Betrusted

Security by design (deve essere) per tutti

betrusted.it

CHI SONO

Valentina Sona

- Laureata in Ingegneria Informatica con specializzazione in **cybersecurity**
- Lavoro presso Betrusted come **Offensive Security Specialist**
- Appassionata di hacking, open source e diritti digitali
- Relatrice a svariati talk & corsi di formazione (tecnici e non).

valentina.sona@betrusted.it

Betrusted

Betrusted

Listen, Research, Act.

LA TUA BOUTIQUE PER LA CYBERSECURITY

PENETRATION TEST

SECURE CODE REVIEW

FORMAZIONE

Q: Qual è l'unica controparte in comune?

A: Gli sviluppatori!

FORMAZIONE

2025: Corso (elettivo) di sicurezza per gli sviluppatori

Security by Design

Sec4DEV

INTR3

X

Betrusted

Betrusted

SEC4DEV

Syllabus

01.

Fondamenti di cybersecurity orientata al software

- Glossario della cybersecurity
- Classi di vulnerabilità più comuni

02.

Best practice orientate al web

- Problematiche di sicurezza legate all'infrastruttura
- Session management (OpenID/Keycloak)
- Input validation

03.

Sicurezza nel cloud

- Threat modeling e shared responsibility
- IAM
- Gestione dei segreti
- CI/CD e container security

04.

