Come applicare il Secure Software Development Life Cycle (SSDLC) per la compliance a DORA

Una roadmap per la resilienza operativa nel settore finanziario

Index

Abstract

Nel contesto di un ambiente digitale sempre più complesso e minacciato da rischi informatici, il regolamento Digital Operational Resilience Act (DORA) emerge come una pietra miliare nell'Unione Europea per assicurare che il settore finanziario possa affrontare efficacemente tali sfide

Questo whitepaper esplora l'importanza cruciale di DORA nel promuovere una cultura di resilienza operativa digitale, sottolineando come le organizzazioni possono trovare difficile implementare i suoi numerosi controlli in maniera corretta e reattiva. In questo contesto, l'adozione di un Secure Software Development Life Cycle (SSDLC) non è solo strategica ma necessaria per integrare la sicurezza e la resilienza fin dalle prime fasi dello sviluppo del software, garantendo che le pratiche di sicurezza diventino parte integrante del processo produttivo piuttosto che essere aggiunte in seguito come misure correttive.

L'obiettivo di questo whitepaper è dimostrare come l'implementazione dell'SSDLC, attraverso la sua natura proattiva e integrata, possa non solo rispondere efficacemente a tali requisiti ma anche portare vantaggi operativi, di business e strategici duraturi per le organizzazioni finanziarie. Mettendo in luce come NTT DATA, con la sua esperienza e competenza nello sviluppo sicuro del software, sia posizionata in modo unico per assistere le organizzazioni in questo percorso, il whitepaper mira a fornire una roadmap concreta per la conformità a parte dei requisiti DORA e oltre, sottolineando l'importanza di un approccio olistico alla resilienza operativa digitale.

DORA e il Secure Software Development Life Cycle (SSDLC):

5 punti di vista per i professionisti del settore finanziario

Il presente whitepaper è strategicamente rivolto a un'ampia varietà di professionisti nel settore finanziario che giocano un ruolo critico nell'assicurare che le pratiche di sviluppo software e le operazioni digitali siano non solo sicure ma anche resilienti e conformi agli standard regolamentari imposti dal Digital Operational Resilience Act (DORA).

- **Integrazione**: il documento fornisce insight cruciali su come integrare le fasi dello SSDLC con i requisiti di DORA, enfatizzando l'importanza di un approccio improntato alla sicurezza e alla resilienza, rispondendo alle domande dei Chief Information Security Officer (CISO), che hanno la responsabilità generale della sicurezza delle informazioni e delle strategie di resilienza operativa digitale all'interno delle loro organizzazioni.
- **Progettazione sicura**: il documento offre a figure come gli Architetti di Sicurezza, che progettano le strutture dei sistemi informatici, una guida su come i principi di progettazione sicura possono essere allineati con gli articoli specifici di DORA, facilitando così lo sviluppo di architetture resilienti e conformi.
- **Codifica e sicurezza**: il whitepaper fornisce indicazioni su pratiche di codifica sicura e l'importanza di integrare la sicurezza sin dalle prime fasi dello sviluppo, in linea con gli obblighi di DORA. Tali indicazioni possono aiutare i Software Engineer nella creazione di applicazioni e sistemi.

- **Miglioramento continuo e adempimento dei requisiti**: il documento mette in luce come l'adeguamento a DORA attraverso l'integrazione del SSDLC possa non solo soddisfare i requisiti regolamentari ma anche promuovere un miglioramento continuo nella sicurezza del software e nella resilienza operativa. Questi aspetti possono essere particolarmente interessanti per i Responsabili di Conformità, che devono garantire che le operazioni e le pratiche aziendali siano in linea con i regolamenti vigenti e i Risk Manager, che devono identificare e mitigare i rischi aziendali, garantendo la stabilità e la sicurezza operativa.
- **Miglioramento della resilienza operativa e definizione delle linee guida**: per rispondere alle necessità dei Chief Information Officer (CIO), responsabili della gestione quotidiana delle operazioni informatiche e di Policymakers e Regolatori, che cercano di comprendere le sfide incontrate dalle entità finanziarie nell'implementare i requisiti di DORA, approfondiamo come mantenere e migliorare la resilienza operativa attraverso pratiche di manutenzione e operazioni sicure, conformemente a DORA e come definire linee guida chiare e fattibili.

