NIS2

Dalla cybersecurity regolata all'ambiente di controllo verificabile

Sintesi esecutiva

NIS2 sposta la cybersicurezza dal reparto tecnico al sistema di governo dell'organizzazione. La direttiva non tratta più la sicurezza delle reti e dei sistemi informativi come una materia separata, confinata a policy IT o controlli periodici. La porta dentro la continuità dei servizi, nella responsabilità degli organi di gestione, nella relazione con i fornitori e nella capacità di ricostruire gli incidenti quando accadono.

Il cambiamento più importante non è soltanto l'ampliamento del perimetro soggettivo. NIS2 chiede alle organizzazioni essenziali e importanti di adottare misure tecniche, operative e organizzative proporzionate al rischio, di governarle a livello apicale, di gestire la supply chain, di notificare gli incidenti significativi e di mantenere un livello di sicurezza adeguato ai servizi erogati. Tutto questo produce una conseguenza pratica: la cybersicurezza diventa un ambiente di controllo che deve poter essere raccontato, verificato e ricostruito.

Dentro questo ambiente di controllo, la domanda di evidenza cresce. Un'organizzazione soggetta a NIS2 deve poter dimostrare che una misura era stata approvata, che un controllo era attivo, che una configurazione era quella dichiarata, che un fornitore era stato valutato, che un incidente è stato documentato in una certa sequenza temporale, che un report non è stato modificato dopo la sua produzione. La conformità sostanziale resta affidata a governance, consulenti, auditor, CISO, funzioni legali e autorità competenti. Ma l'evidenza tecnica diventa il tessuto su cui queste valutazioni si appoggiano.

CertiSigma si colloca qui: non al posto della governance NIS2, ma sotto di essa, come strato crittografico di evidenza. Riceve digest, non contenuti. Attesta l'esistenza e l'integrità temporale di impronte e manifest. Permette di collegare documenti, log, configurazioni, dossier fornitori, report di audit, evidenze di incidente e pacchetti di controllo a una catena verificabile. La formula resta

semplice: prova fuori, contenuto dentro, significato sotto controllo dell'organizzazione.

Il valore non sta nel trasformare CertiSigma in una "*soluzione NIS2*". Sarebbe una riduzione e, in parte, un errore. Il valore sta nel riconoscere che NIS2 rende centrale la capacità di produrre evidenza affidabile. CertiSigma offre un modo leggero, content-blind e verificabile per rafforzare questa capacità nei punti in cui l'organizzazione ha già processi, controlli e responsabilità.

Nota di posizionamento. CertiSigma non certifica la conformità NIS2, non determina il perimetro soggettivo dell'organizzazione, non valuta l'adeguatezza delle misure tecniche, operative e organizzative e non sostituisce CISO, consulenti, auditor, DPO, organi di gestione o autorità competenti. Il servizio fornisce uno strato di attestazione crittografica content-blind su digest e manifest, utilizzabile come supporto evidenziale nei processi di governance, audit, incident response e supply chain security.

1. Perché NIS2 cambia il modo di guardare alla cybersecurity

NIS2 nasce da una constatazione ormai banale solo in apparenza: il digitale è infrastruttura reale. Energia, trasporti, sanità, finanza, acque, servizi digitali, pubblica amministrazione, manifattura critica e filiere di supporto non dipendono più da sistemi informativi accessori. Dipendono da piattaforme, reti, identità digitali, cloud, fornitori gestiti, software, backup, monitoraggio, accessi remoti, dispositivi connessi e catene di subfornitura.

La prima direttiva NIS aveva già introdotto un quadro europeo di sicurezza delle reti e dei sistemi informativi. NIS2 estende e irrigidisce quel quadro. L'obiettivo non è immaginare un mondo senza incidenti. L'obiettivo è ottenere organizzazioni capaci di ridurre il rischio, contenere l'impatto, continuare i servizi, segnalare gli eventi rilevanti e imparare dalla propria esposizione.

Il lessico della direttiva è tecnico, ma la sua logica è organizzativa. Una misura di sicurezza non vale solo perché esiste in un documento. Vale se è approvata, applicata, monitorata, aggiornata, collegata a responsabilità chiare e dimostrabile nel momento in cui serve. In questo senso NIS2 non produce semplicemente un elenco di obblighi. Produce un nuovo standard di narrabilità

del rischio: l'organizzazione deve essere in grado di spiegare come governa ciò da cui dipende.

