügt

Ein One-Pager: Berichtsmonat, fünf KPIs mit Wert, Trendpfeil und Ampel, drei Sätze Kommentar, eine Entscheidung oder ein Bedarf. Präsentieren Sie ihn in einem **bestehenden** Meeting – kein neuer Termin, kein neues Gremium.

Ergebnis: Erster Report ist gehalten, Wiederholung für Monat 2 steht im Kalender.

Was Sie am Anfang NICHT brauchen

- **Kein Dashboard-Tool.** Excel oder Sheets genügen für die ersten Monate vollständig.
- **Keine Automatisierung.** Manuelle Erhebung ist im ersten Quartal völlig in Ordnung.
- **Keine perfekten Daten.** Eine ehrliche 80-Prozent-Zahl schlägt eine perfekte Zahl, die nie kommt.
- **Keine Zielwerte ab Tag 1.** Erst drei Monate Baseline messen, dann Ampel-Schwellen setzen.
- **Kein neues Meeting.** Das Reporting gehört in eine Runde, die es schon gibt.

Fünf Stolpersteine – und wie Sie sie vermeiden

1. **Zu viele KPIs auf einmal.** Zehn halbherzig gemessene Kennzahlen sind wertlos; fünf gepflegte schaffen Vertrauen.
2. **Perfektionismus bei der Datenqualität.** Wer auf saubere Daten wartet, startet nie. Messen, Lücken benennen, verbessern.
3. **KPIs ohne Owner.** Eine Kennzahl ohne verantwortliche Person verwaist innerhalb von zwei Monaten.
4. **Messen ohne Konsequenz.** Wenn Rot keine Reaktion auslöst, ist die Ampel Dekoration. Jede Schwelle braucht eine vereinbarte Folge.
5. **Tool vor Frage.** Erst klären, welche Fragen das Reporting beantworten soll – dann über Werkzeuge reden. Nie umgekehrt.

Nach 30 Tagen: der Ausbaupfad

Monat 2–3: Rhythmus festigen, Baseline vervollständigen, Ampel-Schwellen setzen. Danach 3–5 weitere KPIs aufnehmen – jeder neue Kandidat durchläuft den 3-Fragen-Test.

Monat 4–6: Datensammlung schrittweise automatisieren (Exporte, Skripte). Erste Drill-Downs einführen: von der aggregierten Kennzahl zu ihren operativen Treibern. Die OSMS-Mappings nutzen, um NIS2- und DORA-Nachweise direkt aus vorhandenen KPIs abzuleiten – statt parallel Compliance-Listen zu pflegen.

Ab Monat 6: Management- und Board-Sicht aufbauen (L4-Ebene des Standards). Ab jetzt quartalsweise erweitern statt monatlich – Stabilität schlägt Wachstum.

Checkliste zum Abhaken

- ☐ 5 KPIs per 3-Fragen-Test ausgewählt
- ☐ Pro KPI genau ein Owner benannt
- ☐ Datenquellen geprüft (Zugriff + Exportierbarkeit)
- ☐ 5 Steckbriefe ausgefüllt
- ☐ Erste Messung durchgeführt (manuell ist ok)

- ☐ One-Pager erstellt
- ☐ Reporting-Slot in bestehendem Meeting fixiert
- ☐ Termin für Monat 2 steht

Ressourcen

Standard & Katalog: opensecuritymetrics.org

Maschinenlesbarer KPI-Katalog: osms-catalog.yaml (v0.9.1, YAML/JSON)



OSMS™ ist eine Marke. Alle genannten Frameworks und Standards (NIST CSF, ISO/IEC 27001/27004, CIS Controls, MITRE ATT&CK) sind Eigentum ihrer jeweiligen Rechteinhaber.

Redaktionelle Hinweise – vor Veröffentlichung entfernen

1. Zahlen und KPI-IDs verifiziert gegen osms-catalog.yaml v0.9.1 (Stand 05.07.2026): 327 KPIs, 39 Domänen. Starter-Set: END-001, SOC-002, SOC-003, STD-016, HRM-002 – alle P0/MVP-1.
2. ™ gilt bis zur EUIPO-Registrierung; danach auf ® umstellen.