Gestione delle vulnerabilità e degli incidenti di sicurezza in INFN Cloud

Massimo Sgaravatto
INFN Padova

Sommario

- Vulnerabilità, attacchi
- Gestione delle vulnerabilità in INFN Cloud
- Gestione degli incidenti di sicurezza in INFN Cloud

Vulnerabilità

- Un "difetto" in un componente del sistema che permette comportamenti che violano le proprietà di sicurezza

- Tutte le vulnerabilità sono difetti, ma non tutti i difetti sono vulnerabilità

Tipi di vulnerabilità

- In genere si fa riferimento alle vulnerabilità software
  - Nel codice o nella configurazione

- Ma esistono anche altre forme di vulnerabilità
  - Vulnerabilità hardware
  - Vulnerabilità nei protocolli
  - Vulnerabilità "procedurali" e "organizzative"
    - Es. dovute a personale non adeguatamente formato
    - Es. password scritte su post-it

Attacchi

- Una (o più) vulnerabilità possono essere sfruttate per attaccare un sistema

- L'attaccante che ha preso controllo di un sistema può:
  - Leggere e/o modificare dati
  - Modificare/compromettere il funzionamento del sistema
  - Usare il sistema per attaccare altri sistemi
  - …

Exploit

- Exploit: programma/sequenza di comandi che permettono di "automatizzare" l'attacco

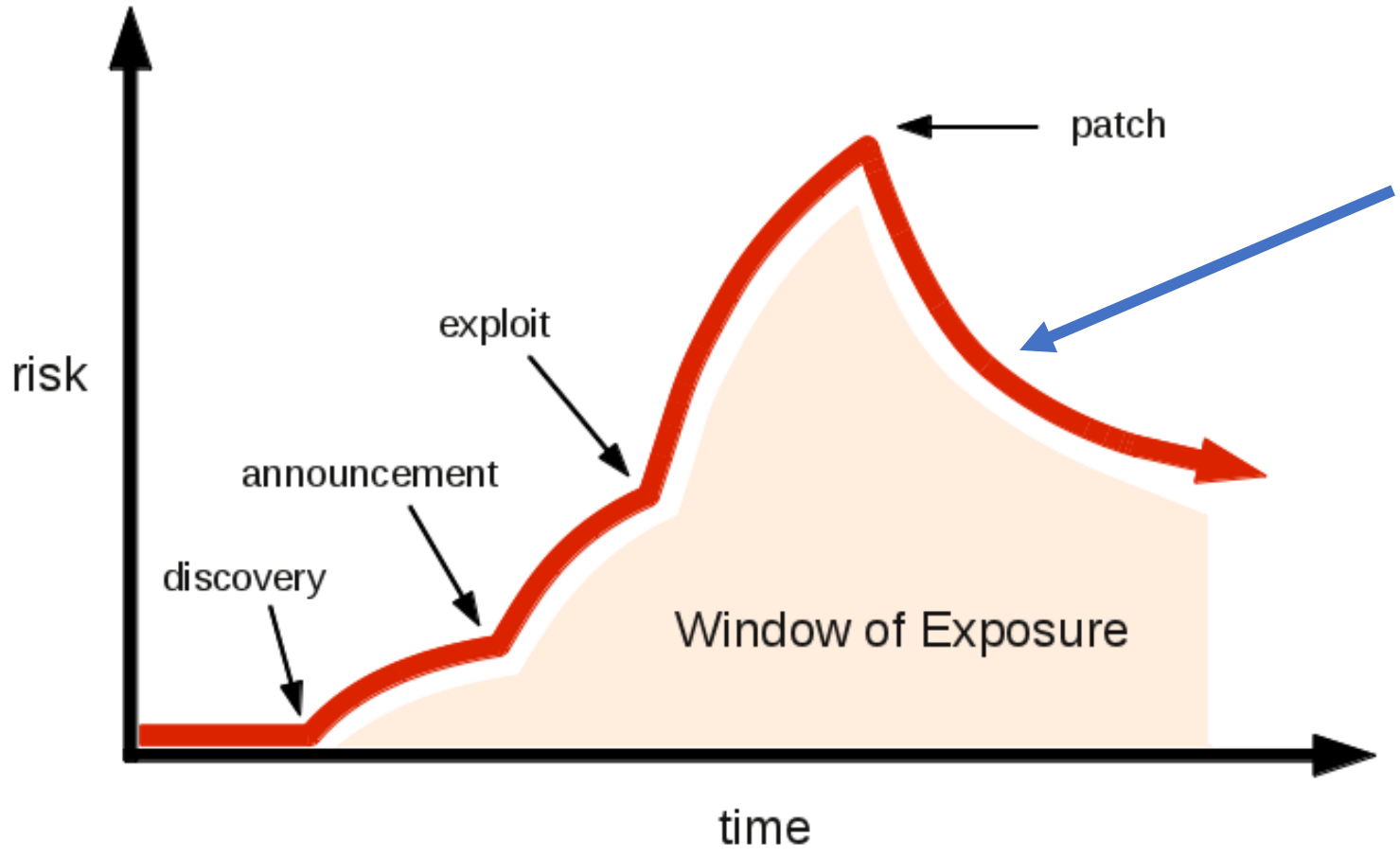
- Exploit resi pubblici permettono anche a persone con scarse competenze di compiere attacchi

Attacchi locali/remoti

- Attacco locale
  - Può essere eseguito solo disponendo di un account locale
    - ... che può essere ottenuto da un attaccante remoto per esempio sfruttando un'altra vulnerabilità

- Attacco remoto
  - Può essere eseguito anche non disponendo di un account locale

Vulnerabilità



Fase in cui la patch viene applicata ai sistemi

A volte la patch può essere resa disponibile prima della pubblicazione di un exploit (caso migliore)

Patch

- Aggiornamento finalizzato alla correzione di una vulnerabilità

- In genere disponibile sotto forma di:
  - Aggiornamento software
  - Modifica nella configurazione di un servizio

- (Temporaneamente) può essere resa disponibile una "mitigation"

Per ridurre il rischio serve ...

Disponibilità di una patch il prima possibile

Installare subito la patch

Applicare tutte le "buone pratiche" per mitigare il rischio associato a vulnerabilità (note o non note) per le quali una patch non è disponibile

Per ridurre il rischio serve

Disponibilità di una patch il prima possibile

Installare subito la patch

Applicare tutte le "buone pratiche" per mitigare il rischio associato a vulnerabilità (note o non note) per le quali una patch non è disponibile

Es. chiudere tutte le porte non strettamente necessarie
Es. evitare software EOL che non ricevono più aggiornamenti di sicurezza

Alcune indicazioni nelle presentazioni di domani

Creazione di un servizio in INFN Cloud

1. L'utente amministratore sceglie di istanziare un servizio del catalogo di INFN Cloud
2. Il layer PaaS sceglie un sito della federazione di INFN Cloud dove istanziare il servizio
3. Viene fatta partire una (o più) Virtual Machine partendo da una immagine fornita dall'admin di quel sito
4. Il servizio viene configurato su queste VM
5. L'utente amministratore usa e gestisce il servizio istanziato
6. L'utente amministratore eventualmente abilita altri utenti

Vulnerabilità e incidenti in INFN Cloud

- Bisogna tenere conto della specifica architettura di INFN Cloud e delle diverse responsabilità
- In INFN Cloud il coordinamento per la gestione delle vulnerabilità e incidenti di sicurezza (attacchi) è affidata al Security Incident Team (SIT)
- Implementando le procedure e direttive definite dal WP4 di INFN Cloud (Security, Policies & Procedures)
- In compliance con le procedure e direttive INFN sull'uso delle risorse informatiche

Vulnerabilità e incidenti: attori coinvolti

- Security Incident Team (SIT) e WP4 di INFN Cloud
- INFN CSIRT
- I gestori dell'infrastruttura INFN Cloud
- Gli sviluppatori dei servizi INFN Cloud
- L'utente amministratore

Vulnerabilità e incidenti: attori coinvolti

- Security Incident Te oud
- INFN CSIRT
- I gestori dell'infrastruttura INFN Cloud
- Gli sviluppatori dei servizi INFN Cloud
- L'utente amministratore

Offre sostegno nella prevenzione e gestione degli incidenti di sicurezza

Stretto coordinamento tra SIT e CSIRT

Vulnerabilità e incidenti: attori coinvolti

- Security Incident Team (SIT)
- INFN CSIRT
- I gestori dell'infrastruttura INFN Cloud
- Gli sviluppatori dei servizi INFN Cloud
- L'utente amministratore

INFN Cloud WP1 e site admin

Responsabili di gestire in maniera sicura e tenere aggiornati i vari servizi dell'infrastruttura

Responsabili di fornire e tenere aggiornate le immagini che vengono usate per le istanze degli utenti

Vulnerabilità e incidenti: attori coinvolti

- Security Incident Team (SIT) e WP4 di INFN Cloud
- INFN CSIRT
- I gestori dell'infrastruttura
- Gli sviluppatori dei servizi INFN Cloud
- L'utente amministratore

INFN Cloud WP5

Responsabili di fornire e tenere aggiornati i vari servizi, configurandoli nella maniera più sicura possibile

Vulnerabilità e incidenti: attori coinvolti

- Security Incident Team (SIT) e WP4 di INFN Cloud
- INFN CSIRT
- I gestori dell'infrastruttura
- Gli sviluppatori dei servizi
- L'utente amministratore

Responsabile di gestire in maniera sicura le istanze amministrate

Responsabile di applicare le istruzioni comunicate dal SIT/CSIRT

INFN Cloud Security Incident Team (SIT)

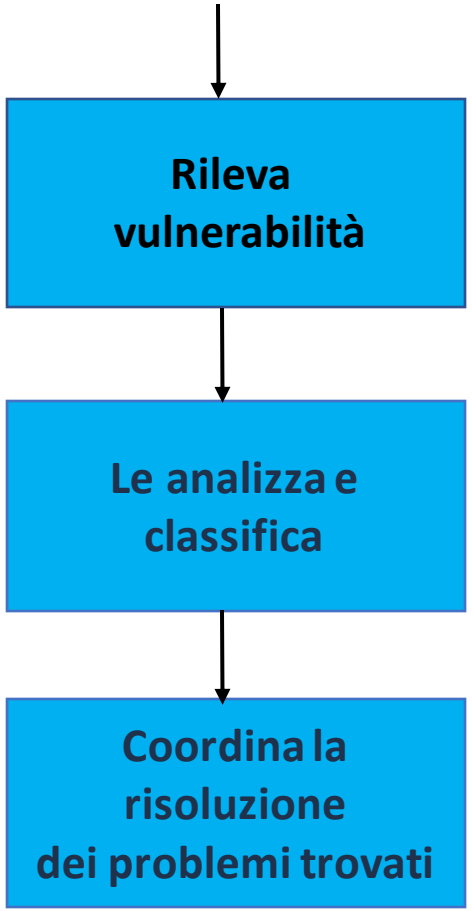
- Composizione attuale
  - Marica Antonacci (BA)
  - Vincenzo Ciaschini (CNAF)
  - Alessandro Italiano (BA)
  - Gianluca Peco (BO)
  - Massimo Sgaravatto (PD)
  - Stefano Stalio (LNGS)