La differenza si vede soprattutto negli incidenti. Prima dell'incidente, la sicurezza appare come insieme di controlli. Durante l'incidente, diventa capacità di decisione. Dopo l'incidente, diventa catena di evidenza. Che cosa è successo, quando è stato rilevato, chi lo ha classificato, quali sistemi sono stati coinvolti, quali fornitori sono stati attivati, quali misure sono state applicate, quali comunicazioni sono state inviate, quali elementi tecnici supportano la ricostruzione. La sicurezza entra così in una dimensione probatoria.

2. Il soggetto NIS2

La direttiva distingue tra entità essenziali ed entità importanti, ma il dato comune è la responsabilità organizzativa. Il perimetro concreto dipende dagli allegati della direttiva, dalle soglie dimensionali, dalle esclusioni e dal recepimento nazionale. In molti casi il punto decisivo non è solo il settore in astratto, ma la funzione svolta, la rilevanza del servizio, la dipendenza da sistemi digitali e la posizione dell'organizzazione nella catena di valore.

Le entità essenziali e importanti operano in settori ad alta criticità o in altri settori critici. La direttiva include, tra gli altri, energia, trasporti, sanità, infrastrutture digitali, gestione dei servizi ICT, acque, spazio, pubblica amministrazione, servizi postali, gestione rifiuti, manifattura critica, alimentare, chimica e alcuni servizi digitali. Il recepimento nazionale definisce poi procedure, registrazioni, classificazioni, autorità competenti e dettagli applicativi.

Questa architettura produce una conseguenza pratica: un'organizzazione non può limitarsi a chiedere se "*è dentro*" o "*è fuori*" in modo astratto. Deve comprendere quale parte dei propri servizi è rilevante, quali sistemi li sostengono, quali fornitori ne condizionano la continuità, quali dati e funzioni sono coinvolti, quali obblighi derivano dal diritto nazionale applicabile e quale livello di evidenza sarà richiesto in caso di audit, incidente o interlocuzione con l'autorità.

Per questo NIS2 non è soltanto una questione di classificazione. È una questione di postura. Una entità soggetta a obblighi NIS2 deve costruire un ambiente di controllo credibile. Le misure devono esistere, ma devono anche lasciare traccia.

Le decisioni devono essere assunte, ma devono poter essere ricostruite. I fornitori devono essere valutati, ma la valutazione deve essere documentata. La continuità deve essere pianificata, ma test e aggiornamenti devono essere provabili.

3. Governance: quando il rischio cyber arriva al livello apicale

Il cuore politico di NIS2 è la governance. L'articolo 20 richiede che gli organi di gestione delle entità essenziali e importanti approvino le misure di cybersecurity risk management, ne supervisionino l'attuazione e possano essere chiamati a rispondere delle violazioni relative a tali misure. La norma prevede anche formazione per i membri degli organi di gestione e incoraggia formazione regolare per il personale.

Questo passaggio cambia il tono della cybersecurity. Non basta che una funzione tecnica implementi controlli ragionevoli. L'organizzazione deve poter mostrare che la sicurezza è entrata nel circuito decisionale. Budget, rischi accettati, priorità di remediation, dipendenze dai fornitori, risultati dei test, incidenti e piani di miglioramento diventano materia di governo.

Il consiglio di amministrazione o l'organo equivalente non deve trasformarsi in un SOC. Deve però poter approvare e sorvegliare un sistema di misure che sia intelligibile. Qui nasce un bisogno concreto di evidenza sintetica, versionata e verificabile: report al management, revisioni del risk register, piani di trattamento, snapshot dello stato dei controlli, risultati delle verifiche, eccezioni approvate, piani di remediation, attestazioni di formazione.

CertiSigma entra in questo punto come memoria dell'ambiente di controllo. Un board pack, un risk report, una versione della policy di sicurezza, una matrice dei rischi o un pacchetto di evidenza su un programma di remediation possono essere conservati internamente dall'organizzazione e attestati esternamente solo nella loro impronta. Il contenuto resta nel perimetro dell'organizzazione. La prova dell'esistenza e dell'integrità di quella versione viene separata dal contenuto stesso.

