Analizzare la Conformità alla DORA: la gestione delle applicazioni in perimetro

Alessio Pennasilico, Comitato Scientifico Clusit
Massimo Tripodi, Country Manager Veracode

16 gennaio 2025 - orario 11.00-12.00

Alessio Pennasilico

Partner, Practice Leader Information & Cyber Security Advisory Team
Security Evangelist & Ethical Hacker

Membro del Comitato Scientifico

Membro del Comitato Direttivo di Informatici Professionisti

Vice Presidente del Comitato di Salvaguardia per l'Imparzialità

Membro del Comitato di schema

Direttore Scientifico della testata

Senior Advisor dell'Osservatorio Cyber Security & Data Protection del Politecnico di Milano

Massimo Tripodi

COUNTRY MANAGER VERACODE

Che cos’è il Digital Operational Resilience Act ?

Il Digital Operational Resilience Act (DORA) è un regolamento dell’Unione Europea (UE) che definisce un quadro normativo obbligatorio e completo per la gestione dei rischi legati alle tecnologie dell’informazione e della comunicazione (ICT) nel settore finanziario dell’UE.

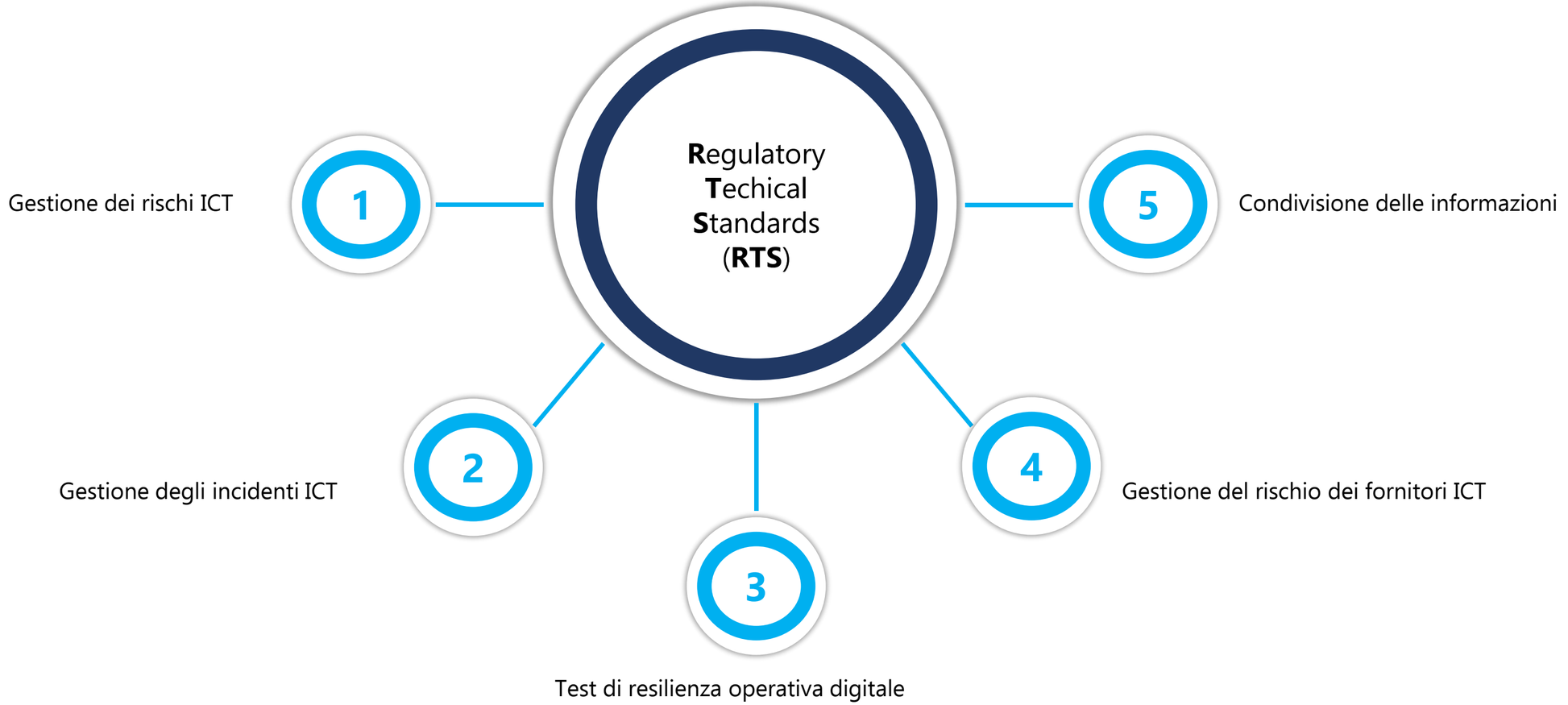
Persegue due obiettivi fondamentali: fornire un approccio completo alla gestione del rischio ICT nel settore dei servizi finanziari e uniformare le normative nazionali già in vigore negli Stati membri dell’UE in materia di rischio ICT.

