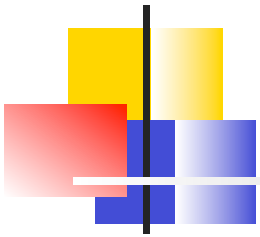


Haruspex

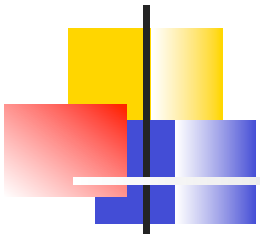
numbers, not words!

Suite Haruspex: valutare e migliorare la robustezza in campo ICT

F.Baiardi - f.baiardi@unipi.it
F.Tonelli – tonelli@di.unipi.it

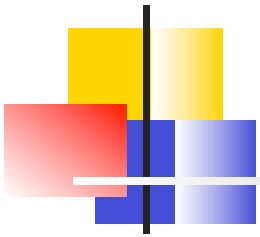
Adottato in 3 NATO cyberdefence

Haruspex
numbers, not words!



Outline

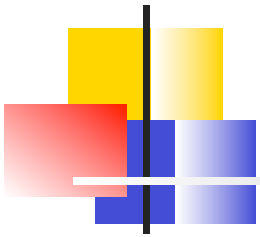
- Haruspex competitive value
- I fondamenti della suite
- Assessment iniziale di un sistema
- Assessment dinamico per rispondere ai
  - Cambiamenti del contesto di un sistema
  - Cambiamenti del sistema



Haruspex – Competitive Value

- Automatizza la simulazione degli attacchi contro un sistema per prevedere *ora* dove gli attacchi avverranno e la loro probabilità di successo
- Utilizza un catalogo per individuare un insieme minimo di contromisure che garantisce di mitigare il rischio in uno scenario e massimizza il ritorno degli investimenti
- Analisi ripetibili per confrontare sistemi diversi
- Supporta tutta la vita di un sistema perchè
  - Permette di analizzare la robustezza di un sistema durante il progetto
  - Anticipa le ripercussioni sulla sicurezza di cambiamenti ad un sistema esistente
  - Permette di scoprire vulnerabilità utilizzabili contro versioni precedenti
- Fonde le informazioni restituite da vulnerability scanning (sistema + web) e da analisi statica del codice sorgente

Haruspex competitive value

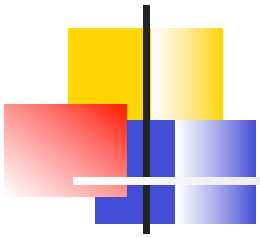


Outline

- Haruspex competitive value

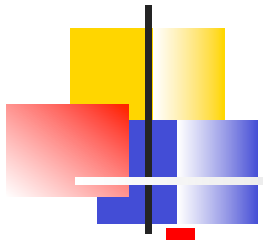
⇒ I fondamenti della suite

- Assessment iniziale di un sistema
- Assessment dinamico per rispondere ai
  - Cambiamenti del contesto di un sistema
  - Cambiamenti del sistema



Haruspex – I fondamenti

- Analisi contestuale del sistema in scenari con uno o più attaccanti che sfruttano privilege escalation
- Esecuzione interattiva dei modelli del sistema e degli attaccanti per simulare i singoli passi di ogni attaccante
- Applicazione del metodo Monte Carlo con esecuzioni ripetute il cui output permette di calcolare
  - le privilege escalation ed i percorsi di attacco
  - la probabilità di successo di ogni attaccante
  - le curve di stress del sistema
  - le contromisure e di valutarne l'efficacia
- Riproducibilità per versioni diverse con stessi attaccanti



Perché privilege escalations?