Questo non decide se il board abbia deliberato bene, se il rischio fosse accettabile o se la misura fosse proporzionata. Quelle sono valutazioni di governo, audit e diritto. Ma consente di evitare una fragilità frequente: mesi dopo, quando serve

ricostruire lo stato dell'ambiente di controllo, l'organizzazione non dipende solo da file locali, cartelle condivise, versioni rinominate, allegati e-mail o esportazioni tardive.

4. Le misure dell'articolo 21

L'articolo 21 è il baricentro operativo della direttiva. Richiede misure tecniche, operative e organizzative appropriate e proporzionate per gestire i rischi che gravano sulla sicurezza dei sistemi di rete e informativi usati dall'entità per le proprie attività o per l'erogazione dei servizi. La direttiva richiama lo stato dell'arte, gli standard europei e internazionali pertinenti, i costi di implementazione, l'esposizione al rischio, la dimensione dell'entità e la gravità potenziale degli incidenti.

Le misure elencate dalla direttiva coprono policy di analisi del rischio e sicurezza dei sistemi informativi, incident handling, business continuity, backup, disaster recovery, crisis management, supply chain security, sicurezza nell'acquisizione, sviluppo e manutenzione dei sistemi, gestione e divulgazione delle vulnerabilità, procedure per valutare l'efficacia delle misure, cyber hygiene, formazione, crittografia, sicurezza delle risorse umane, access control, asset management, autenticazione multifattore o continua e comunicazioni sicure, ove appropriate.

Questa lista non va letta come una checklist piatta. Ogni voce genera artefatti. La risk analysis produce matrici, classificazioni, decisioni e revisioni. L'incident handling produce playbook, timeline, ticket, log, report, comunicazioni e lesson learned. La continuità produce piani, test, restore report e registri di crisi. La supply chain produce valutazioni, questionari, contratti, dichiarazioni, report e registri fornitori. La gestione delle vulnerabilità produce scansioni, priorità, remediation record e accettazioni di rischio. L'asset management produce inventari e snapshot. La formazione produce evidenze di partecipazione e aggiornamenti.

Il punto è semplice: un controllo non è solo una misura. È anche la sua traccia. Senza traccia, il controllo resta più difficile da dimostrare, più fragile in audit e meno utile dopo un incidente. Con una traccia debole, l'organizzazione sa di aver lavorato ma fatica a provarlo. Con una traccia verificabile, il lavoro diventa materiale di governo.

CertiSigma non costruisce il controllo. Rafforza la traccia del controllo. Un export di asset inventory, un report di vulnerability remediation, una policy approvata, un verbale di test di continuità, un pacchetto di evidenza fornitori o una timeline di incidente possono essere ridotti a digest o organizzati in manifest. L'attestazione crittografica non dice che il controllo sia sufficiente. Dice che quello specifico artefatto esisteva in quella forma in quel momento e che una modifica successiva può essere rilevata.

5. Incident reporting

NIS2 rende l'incidente un evento tecnico, organizzativo e comunicativo. L'articolo 23 disciplina gli obblighi di notifica degli incidenti significativi. La direttiva prevede un early warning entro 24 ore dalla conoscenza dell'incidente significativo, una incident notification entro 72 ore, eventuali report intermedi su richiesta e un final report non oltre un mese dalla trasmissione dell'incident notification, con descrizione dettagliata, severità, impatto, probabile causa, misure di mitigazione e, se rilevante, impatto transfrontaliero.

Questo calendario spinge l'organizzazione a una disciplina probatoria molto concreta. Nelle prime ore, l'informazione è incompleta, i log sono frammentari, i sistemi possono essere instabili, i fornitori possono essere coinvolti, le funzioni legale, comunicazione, business continuity e management devono allinearsi. Ogni ricostruzione successiva dipenderà dalla qualità degli artefatti raccolti durante la pressione dell'evento.