Attraverso la lettura di questo whitepaper, i professionisti del settore finanziario acquisiranno una comprensione profonda su come integrare efficacemente le pratiche del SSDLC con i requisiti di DORA, contribuendo non solo alla conformità normativa ma anche al rafforzamento della sicurezza e della resilienza operativa digitale all'interno del loro ecosistema finanziario.

L’imperativo della compliance a DORA e come rispondere alla sfida

L’adesione e la conformità ai requisiti DORA risultano essere mandatori per le entità finanziarie che rientrano all’interno del perimetro di applicabilità. Vista l’importanza del regolamento e del contesto in cui si posiziona, saranno incaricate le autorità di regolamentazione di verificare l’adesione al regolamento che, in caso in cui un’entità finanziaria non sia compliant, potranno applicare sanzioni amministrative, e in alcuni casi penali, alle entità inadempienti. È dunque importante che le entità finanziarie prestino particolare attenzione e si adoperino all’individuazione di strategie per l’adesione a tale regolamento.

Nel presente whitepaper affronteremo i requisiti del regolamento DORA che possono essere integrati o allineati con le tematiche di software security, rappresentando una soluzione complementare, ma non nella sua interezza, a un programma di conformità al regolamento DORA. I requisiti da trattare riguardano tematiche relative ad assicurare valutazioni periodiche del rischio, implementare soluzioni ICT robuste e misure di sicurezza per il trasferimento dei dati, e mantenere alti standard di disponibilità, autenticità, integrità e confidenzialità dei dati. Inoltre, il requisito di pratiche di codifica sicura, test di sicurezza completi e test di resilienza operativa sottolineano la necessità di un approccio integrato per soddisfare questi obiettivi duali di sicurezza e conformità regolamentare.

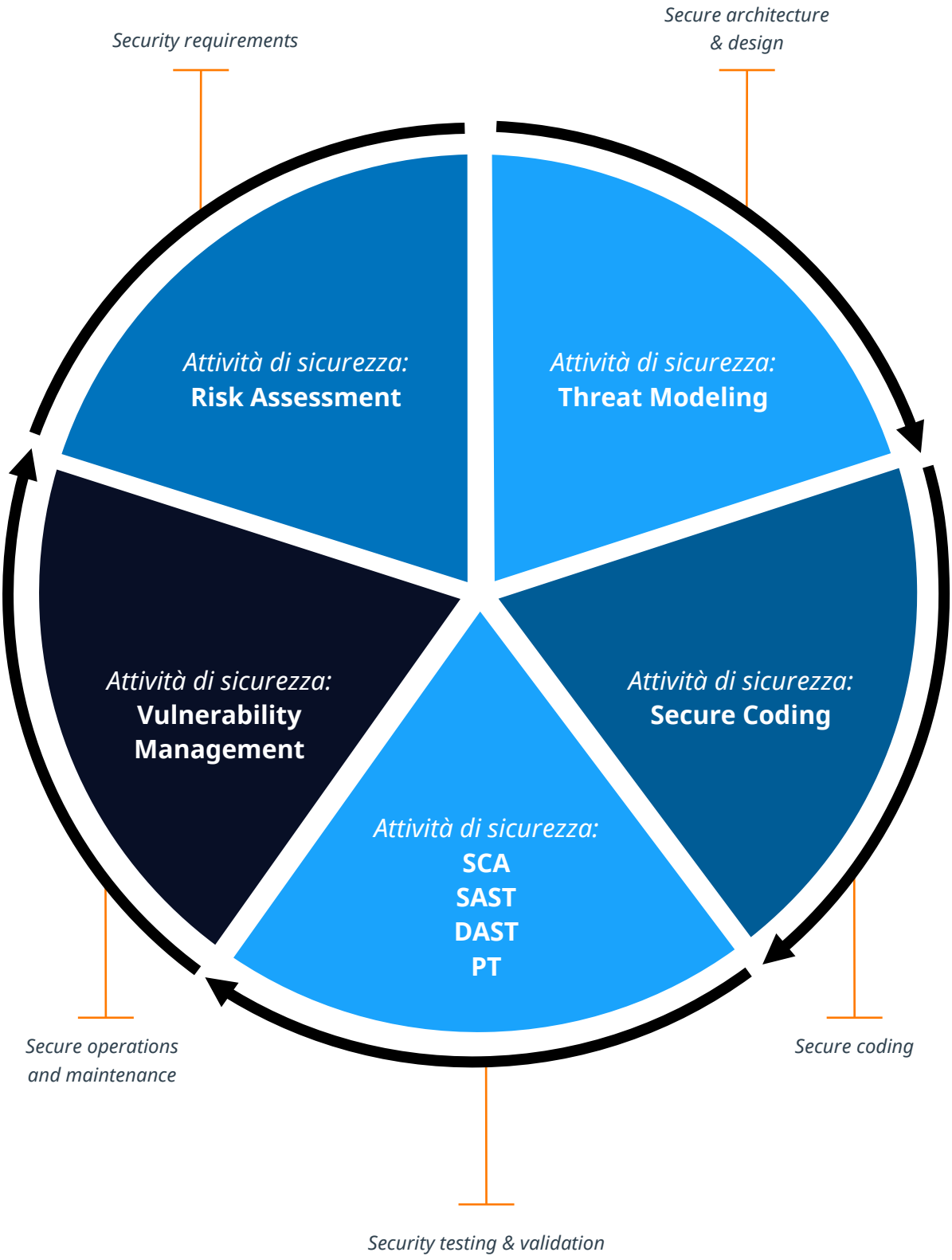
Cos'è il Secure Software Development Life Cycle (SSDLC) e come applicarlo a DORA

