



Oops, mi hanno bucato!


Giuseppe Augiero

28 ottobre 2023 - Linux Day - Dipartimento di Ingegneria - Università di Pisa



YOU HAVE BEEN

HACKED !



Ministero delle Infrastrutture e dei Trasporti

12 m · 🌐

...

✕

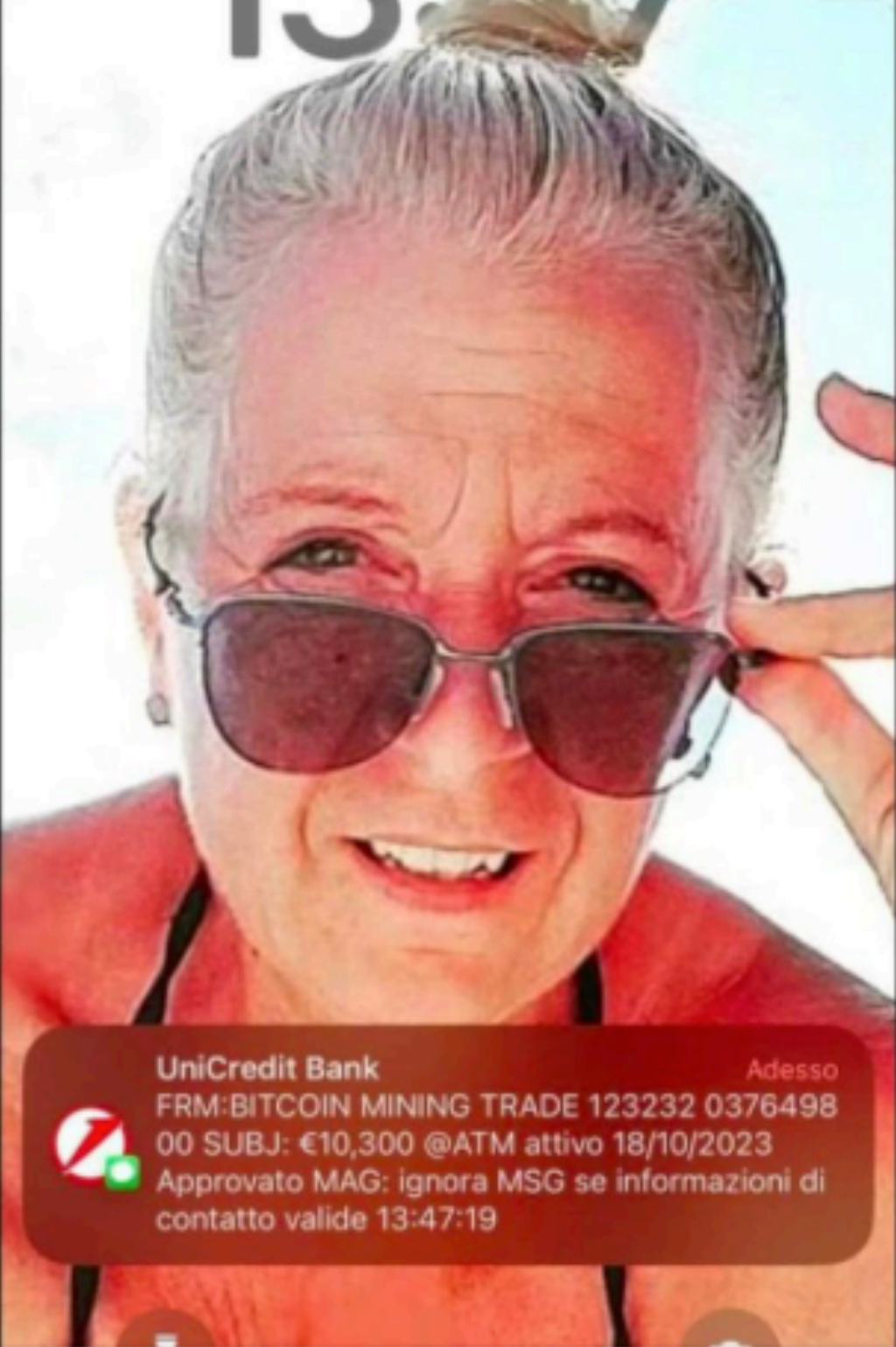
Sono così felice in questo momento. Ho investito 1000€ nel mining di Bitcoin e ho guadagnato 10.300€ entro 5 ore di trading, è stata una benedizione per me e la mia famiglia, onestamente. È davvero legittimo e sicuro, ho effettuato il prelievo ed è sicuro dire che questo mi sta cambiando la vita. Invito tutti voi a partecipare il prima possibile e sarete felici di averlo provato. Scrivi al mio coach su whatsapp +447446196132 se interessato a sapere come funziona