Si applica a tutte le istituzioni finanziarie dell’UE, incluse: entità finanziarie tradizionali quali banche, società di investimento e istituti di credito, ed entità non tradizionali, come fornitori di asset legati a criptovalute e piattaforme di crowdfunding.

Le autorità di vigilanza europee (ESA) sono le autorità di regolamentazione preposte a sorvegliare la conformità e includono l’autorità banca europea (EBA), l’autorità europea degli strumenti finanziari e dei mercati (ESMA) e l’autorità europea delle assicurazioni e delle pensioni e delle pensioni aziendali e professionali (EIOPA).

Il Consiglio dell’Unione Europea e il Parlamento Europeo (organi legislativi responsabili dell’approvazione delle leggi EU) hanno adottato formalmente il regolamento DORA nel novembre 2022. Le entità finanziarie e i fornitori di servizi ICT di terze parti hanno tempo fino al 17 gennaio 2025 per ottemperare ai requisiti.

I 5 pilastri della conformità DORA



Analisi dei 5 pilastri della conformità DORA

1 GESTIONE DEI RISCHI ICT

Le organizzazioni coinvolte devono sviluppare framework esaustivi per la gestione del rischio ICT. Per raggiungere questo obiettivo, è necessario effettuare una mappatura dei propri sistemi ICT, identificando e classificando le funzioni e gli asset critici, oltre a documentare le interdipendenze tra risorse, sistemi, processi e fornitori. Devono inoltre eseguire valutazioni periodiche del rischio sui sistemi ICT, catalogare e classificare le minacce informatiche e descrivere le misure adottate per mitigare i rischi individuati.

2 GESTIONE DEGLI INCIDENTI ICT

Le aziende sono tenute ad adottare procedure per il monitoraggio, la gestione, la registrazione, la classificazione e la segnalazione degli incidenti ICT. A seconda della gravità dell'evento, potrebbe essere necessario informare sia le autorità di regolamentazione sia i clienti e i partner interessati. Per gli incidenti di natura critica, occorre produrre tre diversi tipi di rapporto: un rapporto iniziale per notificare immediatamente le autorità, un rapporto intermedio che descriva i progressi nella risoluzione dell'incidente e un rapporto finale che analizzi a fondo le cause e le implicazioni dell'evento.

3 TEST DI RESILIENZA OPERATIVA DIGITALE

Le entità sono tenute a testare regolarmente i propri sistemi ICT per valutarne la forza delle protezioni e identificare le vulnerabilità. I test dovrebbero includere un'ampia varietà di strumenti e azioni, che vanno dalla valutazione dei requisiti di base (*vulnerability assessment, network security assessment, physical security reviews, soluzioni di scansione del software e source code review, analisi open source, test basati su scenari, test di compatibilità, test di prestazione o test end-to-end*) fino a test più avanzati TLPT.

4 GESTIONE DEL RISCHIO DEI FORNITORI DI SERVIZI ICT

Le società finanziarie devono gestire attivamente i rischi ICT di terze parti, negoziando contratti che includano strategie di uscita, audit e requisiti per accessibilità, integrità e sicurezza. Non sarà possibile collaborare con fornitori ICT non conformi e le autorità potranno sospendere o risolvere contratti inadeguati. Gli istituti finanziari, inoltre, dovranno mappare le proprie dipendenze ICT di terze parti, evitando concentrazioni eccessive presso singoli fornitori o piccolo gruppo di fornitori. I fornitori critici di servizi ICT saranno soggetti alla supervisione diretta delle autorità europee.