security@cloud.infn.it

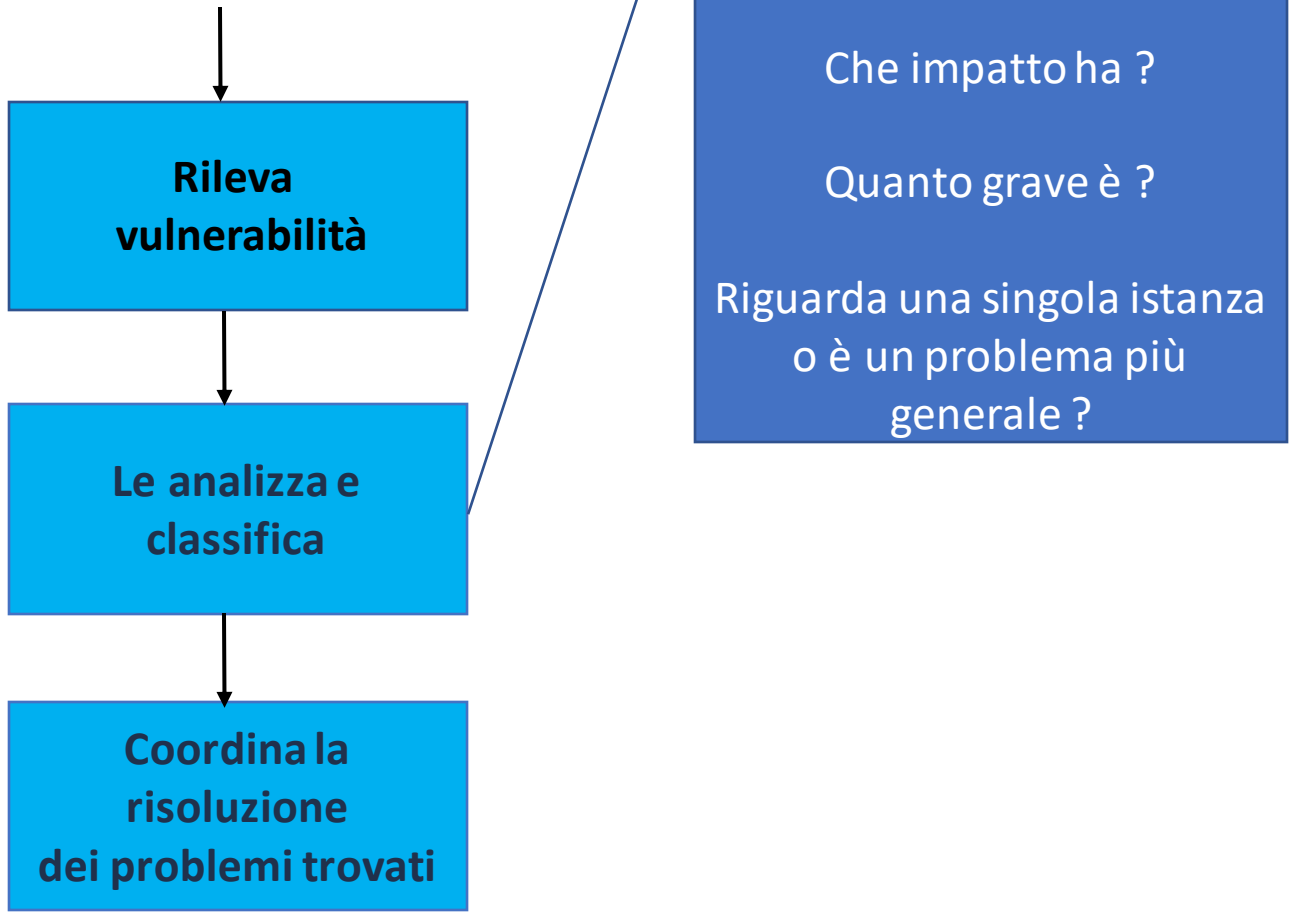
Un mail inviato a questo indirizzo crea un ticket

Per favore non cambiate subject rispondendo a un mail

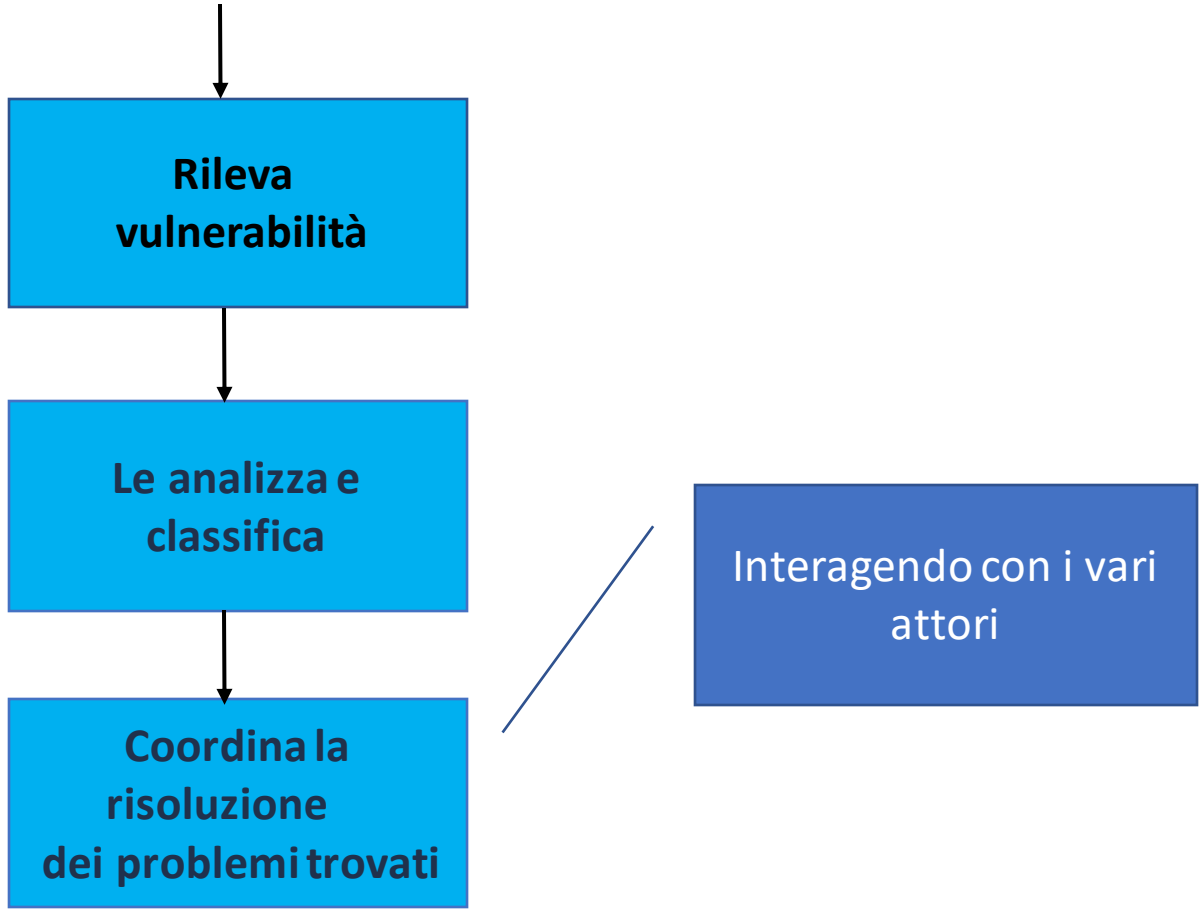
Vulnerabilità: attività del SIT



Vulnerabilità: attività del SIT



Vulnerabilità: attività del SIT

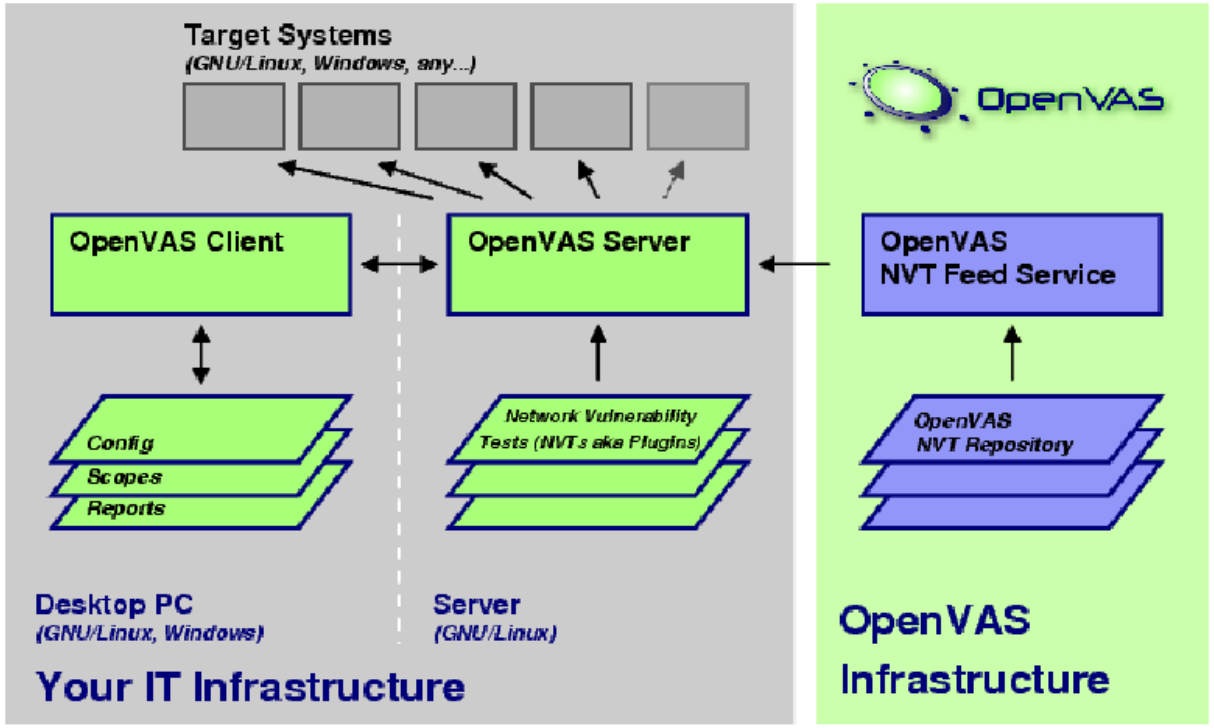


Rilevazione delle vulnerabilità

- Il SIT viene a conoscenza di vulnerabilità (vere o presunte) in diversi modi:
  - Vulnerability scan
  - Notifiche da GARR-CERT (via APM), INFN-CSIRT, ecc.. su vulnerabilità in specifiche istanze
  - Annunci di vulnerabilità in specifici software

Vulnerability scan

- Effettuate attraverso OpenVAS (GreenBone)
- Rileva eventuali vulnerabilità sui servizi esposti dalle istanze



Date	Status	Task	Severity	Scan Results					Actions
				High	Medium	Low	Log	False Pos.	
Thu Jan 9 03:05:08 2020	Done	Immediate scan of IP 192.168.11.137	N/A	0	0	0	0	0	

Report: Results (312 of 734)

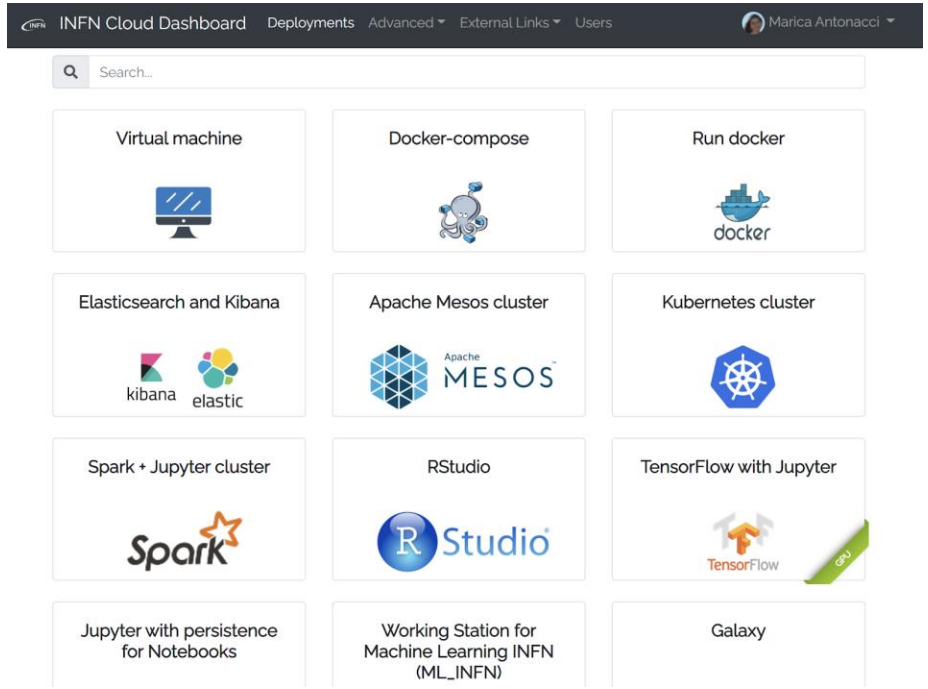
ID: 97cc63d0-65d7-45ee-8ca8-711df1baa7dd
Modified:
Created:
Owner: admin

1 - 100 of 312

Vulnerability	Severity	QoD	Host	Location	Actions
rexec Passwordless / Unencrypted Cleartext Login	10.0 (High)	75%	192.168.11.137	512/tcp	
Samba End Of Life Detection	10.0 (High)	75%	192.168.11.137	445/tcp	
Samba 'TALLOC_FREE()' Function Remote Code Execution Vulnerability	10.0 (High)	75%	192.168.11.137	445/tcp	
PHP Multiple Vulnerabilities - Aug08	10.0 (High)	75%	192.168.11.137	80/tcp	
PHP Version < 5.2.7 Multiple Vulnerabilities	10.0 (High)	75%	192.168.11.137	80/tcp	
PHP End Of Life Detection (Linux)	10.0 (High)	75%	192.168.11.137	80/tcp	
MySQL End Of Life Detection (Linux)	10.0 (High)	75%	192.168.11.137	3306/tcp	
PostgreSQL End Of Life Detection (Linux)	10.0 (High)	75%	192.168.11.137	5432/tcp	