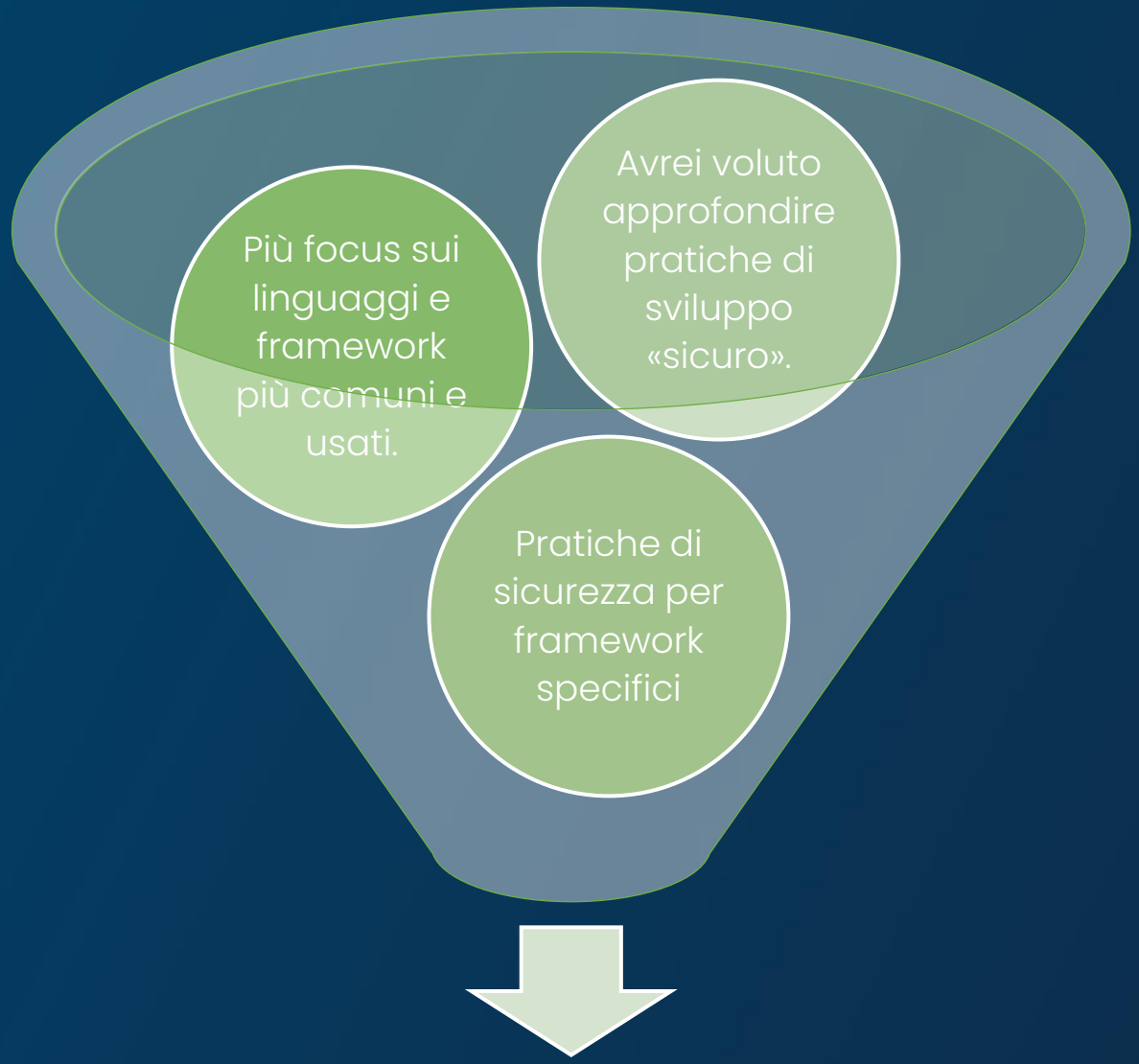
Mobile security

- Cambio di paradigma e differenze fra mobile e web
- Vulnerabilità tipiche mobile
- Gestione degli intent

Betrusted

Feedback ricevuto

- Il corso ha rispettato le tue aspettative?
- Avresti voluto approfondire qualche argomento in particolare?



Betrusted

CHE COS'È?

Security by Design

Un approccio allo sviluppo software e hardware che considera la sicurezza un elemento prioritario, al pari dei requisiti funzionali, su cui bisogna ragionare già dalle fasi iniziali di analisi e progettazione.

Betrusted

Security by Design VS Secure Coding

- Riguarda la parte di progettazione e pianificazione delle funzionalità
- È un approccio che considera l'intero ciclo di vita del software
- È trasversale alle tecnologie usate

- Riguarda la parte di implementazione delle funzionalità
- È uno dei *pilastri* di un approccio Secure by Design
- Comprende sia una parte di metodologia sia una di competenze verticali sulle tecnologie usate

COSA VUOL DIRE SECURITY BY DESIGN

Oltre il codice

Sviluppare software *sicuro* è un processo che copre l'intero ciclo di vita del prodotto.

Betrusted

Security by Design

Perché la sicurezza reattiva sta fallendo

Betrusted

Il modello di sicurezza reattiva

Rilascio software

Trovata una vulnerabilità!

- ❖Penetration Test / altro security assessment
- ❖Ricercatore indipendente / responsible disclosure
- ❖Criminali

Attività di remediation

- ❖Vulnerabilità analizzata dai ricercatori
- ❖Patch rilasciata (dopo quanto?)
- ❖Patch raggiunge tutti gli utenti (dopo quanto?)

Retest / review

- La patch è efficace?
- Introduce altre vulnerabilità?
- È stata applicata a tutte le istanze?

L’esplosione delle CVE

Dal 2016 è iniziata una crescita *esponenziale* nel numero delle vulnerabilità trovate e non accenna ad arrestarsi.

Il 2025 ha toccato il record di quasi 50k CVE.