5 CONDIVISIONE DELLE INFORMAZIONI

Le entità finanziarie sono incoraggiate (e in certi casi obbligate) a scambiare dati e intelligence relativi a minacce, tra cui: indicatori di compromissione, tattiche, tecniche e procedure, segnali di allarme per la cybersicurezza e strumenti di configurazione vulnerabilità e incidenti, sia reciprocamente sia con le autorità di vigilanza. La condivisione deve avvenire nel rispetto del GDPR e delle normative sulla protezione delle informazioni.

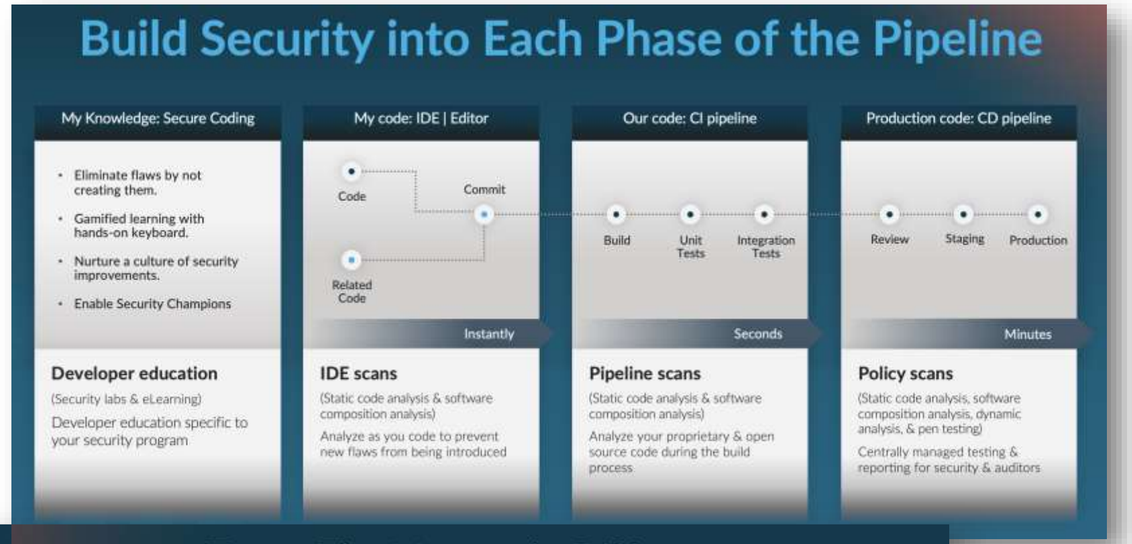
1

Gestione dei rischi ICT

Le organizzazioni coinvolte devono sviluppare framework esaustivi per la gestione del rischio ICT. Per raggiungere questo obiettivo, è necessario effettuare una mappatura dei propri sistemi ICT, identificando e classificando le funzioni e gli asset critici, oltre a documentare le interdipendenze tra risorse, sistemi, processi e fornitori. Devono inoltre eseguire valutazioni periodiche del rischio sui sistemi ICT, catalogare e classificare le minacce informatiche e descrivere le misure adottate per mitigare i rischi individuati.