Vulnerability scan

- Ogni servizio del catalogo di INFN Cloud viene controllato wrt la presenza di vulnerabilità prima di essere messo in produzione
- Questo però non è chiaramente sufficiente
  - Una vulnerabilità può essere scoperta dopo
  - Una vulnerabilità può essere stata introdotta da una configurazione/installazione fatta successivamente alla creazione del servizio



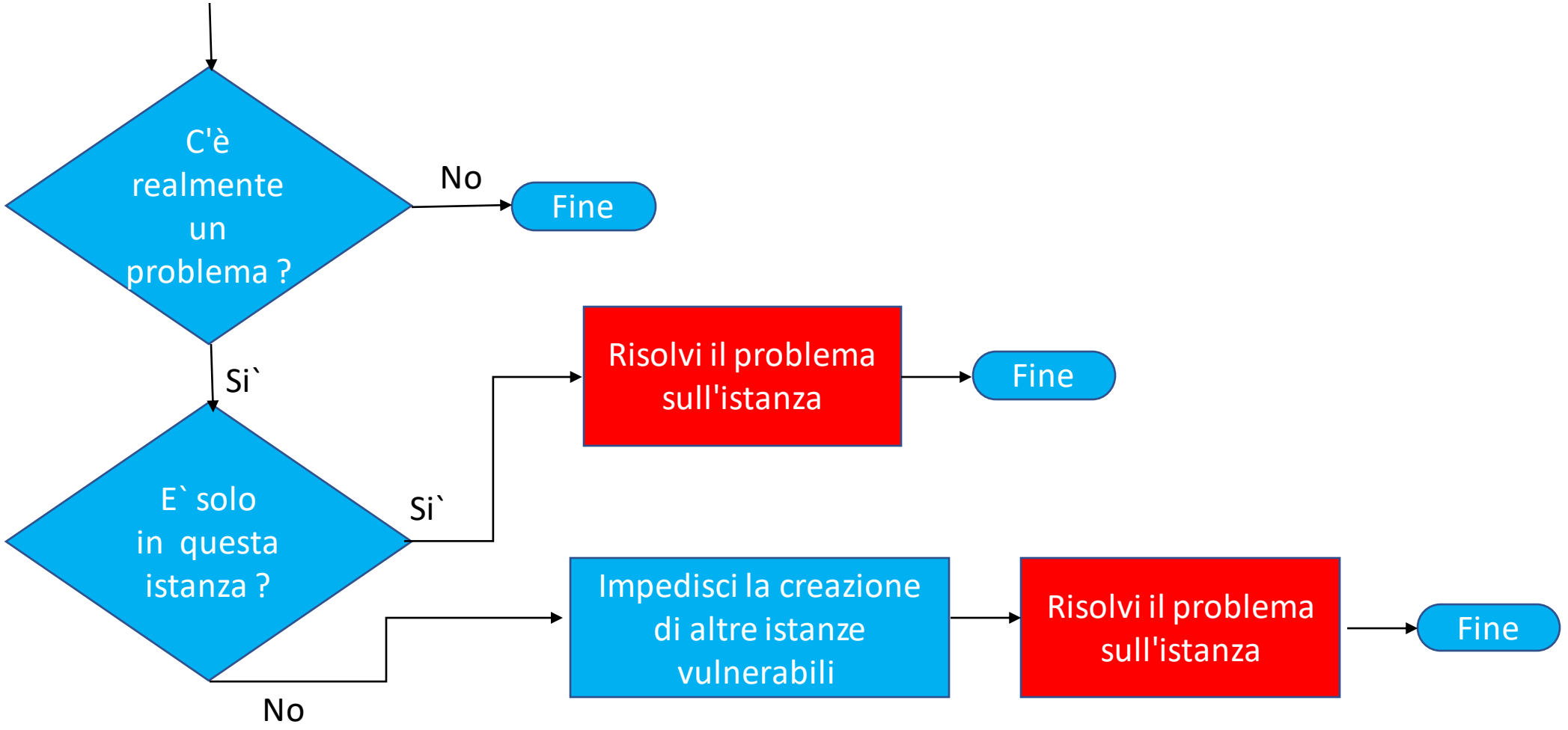
Vulnerability scan

-  Il vulnerability scanner controlla periodicamente tutte le istanze su INFN Cloud

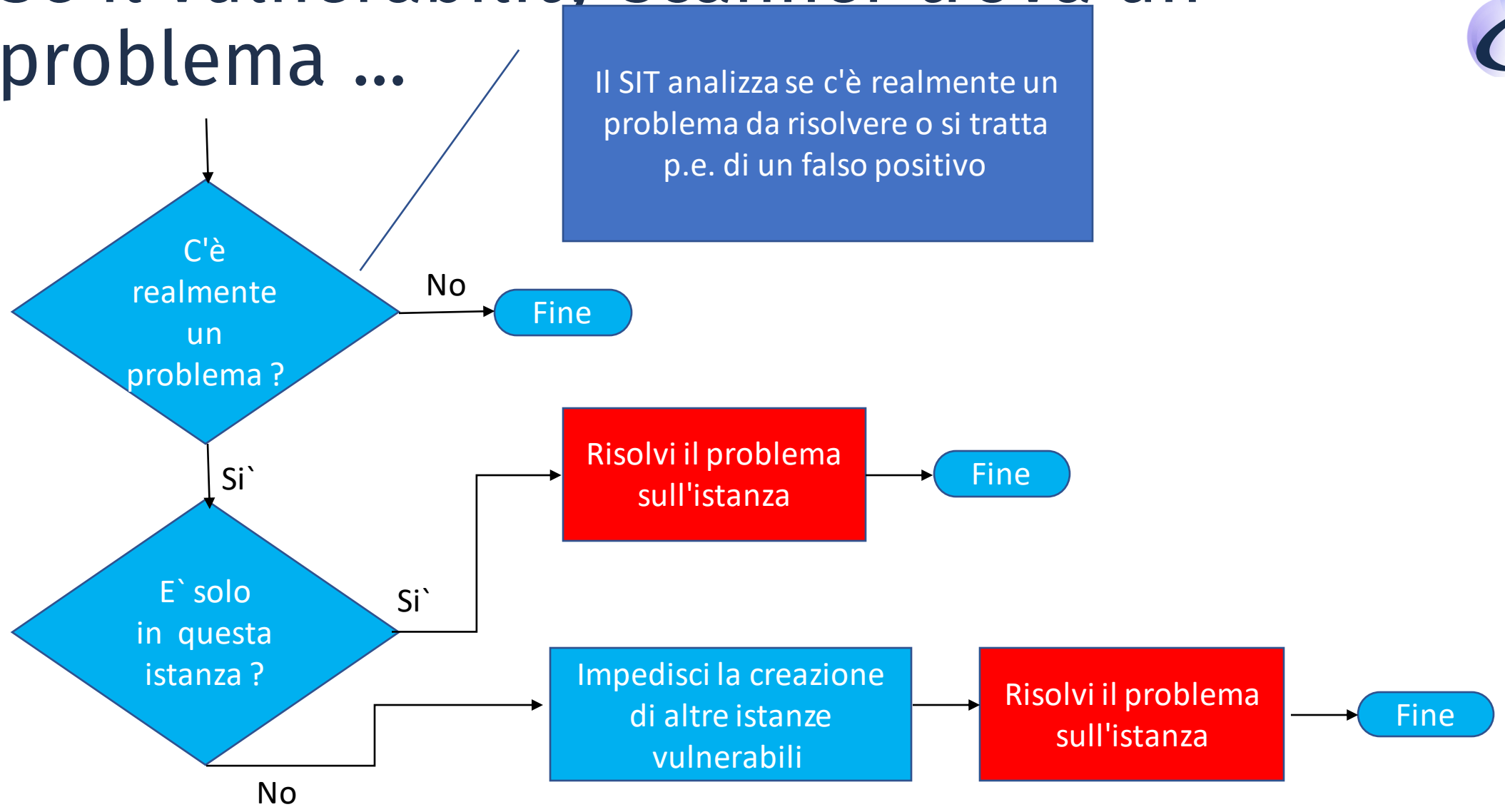
- Scansione fatta almeno 1 volta a settimana, di notte

- Scansione configurata in modo da minimizzare l'impatto

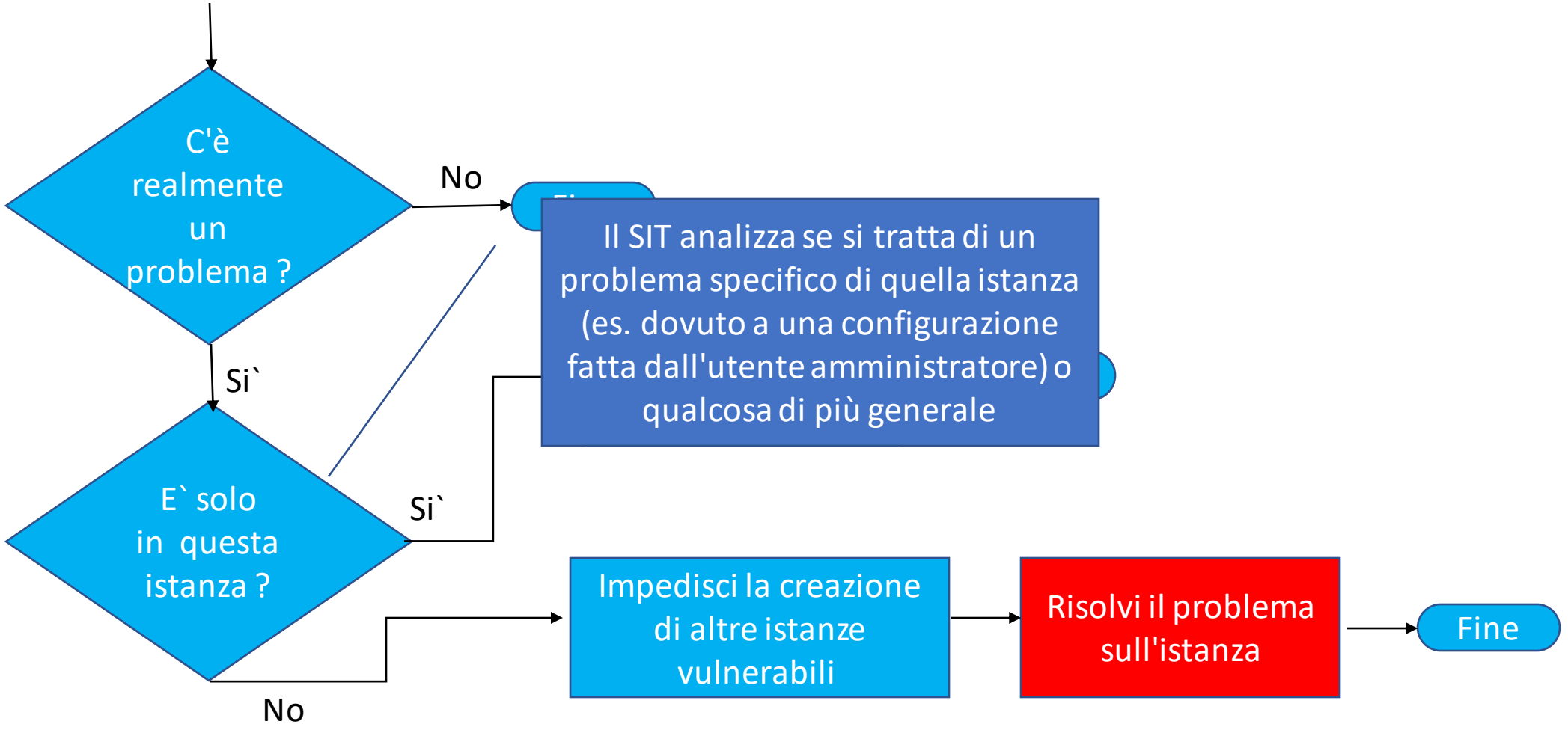
Se il vulnerability scanner trova un problema …



