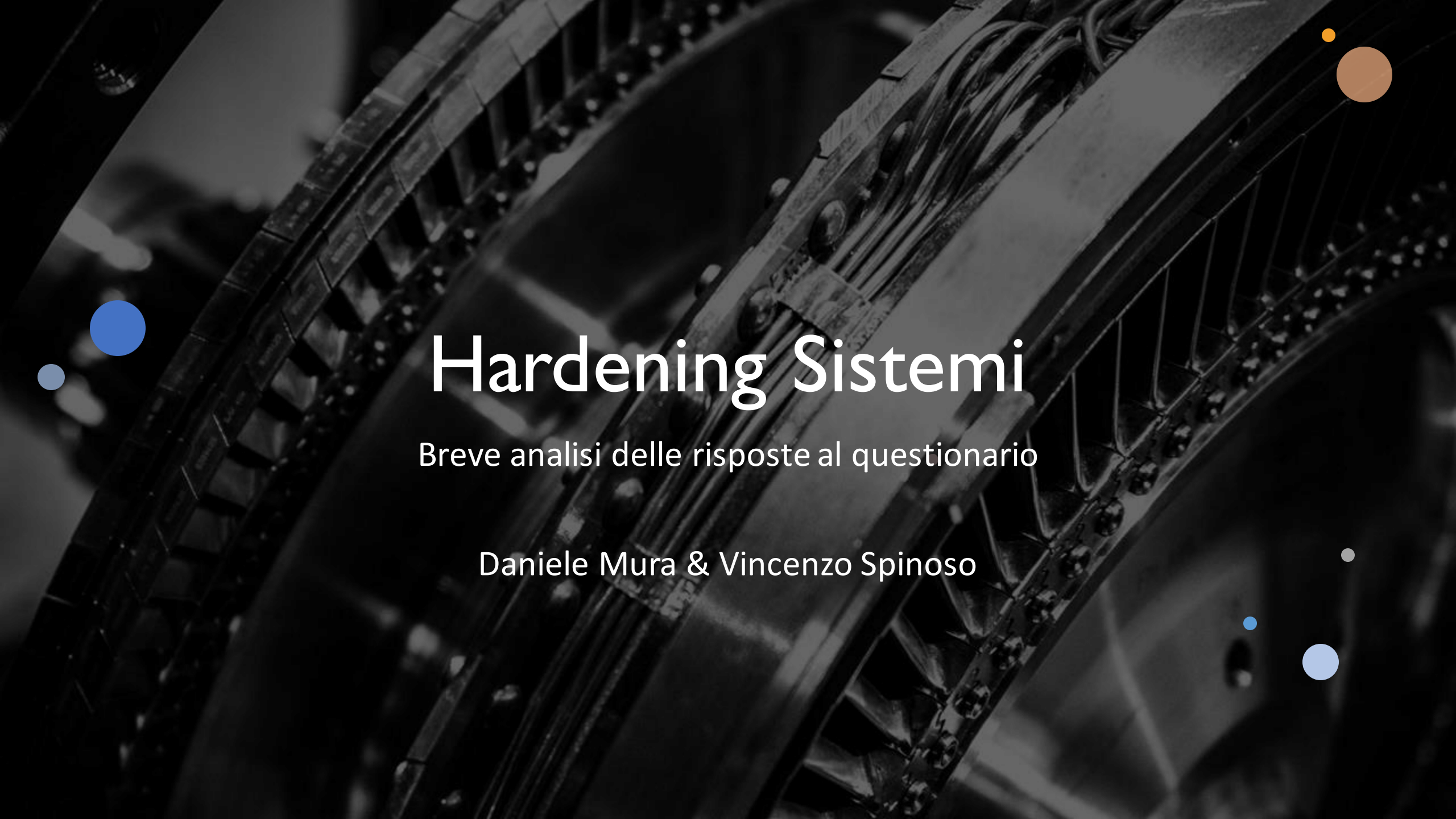

Hardening Sistemi

Breve analisi delle risposte al questionario

Daniele Mura & Vincenzo Spinoso

Obiettivo delle domande

- Avere un fotografia delle attività di hardening nella nostra comunità per capire se/come/quando intervenire
- Conoscere se si fa uso di strumenti particolari con il focus su quanto viene sviluppato in casa
- Stimare il grado di condivisibilità

Idea dietro le domande

- **Consapevolezza**: quanto riteniamo importante l'attività di hardening
- **Dove**: su quale porzione di servizi informatici facciamo hardening
- **Attenzione**: a cosa rivolgiamo la nostra attenzione quando facciamo hardening
- **Fonti**: quali sono le fonti che usiamo per implementare le attività di hardening
- **Strumenti**: quali strumenti usiamo per implementare le attività di hardening
- **Tempo**: quanto tempo (possiamo) dedicare per le attività di hardening
- **Necessità**: quali sono le esigenze per migliorare le attività di hardening

…… cercando di metter in evidenza il perimetro degli interventi.