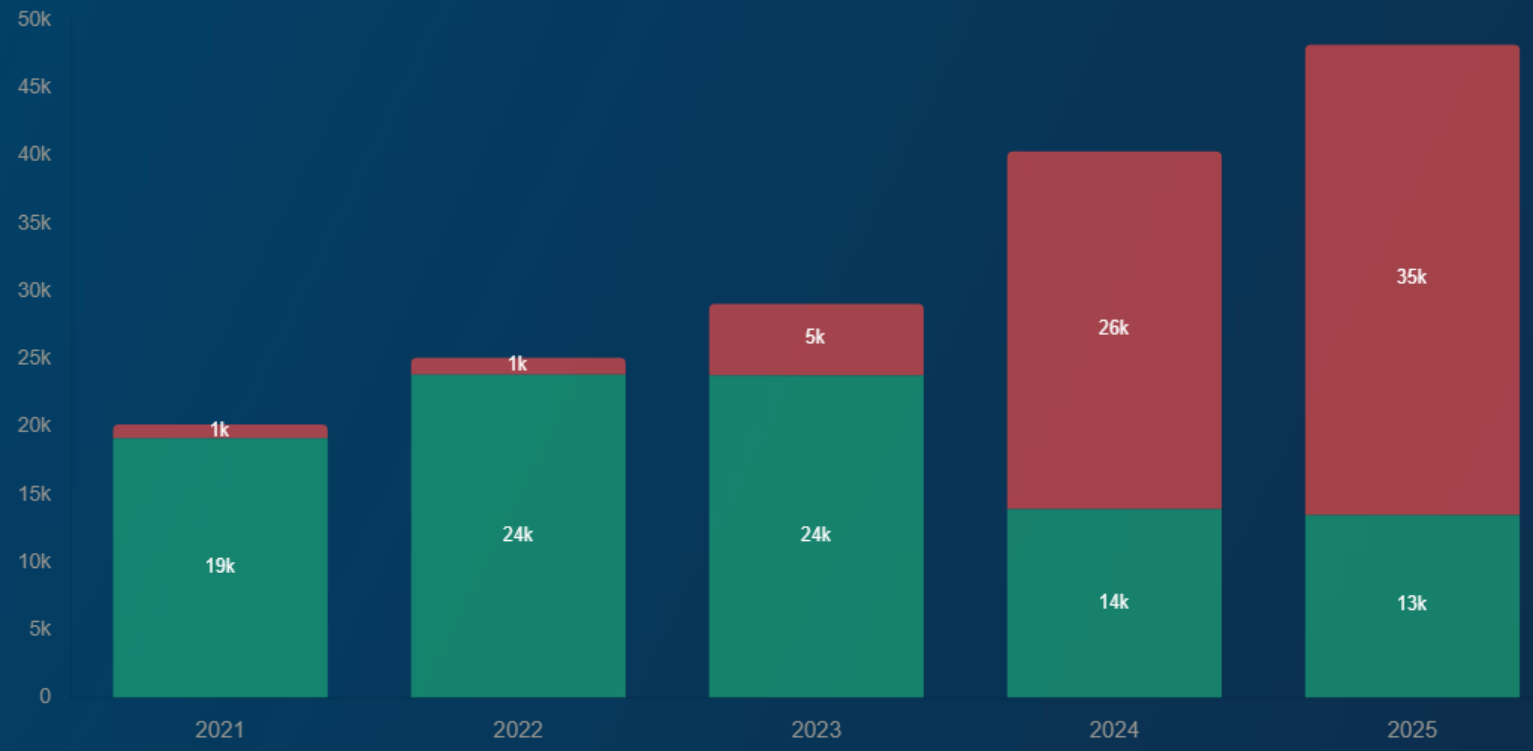
La forchetta previsionale per il 2026 è così ampia che non si esclude si superino le 100k CVE.

Sources: Jerry Gamblin / CVE.ICU (1999–2025 actuals); FIRST 2026 Vulnerability Forecast (2026 projection).

Betrusted

Il backlog dell'enrichment

L'NVD – il principale ente che cataloga e provvede all'analisi delle CVE, non tiene più il passo con le vulnerabilità scoperte.



Sources: CVEDetails (published totals); Jerry Gamblin / CVE.ICU; Zafran 2025 repor.t

Betrusted

Anatomia di una vulnerabilità: i metadati

CVSS

Un sistema di calcolo della severità della vulnerabilità.

Contiene informazioni preziose sulle caratteristiche della CVE.

CWE

Classificazione del tipo di debolezza sfruttata dalla vulnerabilità.

Rappresenta l'effettivo difetto nel programma da correggere.