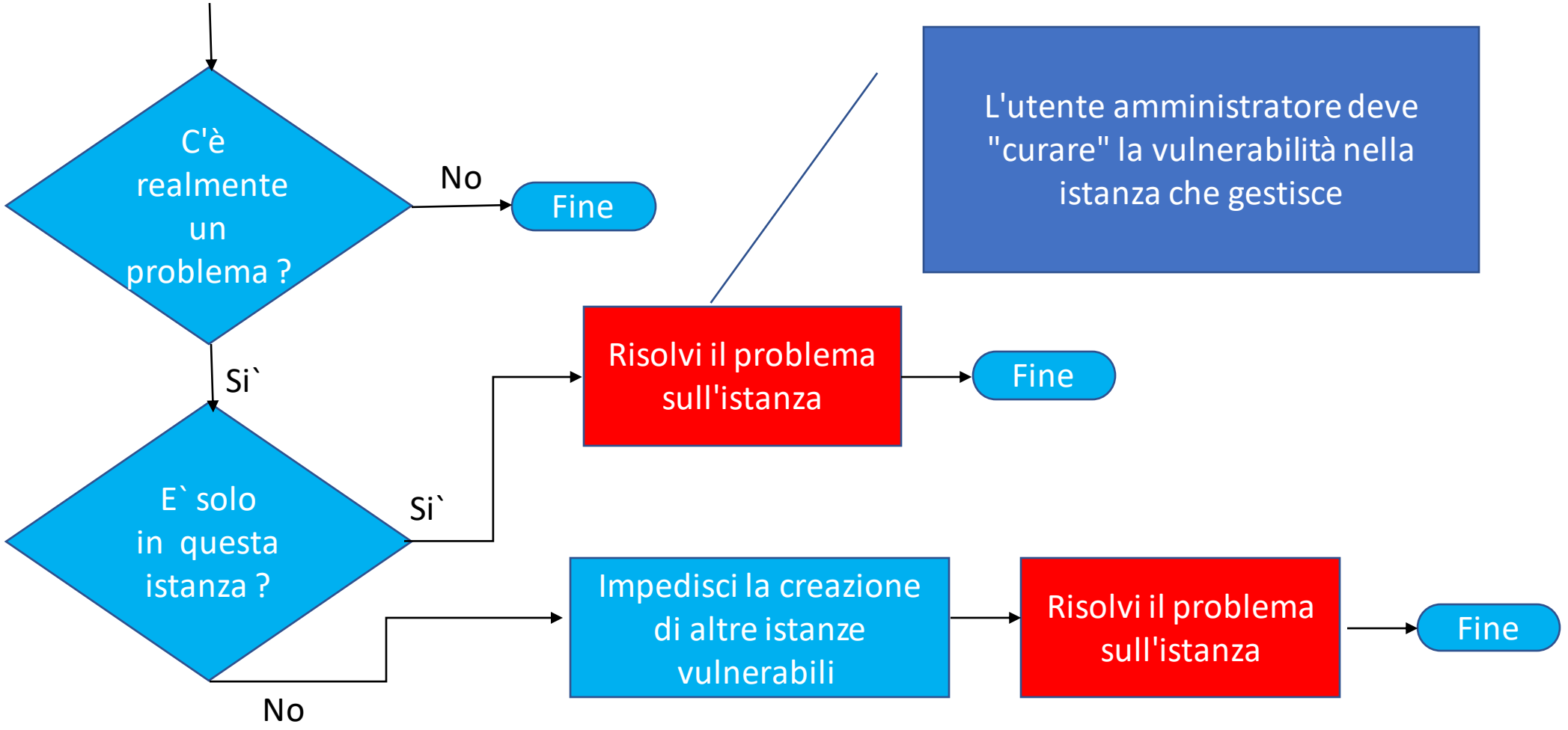
Se il vulnerability scanner trova un problema …



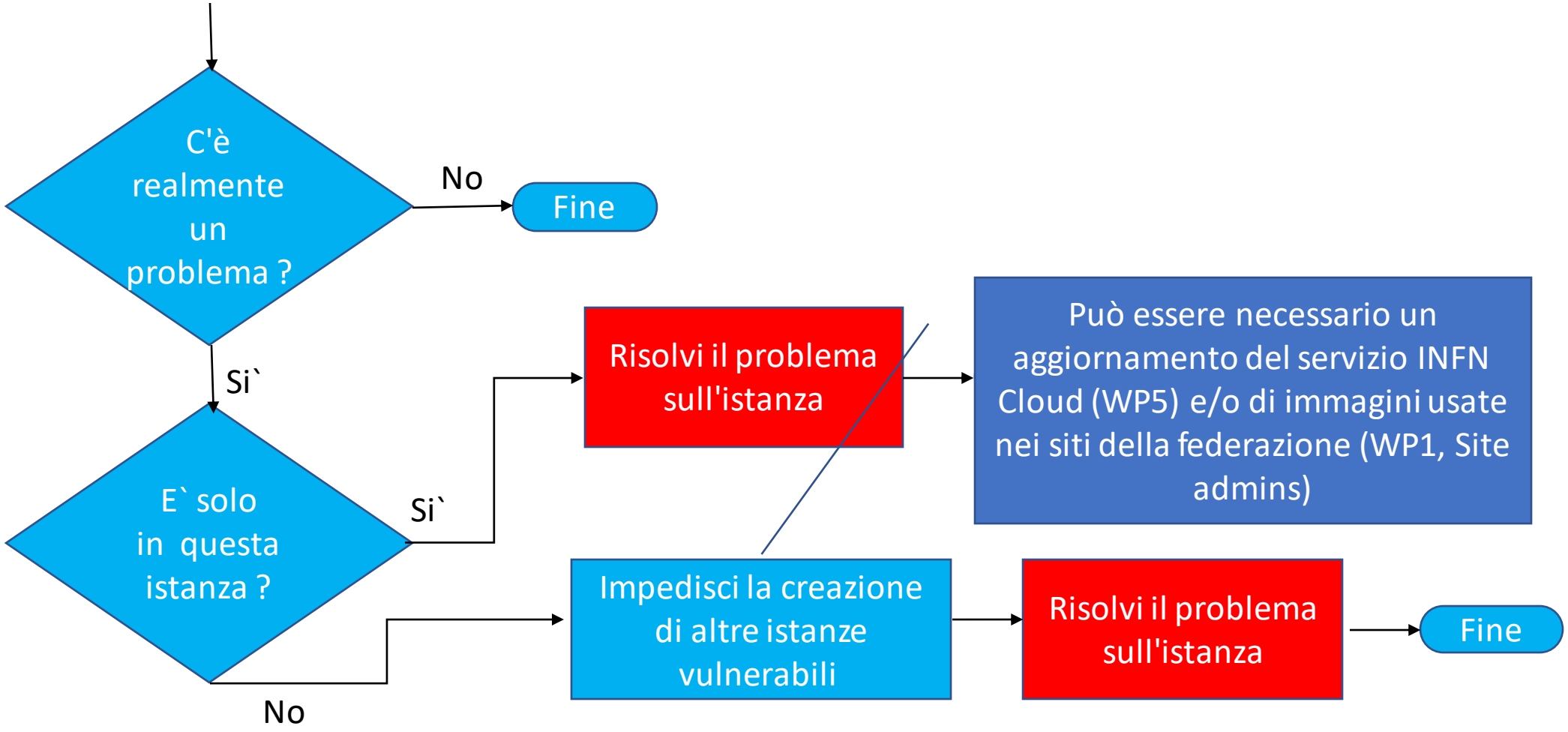
Se il vulnerability scanner trova un problema …



Se il vulnerability scanner trova un problema …



Se il vulnerability scanner trova un problema …



Se c'è un problema da curare nell'istanza …

… Il SIT apre un ticket notificando il rispettivo utente-amministratore (site admin in CC)

Dear user,

You are the owner of a VM called server-aa0fb6da-1[illegible]a-11ec-91f3-fa163e5257e7 (ip address: 192.135.24.144) which is deployed on the INFN Cloud infrastructure.
During the latest security scan, a vulnerability scored 5.0/10 has been found. Here the details:

'Vulnerable' cipher suites accepted by this service via the TLSv1.0 protocol:

TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)

'Vulnerable' cipher suites accepted by this service via the TLSv1.1 protocol:

TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)

'Vulnerable' cipher suites accepted by this service via the TLSv1.2 protocol:

TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)

The whole report for your VM is attached to this message as a pdf file.

You are expected to solve this issue before March 24, 2022. Feel free to send an e-mail to security@cloud.infn.it if you need help or advice on fixing this issue.

Thanks, the INFN Cloud Incident Team.

Report prodotto da OpenVAS con i dettagli del problema e come risolverlo

Risolvere la vulnerabilità nell'istanza

- E` responsabilità dell'utente-amministratore che gestisce quell'istanza
- E` l'unico che ha i privilegi amministrativi per farlo
- Va fatto entro i tempi indicati nel mail mandato dal SIT

Risolvere la vulnerabilità nell'istanza

- Va sempre fatto, anche se l'istanza non è critica e non contiene dati "critici"
  - La vulnerabilità può avere impatto anche su altri sistemi di altri utenti
  - Un incidente di sicurezza può avere ripercussioni su INFN Cloud e sull'Ente (es. reti INFN potrebbero essere "bannate")
- Va fatto per tutti i tipi di servizio

Risolvere la vulnerabilità nell'istanza

- Va sempre fatto, anche se l'istanza non è critica e non contiene dati "critici"
  - La vulnerabilità può avere impatto anche su altri sistemi di altri utenti
  - Un incidente di sicurezza può avere ripercuss
    Cloud e sull'Ente (es. reti INFN potrebbero es
- Va fatto per tutti i tipi di servizio

Ogni servizio viene configurato su una (o più) VM sulle quali l'utente amministratore che ha creato il servizio ha poteri amministrativi

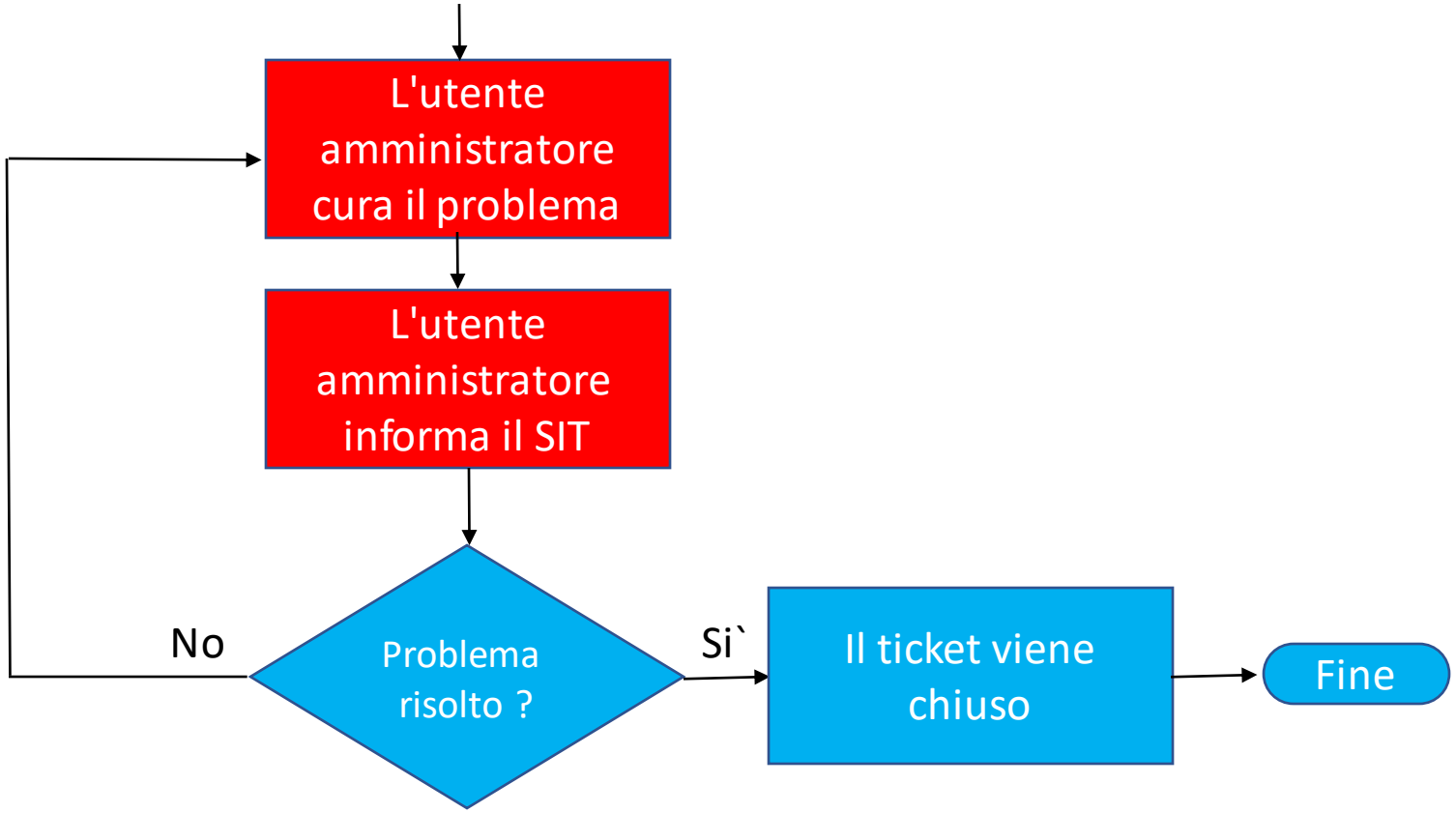
Tempi di risoluzione

Gravità	Vulnerabilità indicata dalla scansione	Tempo limite
Critica	9,10	<= 1 settimana
Alta	6,7,8	6 settimane
Media	4,5	6 mesi
Bassa	1,2,3	8 mesi