- **AGENZIA PER L'ITALIA DIGITALE**

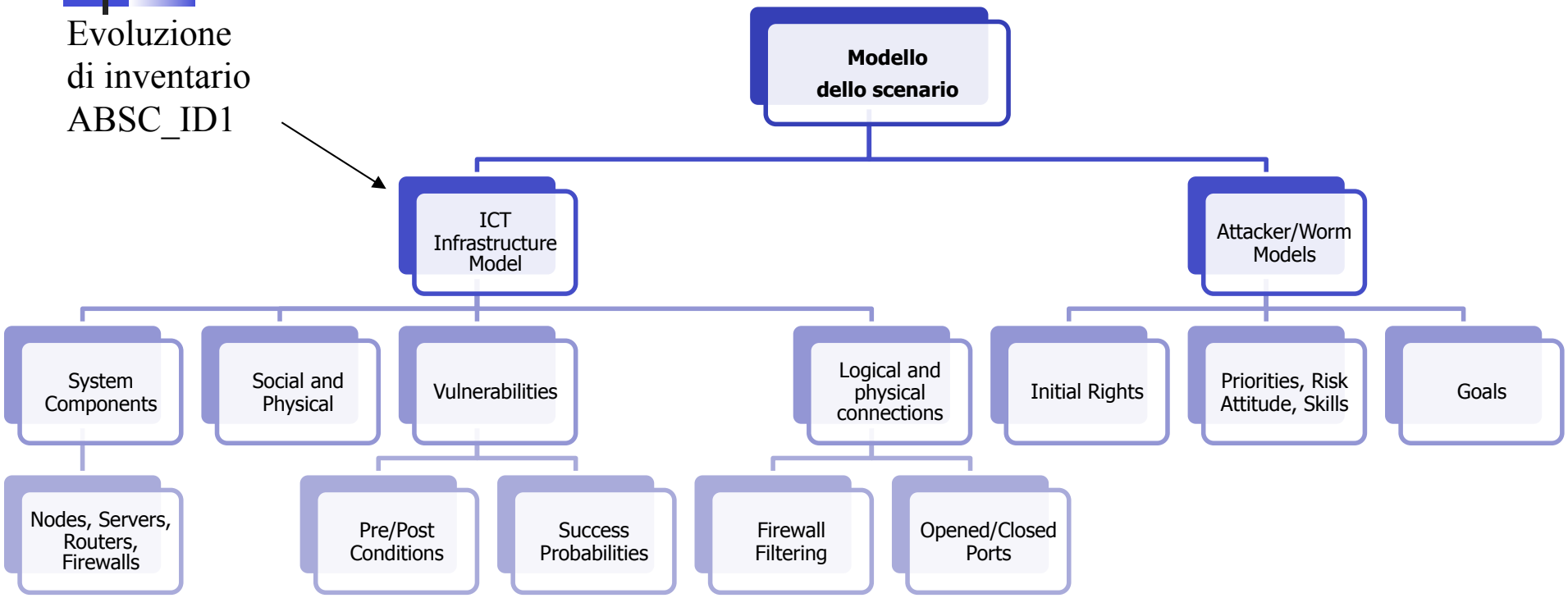
  CIRCOLARE 17 marzo 2017, n. 1/2017

- Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1 agosto 2015). (17A02399)
  (GU Serie Generale n.79 del 4-4-2017)

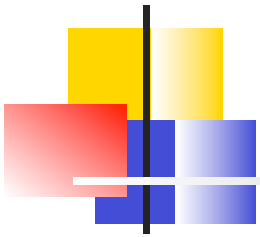
  "Infatti elemento comune e caratteristico degli attacchi più pericolosi è *l'assunzione del controllo remoto della macchina attraverso una scalata ai privilegi*."

Perchè lo scenario ?

Evoluzione
di inventario
ABSC_ID1



Solo lo scenario contiene tutte le informazioni per calcolare e validare contromisure = proprietà emergente dello scenario



Perché Monte Carlo ?

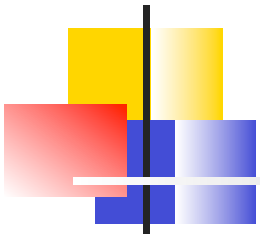
- Già utilizzato negli assessment di sistemi complessi (impianti nucleari …)
- E' l'unico approccio matematico che supera la mancanza di modelli esatti per gli scenari e permette di tener conto di aspetti stocastici per
  - Calcolare in modo trasparente e con il livello di confidenza richiesto
    - I percorsi di attacco utilizzati ed il tempo per percorrerli
    - La probabilità di successo dell'attaccante
  - Scoprire black swan (importance sampling)
  - Automatizzare la valutazione e gestione del rischio
  - Evitare la raccolta di dati storici
- Haruspex è l'unica suite che lo adotta nel campo ICT per simulare in modo ripetuto ed indipendente il comportamento degli attaccanti in uno scenario

Haruspex – Gli strumenti della suite

- Costruzione modello di uno scenario
  - Target system
  - Attaccanti
- Applicazione del metodo Monte Carlo con esecuzione ripetuta dei modelli in uno scenario (simulazione attacchi)
- Calcolo e validazione contromisure
- Aggiornamento modello scenario
- Gestione modelli di scenario

In futuro …

- Analisi BigData di uno scenario (prototipo)
- Monitoraggio e prevenzione (prototipo)

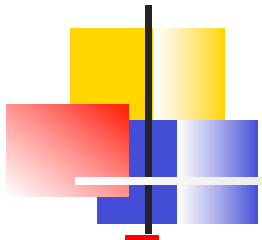


Outline

- Haruspex competitive value
- I fondamenti della suite

⇒ Assessment iniziale di un sistema

- Assessment dinamico per rispondere ai
  - Cambiamenti del contesto di un sistema
  - Cambiamenti del sistema



Haruspex – Assessment Iniziale

- Costruzione dei modelli
  - del sistema a partire dall'inventario del sistema e dalle vulnerabilità
  - delle minacce (interne, esterne, worm)
- Definizione degli scenari di interesse
- Per ogni scenario di interesse, calcolo di
  - percorsi di attacco di ogni attaccante
  - probabilità di successo di un percorso
  - curve di stress del sistema
  - contromisure per lo scenario e loro validazione
- Output = contromisure da applicare e percorsi non bloccati

Quando l'assessment iniziale?

- Può avvenire in momenti diversi della vita di un sistema
- Il momento in cui avviene determina il costo ed il catalogo delle contromisure