Per affrontare i requisiti del DORA relativi alle tematiche precedentemente citate, viene proposto nel presente whitepaper l'utilizzo del SSDLC come strumento per potenziare la resilienza operativa del software e adempiere al contempo ai requisiti del regolamento.

Cos'è il Secure Software Development Life Cycle

L'SSDLC rappresenta un'evoluzione del tradizionale ciclo di sviluppo software, arricchito dall'incorporamento di pratiche di sicurezza in ogni sua fase. Questo approccio non solo mira a produrre applicazioni intrinsecamente più sicure, dotate di meccanismi efficaci per la gestione e la mitigazione dei rischi, ma punta anche a instaurare una cultura della sicurezza su tutto il processo produttivo. Integrando la sicurezza come un elemento fondamentale, le entità finanziarie possono significativamente migliorare la propria capacità di prevenire, rilevare e rispondere a potenziali vulnerabilità, contribuendo così all'obiettivo più ampio della resilienza operativa assicurandosi che le proprie operazioni rimangano resilienti e flessibili di fronte alle sfide poste dal panorama digitale in continua evoluzione.

Prima di affrontare la soluzione dettagliata, occorre fornire una panoramica sull'SSDLC, sulle attività di sicurezza previste in essa e dei principali articoli del regolamento DORA che permettono di coprire tali attività:



Security Requirements

La fase dei Requisiti è un passaggio cruciale in cui vengono identificati e documentati i bisogni e gli obiettivi di sicurezza per le applicazioni software. Questa fase coinvolge la raccolta sistematica dei requisiti di sicurezza da tutti gli stakeholder (IT security, unità di business e utenti finali) per garantire che il software operi in modo sicuro e conformemente alle leggi, regolamenti e politiche applicabili. Di seguito l'attività di sicurezza prevista all'interno di questa fase e gli articoli del regolamento DORA che tale attività permette di coprire:

Attività di sicurezza	Articoli DORA coperti
Risk assessment: questa attività include l'identificazione proattiva delle minacce e delle vulnerabilità, l'analisi quantitativa o qualitativa del loro impatto potenziale e la priorizzazione delle azioni di mitigazione basate sul livello di rischio. L'obiettivo è assicurare che la sicurezza sia integrata nel processo di sviluppo fin dalle sue fasi iniziali, riducendo così i rischi per la sicurezza dei dati e delle applicazioni in modo efficace ed efficiente.	• **Articolo 5**: l'attività di risk assessment garantisce che i dati gestiti dalle applicazioni software soddisfino i rigorosi criteri di protezione, attraverso la specifica dei requisiti che affrontano direttamente i bisogni di sicurezza dei dati. • **Articolo 8**: le attività di valutazione e pianificazione specifica per i sistemi legacy assicurano che i rischi legati ai sistemi preesistenti siano gestiti e mitigati nel contesto dello sviluppo di nuove soluzioni software. • **Articolo 9**: l'attività prevista in questa fase fornisce soluzioni di sicurezza e un quadro di gestione del rischio che affrontano direttamente i rischi associati alla gestione dei dati, garantendo la resilienza operativa contro le minacce alla sicurezza delle informazioni.

