The First 72 Hours Matter

Effective Organizational Response to Security Incidents (NIS2) & data breaches (GDPR)

ALEXANDRU GHEORGHE
Cybersecurity, Data Privacy, AI Regulatory Consultant

DevTalks Romania 2026

datatrail™

Legal Requirements for NIS2 Compliance

What if Companies (Entities) fail to report incidents to Authorities?

Summary of requirements

- Existence of an Incident Response Policy (IRP) – (art. 13 – b) NIS2;
- Define an incident management process (art. 13 – g) NIS2;
- Reporting of a cybersecurity incident to the Incident Response Team (IRT) and the National Cybersecurity Authority

Deadlines to notify Authorities

- **6 Hours**: initial early warning
- **24 Hours**: early warning
- **72 Days**: impact and consequences update report
- 30 Days: final report

Failure to comply leads to Fines

- **EE (Essential Entities):** up to 10M EUR or up to 2% of annual net turnover
- **IE (Important Entities):** up to 7M EUR or up to 2% of the annual net turnover

datatrail™

Can we reduce incident management costs?

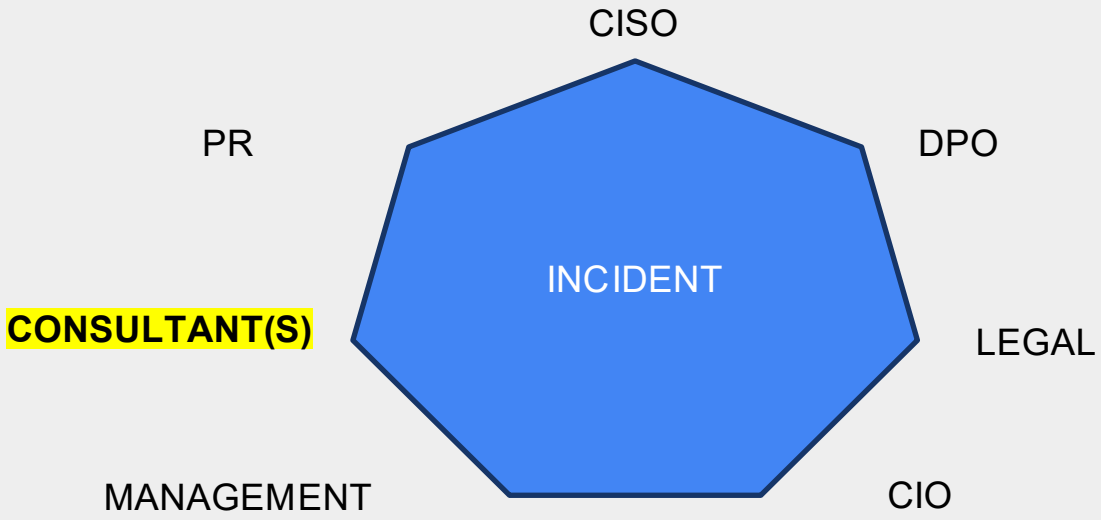
- Incident Management costs for a medium sized company

Based on experience, an average of 7 people (resources) participate in almost every incident.

- ~ 7500 EUR / 72h per incident + opportunity cost

- We took into consideration that the involvement possibility of the resources is not constant;
- Cost is only applicable to Romania;
- The cost includes the alignment overhead in the assessment and notification decision regarding the incident. The cost does not include the resources involved in addressing the impact of a security incident — tech & product, customer support and care.

An average of 7 resources intervene in case of an incident or a data breach



datatrail™

Cyber Security Crisis Management

In Crisis Escalation, time is of essence.
But most incident management plans fail to provide a quick resolution