ATN-Serv

100%

Mercoledì 18 ottobre

13:47





UniCredit Bank

Adesso


FRM:BITCOIN MINING TRADE 123232 0376498

00 SUBJ: €10,300 @ATM attivo 18/10/2023

Approvato MAG: ignora MSG se informazioni di contatto valide 13:47:19

<

Dany Maratea


 Bitcoin (BTC)

€10,300

0.38560878 BTC

▲ 4.82%


Vedi i dettagli



Profitti/perdite

0.03%


▲ €2.609



Prezzo medio di acquisto.

€26,704.25

Transazioni

Tipo	Quantità
<div> Compra</div> <div>lun 16 ott 2023 16:45</div>	<div>+€10,297.39</div> <div>+0.38560878 BTC</div>

Aggiungi transazione

Cosa fare?



Facciamo un passo indietro

Tipologie di incidenti

- ❖ Phishing
- ❖ Dos
- ❖ Vulnerabilità
- ❖ Brute Force
- ❖ Attaccanti interni
- ❖ Account rubati
- ❖ Perdita di dati
- ❖ Errate configurazioni
- ❖ Abuse

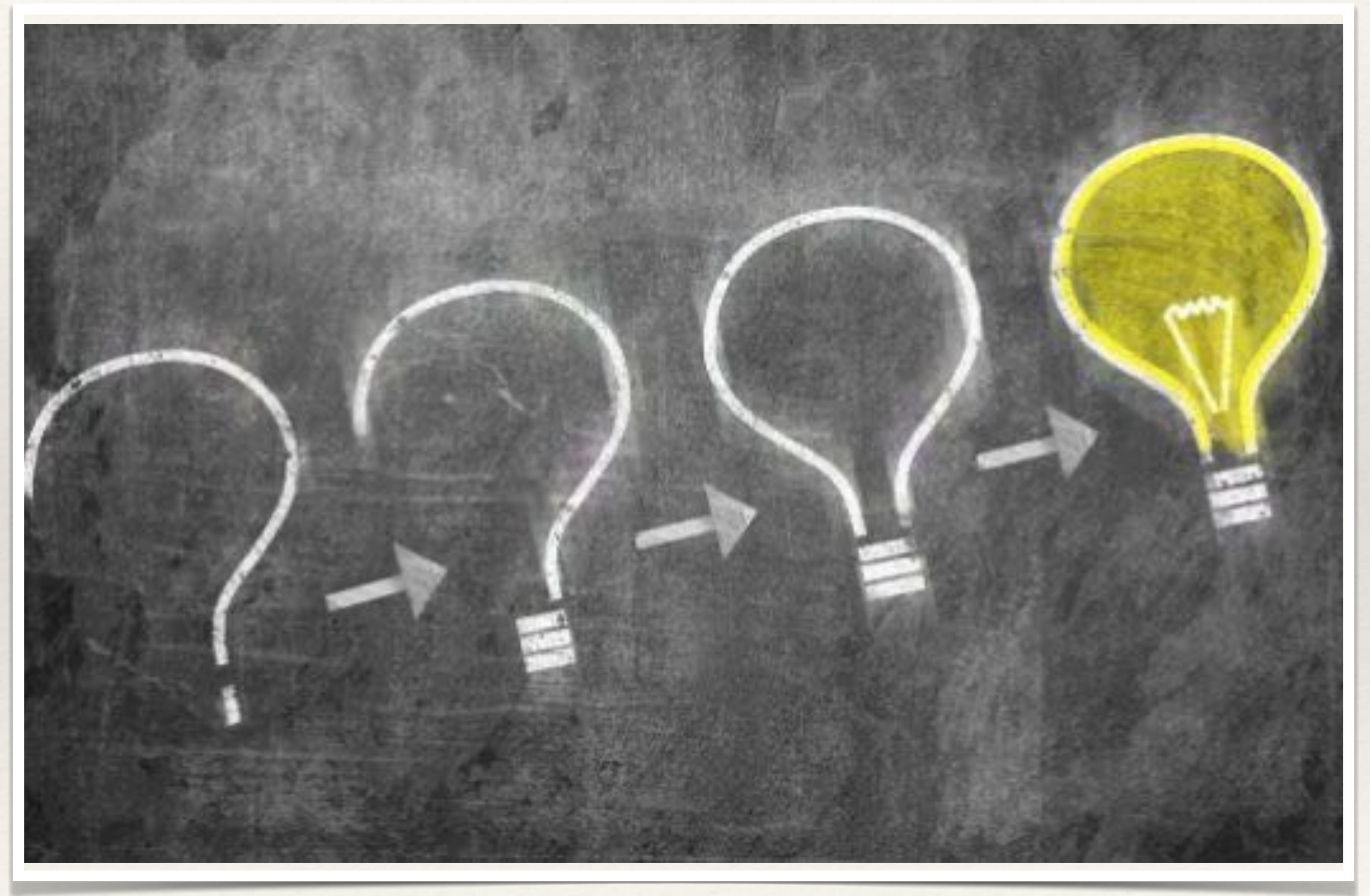


Cloud



Motivazioni

- ❖ CyberWar
- ❖ Economiche
- ❖ Spionaggio
- ❖ Divertimento
- ❖ Vendetta



Day after or before?

Prevenzione

- ❖ **Valutazione del rischio**
 - ❖ Documentare gli asset e le minacce e vulnerabilità di tali risorse.
- ❖ Sviluppare un piano di sicurezza e le relative politiche.
- ❖ Sviluppare un response plan agli incidenti di sicurezza.



Risk Assessment

