



ERA-AI: supporto all'analisi del rischio ISO/IEC 27001 ed estensioni ISO/IEC 27017-27018

Ente sviluppatore: Nextage Srl

Sede: Genova

Ente di applicazione: Interno



PROCESSO/I DI APPLICAZIONE

Qualità, Security



SETTORE/I DI APPLICAZIONE

Tutti i settori



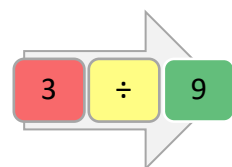
TECNOLOGIE ABILITANTI

Cloud/Piattaforme digitali, Sicurezza informatica, IA/Machine learning



Parole chiave

SaaS, INFORMATION SECURITY, PRIVACY, PREDICTIVE ANALYTICS, NoSQL, DEEP LEARNING



LIVELLO DI MATURITA' TECNOLOGICA (TRL) N°9



Link approfondimenti



Obiettivi

Effettuare analisi del rischio aziendale conforme a standard ISO quali la 27001, le sue estensioni cloud (27017-27018) e privacy (27701), oltre a 22301 e 20000-1, e GDPR.

Soluzione

ERA è una web-app cloud SaaS (Software as a Service) che permette di abbattere i tempi di data entry nell'analisi del rischio, molto onerosi in particolare per le aziende di grandi dimensioni, grazie alla predizione dei valori di vulnerabilità (es. per un'impresa con 100 asset, circa 20.000 valori), supportando l'utente senza sostituirne l'expertise. Tipologia di enduser/stakeholder: IT manager, Risk manager, Compliance officer di aziende certificate o in procinto di certificarsi sulle suddette norme.

La soluzione è basata su un moderno stack tecnologico (Atlas MongoDB, cloud AWS, Node.js, Angular, Bootstrap) e sfrutta algoritmi di AI (deep learning), in particolare reti neurali tabulari, per suggerire agli utenti le vulnerabilità più appropriate per la loro tipologia di azienda. Le tecnologie usate per realizzare il modulo ERA-AI includono: il linguaggio Python, molto diffuso in ambito data science per la sua versatilità nell'elaborazione dei dati; framework di AI fast.ai che a sua volta sfrutta la libreria di deep learning PyTorch.

Fasi di implementazione

Per accedere e utilizzare ERA-AI è sufficiente accedere all'url dell'applicativo web e loggarsi con credenziali rilasciate, senza necessità di installazione alcuna.

Le best practices di sicurezza adottate secondo la metodologia di sviluppo sicuro OWASP garantiscono la riservatezza, integrità e disponibilità dell'informazione contenuta. Il modello di AI è inserito all'interno dell'architettura a microservizi dell'applicativo e viene evocato all'occorrenza per generare l'inferenza.

Risultati ottenuti/attesi

Tempo medio di compilazione risparmiato stimato (o misurato): predizione di 20k valori stimata in circa 6 minuti rispetto a circa 80 ore manuali stimate.