Secure Architecture and Design

Durante questa fase, vengono definite le specifiche di progettazione del software, tenendo conto dei requisiti di sicurezza identificati nella fase precedente. Una volta definito quelli che sono i requisiti del software e dopo aver eseguito l'attività di risk assessment, occorre effettuare un'analisi specifica sulle minacce che potrebbero impattare il software.

Di seguito l'attività di sicurezza prevista all'interno di questa fase e gli articoli del regolamento DORA che tale attività permette di coprire:

Attività di sicurezza	Articoli DORA coperti
Threat Modeling: Il threat modeling è un'attività che permette di identificare i rischi specifici in merito al software in sviluppo. L'importanza di avere un'architettura solida e sicura permette di avere dei sistemi TIC resilienti e aggiornati per proteggere adeguatamente la disponibilità, l'autenticità e la riservatezza dei dati nei sistemi informatici.	• **Articolo 6**: le entità finanziare predispongono un quadro per la gestione dei rischi informatici assicurando un elevato livello di resilienza operativa digitale. Comprende strategie, politiche, procedure e protocolli e strumenti in materia di TIC necessari per proteggere dibitamente e adeguatamente tutti i patrimoni informatici e le risorse TIC, compreso il software. • **Articolo 16**: le entità finanziarie riducono al minimo i rischi informatici attraverso l'uso di sistemi, protocolli e sistemi TIC solidi, resilienti e aggiornati per proteggere adeguatamente la disponibilità, l'autenticità e la riservatezza dei dati nei sistemi informatici e di rete.

Secure Coding

La fase di Secure Coding è il momento in cui il codice viene effettivamente scritto, con un'enfasi particolare sull'integrazione di pratiche di sviluppo sicuro per prevenire vulnerabilità comuni. Durante questa fase, gli sviluppatori incorporano i requisiti di sicurezza definiti precedentemente per garantire che l'applicazione sia resistente alle minacce informatiche.

Di seguito l'attività di sicurezza prevista all'interno di questa fase e gli articoli del regolamento DORA che tale attività permette di coprire:

Attività di sicurezza	Articoli DORA coperti
Sviluppo sicuro: utilizzo delle linee guida e di strumenti automatici (plugin) per lo sviluppo software che forniscano in real-time informazioni su vulnerabilità rilevate su codice appena scritto.	**Articolo 9**: Tale controllo viene coperto sia dall'attività prevista nella fase di Security Requirements, sia da suddetta attività. L'articolo menzione che l'implementazione di metodologie di codifica sicure assicura la protezione dei dati durante il loro trasferimento, minimizzando la possibilità di perdite o alterazioni indesiderate, di intrusioni non consentite, e di vari altri intoppi che potrebbero interferire con l'operatività dell'entità finanziaria.

Security Testing and Validation

In questa fase il software viene sottoposto a diverse tipologie di testing che vanno ad analizzare l'applicativo in questione e permettono di identificare vulnerabilità presenti nel software.

Ogni attività fornisce una prospettiva unica sulle vulnerabilità software, rendendole intrinsecamente sinergiche e complementari. Combinando diverse iniziative di sicurezza, si ottiene un approccio completo rispetto all'analisi delle vulnerabilità, il che contribuisce a garantire risultati ottimali e una protezione complessiva più robusta. Di seguito le attività di sicurezza prevista all'interno di questa fase e gli articoli del regolamento DORA che tali attività permettono di coprire:

Attività di sicurezza	Articoli DORA coperti
Software Composition Analysis (SCA) Tipologia di analisi che valuta la sicurezza delle componenti software che costituiscono l'applicativo. • **Static Application Security Testing (SAST)** Analisi statica del codice sorgente alla ricerca di pattern vulnerabili. • **Dynamic Application Security Testing (DAST)** Analisi che esamina il comportamento dell'applicativo simulando scenari di attacco attraverso l'interazione e l'uso del software in funzione. • **Threat Leading Penetration Test (TLPT)** Analisi che si concentra sulla ricerca e l'exploit di vulnerabilità partendo da una precisa conoscenza sulle minacce che riguardano l'organizzazione.	• **Articolo 24**: introduce i requisiti generali per lo svolgimento dei testi di resilienza operativa digitale • **Articolo 25**: fornisce un'anteprima dei test di sicurezza da effettuare sugli strumenti e sistemi di TIC. • **Articolo 26**: definisce approfonditamente i test avanzati da eseguire su strumenti e sistemi TIC basati su test di penetrazione TLPT. • **Articolo 27**: definisce i requisiti mandatori per i soggetti incaricati dello svolgimento dei test TLPT.

