smeup

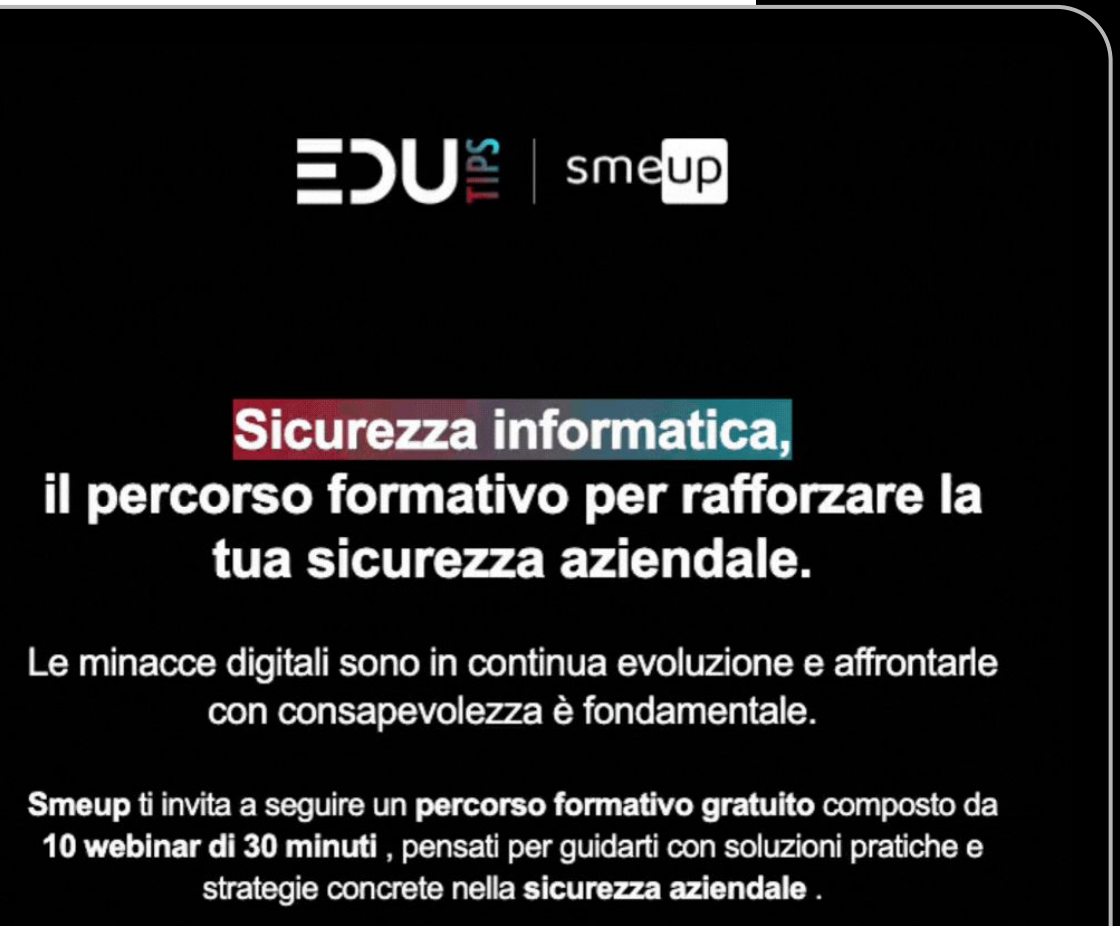
WEBINAR

Incident Response

Affronta un attacco informatico con lucidità ed efficacia.

12 GIUGNO
2025

EDU TIPS
CYBERSECURITY



EDU TIPS Cybersecurity

10 webinar TIPS - 30 minuti al mese
su tematiche specifiche di Cybersecurity

DATA	DESCRIZIONE
28/1	Mese 1: **Sicurezza dell'infrastruttura**
13/2	Mese 2: **Cyber Security Awareness**
13/3	Mese 3: **Data Protection**
10/4	**Mese 4: Identità e accesso**
13/5	Mese 5: **Cloud security**
12/6	**Mese 6: Incident response**
8/7	Mese 7: **Sicurezza delle applicazioni**
11/9	Mese 8: **Analisi delle minacce e vulnerability assessment**
10/10	Mese 9: **Sicurezza delle reti industriali (OT)**
11/11	Mese 10: **Sicurezza in ambito A.I.**

