PENTESTERRA

DEVGUARD SECURITY REVIEW

Cosa C'è Davvero Nel Codice Scritto Dalla Tua AI?

Una revisione di sicurezza (cyber) del tuo codice, delle dipendenze e della pipeline di sviluppo - prima che arrivi in produzione, non dopo.

COS'È DEVGUARD SECURITY REVIEW, IN BREVE

È l'analisi della sicurezza informatica (cyber) del tuo ambiente di sviluppo: dipendenze vulnerabili, segreti esposti nel codice, rischi introdotti da strumenti di AI coding, configurazioni pericolose nella pipeline CI/CD. Il tuo assistente AI ha visto lo schema del tuo database, le tue chiavi API, gli URL dei tuoi servizi interni - sai chi altro potrebbe averli visti?

45
Moduli di rilevamento: supply chain, segreti, AI, IaC, CI/CD

Minuti
Non giorni - i risultati arrivano rapidamente, non in settimane

Codice al Sicuro
Il codice sorgente non lascia mai la tua macchina

LA SITUAZIONE OGGI

CHI SEI

Sei il CTO, l'engineering manager o il responsabile sicurezza di un'azienda il cui team scrive codice - probabilmente anche con l'aiuto di strumenti di AI coding - e che deve sapere davvero cosa finisce nella codebase prima che arrivi in produzione.

COSA È SUCCESSO

Gli assistenti di AI coding sono ormai parte del flusso di lavoro quotidiano. Suggeriscono dipendenze, generano configurazioni, a volte incollano segreti o credenziali direttamente nel codice - e nessuno rivede sistematicamente ciò che producono prima del commit.

IL PROBLEMA

Non sai, con certezza, cosa si nasconde nelle tue dipendenze, nei tuoi hook Git, nella tua pipeline CI/CD, o nella configurazione dei tuoi strumenti AI. Un pacchetto malevolo, un segreto dimenticato in uno storico Git, un hook Git compromesso - queste sono le vie d'accesso più comuni oggi, e restano invisibili a una semplice code review.

PERCHÉ FA MALE

Un segreto esposto nel codice, un pacchetto vulnerabile, un hook Git malevolo possono dare a un attaccante accesso diretto ai tuoi sistemi di produzione - prima ancora che un finding di penetration test venga sollevato. NIS2, ISO 27001 e la maggior parte dei framework di cybersicurezza chiedono esplicitamente evidenza di sicurezza nella catena di sviluppo.

DOVE VUOI ARRIVARE

STATO DESIDERATO

Vuoi sapere, con certezza, cosa si nasconde nella tua codebase e nella tua pipeline di sviluppo - dipendenze, segreti, configurazioni pericolose - prima che diventi un incidente.

LA SOLUZIONE

Una **DevGuard Security Review**: analisi completa della supply chain e delle dipendenze, rilevamento di segreti e credenziali esposte, valutazione del rischio degli strumenti di AI coding, scansione della configurazione Infrastructure-as-Code e della pipeline CI/CD - su 45 moduli di rilevamento diversi.

PERCHÉ È DIVERSO

Non stai comprando l'ennesimo scanner di dipendenze generico. Stai lavorando con [NOME AZIENDA] - fornitore certificato, italiano, con quasi 20 anni di storia nel settore della sicurezza informatica. Probabilmente ci conosci già, o conosci qualcuno - un collega, un fornitore, un concorrente - che è già stato nostro cliente. Molti dei tuoi concorrenti diretti si stanno già rivolgendo a noi. E ogni segnale confermato può entrare nello stesso grafo di attack chain che collega codice, rete e applicazioni web - così un segreto esposto in un repository non resta un finding isolato, ma viene mostrato come parte di un percorso d'attacco reale, con priorità coerenti tra i team.

PROVA CONCRETA

Il risultato è un report PDF completo, pronto da consegnare, con ogni rischio identificato e prioritizzato, e il codice sorgente che non lascia mai la tua macchina durante l'analisi. Se emergono gap più ampi, ti proponiamo le misure aggiuntive per colmarli: vulnerability assessment, penetration test di rete o applicativo, formazione anti-phishing.

Privacy-First

Analisi in locale, nessun upload del codice sorgente

CI/CD Opzionale

Nessuna integrazione obbligatoria per iniziare

6 Ecosistemi

Copertura multi-linguaggio, non solo un singolo stack

COSA INCLUDE DAVVERO

45 moduli di rilevamento reali, non una checklist generica - dalla supply chain ai rischi introdotti dall'AI coding.

Supply chain e dipendenze

Cosa si nasconde davvero nei 347+ pacchetti che il tuo progetto importa.

- Analisi supply chain e dipendenze su 6 ecosistemi
- Rilevamento di pacchetti dannosi noti
- Esportazione SBOM ed estrazione licenze
- Conflitti tra dipendenze peer, rilevamento API deprecate

Segreti e credenziali

Non solo il commit di oggi - anche quello che si nasconde nella storia del repository.

- Rilevamento di segreti e credenziali esposte nel codice
- Token liveness e analisi del raggio d'impatto (blast radius)
- Protezione multi-VCS, scansione dello storico Git e SVN
- Scansione della shell history e dei messaggi di commit

AI, automazione e toolchain

Il rischio specifico introdotto da assistenti AI, agenti e strumenti MCP.

- Rischio toolchain AI e server MCP, rischio di configurazione agenti AI
- Prompt injection su integrazioni LLM, prompt injection indiretta nei contenuti del repo
- Rilevamento del punto cieco del vibe coding, esposizione di vector DB
- RCE da caricamento modello e deserializzazione non sicura

CI/CD e infrastruttura

La pipeline che porta il codice in produzione, non solo il codice stesso.

- Rilevamento di injection nella pipeline CI/CD
- Scansione Infrastructure-as-Code (IaC)
- Rilevamento di repository malevoli e hook Git compromessi
- Export SARIF e suggerimenti di auto-fix

PENTESTERRA

DEVGUARD SECURITY REVIEW

COSA RICEVI

- ✓ Un report PDF completo con ogni rischio identificato e prioritizzato
- ✓ Analisi di supply chain, dipendenze vulnerabili e pacchetti malevoli
- ✓ Rilevamento di segreti e credenziali esposte, anche nello storico Git
- ✓ Valutazione del rischio degli strumenti di AI coding e della pipeline CI/CD
- ✓ Raccomandazioni di remediation concrete, non generiche

COME FUNZIONA

1

Definiamo il perimetro

Repository, pipeline CI/CD, strumenti di sviluppo - stabiliamo insieme lo scope.

2

Analizziamo in locale

Il codice sorgente non lascia mai la tua macchina durante l'analisi.

3

Prioritizziamo il rischio

Ordiniamo i findings per impatto reale, non per volume.

4

Ti consegniamo il report

Un PDF completo con i rischi prioritizzati e le azioni da intraprendere.

Scopri cosa si nasconde nella tua codebase

Un report completo, pronto da presentare a clienti, auditor o al tuo consiglio di amministrazione.

Richiedi la tua DevGuard Review →

info@pentesterra.com · pentesterra.com/devguard