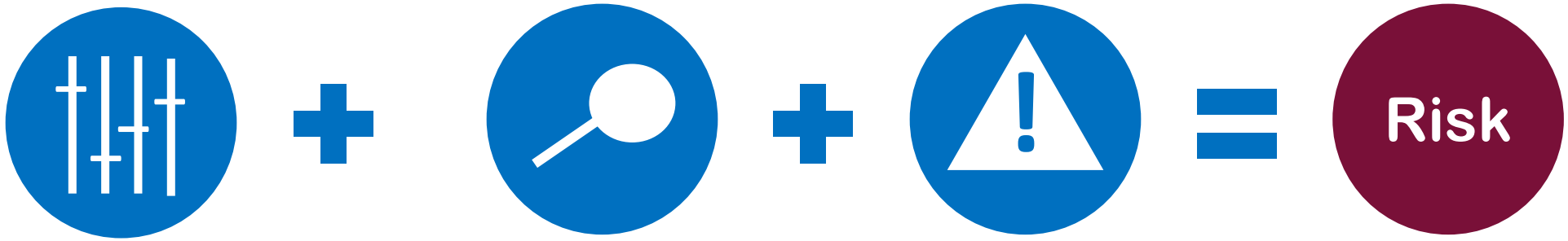
Calcolo del rischio informatico

Intelligent Proactive Monitoring

Intelligent Proactive Monitoring

Step necessari per il calcolo del rischio IT



Identificazione del metodo

In base alla metodologia utilizzata

Scansione

Ricerca all'interno dell'infrastruttura dell'Asset Hw e Sw

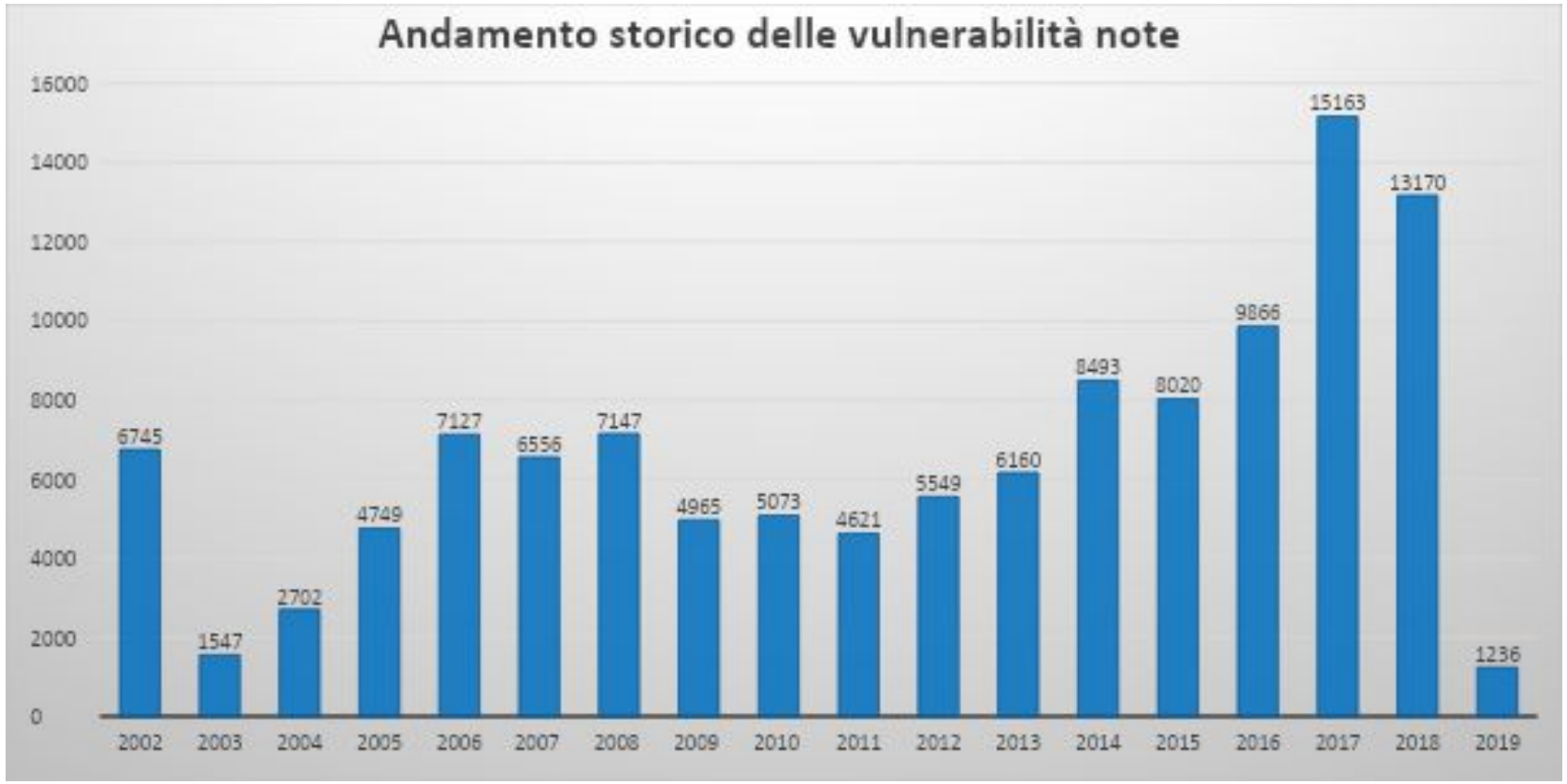
Ricerca vulnerabilità

In base alle vulnerabilità note sull'asset

Rischio

Calcolo del rischio

Elementi necessari per il calcolo del rischio IT



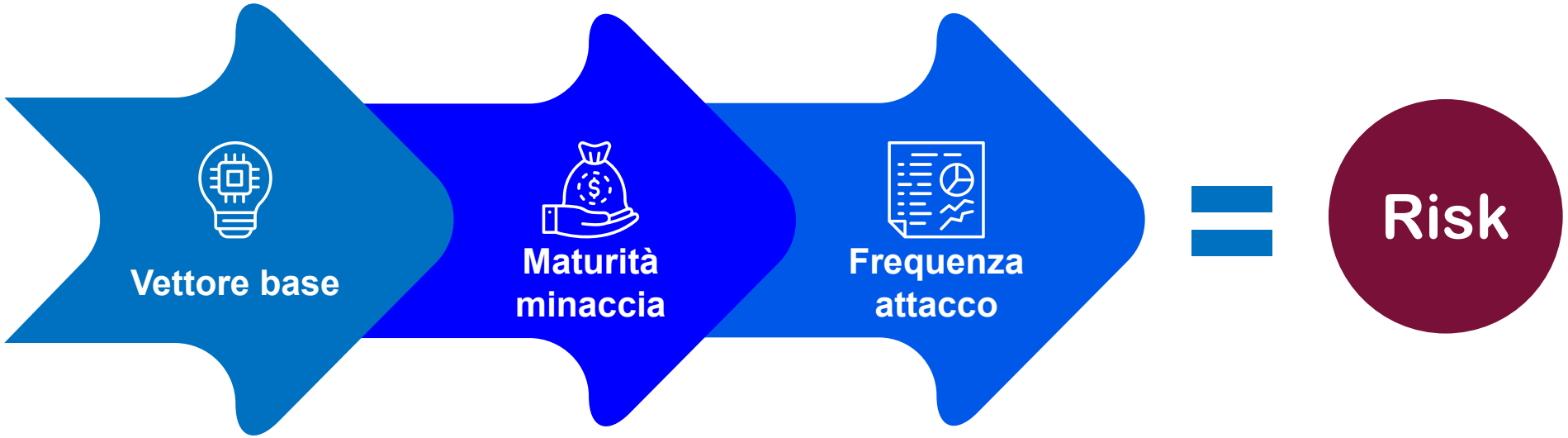
Calcolo del Rischio

1. Metodo Frequency (Umesh, Chanchala «Quantitative Security Risk Evaluation using CVSS by Estimation of Frequency»)

2. Cvss ver. 3.0 secondo le best practice fornite dal NIST per l'applicazione nelle Agenzie Federali (US)

Metodo Frequency

Procedura di calcolo



Fornito dal Mitre

Temporal Score

Frequency Score

Metodo Frequency

Calcolo del Temporal Score

1. Il Temporal Score tiene conto della maturità dell'exploit rispetto alla disponibilità delle patch
2. Temporal Score = BaseScore$*\frac{MaturityOfExploitCode}{Remediation\ Level}$
3. Stima del Remediation Level in base allo studio di Thripati e Singh «Estimating risk level for vunerability using CVSS»
    1. Stimano che il tempo medio di rilascio di una patch vari tra i 23 ed i 40 giorni.