👉 SCOPRI DI PIÙ

EDU TIPS
CYBERSECURITY

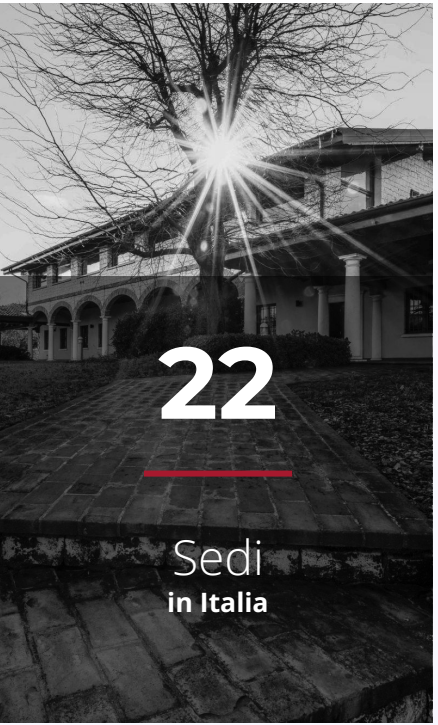
SIMONE
ZABBERONI

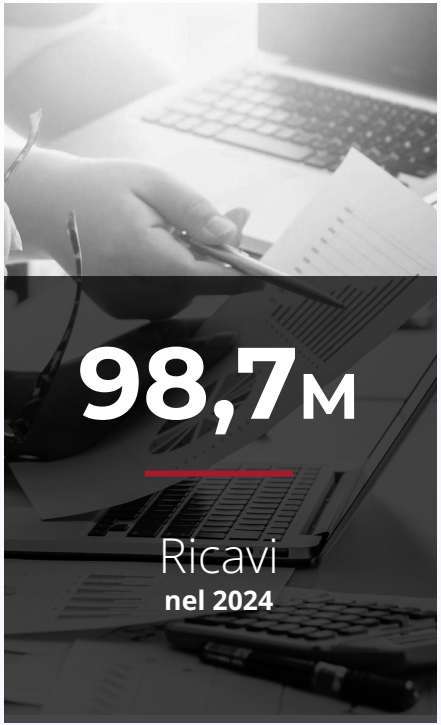
Security Specialist *- smeup ICS*

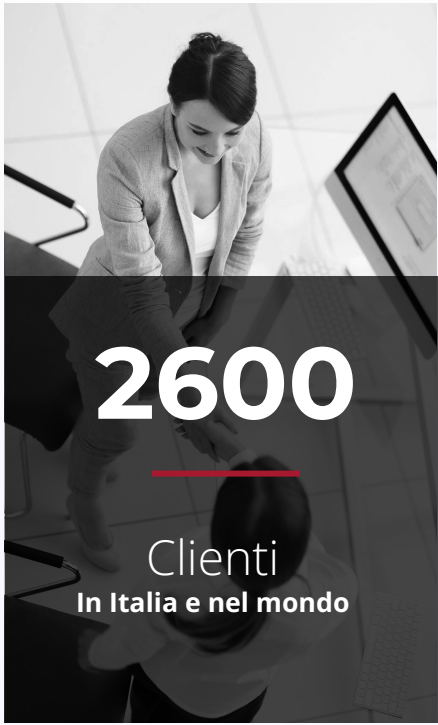
simone.zabberoni@smeup.com

COMPANY **OVERVIEW**

smeup in Numeri.







BUSINESS SECTOR

BUSINESS SOFTWARE APPLICATION

Soluzioni **Software** per **PMI** e **grandi industrie.**

Ogni azienda è unica. smeup lo sa!
Usare la digitalizzazione per sviluppare il business e generare valore, ***insieme***.

- **e** GESTIONALI ERP
- **b** BUSINESS ANALYTICS
- **d** DOCUMENTALE
- **w** WEB & MOBILE APPLICATION
- **f** IOT E INTEGRAZIONE INDUSTRIALE
- **l** LOGISTICA E TRASPORTI

BUSINESS SECTOR

INFRASTRUCTURE, CLOUD & SECURITY

Soluzioni per **Architetture IT** e **servizi gestiti.**

Innovazione e **sicurezza** per rispondere ai bisogni delle aziende.

- i INFRASTRUTTURA
- c CLOUD
- cs CYBER SECURITY
- ps IBM POWER SYSTEMS

INCIDENT **RESPONSE**

Gestire gli incidenti informatici.

Nel panorama attuale della cybersecurity, non è più una questione di "se" subiremo un attacco, ma di "quando". È fondamentale essere preparati a rispondere efficacemente quando l'incidente si verifica.