Il tempo limite è comunque specificato nel mail inviato dal SIT

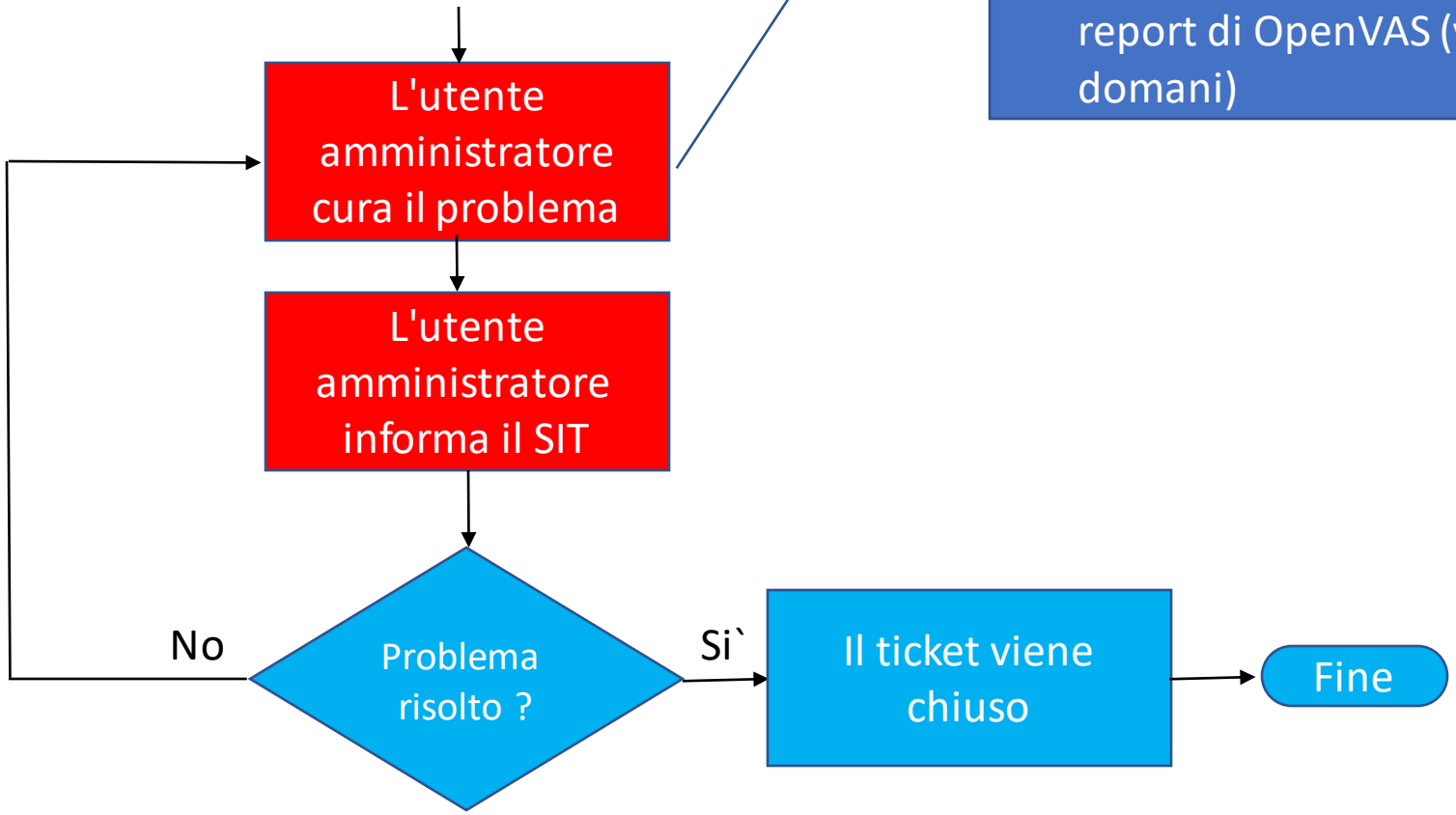
La gravità (e relativo tempo limite) di una vulnerabilità può cambiare

Risolvere la vulnerabilità nell'istanza

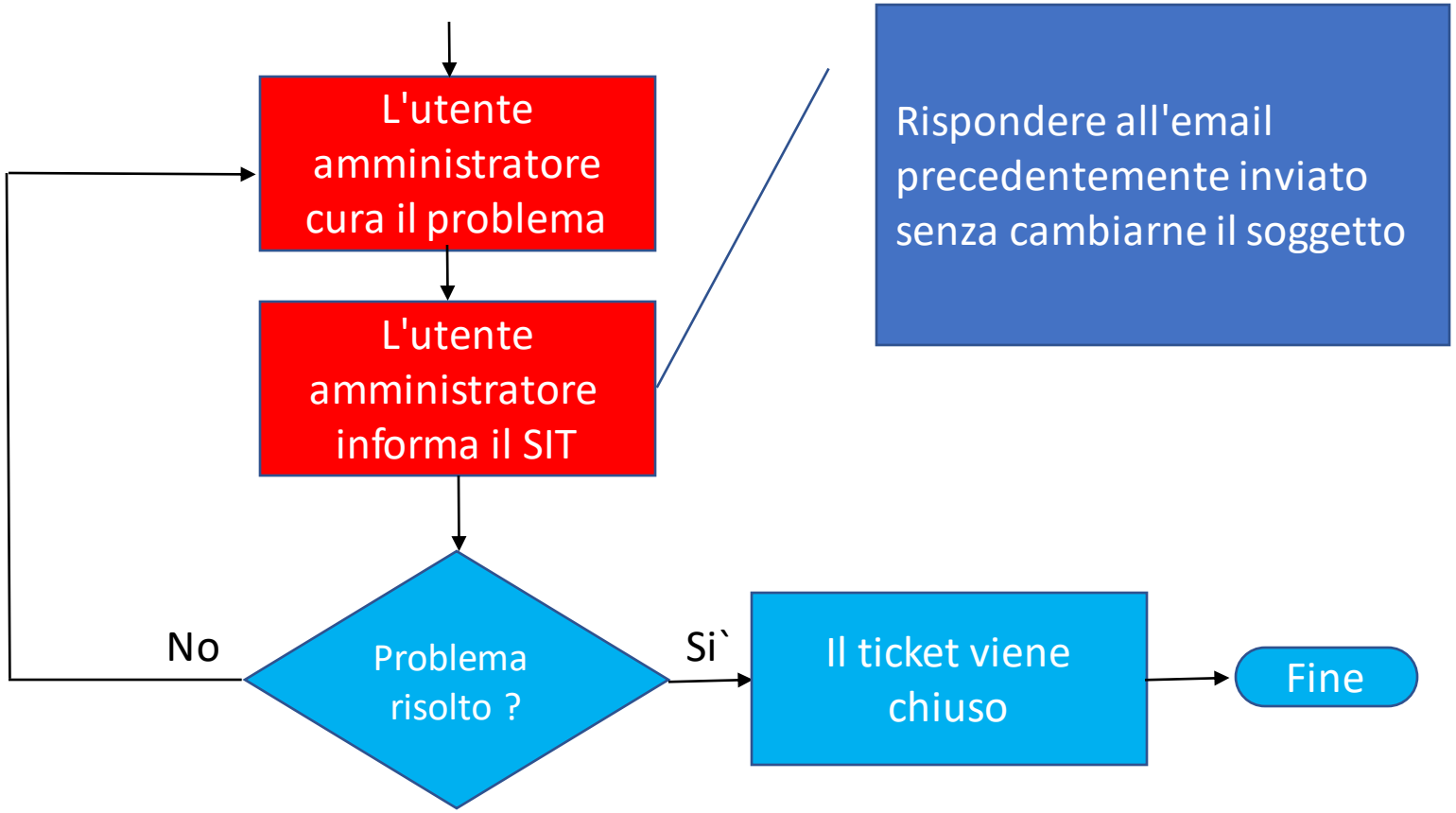


Risolvere la vulnerabilità nel

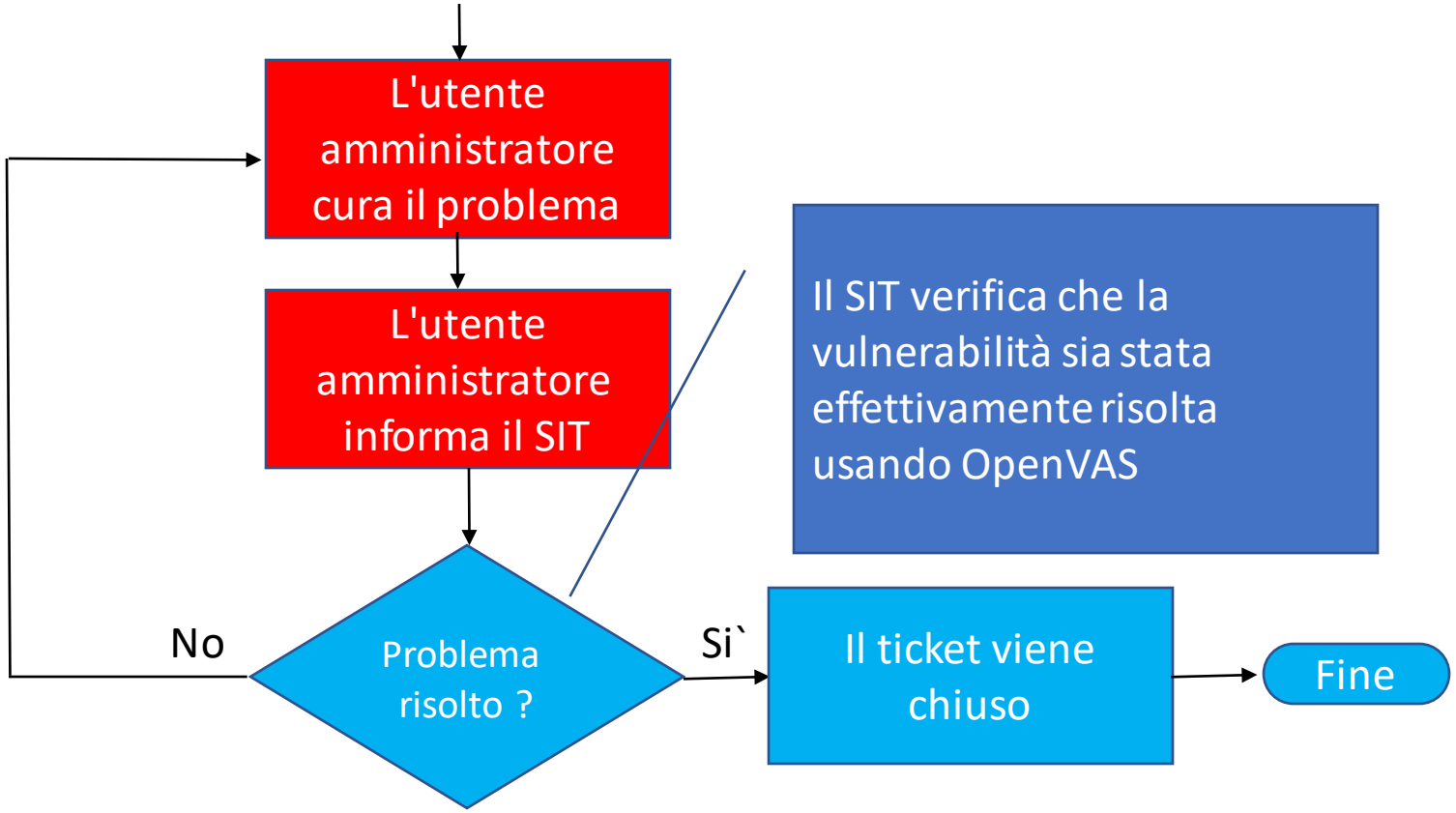
Due possibilità:
1. Distruggere l'istanza (e in caso crearne un'altra)
2. Risolvere il problema facendo riferimento a quanto riportato nel report di OpenVAS (v. presentazione domani)



Risolvere la vulnerabilità nell'istanza



Risolvere la vulnerabilità nell'istanza



Vulnerabilità a bassa gravità

- Sono quelle con "punteggio" < 4
- Tempo di risoluzione: 8 mesi
- L'utente amministratore può decidere di non risolverle, ma deve comunicarlo al SIT

Scansioni autenticate ?

- Stiamo investigando l'opportunità di eseguire scansioni autenticate
- Oltre a un controllo sui servizi esposti, viene fatto anche un controllo dall'interno del sistema
- Permettono un'analisi delle vulnerabilità molto più accurata

Scansioni autenticate ?