Metodo Frequency

Calcolo del Frequency Score

1. Il Frequency Score vuole stimare la frequenza che questa vulnerabilità venga sfruttata, basandosi sull'assunzione che la frequenza aumenta con la facilità di sfruttare la vulnerabilità stessa
2. Si basa sul Tempora Score e sui parametri AV, AC e AU del vettore base
3. Frequency Score = (AV*AC*AU) + Temporal Score

Exploitability Metrics

Attack Vector (AV)*

Local (AV:L)	Adjacent Network (AV:A)	Network (AV:N)

Access Complexity (AC)*

High (AC:H)	Medium (AC:M)	Low (AC:L)

Authentication (Au)*

Multiple (Au:M)	Single (Au:S)	None (Au:N)

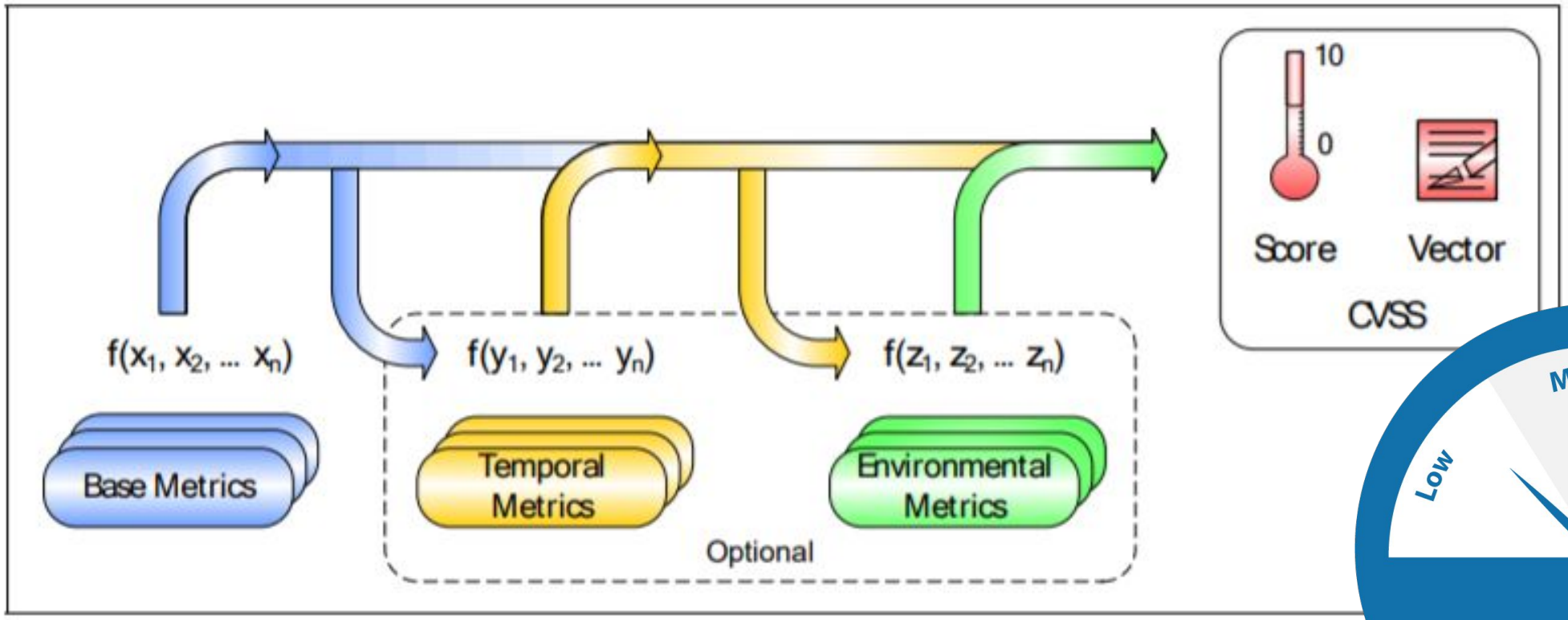
Metodo Frequency

Difetti

1. Non tiene conto della sensibilità dell’asset
2. Una playstation o un server che comanda l’apertura delle saracinesche della diga di Ham hanno lo stesso valore.