Consapevolezza

- Necessario
- Indispensabile
- Fondamentale
- Impegnativa
- Utile
- Incostante
- Insufficiente
- Importante

Nessuno sottovaluta la necessità di svolgere "una qualche attività" di hardening.

Dove

- Soltanto sui servizi core della struttura **2**
- Sia sui servizi core della struttura **+** computer dell'amministrazione/ufficio del personale **13**
- In maniera sistematica su tutti i sistemi informatici della struttura (servizi core, computer amministrazione, computer utenti gestiti dal servizio calcolo etc) **7**

Dove (commenti/suggerimenti)

- problema dei sistemi gestiti dai proprietari
- dipendenza da hardware
- assenza di strumenti per forzare la richiesta di livello di hardening per accesso alla rete
- migliore definizione di cosa sia hardening

Attenzione

- nell'installazione e nella gestione dei sistemi operativi **1**
- nell'installazione e nella gestione dei sistemi operativi **+** nell'installazione e nella gestione degli apparati di rete **8**
- nell'installazione e nella gestione dei sistemi operativi **+** nell'installazione e nella gestione dei servizi web-based **2**
- nell'installazione e nella gestione dei sistemi operativi **+** nell'installazione e nella gestione degli apparati di rete **+** nell'installazione e nella gestione dei servizi web-based **3**
- nell'installazione e nella gestione dei sistemi operativi **+** nell'installazione e nella gestione dei servizi web-based **+** nell'installazione e nella gestione dei database **+** nell'installazione e nella gestione degli apparati di rete **+** nell'installazione e configurazione di alcuni software di uso comune (ad esempio web browser, ms office etc) **8**

Attenzione (commenti/suggerimenti)

- necessario fare hardening su tutto i sistemi
- togliere sempre il superfluo dalle installazioni
- problema di "seguire" sempre gli aggiornamenti da installare
- uso di ACL per mitigare la "debolezza" di alcuni sistemi

Fonti

- best practice sviluppate con l'esperienza personale **3**
- best practice sviluppate con l'esperienza personale **+** best practice suggerite da comunità in rete **3**
- best practice sviluppate con l'esperienza personale **+** best practice suggerite dai produttori **+** best practice suggerite da comunità in rete **2**
- best practice sviluppate con l'esperienza personale **+** best practice suggerite dai produttori **+** best practice suggerite da comunità in rete **+** best practice suggerite dall'AGID **10**
- best practice suggerite dall'AGID **+** best practice suggerite da comunità in rete **4**

Fonti (commenti/suggerimenti)

- best practice o segnalazioni da parte di INFN e GARR
- diffidenza dei suggerimento AGID

Strumenti

- fai uso di tool trovati in rete **8**
- fai uso di tool sviluppati ad hoc personalmente **1**
- fai uso di tool trovati in rete **+** fai uso di tool sviluppati ad hoc personalmente **8**
- non fai uso di tool specifici **5**

Strumenti (commenti/suggerimenti)

- tool portable da chiavetta
- Greenbone Security Manager
- openvas
- fail2ban
- antivirus
- script per controllo anomalia code mail

- diffidenza sugli strumenti trovati on line,

Tempo

- in **maniera sporadica** quando trovo del tempo libero dagli altri impegni **5**
- una volta messo in produzione un sistema mi preoccupo di **installare le patch di sicurezza rilasciate dal produttore** **9**
- una volta messo in produzione un sistema mi preoccupo di **installare le patch di sicurezza rilasciate dal produttore +** in maniera **sporadica** quando trovo del tempo libero dagli altri impegni 6
- una volta messo in produzione un sistema mi preoccupo di **installare le patch di sicurezza rilasciate dal produttore + 1 giorno** alla settimana **3**
- 1 giorno al mese **3**

Tempo (commenti/suggerimenti)

- necessità di più tempo di quanto non emergenze da una valutazione iniziale
- dipendenza tra sistemi che diventano bloccanti e bisogna scegliere se chiudere il servizio o aggiornare una manciata di sistemi
- domanda "imprecisa o mal posta": difficoltà di rispondere, lavoro continuo
- attinenza al DVR
- utilizzo di puppet per gestire gli aggiornamenti

Necessità emerse

- Condivisione (tool e documenti)
- Corsi formazione/aggiornamento periodici

- **Commenti suggerimenti**:
  - aggiungere ore alle giornata :)
  - aumento del personale dedicato, standardizzare le attività