Secure Operation and Maintenance

Durante il rilascio del software, vengono implementate misure di sicurezza per garantire che il software sia distribuito in modo sicuro e che le configurazioni predefinite siano appropriate per mitigare i rischi di sicurezza. Dopo il rilascio, è necessario monitorare e gestire i rischi di sicurezza attraverso patch, aggiornamenti e correzioni di eventuali vulnerabilità scoperte in ambiente di produzione.

Attività di sicurezza

Vulnerability Management: Attività che si occupa del trattamento e monitoraggio costante delle vulnerabilità nei software, garantendo che queste vengano corrette o mitigate tempestivamente. Questa attività è cruciale per mantenere i software sicuri e protetti da minacce emergenti, assicurando una continua resilienza operativa digitale.

Articoli DORA coperti

• **Articolo 7**: per gestire i rischi informatici, le entità finanziarie devono utilizzare e tenere aggiornati sistemi, protocolli e strumenti di TIC che siano proporzionati alle dimensioni delle loro operazioni, affidabili e sufficientemente resilienti per affrontare eventuali picchi di volume di lavoro o l'introduzione di nuove tecnologie.

• **Articolo 13**: si concentra sull'apprendimento e l'evoluzione nell'ambito della gestione dei rischi informatici per le entità finanziarie. Esso sottolinea l'importanza di raccogliere e analizzare informazioni su vulnerabilità, minacce, e incidenti informatici per migliorare la resilienza operativa digitale. Dopo un incidente significativo, è richiesto un esame approfondito per identificare le cause e apportare miglioramenti necessari.

La soluzione di NTT DATA basata su servizi SSDLC

La soluzione dettagliata di NTT DATA, proposta di seguito, include l'offerta di diversi servizi, che possono essere adottati e messi in pratica nel loro insieme o selezionati e utilizzati in maniera parziale e implementati on demand, a seconda delle specifiche esigenze del cliente. La presenta soluzione mira a guidare un'entità finanziaria attraverso una trasformazione verso l'adozione del Secure Software Development Life Cycle, in risposta ai requisiti del regolamento DORA precedentemente citati. L'approccio strutturato prevede i seguenti servizi:

Servizio	Titolo	Descrizione	Output
1	Analisi del contesto AS-IS	Attività che prevede un'analisi dettagliata dell'ambiente IT esistente, delle pratiche di sviluppo software e dei processi di sicurezza in uso. L'obiettivo è di identificare le lacune rispetto ai requisiti del regolamento DORA e alle best practice del SSDLC.	Report dettagliato di maturità AS-IS rispetto all'SSDLC.
2	Analisi dei requisiti	Identificazione dei requisiti di sicurezza mandatori per l'entità finanziaria attraverso un'analisi proattiva dei rischi per garantire che il software sia resiliente.	• Documentazione dei requisiti di sicurezza (obiettivi, scopo, fattori esterni ed interni). • Report di risk assessment.
3	Creazione e revisione di policy, procedure e linee guida	Creazione e/o revisione di policy, procedure e linee guida interne all'entità finanziaria al fine di incorporare i principi di sicurezza informatica fin dalle fasi iniziali dello sviluppo software.	Documentazione interna aggiornata, in linea con il SSDLC.
4	Architettura e design sicuro	Creazione di specifiche tecniche che incorporano i requisiti di sicurezza, con l'obiettivo di costruire un'architettura solida e resiliente alle minacce informatiche.	Report di Threat Modeling.
5	Installazione (strumenti) ed esecuzione di testing di sicurezza	Integrazione di strumenti di testing di sicurezza all'interno della pipeline di sviluppo. Esecuzione di attività di testing di sicurezza regolari (SCA, SAST, DAST, TLPT) per identificare e mitigare vulnerabilità o problemi di sicurezza nel software dell'entità.	• Ambiente di sviluppo integrato con strumenti di security testing, configurati e pronti all'uso. • Report SCA, SAST, DAST, TLPT.