In questa fase, l'evidenza tradizionale è fragile. Screenshot, export SIEM, ticket, timeline, note di triage, elenchi di indicatori, report forensi, comunicazioni ai fornitori e bozze di notifica possono cambiare rapidamente. Alcuni file saranno corretti, integrati o sostituiti. Questo è normale. Il problema è distinguere le versioni, dimostrare quando sono state prodotte e collegarle al percorso decisionale.

Uno strato di attestazione content-blind consente di costruire una catena minima di integrità senza trasferire il contenuto sensibile dell'incidente a un ulteriore osservatore esterno. L'organizzazione conserva log, report, immagini, esportazioni, timeline e comunicazioni nel proprio ambiente. Verso CertiSigma

può essere trasmesso solo il digest del file o il digest di un manifest che elenca gli artefatti del pacchetto di incidente. La prova esce; il contenuto resta dentro.

Questa logica è particolarmente importante quando l'incidente riguarda dati personali, vulnerabilità non divulgate, architetture interne, relazioni con fornitori, indirizzi IP, credenziali, indicatori non pubblici o elementi di sicurezza nazionale. La catena di evidenza deve rafforzare la posizione dell'organizzazione, non creare una nuova superficie di esposizione.

6. Supply chain security

NIS2 tratta la supply chain come parte della cybersecurity, non come appendice contrattuale. L'articolo 21 richiama espressamente la sicurezza della catena di fornitura e gli aspetti di sicurezza nelle relazioni tra l'entità e i suoi fornitori diretti o service provider. La direttiva chiede inoltre di tenere conto delle vulnerabilità specifiche dei fornitori e della qualità complessiva dei prodotti e delle pratiche di cybersecurity, incluse le procedure di sviluppo sicuro.

Per una entità soggetta a NIS2, questo significa che il fornitore non è più solo oggetto di procurement. È un elemento del rischio operativo. Un cloud provider, un MSP, un manutentore OT, un software vendor, un provider logistico, un gestore di edificio, un fornitore sanitario, un document management provider o un partner digitale possono incidere su continuità, riservatezza, integrità e disponibilità dei servizi.

La supply chain security produce grandi quantità di evidenza: questionari, assessment, contratti, SLA, dichiarazioni, certificazioni, report di audit, piani di remediation, registri di subfornitura, comunicazioni di incidente, eccezioni, approvazioni e riesami periodici. Il valore di questa evidenza non dipende solo dalla sua presenza. Dipende dalla capacità di collegarla al fornitore corretto, alla versione corretta del servizio, alla data corretta e alla decisione interna che ne è derivata.

Qui CertiSigma può funzionare come ponte tra la due diligence commerciale e la memoria tecnica. Il soggetto NIS2 può ricevere un dossier fornitore, conservarlo nei propri sistemi, calcolarne un manifest e attestare l'impronta del pacchetto. In questo modo, mesi dopo, è possibile dimostrare quale evidenza era disponibile al

momento della qualificazione o del rinnovo, quale versione era stata valutata e se il pacchetto è cambiato.

Il documento "*NIS2 per l'evidenza dei fornitori*" guarda lo stesso problema dal lato del vendor indiretto: come preparare un pacchetto leggibile per un cliente regolato. Questo documento guarda dal lato dell'entità NIS2: come assorbire, organizzare e rendere verificabile l'evidenza ricevuta o prodotta lungo la supply chain.

7. I sistemi di controllo producono prove, ma non sempre robuste

GRC, SIEM, ticketing, document management, cloud drive e audit tool sono necessari, ma non risolvono da soli il problema dell'evidenza. Questi sistemi producono registrazioni preziose: log, ticket, workflow, approvazioni, report, esportazioni, allegati, snapshot. Tuttavia, spesso custodiscono la prova nello stesso ecosistema operativo che deve essere valutato, compromesso, migrato o contestato.

Un log è utile, ma può essere incompleto, ruotato, alterato o conservato in un ambiente oggetto dell'incidente. Un ticket è utile, ma la sua cronologia dipende dalla piattaforma. Un file in un cloud drive è comodo, ma può essere rinominato, sostituito, duplicato o esportato senza una catena di integrità forte. Un report di audit è importante, ma la domanda può diventare: quale versione era disponibile in quella data? Un export SIEM può essere determinante, ma occorre dimostrare quando è stato prodotto e che cosa conteneva.