- ❖ **Minacce:** occorre identificare gli elementi negativi che prendono di mira i tuoi sistemi.
- ❖ **Vulnerabilità:** difetti o punti deboli nei propri sistemi. Questi sono in continua evoluzione.
- ❖ Priorità dei rischi in base alle vulnerabilità, alle minacce e alla probabilità che si verifichino.

The diagram is a risk matrix titled 'Risk Matrix Example'. It features a vertical axis labeled 'Likelihood' with five categories: Very Likely, Likely, Possible, Unlikely, and Very Unlikely. The horizontal axis is labeled 'Severity' with five categories: Negligible, Minor, Moderate, Significant, and Severe. The matrix cells contain risk levels: 'Low Med', 'Medium', 'Med Hi', 'High', and 'High' for Very Likely; 'Low', 'Low Med', 'Medium', 'Med Hi', and 'High' for Likely; 'Low', 'Low Med', 'Medium', 'Med Hi', and 'Med Hi' for Possible; 'Low', 'Low Med', 'Low Med', 'Medium', and 'Med Hi' for Unlikely; and 'Low', 'Low', 'Low Med', 'Medium', and 'Medium' for Very Unlikely. The cells are color-coded: green for Low/Low Med, yellow for Medium/Med Hi, and red for High. An arrow points right above the Severity header, and an arrow points up to the left of the Likelihood header. Below the matrix, the text 'Likelihood X Severity = Risk Level' is displayed.