CPE

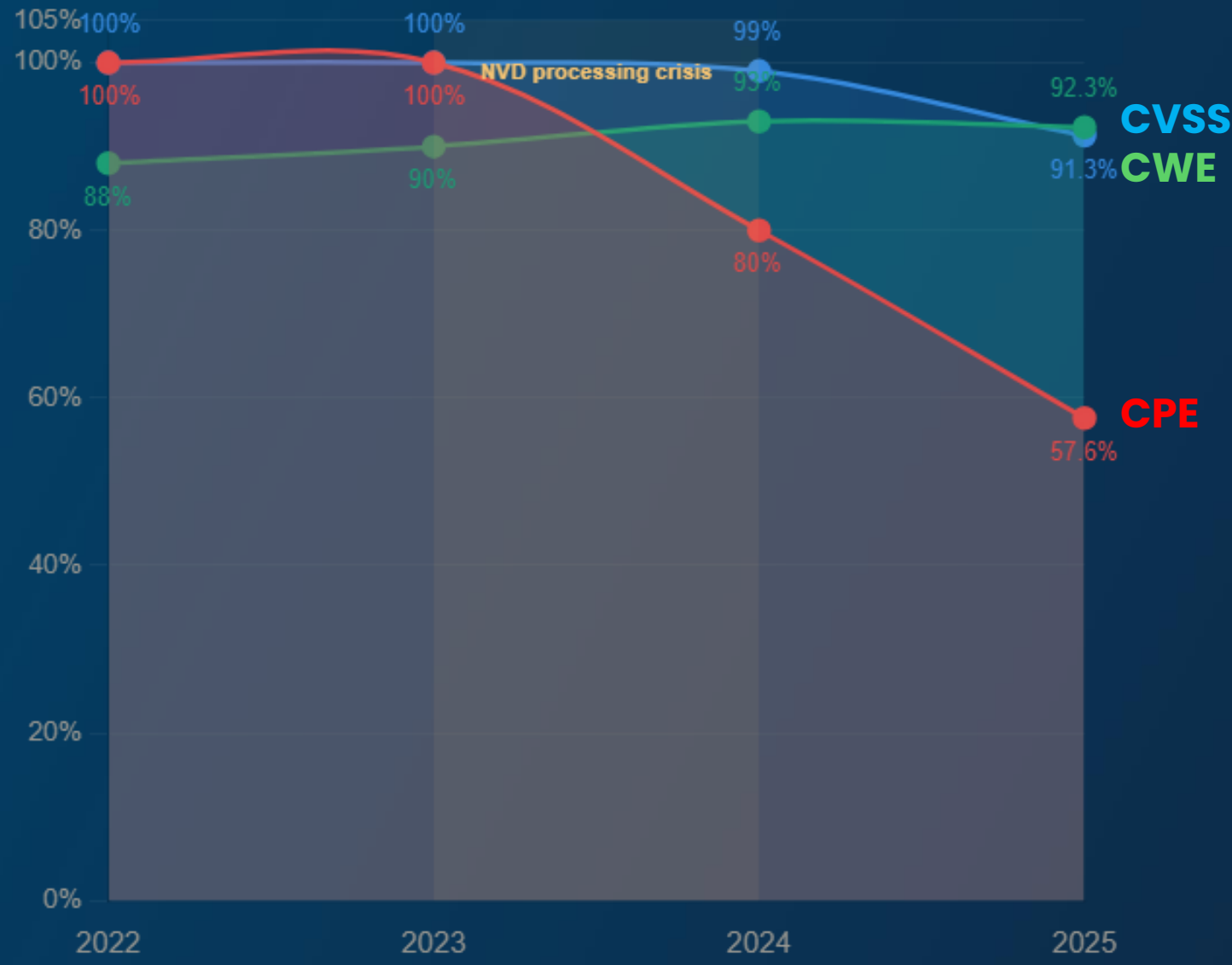
Elenco del software, delle versioni e delle piattaforme affette.

Fondamentale per tutti i sistemi di rilevamento automatico delle vulnerabilità su scala.

Un declino di qualità

CVSS e CWE sono spesso contribuite dai ricercatori che scoprono la vulnerabilità.

Le CPE richiedono ricerca specifica su quelle vulnerabilità, e stanno progressivamente sparendo



Betrusted

Un ritmo insostenibile

L'AI sta accelerando tutti i fattori di questa situazione: più vulnerabilità scoperte, più vulnerabilità introdotte, più vulnerabilità *sfruttate*.