- Richiederebbe la presenza di un account non privilegiato sul sistema
  - Accessibile solo attraverso chiave SSH e solo dal server OpenVAS
  - L'account sarebbe automaticamente configurato al momento della creazione del servizio

- Comunicheremo opportunamente se si deciderà di implementarle anche nelle istanze degli utenti

Vulnerabilità non rilevate da OpenVAS

- Viene mandato un mail (in genere a tutti gli utenti) per segnalare il problema

- Nel mail è indicato
  - Il tipo di servizio coinvolto
  - Le action necessarie
  - Il tempo limite per applicarle

Esempio

```
--------------------------------------------------------------------------------

An English version of this message follows the Italian one

--------------------------------------------------------------------------------

Sono state annunciate due vulnerabilita` del kernel linux (CVE-2021-22555 e CVE-2021-3715) che possono permettere a un utente di ottenere accesso privilegiato.

Attenzione: si tratta di due vulnerabilita` diverse rispetto alla vulnerabilita` CVE-2021-33909 di cui vi avevamo riportato a Luglio.


Azioni richieste
================

Gli amministratori di servizio che hanno istanziato uno o piu' servizi "Virtual Machine" devono aggiornare il kernel di queste macchine virtuali facendo riferimento alle istruzioni riportate sot
Questo deve essere fatto entro 6 settimane


Istruzioni per virtual machine Centos7
--------------------------------------

Dare il comando:


uname -r


Se viene riportata una versione del kernel maggiore o uguale a 3.10.0-1160.42.2, la macchina virtuale non presenta queste vulnerabilita`.
In caso contrario, per aggiornare il kernel si puo` usare il seguente comando (il comando potrebbe non aggiornare nessun pacchetto se il nuovo kernel e` stato gia` installato dal sistema di aggi


sudo yum clean all && yum -y update kernel*


Per abilitare l'uso del nuovo kernel, e` necessario un reboot:
```

Conferma esplicita

- Nel caso di vulnerabilità critiche o che abbiano impatto rilevante, il SIT può chiedere esplicita conferma che siano state applicate le indicazioni date

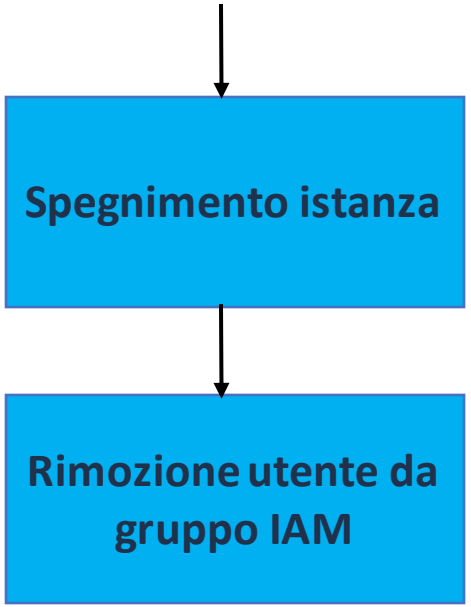
- La non risposta è interpretata come il non avere risolto la vulnerabilità nei tempi stabiliti

Vulnerabilità non risolta

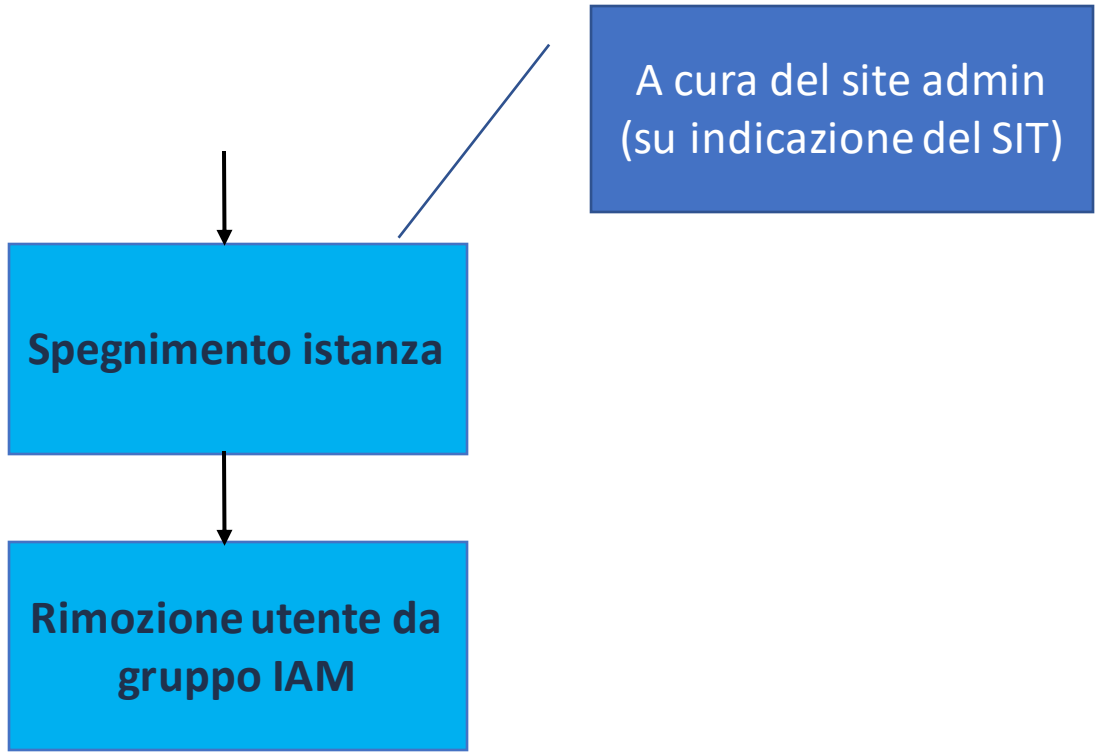
- Se la vulnerabilità in una istanza non viene curata nei tempi prestabiliti, viene isolata

- Viene rimessa in rete solo quando la vulnerabilità viene risolta

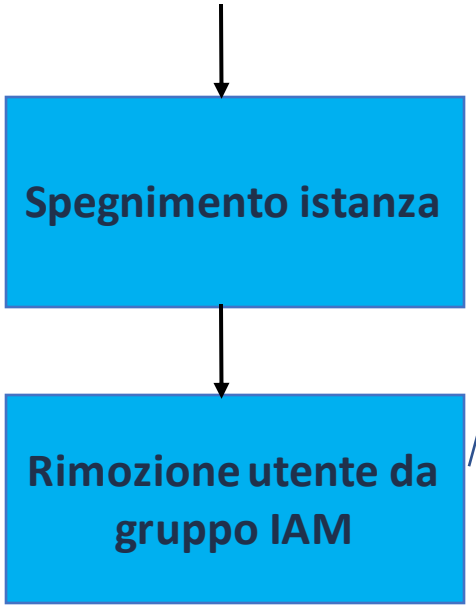
Isolamento di una istanza



Isolamento di una istanza



Isolamento di una istanza



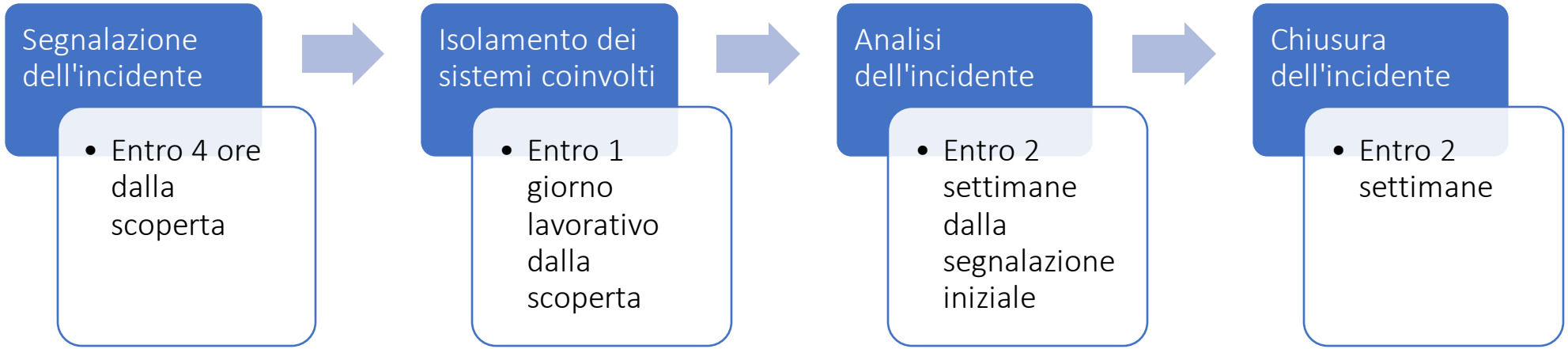
Per evitare che l'utente amministratore riaccenda l'istanza.

L'utente amministratore non potrà istanziare altri servizi nella quota assegnata a quel gruppo.

"Riabilitazione" di una istanza isolata

1. L'utente amministratore comunica l'indirizzo IP da cui si collegherà
2. Il site admin riaccende l'istanza abilitandone l'accesso solo dall'IP indicato dall'utente amministratore
3. L'utente amministratore si collega alla istanza e risolve la vulnerabilità
4. Il site admin ripristina il setting di rete originario dell'istanza
5. L'utente amministratore viene riabilitato nel gruppo IAM dove era stato prima rimosso

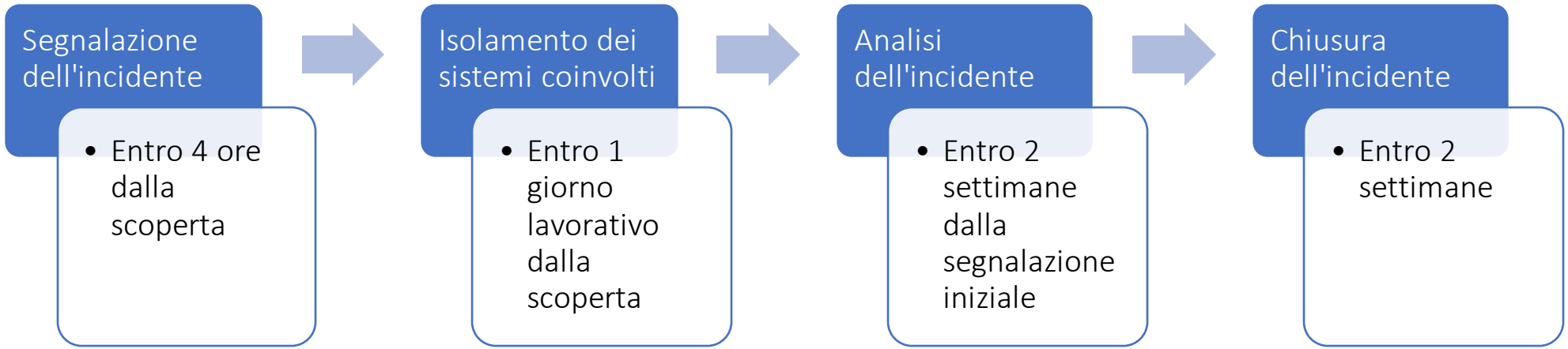
Gestione di un incidente (attacco)



Gestione di un incidente (attacco)

Chi scopre un incidente (vero o sospetto) deve comunicarlo subito al SIT

Il SIT informa l'INFN CSIRT

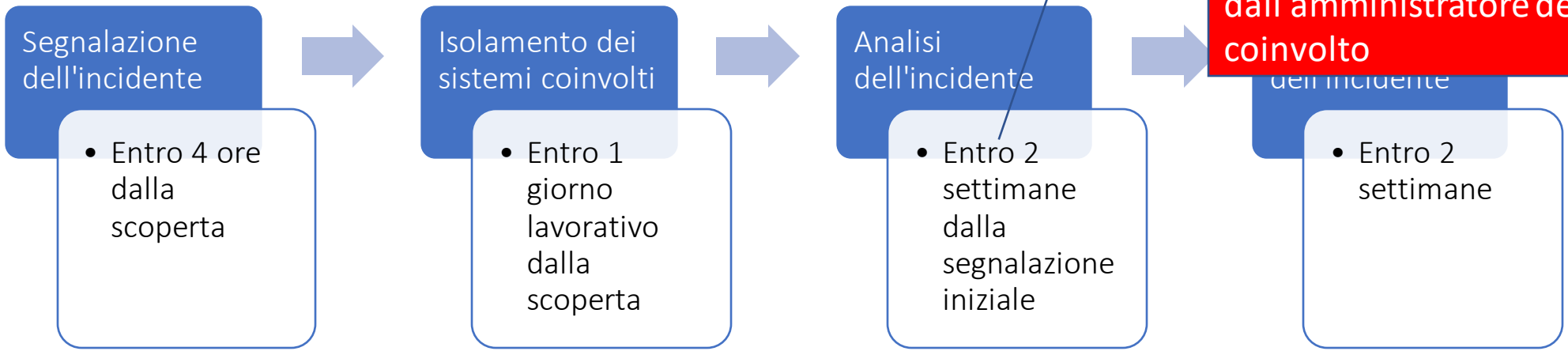


Gestione di un incidente (attacco)

