

01001100 01001111 01000111



INTERVENTO • 15 MINUTI

Chi legge i tuoi log?

La filiera del SOC tra MDR, subappalto e privacy invisibile

Edoardo Ferri

Il Cibernetico • Consulente tecnico-forense • Auditor di terza parte

Aprile 2026

La domanda che nessuno fa al board

“

Chi sta leggendo, in questo preciso istante, i log della tua organizzazione?



Quale persona fisica?



In quale Paese, quale giurisdizione?



Con quale contratto e quali NDA?



Con quali privilegi amministrativi?

9 organizzazioni su 10 non sanno rispondere.

Cosa impone davvero la NIS2

Catena normativa di riferimento

Dir. (UE) 2022/2555

NIS2 — art. 21 (misure tecniche), art. 23 (responsabilità organi di gestione)

D.Lgs. 138/2024

Recepimento italiano — artt. 23 e 24, in vigore dal 16 ottobre 2024

Det. ACN n. 164179/2025

Specifiche tecniche di base, 14 aprile 2025

GDPR artt. 28, 35, 44-49

Responsabile, DPIA, trasferimenti extra-SEE

ISO/IEC 27001:2022

Controlli A.5.21, A.5.22 — gestione fornitori ICT

NIST SP 800-61 Rev. 3

Incident Response (2025) — trust boundary col fornitore esterno

NIST SP 800-161r1

Cybersecurity Supply Chain Risk Management



Il principio cardine

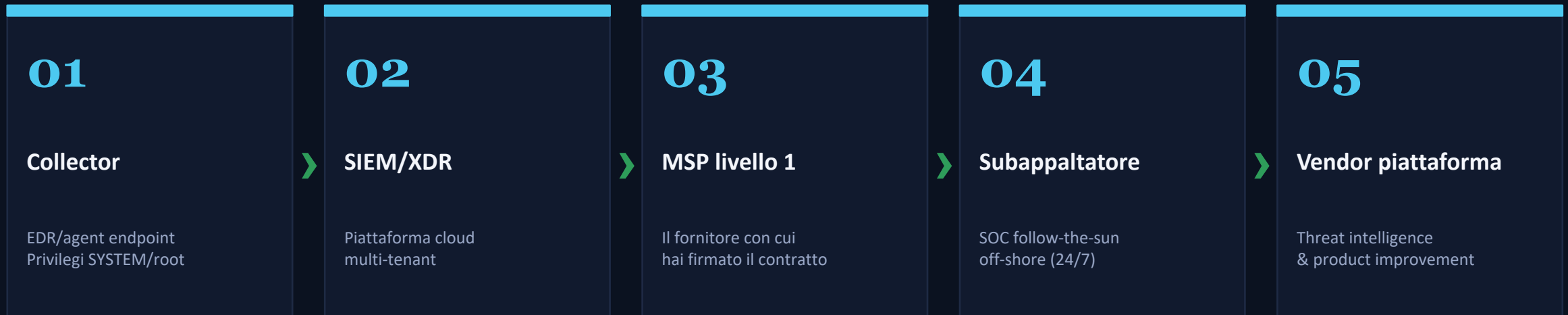
La responsabilità della sicurezza della supply chain ICT resta in capo al soggetto regolato, anche quando esternalizza.

Il fornitore MDR è:

Responsabile del trattamento ex art. 28 GDPR

ICT third-party provider soggetto a due diligence tecnicamente verificabile

I 5 livelli che il cliente non vede



Dato ENISA — Threat Landscape for Supply Chain Attacks

Oltre il 60% dei fornitori europei di servizi gestiti di sicurezza utilizza almeno un subappaltatore extra-UE per la copertura oraria estesa.