Metodo CVSS 3.0

Calcolo del Frequency Score

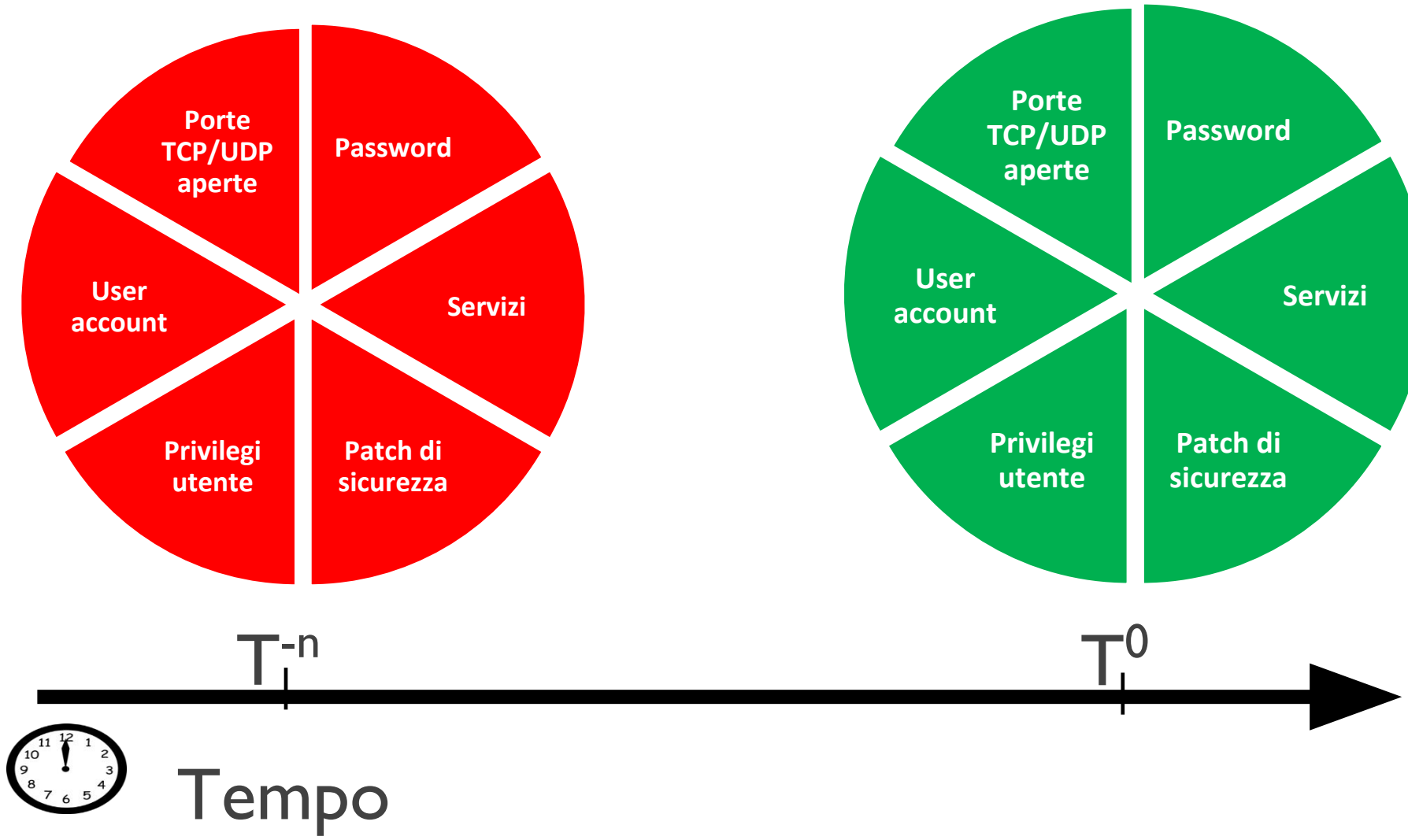


Security Analyzer: esempio

Dashboard

- Trend del rischio
- Trend vulnerabilità
- Statistiche
- Top 10 elementi a rischio
- …