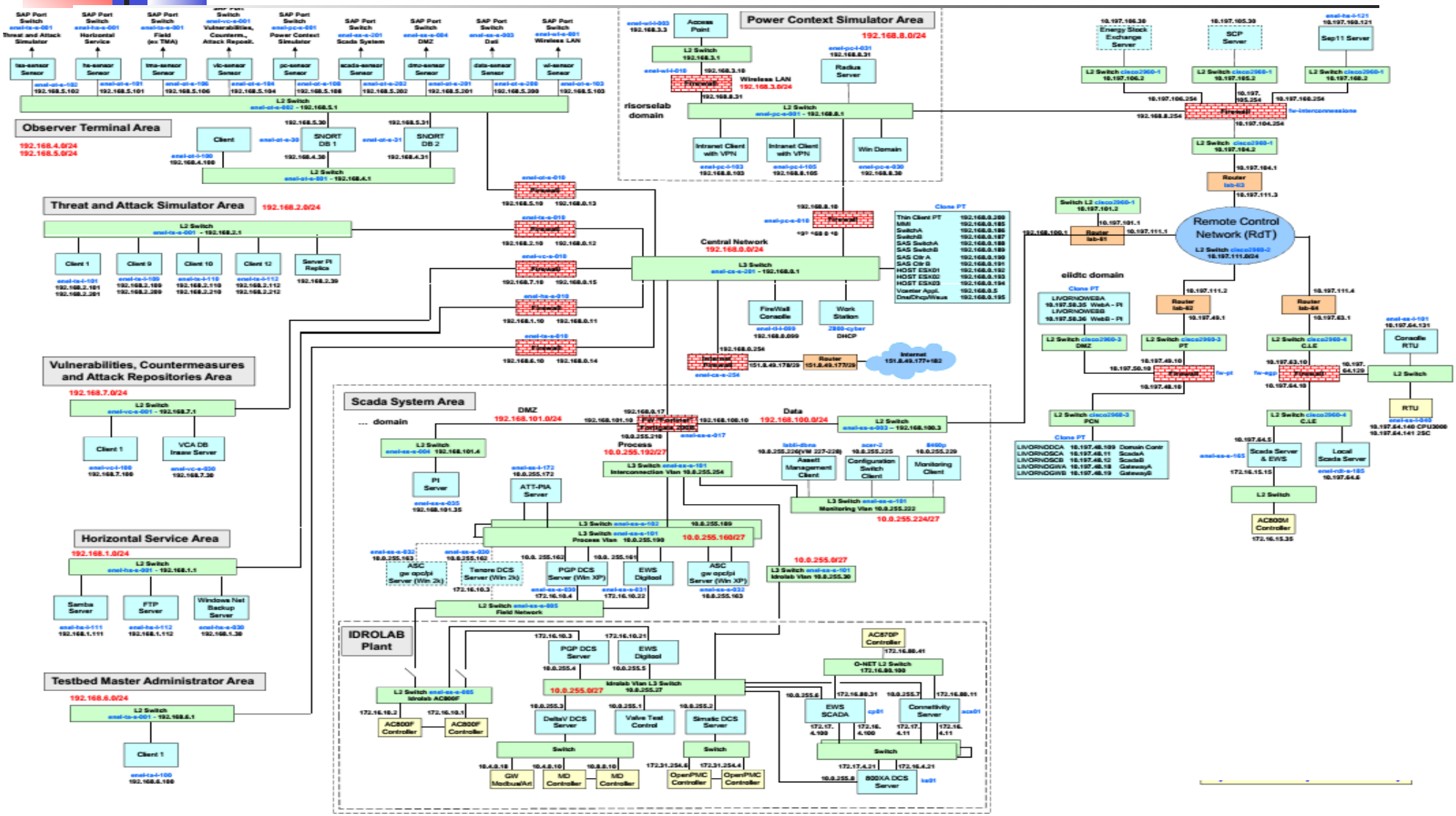
Costo minimo delle contromisure e dell'assessment, catalogo illimitato (resilient design)

Basso costo contromisure e catalogo ridotto

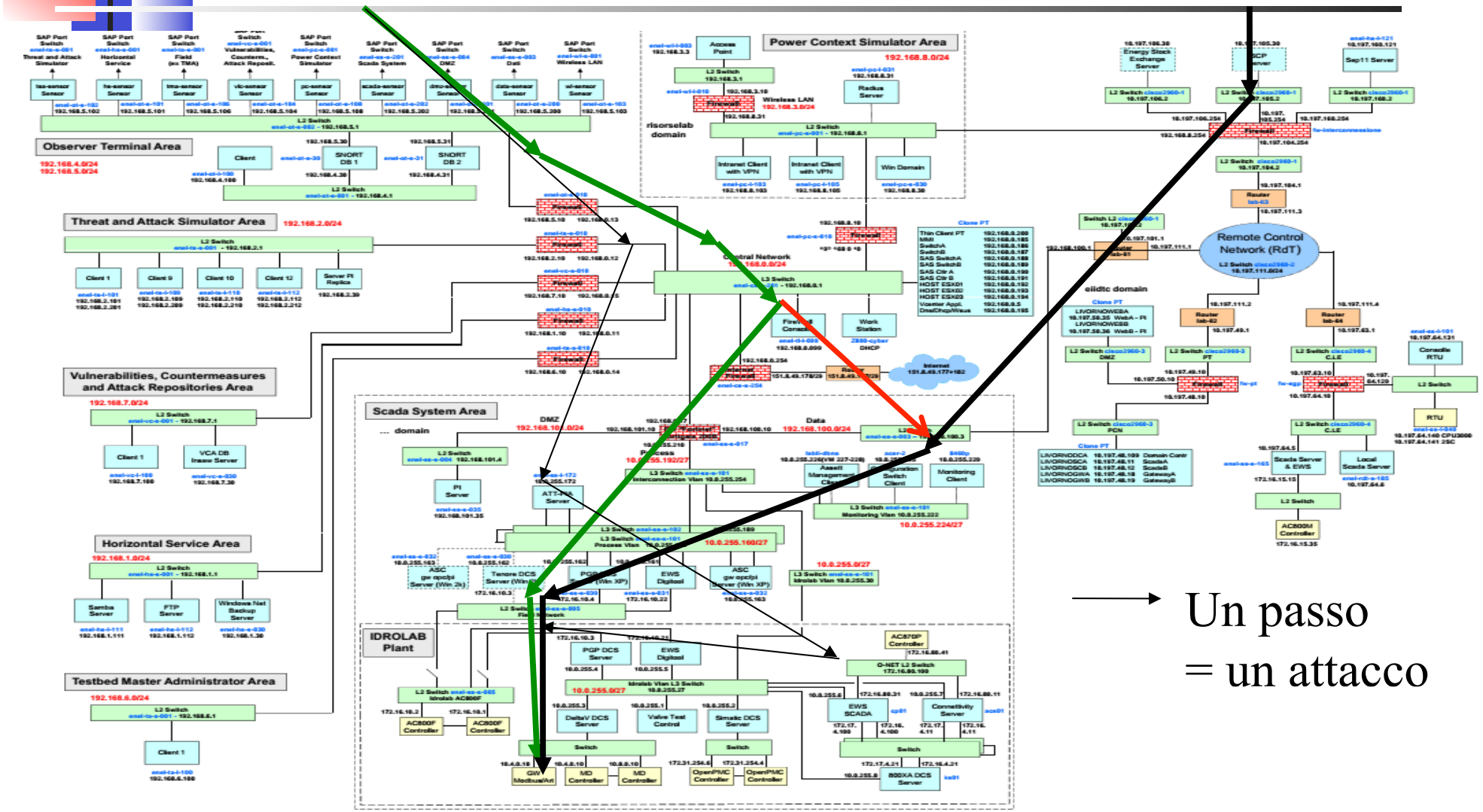
Costo di assessment e di contromisure più alto, catalogo limitato

