

Security by design per lo spazio: come Celeste Technologies ha rafforzato la sicurezza della sua RAN satellitare 5G



Executive Summary

Celeste Technologies sta sviluppando SmartgNB, un gNodeB software-defined per le reti non terrestri (NTN), progettato per estendere le comunicazioni 5G nello spazio. Prima del deployment sul mercato, Celeste ha collaborato con HWG Sababa per un'attività avanzata di product security testing che ha combinato secure code review, threat modeling e fuzz testing.

Il progetto ha consentito di identificare le vulnerabilità di sicurezza e definirne le priorità di risoluzione, migliorare la resilienza del software e integrare pratiche di sviluppo sicuro nelle future release del prodotto, rafforzando l'approccio secure-by-design di Celeste prima del lancio commerciale e supportando la preparazione dell'azienda per future collaborazioni con operatori e stakeholder istituzionali.

Risultati principali

- Oltre 20 interventi di miglioramento della sicurezza individuati e gestiti prima del lancio commerciale
- 8 criticità confermate come sfruttabili in ambiente operativo e risolte prima del deployment
- Maggiore resilienza del sistema grazie ad attività avanzate di validazione e testing della sicurezza
- Pratiche di sviluppo sicuro integrate nei processi di engineering
- Creazione delle basi per attività continuative di fuzz testing e futuri security assessment
- Maggiore preparazione per il deployment in ambienti di comunicazione critici

Profilo aziendale

Per superare i limiti delle tradizionali reti terrestri e abilitare nuovi casi d'uso, gli standard delle telecomunicazioni stanno integrando attivamente le comunicazioni satellitari nell'ecosistema 5G. Incorporando le reti satellitari direttamente nelle specifiche 3GPP, il settore sta creando un framework unificato in grado di garantire una connettività resiliente anche nelle aree remote e negli ambienti mission-critical, a complemento delle infrastrutture di rete terrestri esistenti.

Persu supportare questa evoluzione, Celeste Technologies, azienda italiana deep-tech, sviluppa infrastrutture 5G completamente software-defined, progettate specificatamente per le reti spaziali. La sua soluzione di punta, SmartgNB, è uno stack software virtualizzato per stazioni radio base 5G (gNodeB), concepito per estendere le comunicazioni mobili standard e conformi alle specifiche 3GPP agli ambienti satellitari.

A differenza delle infrastrutture di telecomunicazione tradizionali, basate su piattaforme hardware e software strettamente integrate, l'approccio software-defined di Celeste garantisce maggiore flessibilità, scalabilità e interoperabilità nelle reti satellitari di nuova generazione.

Operando all'intersezione tra telecomunicazioni e tecnologie spaziali, l'azienda contribuisce allo sviluppo di una nuova generazione di servizi di connettività satellitare, affrontando al contempo le sfide tecniche legate al deployment di infrastrutture di comunicazione critiche nello spazio.

Principali sfide

Per Celeste Technologies, la sfida non era semplicemente sviluppare una nuova soluzione per le telecomunicazioni, ma dimostrare che una giovane realtà operante in un mercato emergente fosse in grado di offrire una tecnologia all'altezza delle aspettative di futuri operatori, stakeholder istituzionali e ambienti di comunicazione critici.

Poiché la piattaforma è destinata a infrastrutture satellitari, sicurezza, resilienza e affidabilità dovevano essere considerate fin dalle prime fasi dello sviluppo, anziché essere affrontate successivamente attraverso iniziative di compliance o in risposta a specifiche richieste dei clienti.

Sicurezza in un Ambiente Spaziale. I sistemi installati a bordo dei satelliti presentano possibilità di intervento fisico estremamente limitate, rendendo necessari elevati livelli di affidabilità e resilienza fin dalla progettazione.

Vincoli di Prestazioni Real-Time. La piattaforma opera in un contesto real-time con stringenti requisiti di latenza, limitando la possibilità di introdurre controlli di sicurezza che potrebbero compromettere le prestazioni.

Architettura Complessa e Multi-Interfaccia. La presenza di molteplici interfacce di comunicazione e controllo amplia la superficie di attacco e richiede un'attenta validazione della sicurezza.

Bilanciare Innovazione e Sicurezza. In quanto azienda in rapida crescita con solide competenze di R&D, Celeste doveva conciliare cicli di sviluppo rapidi con pratiche di secure coding e requisiti di robustezza del prodotto nel lungo periodo.

“Sapevamo fin dall’inizio che la cybersecurity doveva essere una priorità. Stiamo sviluppando un’infrastruttura di telecomunicazioni critica e volevamo che la sicurezza fosse parte integrante della roadmap di prodotto fin dalle prime fasi, anziché essere aggiunta in un secondo momento per rispondere alle richieste del mercato.”