Betrusted

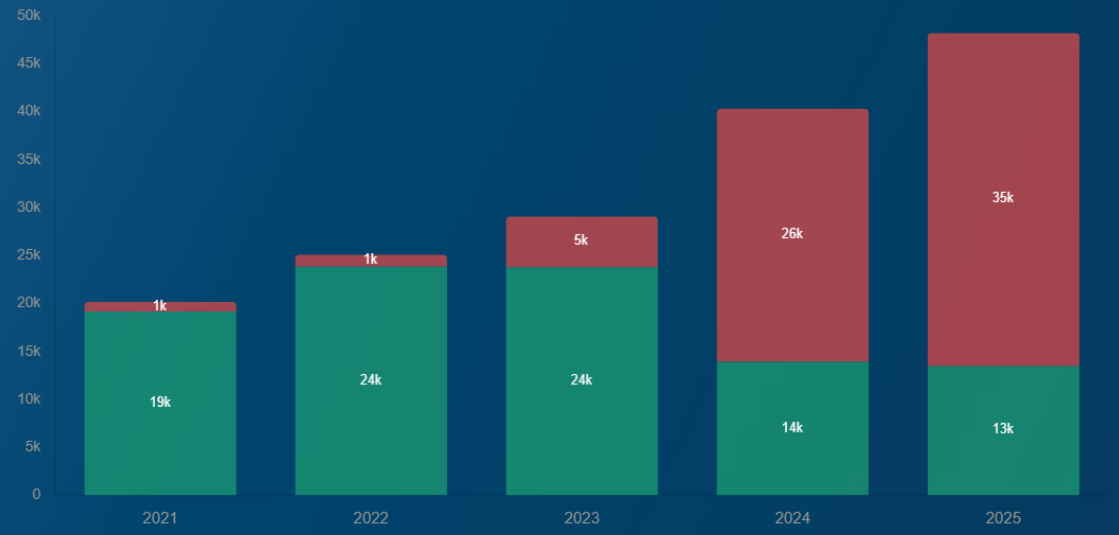
Security by Design

Ma io che c'entro?

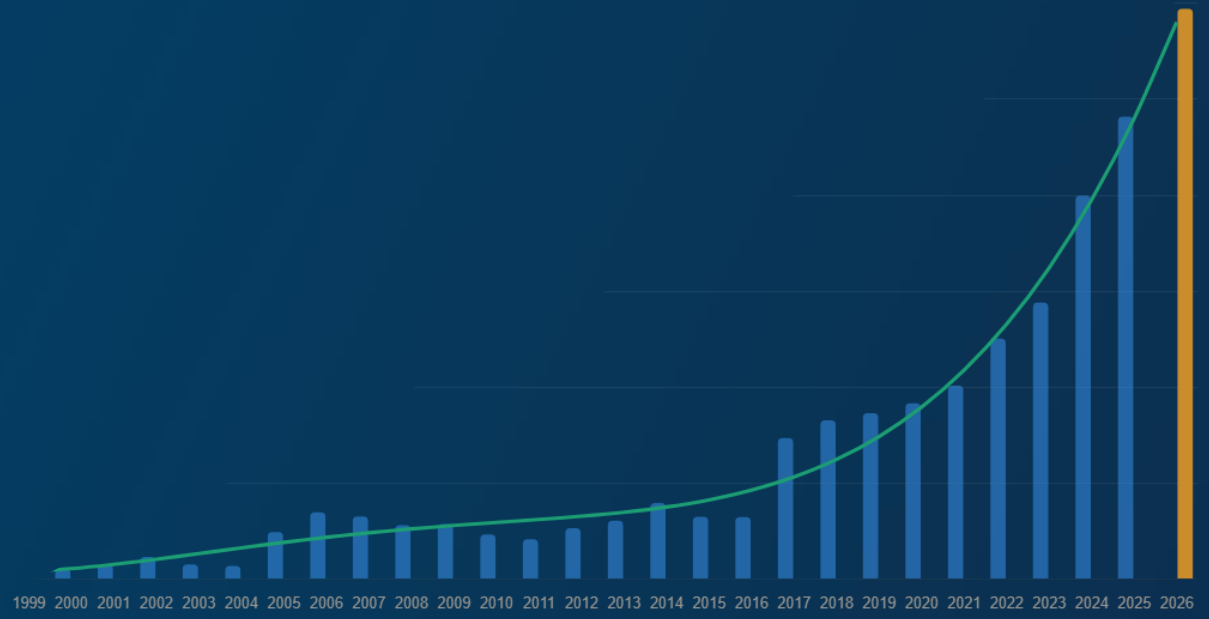
Betrusted

MA IO CHE C'ENTRO?

Efficienza vs vulnerabilità



Security researchers



Sviluppatori*

Betrusted

MA IO CHE C'ENTRO?