Tempo di vita di un sistema

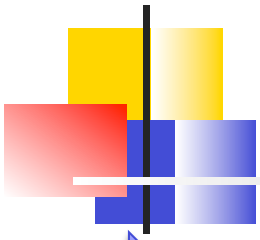
Scenario Esempio – Sistema Target



Possibili percorsi dell'attaccante



Scenario esempio - prob. succ. attaccante 99%



Diritti Iniziali

- Diritti di Amministrazione su un PC esterno connesso al backbone aziendale

Obiettivi

- Diritti di Amministrazione o Denial of Service su alcuni tablet utilizzati
- Diritti di Amministrazione sui server collegati ai PLC per controllo

Impatto

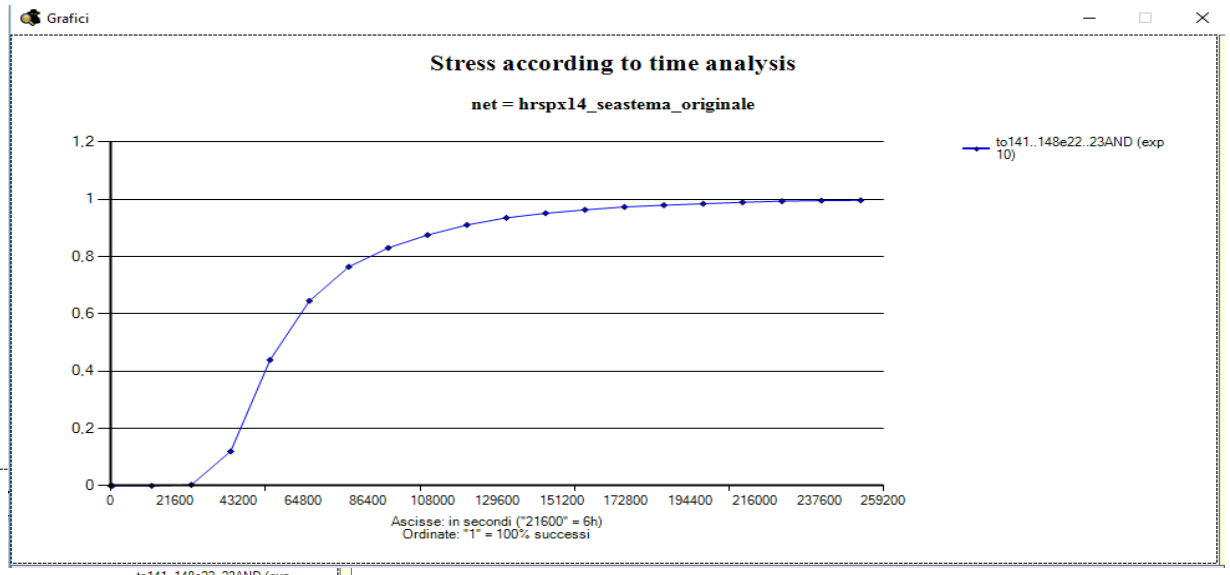
- Manomissione dei sistemi di automazione
- Falsificazione delle informazioni relative a
  - sistema di automazione,
  - stato del sistema,
  - posizione del personale

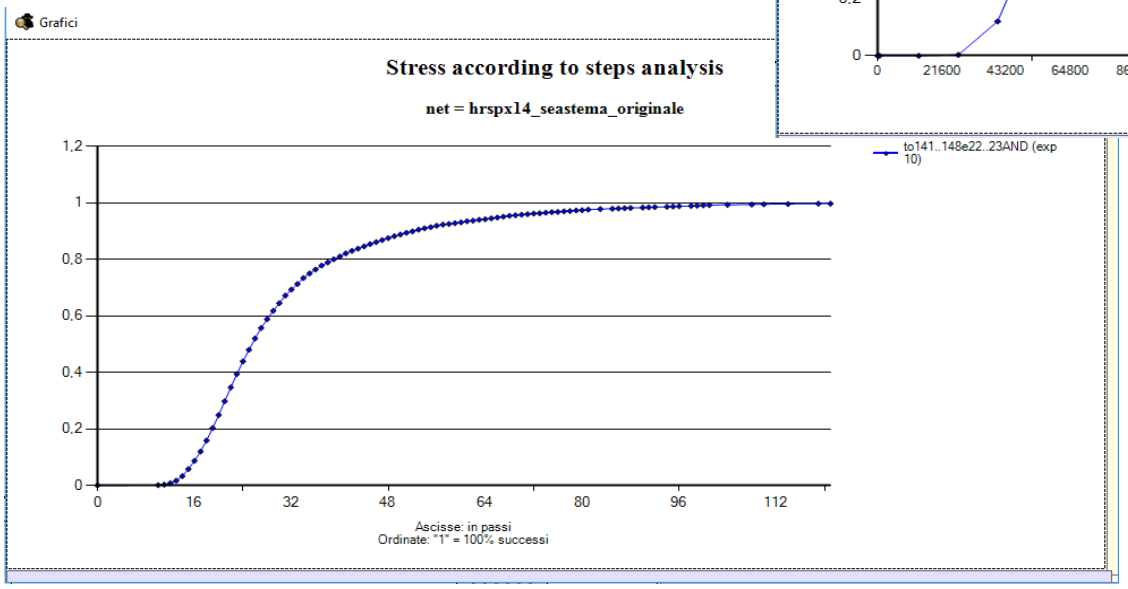
Assessment – Risultati - Stress Curve

- Stress(t) = probabilità di successo degli attaccanti al tempo t
- Predice in modo quantitativo la robustezza del sistema e la sua capacità di resistere agli attaccanti in uno scenario
- Misura in modo completo e consistente se, come e quando un sistema resiste o cede (1-stress) in uno scenario
- Valori medi non bastano ⇔ "Molte persone alte 1.80 m. sono affogate attraversando ruscelli profondi 1m in media."
- Solo il metodo Monte Carlo permette di calcolarla
- Utilizzata per valutare l'impatto di un attaccante
- NATO award on cyber awareness– Ottobre 2016