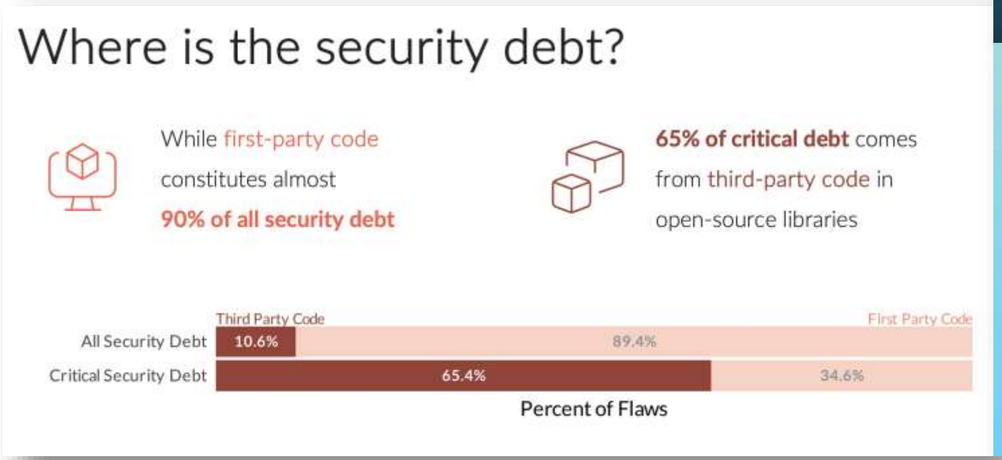
2 Gestione degli incidenti ICT

Le aziende sono tenute ad adottare procedure per il monitoraggio, la gestione, la registrazione, la classificazione e la segnalazione degli incidenti ICT. A seconda della gravità dell'evento, potrebbe essere necessario informare sia le autorità di regolamentazione sia i clienti e i partner interessati. Per gli incidenti di natura critica, occorre produrre tre diversi tipi di rapporto: un rapporto iniziale per notificare immediatamente le autorità, un rapporto intermedio che descriva i progressi nella risoluzione dell'incidente e un rapporto finale che analizzi a fondo le cause e le implicazioni dell'evento.



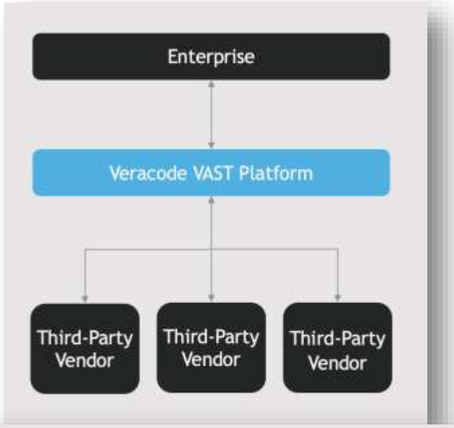
3 Test di resilienza operativa digitale

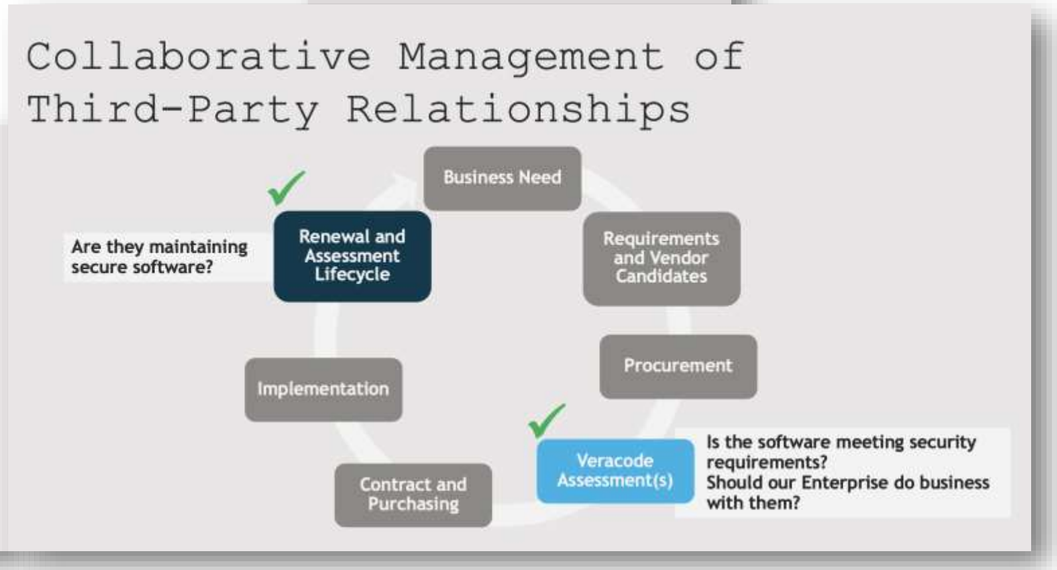
Le entità sono tenute a testare regolarmente i propri sistemi ICT per valutarne la forza delle protezioni e identificare le vulnerabilità. I test dovrebbero includere un'ampia varietà di strumenti e azioni, che vanno dalla valutazione dei requisiti di base (*vulnerability assessment, network security assessment, physical security reviews, soluzioni di scansione del software e source code review, , analisi open source, test basati su scenari, test di compatibilità, test di prestazione o test end-to-end*) fino a test più avanzati TLPT.



4 Gestione del rischio dei fornitori ICT

Le società finanziarie devono gestire attivamente i rischi ICT di terze parti, negoziando contratti che includano strategie di uscita, audit e requisiti per accessibilità, integrità e sicurezza. Non sarà possibile collaborare con fornitori ICT non conformi e le autorità potranno sospendere o risolvere contratti inadeguati. Gli istituti finanziari, inoltre, dovranno mappare le proprie dipendenze ICT di terze parti, evitando concentrazioni eccessive presso singoli fornitori o piccolo gruppo di fornitori. I fornitori critici di servizi ICT saranno soggetti alla supervisione diretta delle autorità europee.