Gli attacchi informatici sono diventati sempre più sofisticati, automatizzati e personalizzati grazie all'intelligenza artificiale. Il metodo "Assume Breach" ci impone di prepararci non solo alla prevenzione, ma soprattutto alla risposta rapida ed efficace.

- Gli attacchi informatici sono diventati sempre più sofisticati e automatizzati con l'AI
- La sola prevenzione non basta più, serve un approccio integrato
- Il metodo "Assume Breach" ci impone di prepararci alla risposta rapida
- Scenari come ransomware e interruzioni servizi sono sempre più frequenti

RAPPORTO **CLUSIT 2025**

Cybersecurity oggi.

I dati 2024 confermano un peggioramento delle minacce in Italia. Ecco perché è urgente essere preparati.

Non solo crescono gli attacchi, ma peggiora anche la **gravità degli incidenti**: l'indice di gravità media aumenta ogni anno da 5 anni consecutivi.

71,7%

Credential Phishing
è la minaccia più diffusa

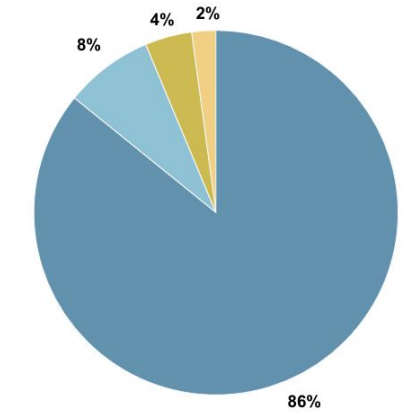
+35%

Crescita attacchi phishing
in Italia (2023-2024)

+27,4%

Aumento incidenti rilevati
(da 2.779 a 3.541)

Tipologia e distribuzione attaccanti 2024



© Clusit - Rapporto 2025 sulla Cybersecurity

- Cybercrime 86%
- Hacktivism 8%
- Espionage / Sabotage 4%
- Information Warfare 2%

p) Risposta agli incidenti e ripristino.	RS.MA-01: punti 1, 2 e 3. RS.CO-02: punti 1 e 2. RC.RP-01: punto 1.

5.1.1. **RS.MA-01**: Il piano di risposta agli incidenti è eseguito in coordinamento con le terze parti interessate una volta dichiarato un incidente.

1. È definito, attuato, aggiornato e documentato un piano per la gestione degli incidenti di sicurezza informatica e la notifica al CSIRT Italia, in accordo a quanto previsto dall'articolo 25 del decreto NIS, che comprende almeno:
   a) le fasi e le procedure di gestione e notifica degli incidenti con l'indicazione dei relativi ruoli e delle responsabilità;
   b) le procedure per la predisposizione e la trasmissione delle relazioni di cui all'articolo 25, comma 5, lettere c), d) ed e) del decreto NIS;
   c) le informazioni di contatto per la segnalazione degli incidenti;
   d) le modalità di comunicazione interna, anche con riguardo al coinvolgimento degli organi di amministrazione e direttivi, ed esterna;
   e) la reportistica da utilizzare per la documentazione dell'incidente.
2. Il piano di cui al punto 1 è approvato dagli organi di amministrazione e direttivi.
3. Il piano di cui al punto 1 è riesaminato e, se opportuno, aggiornato periodicamente e comunque almeno ogni due anni, nonché qualora si verifichino incidenti significativi, integrando le relative lezioni apprese, o mutamenti dell'esposizione alle minacce e ai relativi rischi.

Le organizzazioni soggette alla NIS2 devono implementare misure specifiche di cybersecurity e incident response.

Fonte: ACN - Agenzia per la Cybersicurezza Nazionale

CONTESTO **NORMATIVO**

Direttiva NIS2.

La normativa europea impone obblighi precisi sulla gestione degli incidenti informatici.
Non è più una scelta, ma un requisito di legge.

OBBLIGHI PRINCIPALI

- **Piano di gestione incidenti** - capacità di rilevare e gestire gli incidenti
- **Notifica entro 24h** in caso di attacco grave
- Backup, monitoraggio e test regolari
- **Misure di resilienza** e gestione vulnerabilità

GOVERNANCE

La cybersecurity è anche responsabilità del management.

⚠️ SANZIONI ⚠️

Fino a **10 milioni €** o **2%** del **fatturato globale.**

o) Monitoraggio degli eventi di sicurezza.	DE.CM-01: punti 1, 2, 4, 5 e 6. DE.CM-09: punto 1.

4.1.1. **DE.CM-01**: Le reti e i servizi di rete sono monitorati per individuare eventi potenzialmente avversi.