Likelihood	Severity				
	Negligible	Minor	Moderate	Significant	Severe
	Very Likely	Low Med	Medium	Med Hi	High
	Likely	Low	Low Med	Medium	Med Hi
	Possible	Low	Low Med	Medium	Med Hi
	Unlikely	Low	Low Med	Medium	Med Hi
	Very Unlikely	Low	Low	Low Med	Medium

Risk Matrix Example

Likelihood X Severity = Risk Level

Vettori di attacco

- ❖ Account rubati e brute force.
- ❖ Attacchi interni: che ci crediate o no, gli studenti e persino i professori sono un vettore di attacco.
- ❖ Vulnerabilità del software -
 - ❖ Errata configurazione dei sistemi
 - ❖ Cattiva gestione delle patch
 - ❖ Vulnerabilità note non risolte
 - ❖ Attacchi zero-day
- ❖ Codice malevolo (virus, worm, cavalli di Troia, ransomware, ecc...)



Qualcosa non va...

- ❖ Sono sintomo di anomalie:
 - ❖ Performance ridotte.
 - ❖ Maggiore traffico di rete.
 - ❖ Direttrici di rete inaspettate.
 - ❖ Storage pieno.
 - ❖ Utenti lamentano di azioni sospette con i propri account.
 - ❖ Accessi a orari insoliti.



... meglio verificare

- ❖ Avvisi diretti dai propri servizi di monitoraggio
- ❖ Analisi automatizzata di log e correlazioni.
- ❖ Avvisi provenienti da fonti attendibili di attività dannose o vulnerabilità appena esposte
- ❖ Avvisi di vulnerabilità



Gestione dei Log

- ❖ I log sono la fonte di tutte le azioni investigative che possiamo portare a termine.
- ❖ È importante stabilire procedure di gestione dei log .
- ❖ Per progetti e infrastrutture di grandi dimensioni ciò richiede, in genere, una soluzione di gestione dei log dedicata.



I log

- ❖ Log capture.
- ❖ Log retention.
- ❖ Log storage.
- ❖ Devono essere “sicuri”.
- ❖ Il tempo non può essere una opinione.