L'ingegneria del software è un ambito in evoluzione

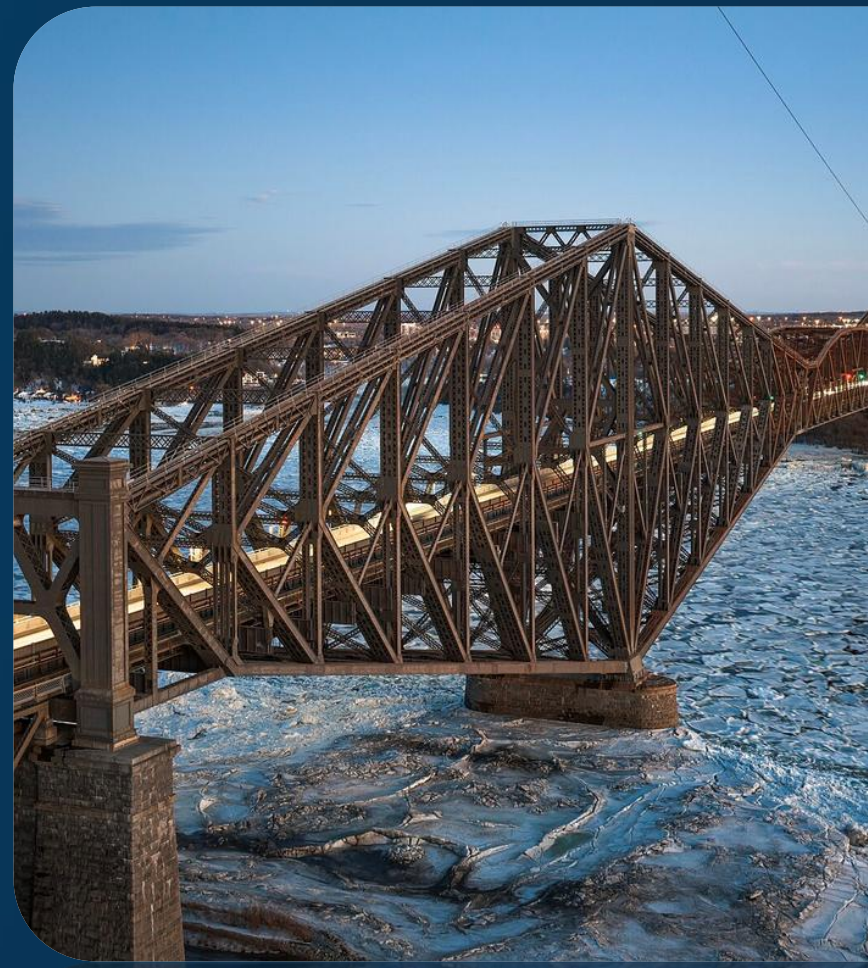
1. Migliaia di anni di esperienza in meno rispetto ad altri ambiti di ingegneria
2. «Se c'è una crepa nella casa, lo vede anche il postino»

Betrusted

MA IO CHE C'ENTRO?

Nuove responsabilità

1. Threat modeling
2. Security testing & code review
3. Garanzie di supporto, patching, updates
4. Supply chain & SBOM



Betrusted

Syllabus

01.

Perché Security by design?

- Introduzione al concetto e alle motivazioni del corso
- Fondamenti di cybersecurity

02.

Pianificazione e progettazione

- Framework di threat modeling
- Progettare per un assumed breach scenario
- Secure code review 101

03.

Security nella pipeline

- Static Application Security Testing, Software Composition Analysis CI/CD e container security
- Supply chain security

04.

???

- Vuota perché devo lasciarmi del margine
- Per gestire le aspettative stavolta

MA IO CHE C'ENTRO?

Il resto del feedback

Formare i programmatori *non basta*.

Security by design *deve essere per tutti*!

Betrusted

SECURITY BY DESIGN DEVE ESSERE…

Per gli sviluppatori

- Sempre più AI significa che parte del lavoro degli sviluppatori diventa, in sostanza, una secure code review.
- Progettazione: consapevolezza, quando si scrive una funzione, dei rischi comunemente associato
- Testing: i test di sicurezza di base vanno implementati al pari di quelli funzionali

Betrusted

SECURITY BY DESIGN DEVE ESSERE…

Per i DevOps

- Testing: i test di sicurezza di base vanno implementati al pari di quelli funzionali
- Infrastruttura: setup di tool di analisi del codice e inclusione delle analisi automatizzate all'interno della pipeline (e.g. SAST, SCA…)

Betrusted

SECURITY BY DESIGN DEVE ESSERE…

Per i product owner, delivery manager, scrum master etc…

- Garantire i mezzi e i tempi agli sviluppatori per applicare le pratiche di sviluppo sicuro
- Includere nella pianificazione e nella progettazione, assicurarsi che la sicurezza non venga sacrificata per delivery più veloci

Betrusted


Observation, Feedback
Principles
Practices
(Baseline) Controls
Risk Negotiation
Change Management
Secure Software Design
Secure Development
Secure Default Configuration
Supply Chain Security
Code Integrity
Vulnerability Remediation
Secure By Design

Betrusted

Betrusted

Via Gerolamo Gaslini, 2
20900 Monza (MB)

P.IVA
13017610968

Codice fiscale
13017610968

Contatti
+39 039.28.45.774
info@betrusted.it
betrusted.it