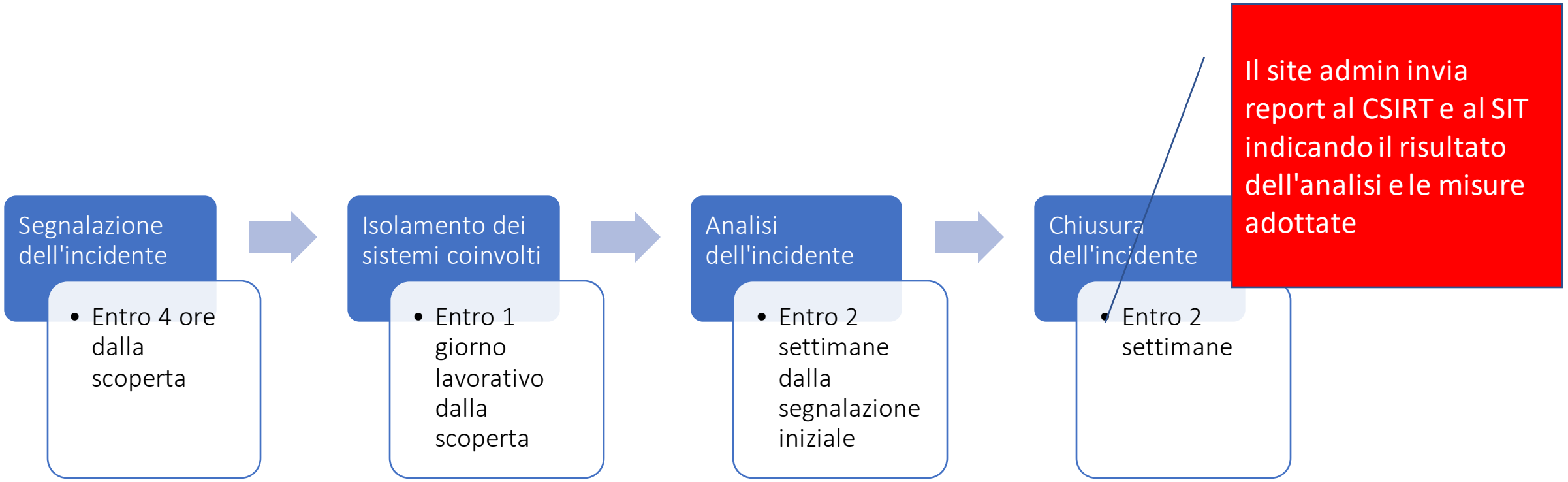
Gestione di un incidente (attacc

- Da dove è partito l'attacco ?
- Evidenze di compromissione ?
- Vulnerabilità sfruttate ?
- Tipo di attacco ?
- Cosa ha fatto l'attaccante ?
- Dati compromessi ?
- Account compromessi ?

Da parte del site admin e dall'amministratore del sistema coinvolto



Gestione di un incidente (attacco)



Riferimenti

- INFN Cloud Policies & Procedures

  https://www.cloud.infn.it/policies-procedures/

  - Scansioni di sicurezza e gestione degli incidenti su INFN CLOUD

- INFN CSIRT web site

  https://www.csirt.infn.it

- INFN DPO (Data Protection Officer) web site

  https://dpo.infn.it/

Grazie per l'attenzione !

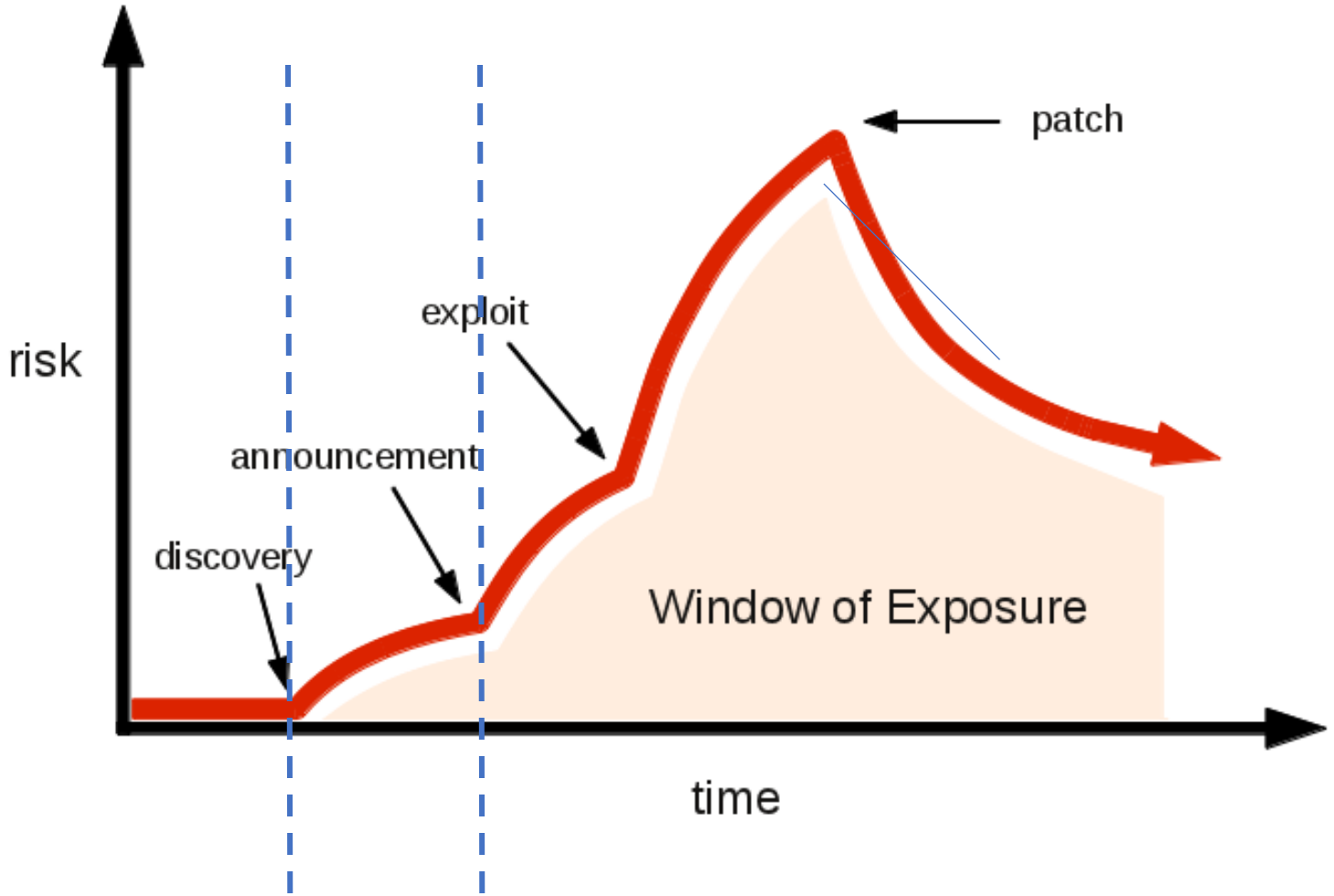
Backup slides

Esempio: root escalation

- Utente locale acquisisce privilegi amministrativi sfruttando una vulnerabilità

- Scenario tipico
  1. Attaccante remoto accede a un account locale non privilegiato sfruttando un'altra vulnerabilità
     - Es. account con password "debole"
     - Es. stessa password usata in altro sito che è stato oggetto di un data breach
  2. Usando la vulnerabilità di tipo root escalation l'attaccante acquisisce privilegi amministrativi

Zero day exploit



Zero day exploit:
Attacco per vulnerabilita`
non ancora pubblica

Data Breach

- Violazione di sicurezza che comporta la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati

- Può avvenire a seguito di un attacco informatico ma può avere altre cause (es. furto o smarrimento di un dispositivo informatico)

Dati personali

Qualsiasi informazione riguardante una persona fisica («interessato») identificata o identificabile

V. "Norme per il trattamento di dati personali nell'INFN" *

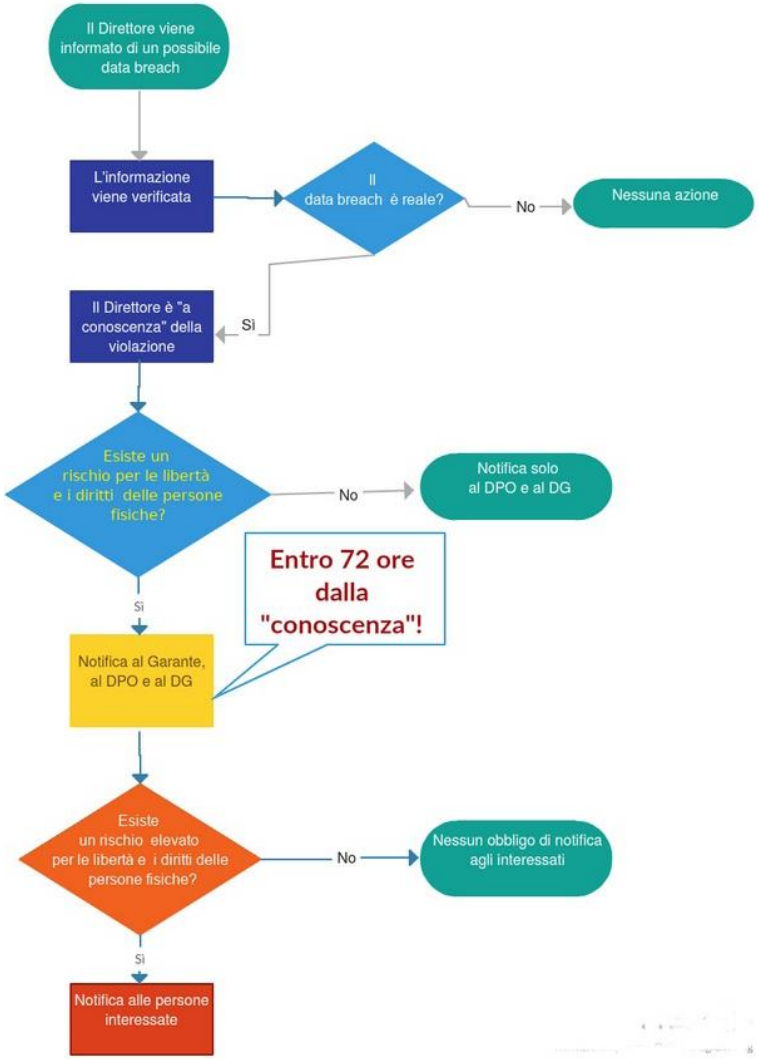
* https://dpo.infn.it/wp-content/uploads/2018/12/Norme_Trattamento_Dati_Personali_INFN.pdf

Procedura per data breach

- Non esiste (almeno al momento) una procedura specifica per INFN Cloud

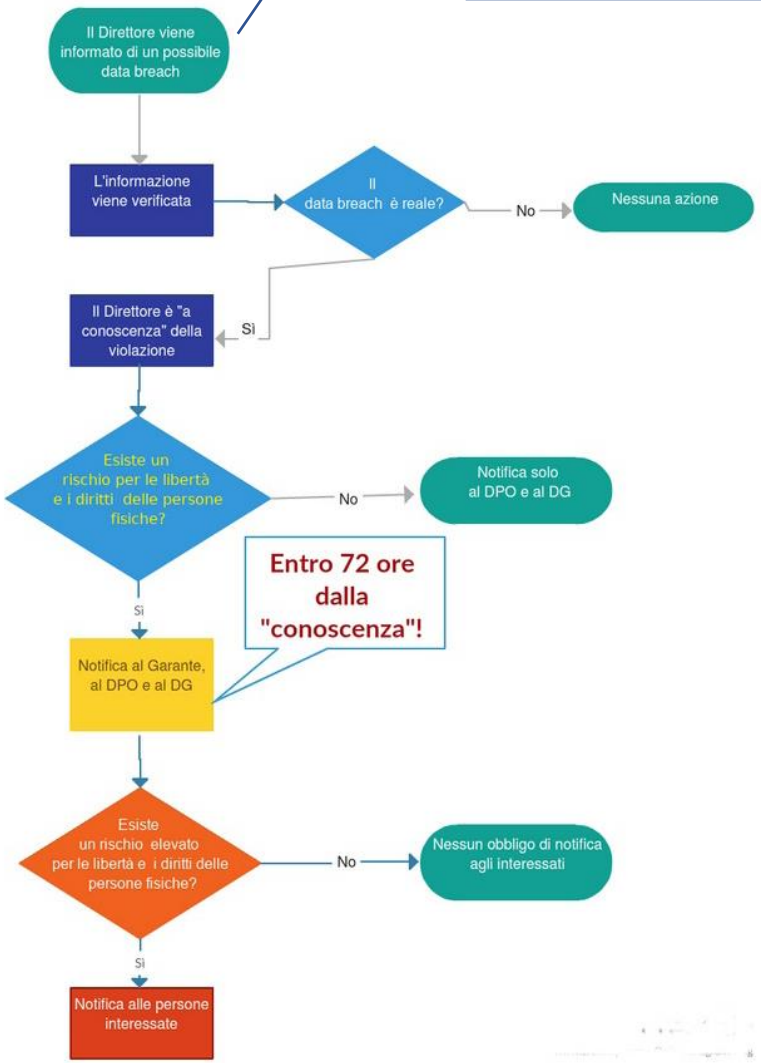
- Vale quindi la normale procedura da utilizzare nell'INFN (v. presentazione del I modulo)