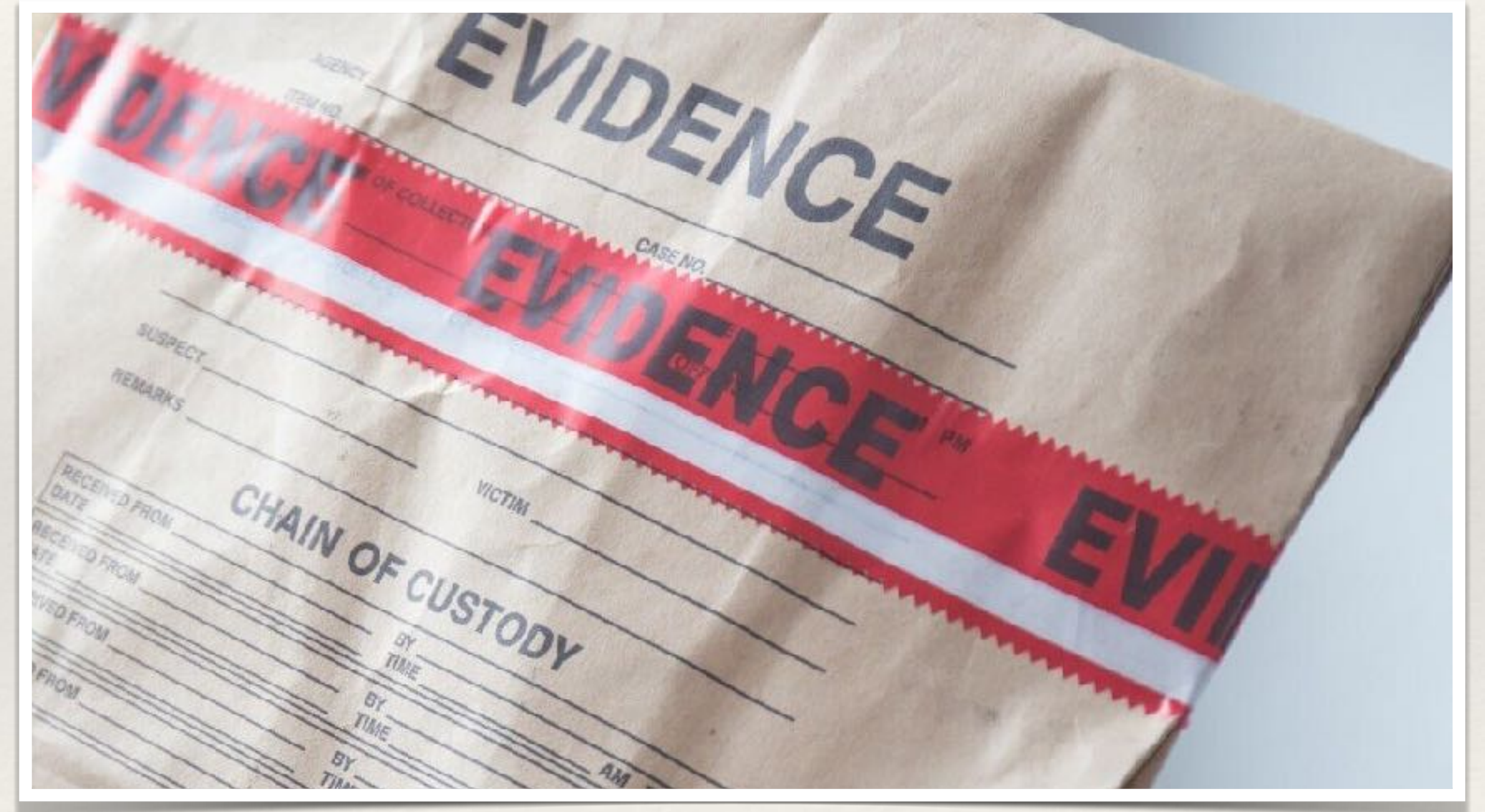
Analisi dei Log

- ❖ E' necessario esaminare e analizzare regolarmente i log.
- ❖ **L'automazione è FONDAMENTALE**
- ❖ Occorre usare gli strumenti di correlazione per una visione d'insieme e per ridurre i falsi positivi.
- ❖ L'analisi dei log dovrebbe includere il monitoraggio in tempo reale.
- ❖ Configurare un sistema di segnalazione basato sulle priorità.



Secure evidence

- ❖ Dobbiamo conservare e lasciare inalterate le evidenze che ci interessano.
- ❖ Garantire la catena di custodia.



A black and white photograph of a cable-stayed bridge tower, viewed from a low angle looking up. The tower's structure, including its pylon and stay cables, is silhouetted against a dramatic, cloudy sky. The text "Bastano i log?" is overlaid in a red, serif font across the middle of the image.

Bastano i log?

Response!