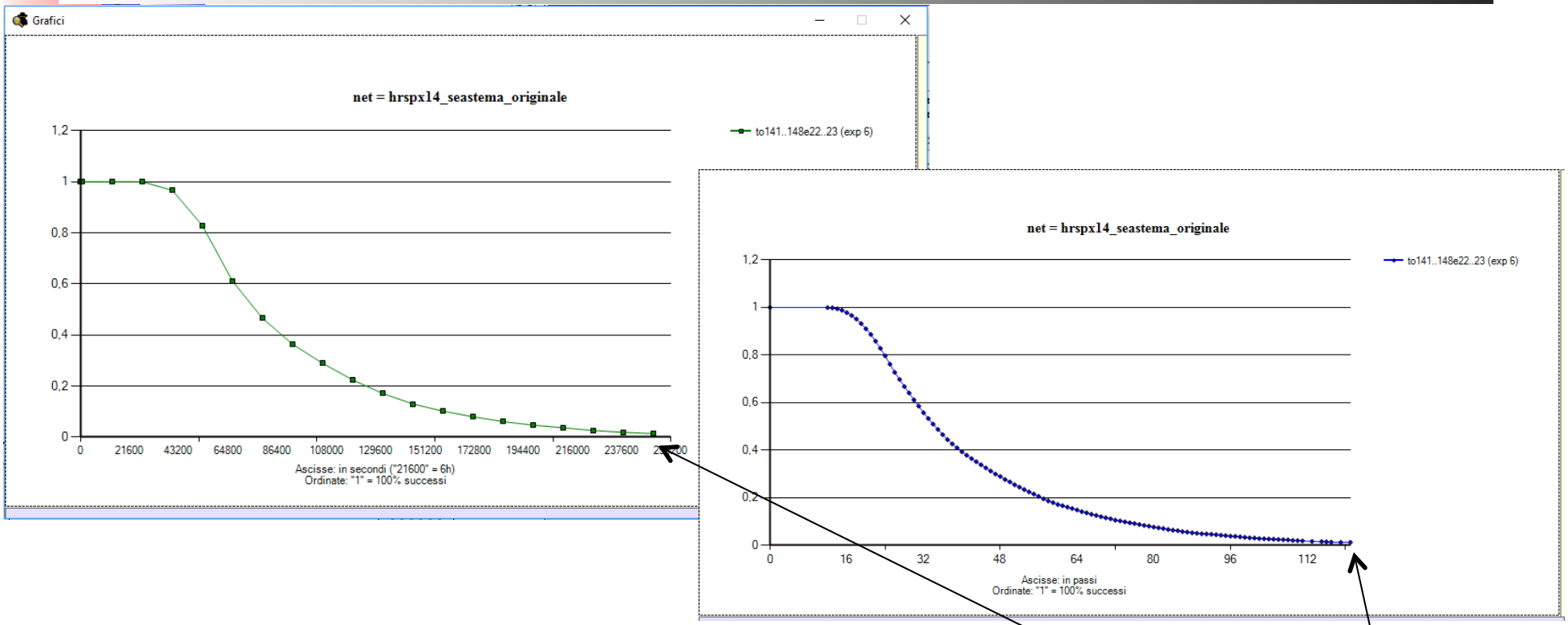
Scenario esempio – Stress Curve

La probabilità di successo è superiore al 90% dopo 30 ore o dopo aver eseguito 60 attacchi