– Fabio Marconi, Co-Founder e Product Manager di Celeste Technologies

La soluzione: product security assessment e penetration testing

Per affrontare queste sfide, Celeste Technologies ha collaborato con HWG Sababa per condurre un'attività avanzata di penetration testing sul proprio gNB software-defined per reti 5G NTN. L'intervento si è concentrato sulla validazione della sicurezza e della resilienza di una codebase altamente complessa, composta da milioni di righe di codice e basata su protocolli avanzati di telecomunicazione conformi agli standard internazionali 3GPP.

Per garantire una valutazione approfondita sia a livello architetturale sia implementativo, l'assessment ha combinato tre attività complementari:

Secure Code Review

Un'analisi approfondita del codice sorgente ha consentito di identificare vulnerabilità, pratiche di coding non sicure e opportunità di miglioramento della resilienza del software, preservando al contempo i requisiti prestazionali.

Threat Modeling

L'architettura del sistema e le relative interfacce sono state analizzate per identificare potenziali vettori di attacco, valutare i punti di esposizione e prioritizzare le attività di mitigazione.

Fuzz Testing

È stato creato un ambiente di test dedicato per valutare la risposta della piattaforma a input inattesi o malformati, individuando potenziali debolezze in grado di compromettere stabilità, affidabilità o sicurezza.

Scope of Testing

- Analisi del codice e identificazione delle vulnerabilità
- Threat modeling a livello architetturale
- Ambiente di simulazione dedicato
- Fuzz testing avanzato per la validazione della resilienza
- Indicazioni operative di remediation a supporto delle future attività di sviluppo

“È stata una collaborazione a tutti gli effetti. Il team di HWG Sababa ha compreso rapidamente gli aspetti chiave della nostra tecnologia, fornendoci analisi, indicazioni e raccomandazioni concrete che hanno rafforzato fin da subito sia il nostro prodotto sia i nostri processi di sviluppo.”

– Vincenzo Icolari, Responsabile Ricerca e Sviluppo di Celeste Technologies

Risultati e impatto sul business

L'iniziativa ha prodotto miglioramenti immediati sul fronte della sicurezza, contribuendo al tempo stesso a rafforzare la strategia di sviluppo del prodotto, ridurre i rischi prima del lancio commerciale e aumentare la preparazione dell'azienda verso future opportunità di mercato.

Rafforzamento della sicurezza

L'assessment ha identificato oltre 20 aree di miglioramento della sicurezza all'interno della piattaforma, incluse 8 vulnerabilità confermate come sfruttabili in ambiente operativo. I risultati hanno permesso a Celeste di definire una roadmap di remediation basata sulle priorità, consentendo al team di engineering di affrontare tempestivamente i rischi più critici nelle prime fasi del ciclo di sviluppo del prodotto e rafforzare ulteriormente la sicurezza del proprio gNB software-defined per reti NTN.

Processi di sviluppo più solidi

Le evidenze emerse e le raccomandazioni fornite hanno consentito a Celeste di perfezionare il proprio approccio ingegneristico e consolidare i principi di secure coding lungo l'intero ciclo di sviluppo del prodotto. Le attività di security testing sono state integrate più strettamente nei processi di sviluppo, riducendo il rischio di problematiche ricorrenti nelle future release.

Crescita delle competenze interne

Oltre all'identificazione delle vulnerabilità, HWG Sababa ha fornito metodologie, approcci di testing e indicazioni operative integrabili nei processi interni di validazione di Celeste. Questo trasferimento di competenze ha contribuito a creare le basi per attività continuative di security testing, accompagnando l'evoluzione della piattaforma nel tempo.

Preparazione strategica

Affrontando la sicurezza fin dalle prime fasi del ciclo di vita del prodotto, Celeste ha rafforzato la propria capacità di adottare e dimostrare un approccio maturo e proattivo alla cybersecurity. Il progetto ha inoltre aumentato la preparazione dell'azienda verso future collaborazioni con operatori di telecomunicazioni, organizzazioni istituzionali e altri stakeholder attivi in contesti di comunicazione critici, dove sicurezza e resilienza rappresentano criteri di valutazione fondamentali.

L'attività ha consentito a Celeste di dimostrare come la cybersecurity sia parte integrante del processo di sviluppo del prodotto, un elemento chiave per costruire fiducia presso futuri clienti, operatori e partner dell'ecosistema.

Con la continua evoluzione della piattaforma, Celeste sta valutando l'introduzione di attività continuative di fuzz testing e di ulteriori iniziative di validazione della sicurezza, con l'obiettivo di supportare la resilienza e la scalabilità del prodotto e aumentarne la preparazione al deployment.

"Il valore del progetto è andato ben oltre la semplice identificazione e risoluzione delle vulnerabilità. Abbiamo rafforzato il nostro processo di sviluppo, dotando il team di strumenti e metodologie in grado di evolvere insieme al prodotto. Non abbiamo ricevuto solo un elenco di interventi da effettuare: abbiamo migliorato il nostro approccio alla cybersecurity, integrandolo nella cultura del nostro team di engineering e nella roadmap di sviluppo del prodotto a lungo termine."

– Chiara Grasselli, Esperta di Cybersecurity di Celeste Technologies