INFN Data Breach procedure



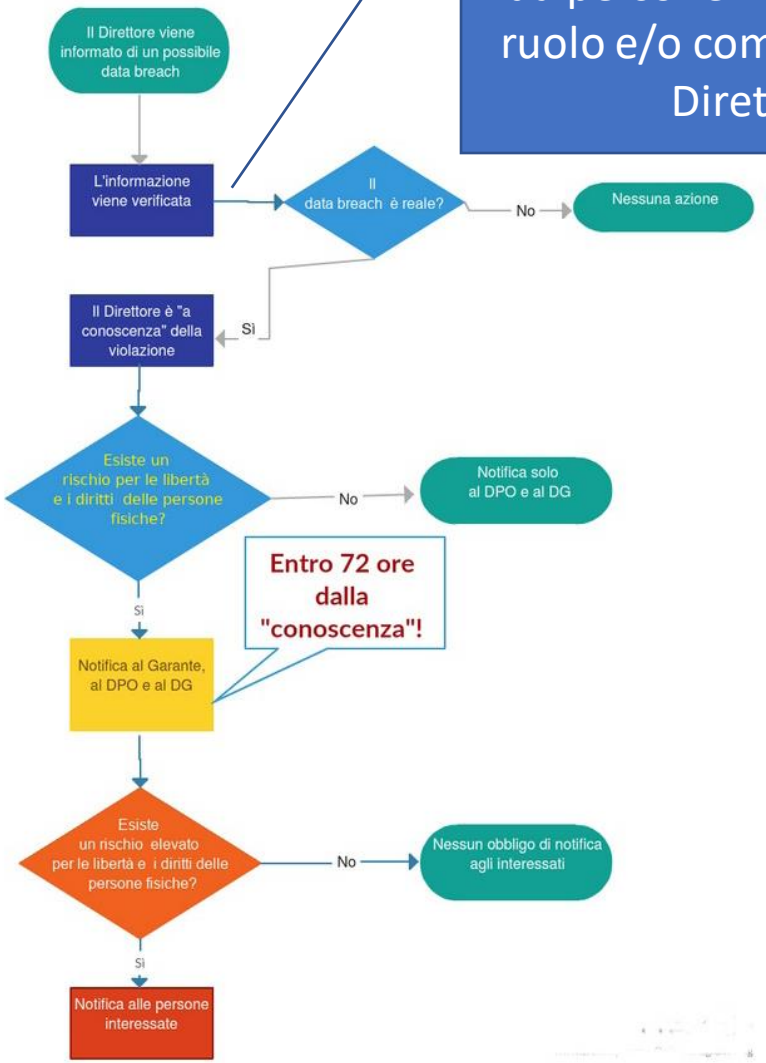
INFN Data Breach proc

Chi e` a conoscenza di un data breach (reale o sospetto) deve avvertire Direttore e referente locale del DPO

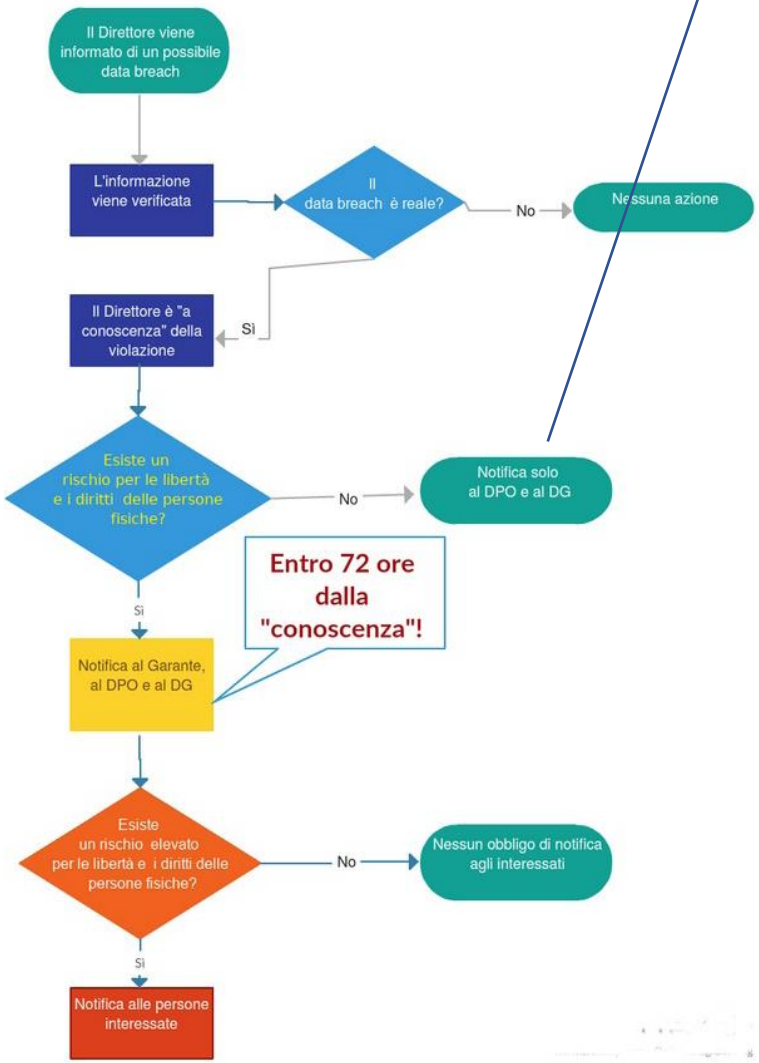


INFN Data Breach procedure

Data breach viene verificato da persone incaricate (per ruolo e/o competenza) dal Direttore

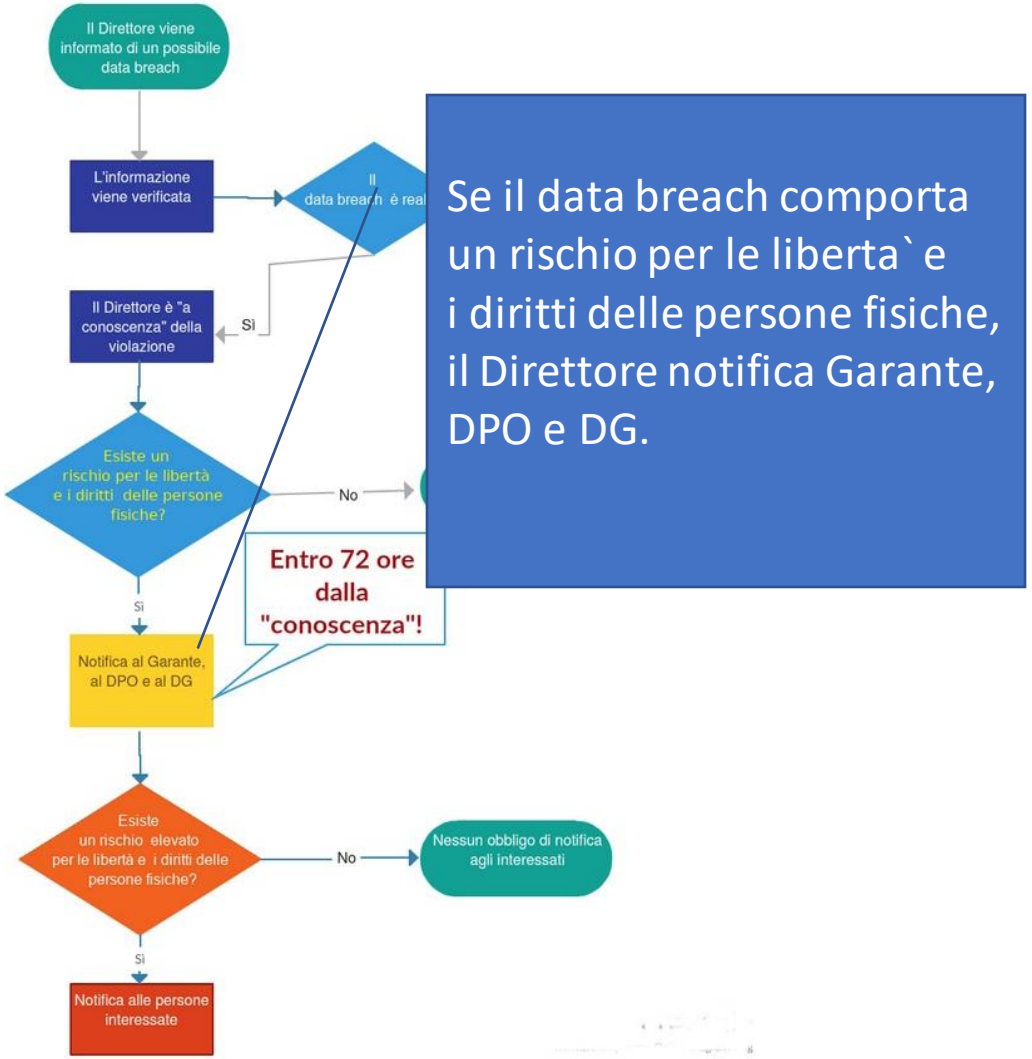


INFN Data Breach procedure



Se il data breach non comporta un rischio per le liberta` e i diritti delle persone fisiche, il Direttore notifica DPO e DG. Viene indicato il risultato dell'analisi e le azioni da intraprendere

INFN Data Breach procedure

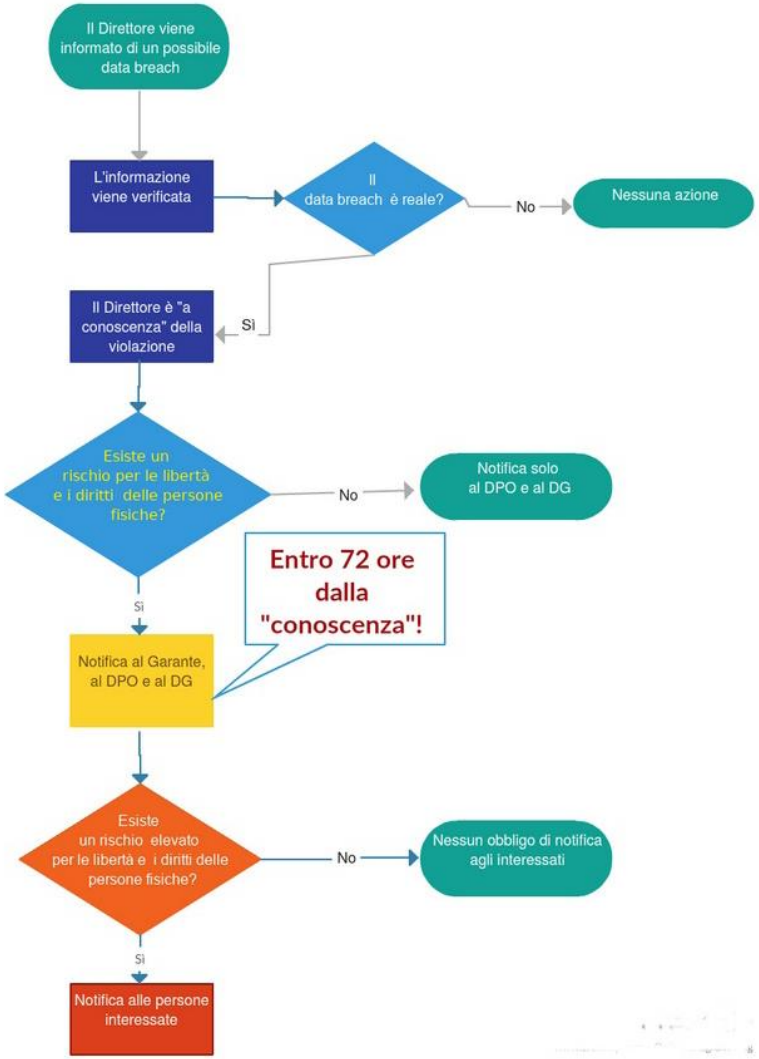


Se il data breach comporta un rischio per le liberta` e i diritti delle persone fisiche, il Direttore notifica Garante, DPO e DG.

INFN Data Breach procedure

Se c'e` un rischio elevato per le liberta` e i diritti delle persone fisiche, il Direttore informa gli interessati sulle conseguenze della violazione e sulle azioni che verranno intraprese

INFN Data Breach procedure



Il Direttore notifica il CSIRT

Il Direttore eventualmente provvede alla denuncia all'autorita` giudiziaria