Servizio	Titolo	Descrizione	Output
6	Formazione del personale	Programma di formazione mirato per sviluppatori, tester e manager di progetto per sensibilizzare e formare sulle best practice di sicurezza nello sviluppo software e sull'uso degli strumenti di testing di sicurezza.	Personale formato e consapevole delle proprie responsabilità nella creazione di software resiliente e sicuro.
7	Monitoraggio e supporto continuo	Servizi di supporto per monitorare l'efficacia delle nuove pratiche e per aggiornare le policy e gli strumenti in risposta all'evoluzione delle minacce informatiche e dei requisiti normativi.	Implementazione e gestione del sistema di tracciamento delle vulnerabilità (es. Serive now, Jira, etc)

Questo approccio non solo garantisce l'aderenza a parte dei requisiti DORA ma migliora anche la qualità e la sicurezza dei prodotti software sviluppati, minimizzando i rischi operativi e migliorando la fiducia dei clienti e degli stakeholder.

Benefici per il business nel settore finanziario

L'introduzione dell'SSDLC nelle pratiche aziendali rappresenta un cambiamento strategico cruciale per le entità finanziarie, specialmente in risposta a parte dei requisiti stabiliti dal regolamento DORA. Questo regolamento sottolinea l'importanza della resilienza operativa digitale per il settore finanziario, richiedendo l'integrazione della sicurezza informatica fin dalle fasi iniziali dello sviluppo del software. L'adozione di SSDLC non solo risponde a queste esigenze ma porta con sé una serie di benefici significativi per le aziende, inclusa la riduzione dei rischi operativi, il miglioramento della qualità e della sicurezza dei prodotti software, il rafforzamento della fiducia da parte dei clienti e degli stakeholder, nonché il posizionamento come leader nell'innovazione digitale sicura

Oltre a promuovere un miglioramento continuo nella sicurezza del software e nella resilienza operativa, l'integrazione dell'SSDLC consente alle entità finanziarie di evitare sanzioni economiche garantendo la conformità con parte dei rigorosi standard imposti da DORA. Questo approccio proattivo non solo assicura la sicurezza e la resilienza dei prodotti software ma protegge anche l'azienda da potenziali conseguenze finanziarie e reputazionali negative derivanti dalla non conformità.

Conclusioni

In questo whitepaper abbiamo esplorato in dettaglio l'importanza cruciale dell'integrazione del SSDLC in risposta a diversi requisiti imposti dal regolamento DORA per le entità finanziarie. La soluzione proposta, dettagliata nel documento, sottolinea l'importanza di adottare una strategia per la sicurezza dello sviluppo software.