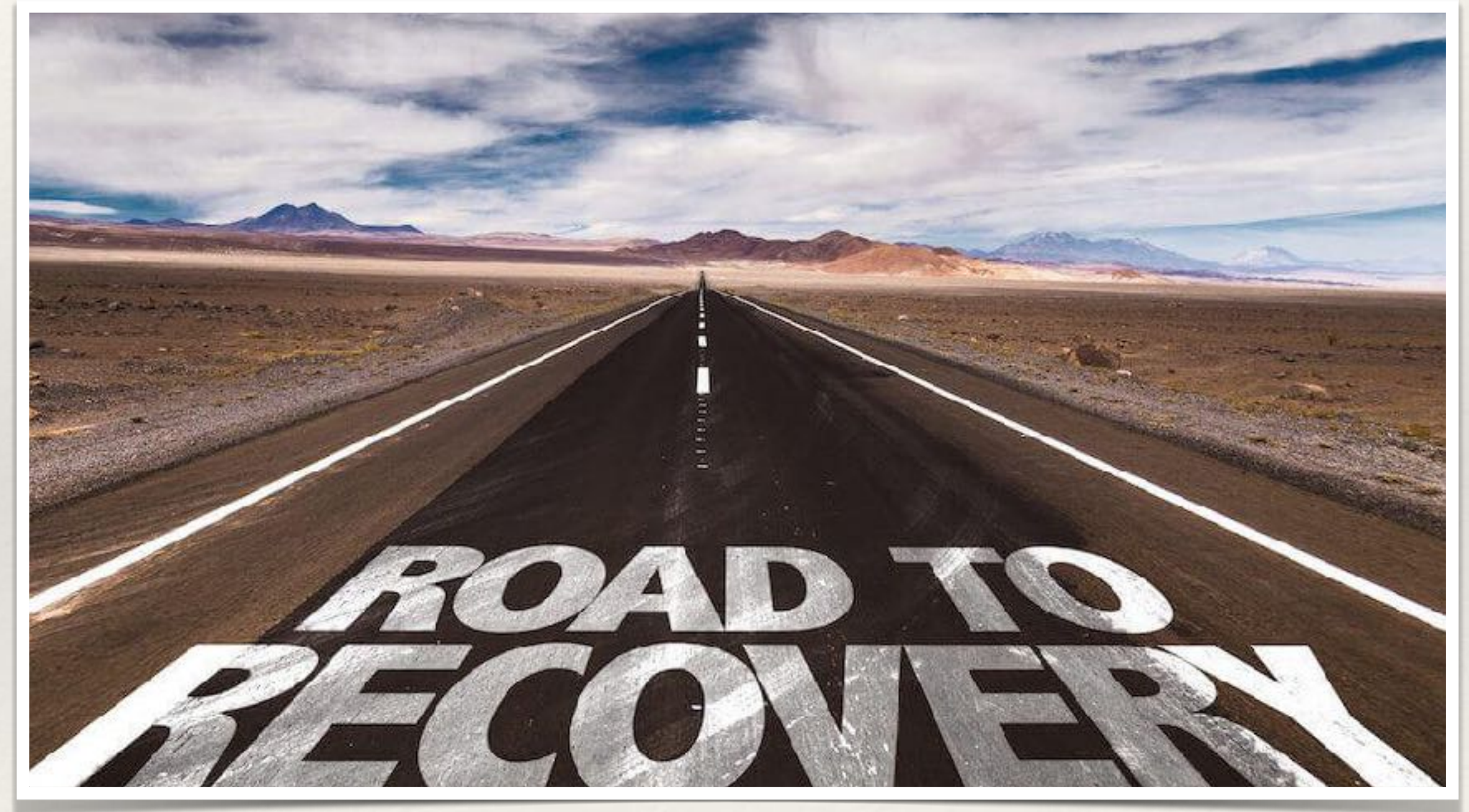
Contenimento

- ❖ Deve definire una strategia:
 - ❖ Ridurre i danni.
 - ❖ Ridurre al minimo la corruzione delle prove.
 - ❖ In che modo influisce sulla disponibilità del servizio.
 - ❖ Quanto tempo ci vuole per implementare
 - ❖ Efficacia.



Recovery e Eradicazione

- ❖ Rimozione di virus, falle di sicurezza.
- ❖ Disabilitazione account.
- ❖ Restore del sistema e dei servizi.
- ❖ Fixare le vulnerabilità.
- ❖ **Imparare la lezione.**



Siamo al sicuro?

- ❖ Abbiamo realmente eradicato tutto?
- ❖ Sappiamo quale sia stato il vettore di attacco?
- ❖ Tutti i file che hanno subito modifiche sono stati identificati?
- ❖ Sorvegliato speciale.



Data Breach

- ❖ La falla di sicurezza potrebbe essere una falla relativa alla privacy e quindi ai nostri dati.