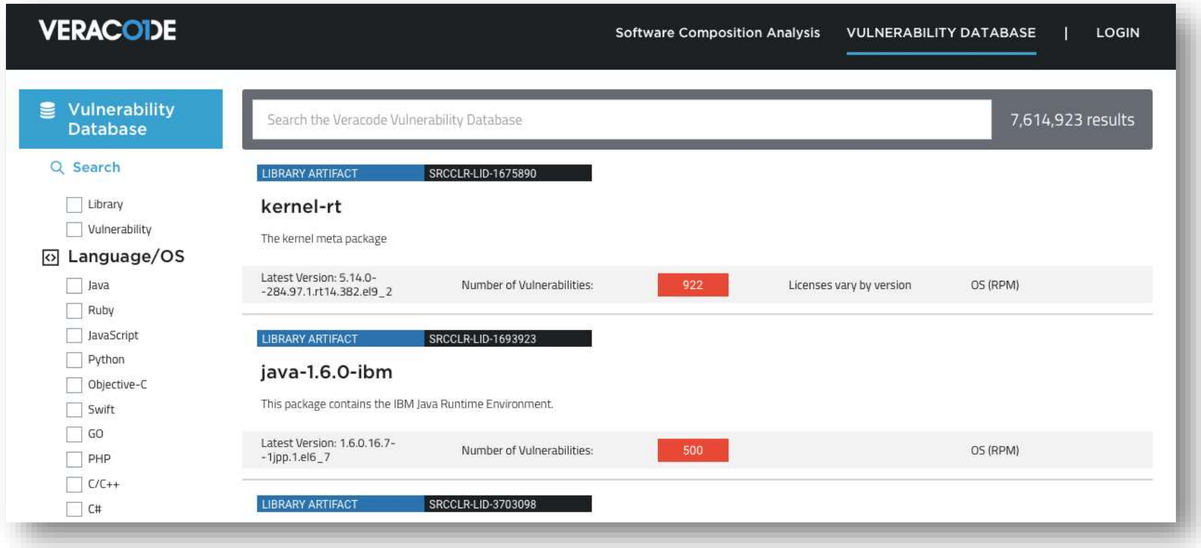




5

Condivisione delle informazioni

Le entità finanziarie sono incoraggiate (e in certi casi obbligate) a scambiare dati e intelligence relativi a minacce, tra cui: indicatori di compromissione, tattiche, tecniche e procedure, segnali di allarme per la cybersicurezza e strumenti di configurazione vulnerabilità e incidenti, sia reciprocamente sia con le autorità di vigilanza. La condivisione deve avvenire nel rispetto del GDPR e delle normative sulla protezione delle informazioni.



GESTIONE DEI RISCHI ICT

1

Le organizzazioni coinvolte devono sviluppare framework esaustivi per la gestione del rischio ICT. Per raggiungere questo obiettivo, è necessario effettuare una mappatura dei propri sistemi ICT, identificando e classificando le funzioni e gli asset critici, oltre a documentare le interdipendenze tra risorse, sistemi, processi e fornitori. Devono inoltre eseguire valutazioni periodiche del rischio sui sistemi ICT, catalogare e classificare le minacce informatiche e descrivere le misure adottate per mitigare i rischi individuati.

Veracode Risk Manager (VRM) offre una visione chiara del rischio, semplificando la gestione del crescente backlog di vulnerabilità di sicurezza provenienti da diversi sistemi. Consente di ridurre significativamente tali rischi, identificando le cause principali di ogni problema di sicurezza e suggerendo azioni mirate per minimizzare i rischi più critici con il minimo sforzo.

GESTIONE DEGLI INCIDENTI ICT

2

Le aziende sono tenute ad adottare procedure per il monitoraggio, la gestione, la registrazione, la classificazione e la segnalazione degli incidenti ICT. A seconda della gravità dell'evento, potrebbe essere necessario informare sia le autorità di regolamentazione sia i clienti e i partner interessati. Per gli incidenti di natura critica, occorre produrre tre diversi tipi di rapporto: un rapporto iniziale per notificare immediatamente le autorità, un rapporto intermedio che descriva i progressi nella risoluzione dell'incidente e un rapporto finale che analizzi a fondo le cause e le implicazioni dell'evento.