Processo di Hardening

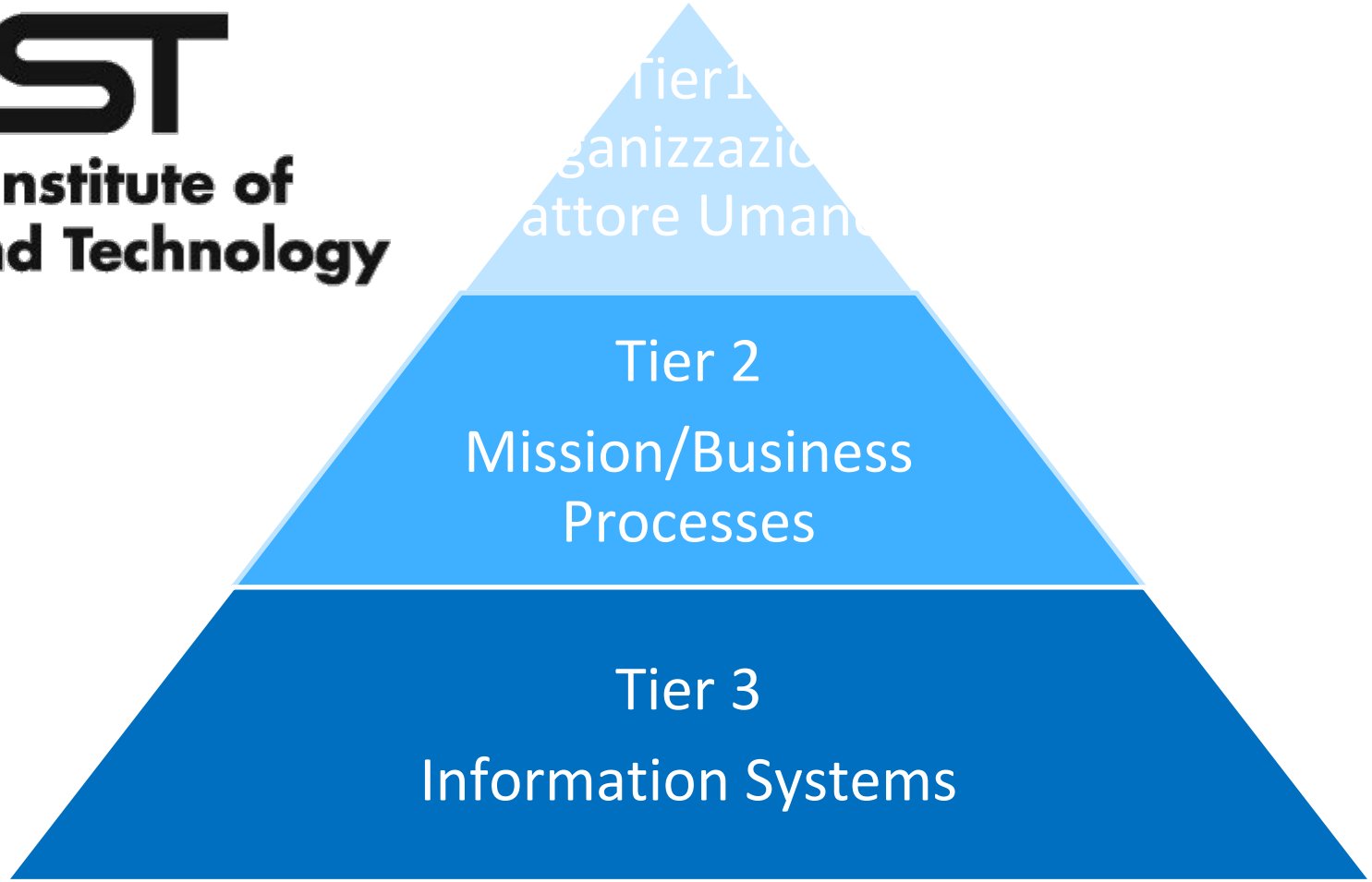


Processo di Hardening

Fase finale

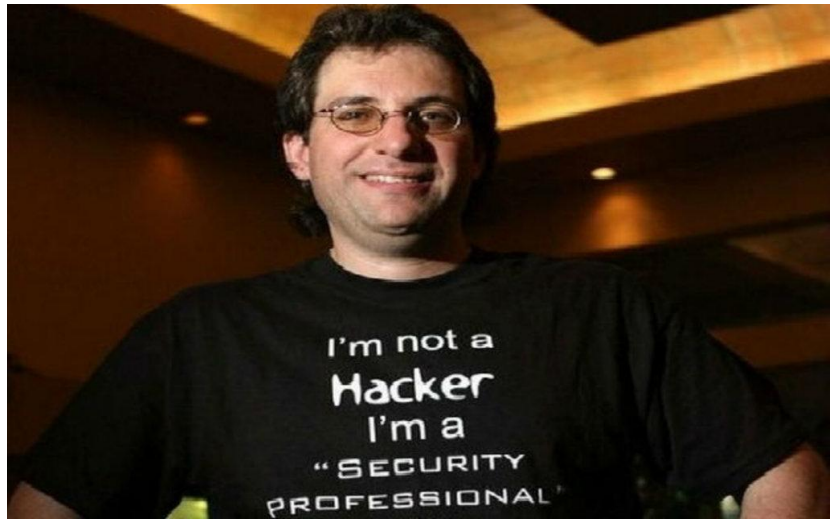
Information Security Continuous Monitoring