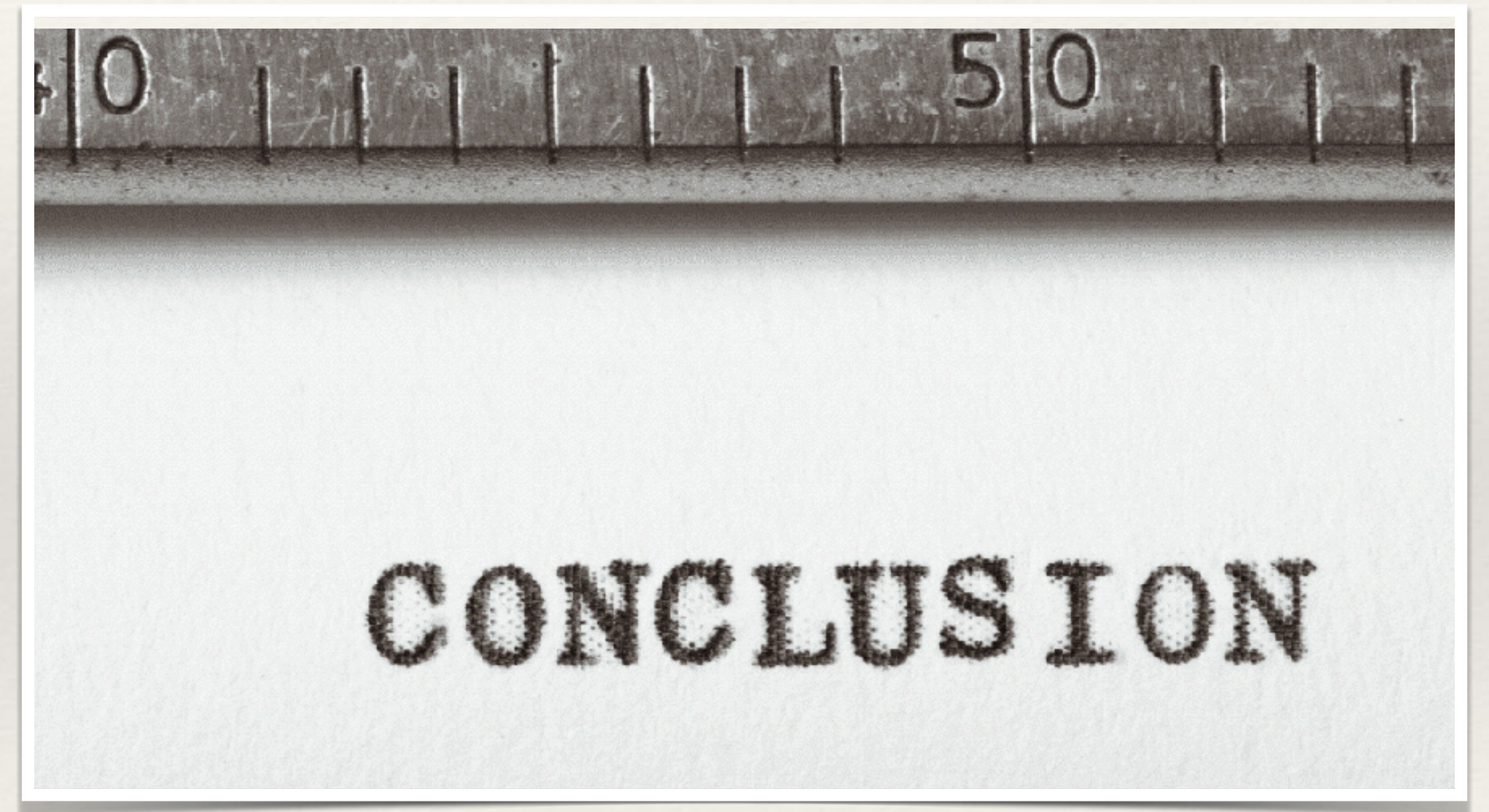
La comunicazione

- ❖ Mai dimenticare l'importanza della comunicazione.



In conclusione

- ❖ Basta “rimettere le cose apposto”?
- ❖ Perché è successo?
- ❖ Possiamo evitare che accada di nuovo?
- ❖ Importanza delle informazioni.



Web: augiero.it
Email: talk@augiero.it



Oops, mi hanno bucato!
Giuseppe Augiero

28 ottobre 2023 - Linux Day - Dipartimento di Ingegneria - Università di Pisa