Quando la filiera si rompe: casi accertati

2020

SolarWinds

Compromissione build chain.
~18.000 organizzazioni colpite.
(CISA AA20-352A)

2021

Kaseya VSA

Ransomware via RMM.
~1.500 aziende, 60 MSP.
(ENISA, nov 2021)

2023

Okta Support

File HAR esfiltrati con
token di sessione validi.
(Indagine interna Okta)

2024

CrowdStrike

Update Falcon difettoso:
~8,5M dispositivi in BSOD.
(Post Incident Review, lug 2024)

2024

Caso Equalize (IT)

Accessi abusivi a banche dati
dall'interno della filiera tecnica.
(Procura di Milano)

Il software che legge i tuoi log È un perimetro di fiducia. Una sua compromissione è un single point of catastrophic failure.

Cosa c'è davvero nei tuoi log

“I log sono dati tecnici” — è un assunto tecnicamente errato.

| | | |
|---|---|---|
| 1 | Identificativi diretti e indiretti | username, email, IP riconducibili, MAC dei dispositivi BYOD, numeri VoIP |
| 2 | Contenuti sostanziali | subject email, URL con query string (codici fiscali, diagnosi, IBAN), DNS query, User-Agent |
| 3 | Dati particolari (art. 9 GDPR) | salute, orientamento, opinioni politiche, religione, affiliazioni sindacali — via DNS/proxy |
| 4 | Credenziali in chiaro | password digitate nel campo username finiscono nei log di autenticazione fallita |
| 5 | Segreti industriali | command line con API key, connection string, JWT, PowerShell script block log |

EDPB Guidelines 07/2020 • Landauer et al., Computers & Security (2023) • NIST SP 800-92

Il dato che gli auditor trovano sempre



Cosa serve per essere compliant

- ✓ **Autorizzazione al subappalto**
art. 28(2) GDPR — autorizzazione specifica o generale documentata
- ✓ **Base giuridica per trasferimenti**
artt. 44–49 GDPR — SCC ex Decisione UE 2021/914
- ✓ **Transfer Impact Assessment**
post-sentenza Schrems II (CGUE C-311/18), valutazione caso per caso
- ✓ **Subprocessor list aggiornata**
nome legale, Paese, funzioni, dati acceduti, base giuridica
- ✓ **DPIA estesa al SOC**
art. 35 GDPR — riconoscere log come dati personali a rischio elevato

I 3 pilastri della verifica indipendente



01

Tracciabilità documentale

Subprocessor list aggiornata: nome legale, Paese, funzioni, dati, base giuridica.

ISO/IEC 27036 • art. 28 GDPR



02

Verifica tecnica indipendente

ISO/IEC 27001 con SoA su A.5.21–A.5.22, SOC 2 Type II o ISAE 3402, pen-test annuali della piattaforma SOC.

AICPA TSC • ISAE 3402



03

Diritti di audit ed exit plan

Audit on-site sui subappaltatori, portabilità, restituzione e cancellazione certificata dei dati.

NIST SP 800-161r1

Tre misure tecniche da adottare oggi



Log minimization & pseudonimizzazione alla fonte

Field-level encryption o hashing dei dati personali non strettamente necessari, prima che il log lasci il perimetro.

STRUMENTI / PATTERN

Logstash filter • Cribl • Sentinel transformation rules



Segregazione del control plane

Chiavi di cifratura dei log archiviati e account amministrativi di più alto privilegio sotto controllo esclusivo del cliente.

STRUMENTI / PATTERN

BYOK / HYOK • Privileged Access Workstation



Monitorare il monitor

UEBA sugli operatori del SOC, con log separati e fuori dalla loro portata. Reporting al comitato rischi, non all'IT.

STRUMENTI / PATTERN

Security Assurance • Four-eyes principle

Chi legge i tuoi log?

01

Esternalizzare è legittimo

Spesso necessario, e in molti casi un innalzamento oggettivo della sicurezza rispetto a una gestione interna sottodimensionata.

02

La responsabilità non si esternalizza

Chi firma il contratto resta — di fronte al regolatore e agli interessati — l'unico soggetto giuridicamente responsabile.

Rendere visibile ciò che la filiera tende a rendere invisibile.