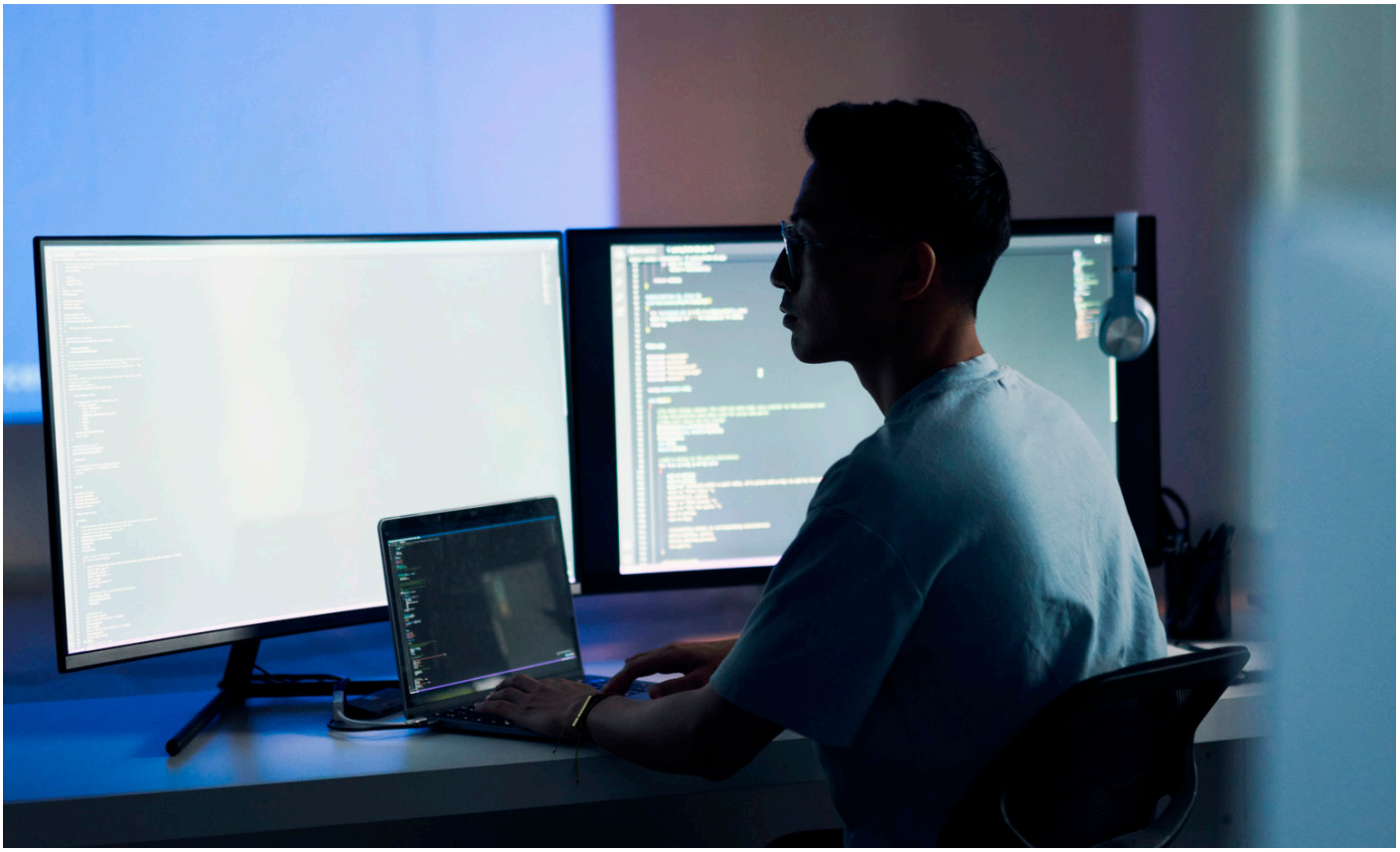
L'approccio presentato enfatizza l'importanza di una valutazione AS-IS dell'ambiente IT esistente, dell'analisi dei requisiti di sicurezza, della revisione e della creazione di policy e procedure, della progettazione di un'architettura e di un design sicuri, dell'integrazione di strumenti di testing di sicurezza, della formazione del personale, e infine, del monitoraggio e supporto continuo. Questi passaggi sono fondamentali per garantire che le pratiche di sicurezza siano integrate in ogni fase dello sviluppo del software, conformemente ai rigorosi standard imposti da DORA. L'utilizzo dell'SSDLC presenta numerosi vantaggi per le entità finanziarie, inclusa la riduzione dei rischi operativi, il miglioramento della qualità e della sicurezza dei prodotti software e il rafforzamento della fiducia da parte dei clienti e degli stakeholder. L'adozione di un approccio SSDLC consente alle entità di anticipare e mitigare efficacemente le minacce informatiche, assicurando al contempo che i prodotti software siano progettati con la resilienza necessaria per resistere agli attacchi, riducendo così le vulnerabilità e le potenziali violazioni dei dati.

Questo documento evidenzia la crescente necessità per le entità finanziarie di aderire a standard elevati di resilienza operativa digitale. In ultima analisi, l'integrazione dell'SSDLC non è soltanto una misura per rispettare i requisiti normativi; è una strategia essenziale per costruire un'infrastruttura IT robusta, capace di sostenere le sfide del panorama digitale in continua evoluzione. Incoraggiando un approccio proattivo alla sicurezza dello sviluppo software, le entità finanziarie possono assicurarsi non solo di essere in linea con il regolamento DORA, ma anche di posizionarsi come leader nell'innovazione digitale sicura nel settore finanziario.

Key takeaway

Dal presente documento, che sottolinea l'importanza cruciale di DORA nel garantire che il settore finanziario europeo sia pronto per affrontare efficacemente le minacce informatiche contro la resilienza operativa, si possono evincere i seguenti key takeaway:

- SSDLC come soluzione per la compliance a parte dei requisiti di DORA
- Benefici operativi e strategici attraverso un miglioramento della sicurezza del software
- Sicurezza integrata nel processo di sviluppo
- L'SSDLC aiuta a prevenire le vulnerabilità fin dall'inizio, migliorando cosi la resilienza operativa
- NTT DATA, con la sua forte esperienza, può supportare le entità finanziare verso la compliance ai requisiti di DORA
- È fondamentale un approccio proattivo alla sicurezza del software per permettere alle organizzazioni di mitigare efficacemente




NTT DATA