Scenario esempio – Crash Curve = 1-Stress

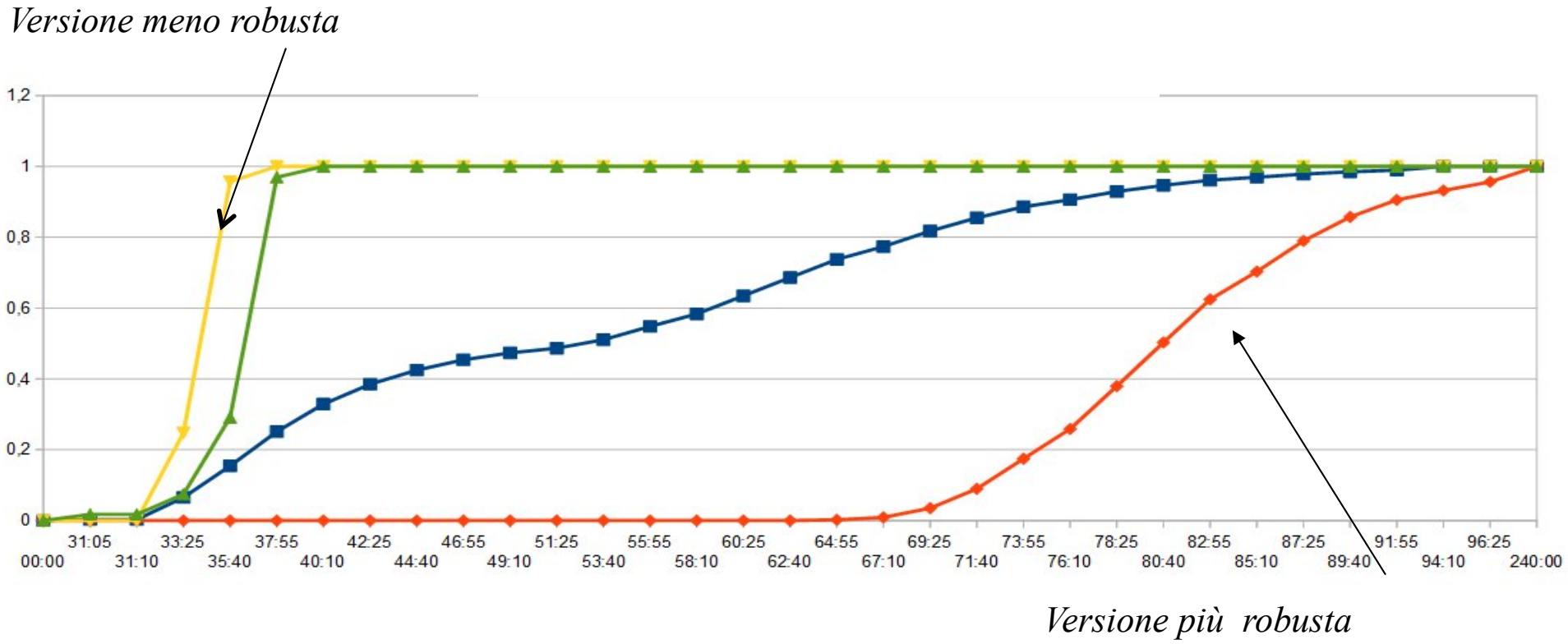


Il sistema è completamente compromesso
dopo 66 ore o dopo aver eseguito 112 attacchi

crash !!

Stress Curve – Resilient Design

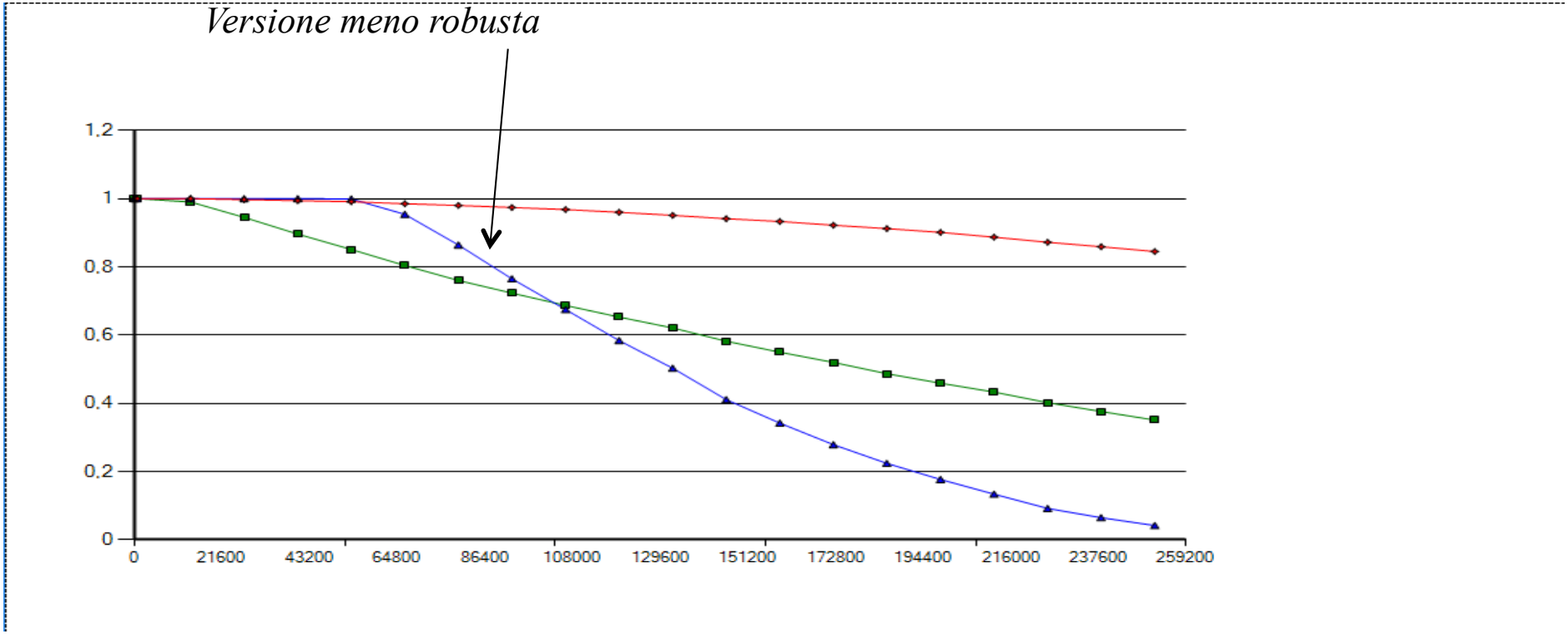
Scoprire in fase di progetto la versione meno robusta



- 4 versioni = 4 curve di stress
- Unità di tempo = ore

Crash Curve – Resilient Design

Scoprire in fase di progetto la versione meno robusta

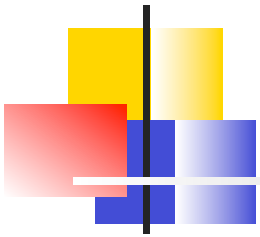


- Unità di tempo = secondi

Assessment – Risultati – Contromisure

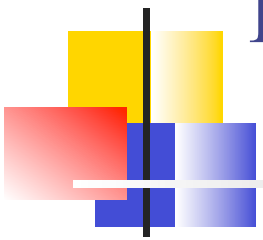
- Haruspex seleziona il più piccolo insieme di contromisure che annulla o almeno mitiga il rischio nello scenario
- Le contromisure sono scelte in un catalogo definito a priori
  - Patch (soluzione di default)
  - Segmentazione/Micro Segmentazione
  - Sandbox
  - Regole di routing e firewalling
  - Honeypot
  - ….
- Costi si riducono di alcuni ordini di grandezza rispetto ad una strategia *patch all*
- Viene aggiornato il modello e simulati nuovamente gli attaccanti per verificare la convenienza e l'efficacia delle contromisure
- Approccio iterativo (verifica-scelta nuove contromisure)