Veracode fornisce strumenti avanzati per identificare, evidenziare e risolvere, anche attraverso il supporto dell'intelligenza artificiale (**Veracode FIX**), le vulnerabilità sin dalle prime fasi del ciclo di vita dello sviluppo del software, contribuendo a prevenire incidenti legati a vulnerabilità applicative. Inoltre, consente di generare report dettagliati che facilitano gli audit e offrono una visione chiara delle lacune di sicurezza all'interno dell'organizzazione.

TEST DI RESILIENZA OPERATIVA DIGITALE

3

Le entità sono tenute a testare regolarmente i propri sistemi ICT per valutarne la forza delle protezioni e identificare le vulnerabilità. I test dovrebbero includere un'ampia varietà di strumenti e azioni, che vanno dalla valutazione dei requisiti di base (*vulnerability assessment, network security assessment, physical security reviews, soluzioni di scansione del software e source code review, analisi open source, test basati su scenari, test di compatibilità, test di prestazione o test end-to-end*) fino a test più avanzati TLPT.

Veracode propone una piattaforma integrata per la sicurezza delle applicazioni, progettata per supportare le organizzazioni nell'identificazione e mitigazione delle vulnerabilità software, migliorando al contempo la protezione lungo tutto il ciclo di vita dello sviluppo (SDLC). Questa soluzione unificata comprende strumenti avanzati come l'analisi statica del codice sorgente (**SAST**), la valutazione delle librerie open source e dei componenti di terze parti (**SCA**) e l'analisi dinamica delle applicazioni in esecuzione (**DAST**), garantendo una copertura completa e affidabile per ogni fase del processo di sviluppo.

GESTIONE DEL RISCHIO DEI FORNITORI DI SERVIZI ICT

4

Le società finanziarie devono gestire attivamente i rischi ICT di terze parti, negoziando contratti che includano strategie di uscita, audit e requisiti per accessibilità, integrità e sicurezza. Non sarà possibile collaborare con fornitori ICT non conformi e le autorità potranno sospendere o risolvere contratti inadeguati. Gli istituti finanziari, inoltre, dovranno mappare le proprie dipendenze ICT di terze parti, evitando concentrazioni eccessive presso singoli fornitori o piccolo gruppo di fornitori. I fornitori critici di servizi ICT saranno soggetti alla supervisione diretta delle autorità europee.

Veracode Vendor Application Security Testing (VAST) offre uno strumento di valutazione del rischio di terze parti facile da usare, in grado di fornire rapidamente un voto "pass/fail" per ogni software di terze parti. La soluzione di gestione del rischio di terze parti utilizza test statici per analizzare i binari piuttosto che il codice sorgente, consentendo ai fornitori di sottoporre il proprio software a test senza dover rivelare il codice sorgente o la proprietà intellettuale.

CONDIVISIONE DELLE INFORMAZIONI

5

Le entità finanziarie sono incoraggiate (e in certi casi obbligate) a scambiare dati e intelligence relativi a minacce, tra cui: indicatori di compromissione, tattiche, tecniche e procedure, segnali di allarme per la cybersicurezza e strumenti di configurazione vulnerabilità e incidenti, sia reciprocamente sia con le autorità di vigilanza. La condivisione deve avvenire nel rispetto del GDPR e delle normative sulla protezione delle informazioni.

Veracode (SCA), grazie a una knowledge base costantemente aggiornata sulle minacce nel campo applicativo e al supporto di linee guida per la remediation, offre un contributo concreto nella prevenzione dei rischi. Inoltre, favorisce la condivisione delle informazioni e delle best practice, contribuendo a migliorare l'efficacia dei processi di sicurezza.

Veracode Security Platform

VERACODE

Conclusioni

La complessità della normativa DORA e le numerose attività necessarie, che coinvolgono diversi attori e richiedono evidenze puntuali di accountability, rendono fondamentale l'adozione di una piattaforma integrata di supporto. Soluzioni in grado di tracciare ogni passaggio e fornire report completi, aiutano le organizzazioni a gestire efficacemente tutte le richieste di conformità e a mantenere una solida governance del rischio. Investire in tecnologie che semplifichino la gestione di questi processi, garantendo trasparenza e sicurezza, è oggi la chiave per rimanere competitivi e rispondere con prontezza alle sfide poste da un contesto regolatorio in continua evoluzione.

Q&A