1. Per almeno i sistemi informativi e di rete rilevanti, sono presenti, aggiornati, mantenuti e configurati in modo adeguato strumenti tecnici per rilevare tempestivamente gli incidenti significativi.
2. Sono definiti e documentati i livelli di servizio attesi (SL) dei servizi e delle attività del soggetto NIS anche ai fini di rilevare tempestivamente gli incidenti significativi.
3. Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e documentate le procedure in relazione ai punti 1 e 2.
4. Per almeno i sistemi informativi e di rete rilevanti, sono utilizzati strumenti di analisi e filtraggio sul flusso di traffico in ingresso (ivi inclusa la posta elettronica).
5. Per almeno i sistemi informativi e di rete rilevanti, ai fini di cui al punto 1, sono monitorati gli accessi da remoto, le attività dei sistemi perimetrali (ad esempio router e firewall), gli eventi amministrativi di rilievo, nonché gli accessi eseguiti o falliti alle risorse di rete, alle postazioni terminali e agli applicativi al fine di rilevare gli eventi di sicurezza informatica.
6. Per almeno i sistemi informativi e di rete rilevanti, ai fini di cui al punto 1, sono definiti, monitorati e documentati parametri quali-quantitativi per rilevare gli accessi non autorizzati o con abuso dei privilegi concessi.
7. Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e documentate le procedure in relazione ai punti 4, 5 e 6.

IDENTIFICARE GLI **INCIDENTI**

Nis2 e Incident Detection.

L'identificazione tempestiva degli incidenti è cruciale per limitare i danni. La NIS2 richiede sistemi di monitoraggio proattivi, non reattivi.

IL **PROBLEMA**

"Stamattina tutti i sistemi sono cifrati, non si lavora" - **questo non è incident detection, è un disastro.**

Molti attacchi si concretizzano settimane o mesi dopo la prima intrusione: **bisogna reagire prima!**

LA **SOLUZIONE NIS2**

Sistemi di monitoraggio degli eventi di sicurezza per:

- **Reagire tempestivamente** agli eventi sospetti
- **Filtrare i falsi positivi** ed evitare l'overload
- **Supportare il recupero** in caso di incidente confermato

OBBLIGO DI **NOTIFICA**

NIS2 - 24 ore per comunicare.

Identificato l'incidente, scatta l'obbligo di notifica alle autorità competenti.
Il tempo è cruciale: solo 24 ore per la prima comunicazione.

COSA NOTIFICARE

- **Incidenti gravi** che impattano servizi essenziali
- **Violazioni di dati** con potenziale danno significativo
- **Interruzioni prolungate** dei sistemi critici

COME E QUANDO

- **Entro 24 ore** dalla scoperta dell'incidente
- **Tramite portale ACN** dedicato
- **Informazioni essenziali** anche se incomplete

RESPONSABILITÀ

La notifica è **responsabilità del management**, non solo dell'IT.

Fonte: ACN - Specifiche tecniche NIS2 2025 - Allegato 1
Fonte: ACN - Specifiche tecniche NIS2 2025 - Allegato 2
Fonte: ACN - Incidenti significati di base per i soggetti importanti - Allegato 3
Fonte: ACN - Incidenti significativi di base per i soggetti essenziali - Allegato 4

IMPATTO DEGLI **ATTACCHI**

Le conseguenze reali.

Gli attacchi moderni utilizzano tecniche distruttive e "doppio ricatto" (crittografia + leak dei dati). L'obiettivo principale è sempre l'estorsione di denaro, ma i danni vanno ben oltre.

IMPATTI DIRETTI

- **Riscatto ed estorsione**
  pagamento immediato richiesto
- **Interruzione operativa**
  produzione e servizi fermi
- **Costi di contenimento**
  risorse per gestire l'emergenza

IMPATTI INDIRETTI

- **Danno reputazionale**
  perdita di fiducia del mercato
- **Perdita clienti**
  fidelizzazione compromessa
- **Furto proprietà intellettuale**
  vantaggio competitivo perso
- **Responsabilità legali**
  dirigenti esposti personalmente
- **Spese legali e multe**
  costi normativi e procedurali

LA REALTÀ

Lo **scopo** principale **degli attaccanti** è l'**estorsione di denaro**, ma le **conseguenze** per l'azienda **durano anni.**

ASSENZA DI UN **INCIDENT RESPONSE PLAN**

Perché è un rischio non avere un piano?

In caso di attacco informatico, non si tratta solo di gestire aspetti tecnici: c'è **una forte componente emotiva e organizzativa** da affrontare.