Vulnerabilità vs Scanning vs Contromisure



- Le contromisure come emerging property
- L'insieme minimo delle contromisure da adottare dipende dallo scenario **non dal risultato dello scanning o dalle contromisure disponibili** (lo scanning è lo stesso in ogni scenario)
- Haruspex sfrutta questa proprietà per
  - minimizzare il numero di contromisure
  - ottimizzare il costo delle contromisure
  - individuare delle contromisure senza conoscere le vulnerabilità sfruttate da attaccante (what-if)

Formalizzazione di un assessment iniziale

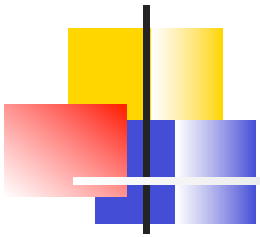


- La metodologia H-RAM^2 è ispirata ad approcci come CRAMM o Magerit molto diffusi in ambito europeo
- Le caratteristiche principali :
  - 10 passi per valutare e gestire rischio in modo automatico e cost-effective
  - indica ad ogni passo gli strumenti Haruspex da usare per annullare il rischio
  - è ottimizzata per
    - ridurre il costo di valutazioni periodiche
    - accompagnare la vita del sistema

I 10 passi di H-RAM^2

1. Definizione del perimetro
2. Definizione del sistema target
3. Produzione del modello del sistema target
4. Definizione degli asset da proteggere
5. Acquisizione vulnerabilità
6. Acquisizione degli attacchi
7. Definizione del modello delle minacce
8. Valutazione quantitativa del rischio ICT
9. Selezione e valutazione delle contromisure
10. Gestione statica e dinamica del rischio ICT

Ripetuti in assessment periodico



Outline

- Haruspex competitive value
- I fondamenti della suite
- Assessment preliminare di un sistema

⇒ Assessment dinamico per rispondere ai

  - Cambiamenti del contesto di un sistema
  - Cambiamenti del sistema

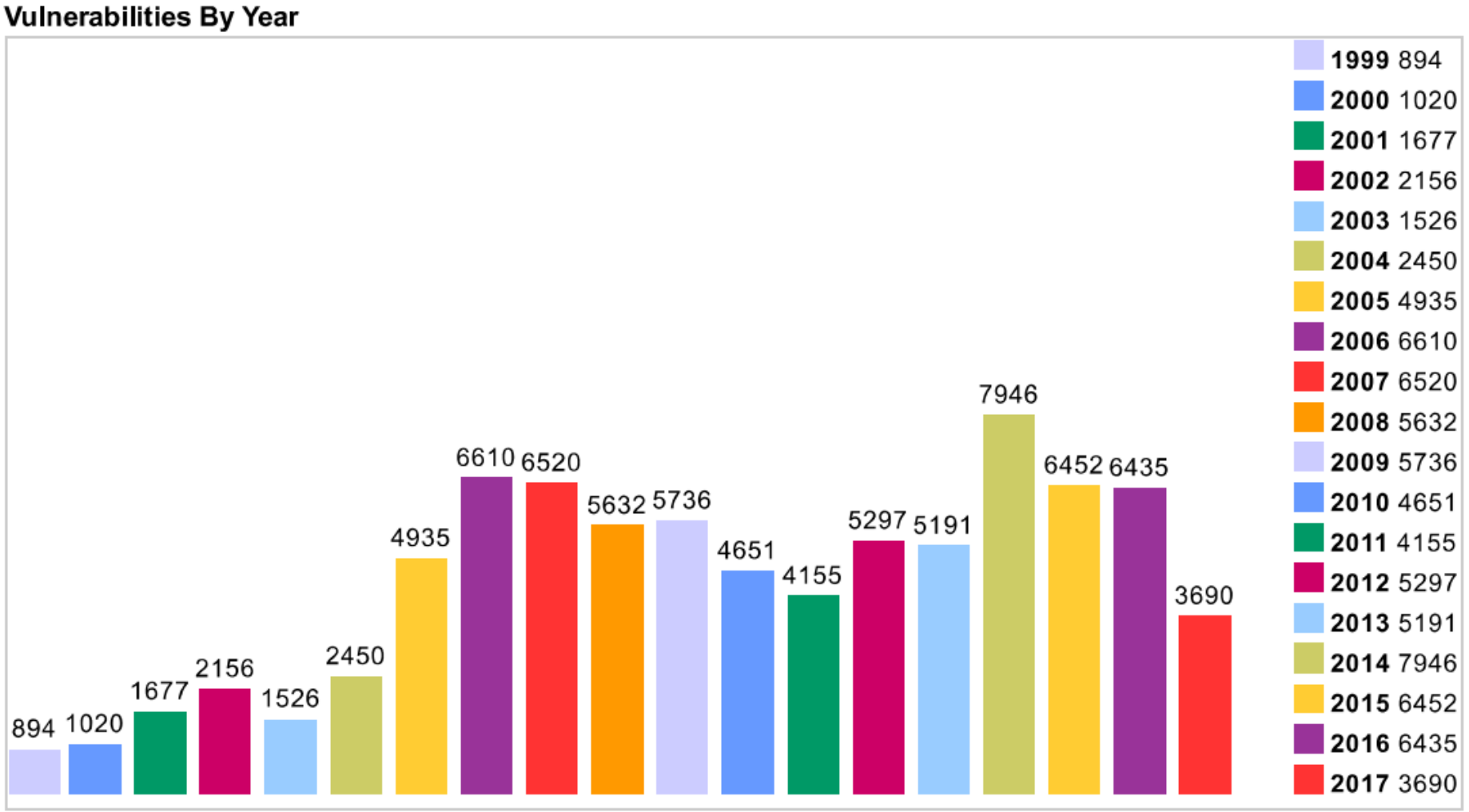
Assessment Dinamico

- Nella vita di un sistema sono necessari frequenti assessment per valutare il rischio generato da cambiamenti
  - Al contesto in cui il sistema opera
  - Al sistema stesso
- Gli strumenti Haruspex operano in parallelo al sistema target
  - acquisiscono i cambiamenti,
  - eseguono automaticamente il nuovo assessment
    - sfruttando il modello del sistema già creato
    - senza disturbare il normale funzionamento del sistema
  - calcolano le contromisure per rispondere ai cambiamenti