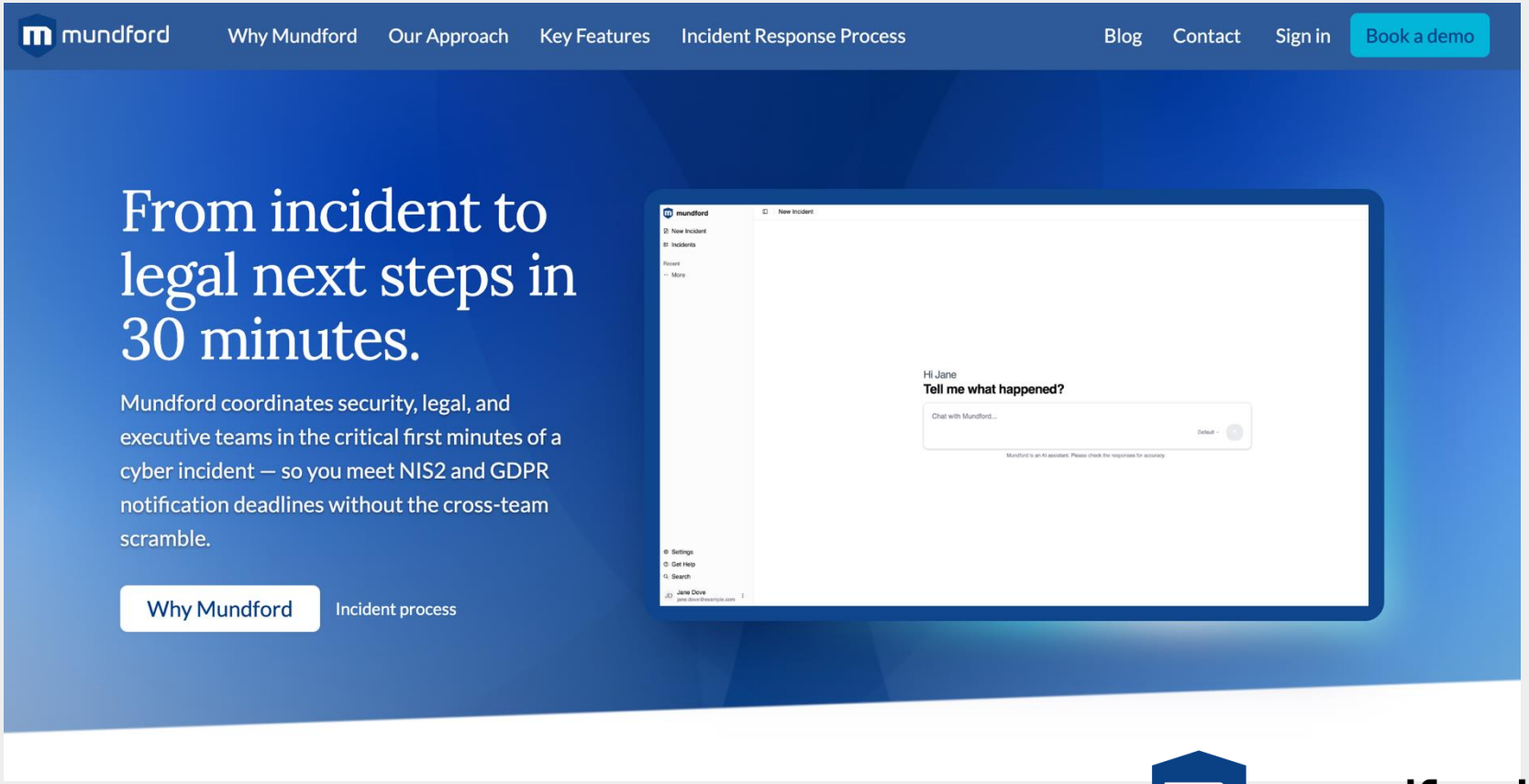
- unclear escalation paths in the first stages of incident response
- increased coordination overhead between decision making stakeholders
- lack of appropriate expertise in most of the companies
- time-critical reporting deadlines due to legal requirements – 24h for NIS2
- uncertainty in the impact assessment and the required legal next steps
- missing traceability of actions taken, leading to loss of organizational memory.

datatrail™

DevTalks Romania 2026

THE FUTURE OF INCIDENT RESPONSE

datatrail™


mundford
Why Mundford
Our Approach
Key Features
Incident Response Process
Blog
Contact
Sign in
Book a demo
From incident to legal next steps in 30 minutes.
Mundford coordinates security, legal, and executive teams in the critical first minutes of a cyber incident — so you meet NIS2 and GDPR notification deadlines without the cross-team scramble.
Why Mundford
Incident process
New Incident
Incidents
Recent
More
Settings
Get Help
Search
Jane Dove
Hi Jane
Tell me what happened?
Chat with Mundford...
Default
Mundford is an AI assistant. Please check the responses for accuracy.

mundford

- **Mundford** is your AI agent in the first stages of a cyber security incident or a data breach.
- **Mundford** combines the essential expertise of a CISO, Lawyer, and DPO to ensure your organization can respond rapidly to a cyber incident and meet strict European legal deadlines (GDPR, NIS2, DORA, AI Act).
- **Mundford** recommends in under 30 minutes, what you need to do right after an incident, focusing on and starting with, your immediate legal obligations.
- **Mundford** helps you submit the correct incident notification forms to the Authorities.

datatrail™

Contact us

hello@datatrail.eu

(+40) 723 311 237

https://www.datatrail.eu/

https://www.mundford.ai/

Alexandru Gheorghe

datatrail™