- Proprietari preoccupati per **mancati incassi**, danni reputazionali e sanzioni.
- Tensione su chi teme di essere **ritenuto responsabile**.
- Operai in cassa integrazione per fermo della produzione.
- Pressioni su chi deve **isolare, ripristinare, comunicare**.

> ***Senza un piano**, regna il caos.*
> *Vogliamo davvero lasciare tutto al caso?*

PER ANALOGIA...

Guidare **una moto senza casco e senza assicurazione** si può. Ma se succede qualcosa...

- Se ci fermano: multa (audit)
- Se cadiamo: ci si fa più male (recovery lento e costoso)
- Se non c'è assicurazione: altra sanzione (non conformità)

Prepararsi è meglio che reagire nel panico.

LO **STRESS**

Il fattore umano.

Anche lo stress e la pressione fanno parte dell'emergenza.

Durante un attacco, chi gestisce la crisi è sottoposto a forte tensione emotiva e operativa.
Un piano ben definito aiuta a ridurre l'impatto psicologico e organizzativo.

Per approfondire:
📄 Northwave – The Mental Impact of Ransomware Attacks
📰 ComputerWeekly – The human toll of ransomware
📊 Talion – Ransomware: Costs beyond the cash

> *Gli attacchi informatici non colpiscono solo i sistemi, ma anche le persone.*

IMPATTO PSICOLOGICO E ORGANIZZATIVO:

- Tensione e ansia tra i responsabili IT e sicurezza
- Stress acuto nei team operativi coinvolti
- Paura, senso di colpa, difficoltà nella comunicazione interna
- Pressione da parte di clienti, fornitori e direzione
- Rischio di burnout per chi gestisce il ripristino

Un buon piano di Incident Response non elimina il problema, ma aiuta a gestirlo meglio, riducendo stress, confusione e danni secondari.

IL PIANO DI **INCIDENT RESPONSE**

“Vado matto per i piani ben riusciti”.

Un piano di Incident Response è **una guida chiara per gestire gli attacchi informatici in modo coordinato e tempestivo.**
Non si improvvisa: serve sapere **chi fa cosa, come si comunica, come si limita il danno.**

01 **Preparazione**
Asset inventory, analisi del rischio, strumenti, ruoli e procedure definite.

02 **Identificazione**
Monitoraggio e rilevamento tempestivo delle minacce.

03 **Contenimento**
Isolamento e blocco della propagazione del danno.

04 **Eradicazione**
Rimozione della causa dell’incidente.

05 **Recupero**
Ripristino dei sistemi e ritorno alla normalità operativa.

06 **Lesson Learned**
Analisi post-evento per migliorare processi e difese future.

FOCUS **MDR**

Managed Detection and Response.

L’MDR (Managed Detection and Response) è un servizio che protegge le aziende dalle minacce informatiche, monitorando i sistemi 24 ore su 24, 7 giorni su 7.

Grazie a strumenti avanzati, come l’intelligenza artificiale e il machine learning, l’MDR rileva attività sospette, analizza i dati in tempo reale e risponde rapidamente per bloccare eventuali attacchi.

MONITORAGGIO CONTINUO

Controllo costante dei sistemi aziendali **per individuare minacce**.

ANALISI INTELLIGENTE

L’IA e il machine learning **riconoscono schemi anomali e riducono i falsi allarmi.**

INTERVENTO RAPIDO

Un team di esperti verifica le segnalazioni 24/7 e, quando possibile, il **sistema risponde** automaticamente alle **minacce per proteggere l’azienda**.

COSA **FARE**

Consigli pratici e riferimenti utili.

Da dove partire:

- Mappatura degli asset e valutazione dei rischi (risk assessment e asset inventory)
- Applicazione dei principi di proporzionalità
- Rispetto delle normative vigenti (GDPR, NIS2...)
- Pianificare investimenti in sicurezza non solo per obbligo, ma per protezione reale
- Considerare i requisiti NIS2 anche se non formalmente soggetti

STRUMENTI E RIFERIMENTI UTILI

- ACN – Agenzia per la Cybersicurezza Nazionale
- Cybersecurity Framework Italiano
- **ISO 27001 – Annex A.16:** Information Security Incident Management
- **NIST SP800-61r3:** Incident Response Recommendations & Cyber Risk Management


EDU TIPS
Q&A

smeup

smeup.com

Thank you!

SIMONE **ZABBERONI**

Security Specialist @smeup ICS

simone.zabberoni@smeup.com

EDU TIPS CYBERSECURITY