Assessment Dinamico – Nuovo contesto

- La più frequente modifica del contesto è la scoperta di una nuova vulnerabilità del sistema o ad un nuovo worm
- Haruspex aggiorna automaticamente il modello del sistema creato per l'assessment iniziale ed esegue esperimenti per scoprire in tempo reale
  - Quali percorsi di attacco apre la nuova vulnerabilità
  - Quale è il livello di diffusione del nuovo worm
  - Quali contromisure applicare per
    - mitigare o annullare il rischio generato dalla nuova vulnerabilità
    - limitare la diffusione del worm
- Haruspex permette di creare e gestire un database con il modello attuale e quelli storici per analisi forensi

Nuove vulnerabilità???



Assessment Dinamico – Nuovo Contesto + Forensics

- L'assessment per calcolare le ripercussioni di una nuova vulnerabilità può scoprire che in passato il sistema può essere stato attaccato con successo
- Ulteriori assessment possono utilizzare il modello delle versioni precedenti del sistema
- Questi assessment hanno il ruolo di
  - Ricercare indicatori di una compromissione e malware
  - Riportare il sistema sotto il controllo del proprietario
  - Definire nuovi scenari in base alle informazioni acquisite dall'attaccante o alle risorse che può aver controllato

Perché forensics?

AGENZIA PER L'ITALIA DIGITALE

CIRCOLARE 17 marzo 2017, n. 1/2017

- Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015). (17A02399) (GU Serie Generale n.79 del 4-4-2017)

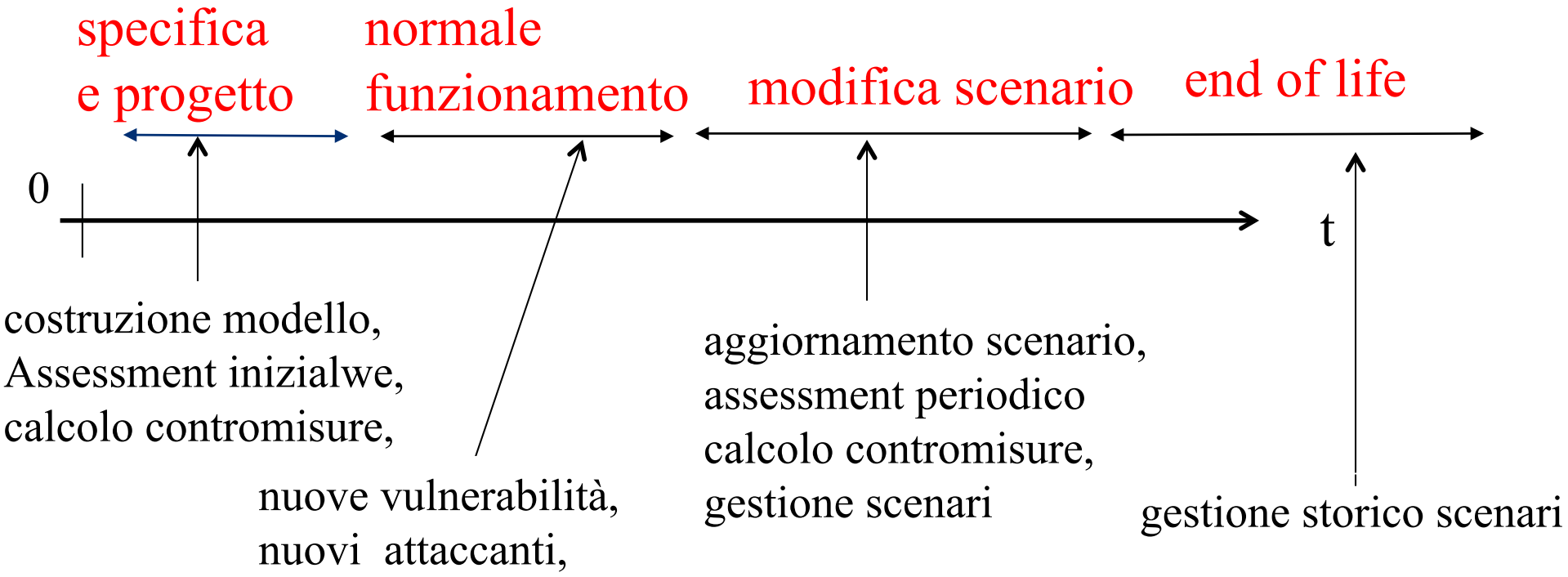
  «le misure preventive, destinate ad impedire il successo dell'attacco, devono essere affiancate da efficaci strumenti di rilevazione, *in grado di abbreviare i tempi, oggi pericolosamente lunghi,* che intercorrono dal momento in cui l'attacco primario è avvenuto e quello in cui le conseguenze vengono scoperte»

Assessment Dinamico – Modifiche al sistema

- Ulteriori cambiamenti possono essere dovuti a
  - Nuove applicazioni
  - Nuove connessioni
  - Nuove politiche di filtraggio
  - Nuove configurazioni dei nodi
  - Nuovi nodi
- Haruspex può valutare proattivamente (in parallelo, in tempo reale) il rischio generato da tali modifiche e calcolare le contromisure da applicare *insieme alle modifiche* per mitigare/annullare il rischio

Ricapitolando …

Haruspex è una suite di strumenti che automatizza la previsione, la mitigazione e l'annullamento del rischio ICT in tutta la vita di un sistema (ed oltre …)



Grazie per l'attenzione

xkcd: Security Advice