National Institute of Standards and Technology



Il fattore umano

Una azienda può spendere centinaia di migliaia di dollari in firewall, sistemi di intrusion detection o di crittografia, ma se un hacker può chiamare una persona fidata all'interno dell'azienda e riesce a farsi rilasciare informazioni sensibili allora tutti i soldi spesi per la tecnologia sono stati buttati



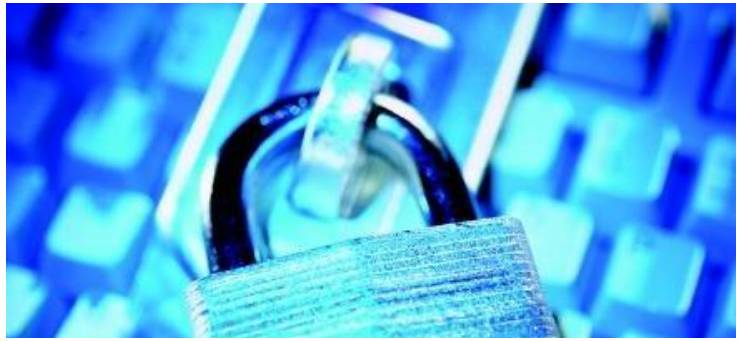
Kevin David Mitnick, detto Condor

WANTED
BY U.S. MARSHALS

NOTICE TO ARRESTING AGENCY: Before arrest, validate warrant through National Crime Information Center (NCIC).
United States Marshals Service NCIC entry number: (NIC/ W721460021).

NAME: .....MITNICK, KEVIN DAVID
AKS (S): .....MITNIK, KEVIN DAVID
MERRILL, BRIAN ALLEN

DESCRIPTION:
Sex: .....MALE
Race: .....WHITE
Place of Birth: .....VAN NUYS, CALIFORNIA
Date(s) of Birth: 08/06/63; 10/18/70
Height: .....5'11"
Weight: 190
Eyes: .....BLUE
Hair: .....BROWN
Skintone: .....LIGHT
Scars, Marks, Tattoos: .....NONE KNOWN



Truffe BEC

Business Email Compromise

Fasi della truffa

“ Caro A. dovresti fare un bonifico di mezzo milione di euro su questo contocorrente xxxxxxx. Metti come causale “Prima tranche per avvio attività rif. Contratto 784784”. Non mi chiamare perché sono in giro con il presidente e non posso parlare”

Perdite totali dal 2013 al 2018

$13.000.000.000,00

Aziende cha cadono giornalmente vittima di truffe BEC

400

01

Violazione della mailbox

Viene violata la mailbox della vittima ottenendo l’accesso a tutta la sua corrispondenza.

02

Studio

Il criminale studia la corrispondenza facendosi una idea chiara delle gerarchie e delle procedure aziendali.

03

Attacco

Il criminale sferra una attacco mirato.

Può capitare a tutti!

ilsussidiario.net

Lazio e Feyenoord truffati da hacker/ Affare de Vrij: ha rubato 2 milioni a Lotito

14 giorni fa

Viola News

Un hacker ha truffato la Lazio nell'affare de Vrij?

14 giorni fa

fcinter1908

Cessione de Vrij, spunta un hacker francese. Avv. Lazio: "Noi abbiamo pagato, ora..."

Fcinternews.it

Lazio e Feyenoord truffate nell'affare De Vrij: un hacker francese indagato per aver intascato 2 milioni di euro

14 giorni fa

Corso di Security Awareness

1. La minaccia
2. Password e loro gestione
3. La crittografia per la protezione delle informazioni personali
4. Il Phishing
5. Le Fake News
6. Il social engineering
7. Online e mobile banking

8. Shopping on line
9. I Social network
10. Accesso alle reti Wireless
11. I supporti removibili
12. I servizi di Geolocalizzazione
13. Le truffe Business Email Compromise
14. Il GDPR

THANK YOU.

Vincenzo Calabrò

www.vincenzocalabro.it