NIS2 non impone necessariamente una tecnologia specifica per risolvere questa fragilità. La questione è architetturale. L'ambiente di controllo ha bisogno di una memoria separata, leggera e verificabile dell'esistenza e dell'integrità dei suoi artefatti più importanti. Non serve duplicare tutti i contenuti presso un terzo. Serve poter provare che un contenuto conservato internamente corrisponde a una impronta attestata esternamente.

Questa separazione è la ragione per cui un evidence layer crittografico ha senso. Non sostituisce i sistemi che producono il lavoro. Li accompagna. Il GRC continua a gestire controlli e workflow. Il SIEM continua a raccogliere eventi. Il DMS continua a conservare documenti. Il ticketing continua a gestire remediation e

incidenti. CertiSigma si limita a produrre una prova indipendente sull'impronta di artefatti selezionati.

8. CertiSigma nel suo posto naturale

Il posto naturale di CertiSigma è tra l'ambiente interno di controllo e il bisogno esterno di verificabilità. L'organizzazione conserva contenuto, significato, responsabilità, classificazione, contesto e decisione. CertiSigma riceve un digest crittografico o una radice di manifest e produce una attestazione verificabile. La prova viene esternalizzata; il contenuto rimane nel perimetro organizzativo.

Questa posizione è piccola, ma forte. Piccola perché CertiSigma non decide il perimetro NIS2, non interpreta il recepimento nazionale, non valuta l'adeguatezza delle misure, non sostituisce audit, consulenza legale, SOC, CISO, DPO o organi di gestione. Forte perché rafforza una funzione trasversale: la capacità di dimostrare l'esistenza e l'integrità temporale degli artefatti che il sistema di controllo produce.

L'infrastruttura CertiSigma lavora su impronte. Il file, il documento, il log, il report, il dataset o il manifest restano nell'ambiente dell'organizzazione. Il servizio può attestare digest SHA-256 e organizzare l'evidenza su più livelli: una firma immediata T0, una validazione temporale qualificata T1 su radice Merkle aggregata tramite TSA esterna, e un ancoraggio T2 tramite OpenTimestamps su Bitcoin. Il modello è pensato per evitare che la produzione di prova richieda il trasferimento del contenuto sostantivo.

In un contesto NIS2, questa caratteristica conta. Le evidenze di controllo possono includere informazioni sensibili: architetture, vulnerabilità, fornitori critici, asset, configurazioni, log di incidente, dati personali, procedure interne, piani di continuità. Un'organizzazione può avere bisogno di dimostrare senza divulgare più del necessario. CertiSigma risponde a questa esigenza con un principio semplice: content-blind by architecture.

Il suo ruolo è quindi quello di uno strato di prova, non di uno strato di giudizio. Il giudizio rimane all'organizzazione, ai suoi consulenti, agli auditor e alle autorità competenti. La prova crittografica rende più solido il materiale su cui quel giudizio si esercita.

9. Dove CertiSigma può entrare nell'ambiente di controllo NIS2

L'integrazione più credibile è selettiva. Non ogni file merita attestazione. Non ogni evento deve essere sigillato. Il valore emerge quando l'organizzazione individua gli artefatti che hanno peso probatorio, decisionale o operativo nel proprio sistema di controllo.

Governance e reporting al management

Report periodici sui rischi cyber, versioni approvate di policy, esiti di review, piani di trattamento, stati di remediation, verbali rilevanti, materiali di formazione per organi di gestione e pacchetti di evidenza per audit possono essere attestati come manifest. L'obiettivo è conservare una memoria verificabile dello stato dell'ambiente di controllo nel tempo.

Risk management e asset management

Inventari di asset critici, snapshot di classificazioni, registri delle eccezioni, versioni di risk assessment, mappature di sistemi e servizi, baseline di configurazione e registri di accesso possono essere collegati a impronte attestate. La prova non sostituisce l'inventario; ne rafforza l'integrità storica.

Incident handling

Durante un incidente, timeline, export di log, indicatori di compromissione, report forensi, immagini o hash di artefatti, comunicazioni interne, notifiche preparate, decisioni di escalation e misure di mitigazione possono essere organizzati in pacchetti progressivi. L'attestazione consente di distinguere le versioni e di dimostrare quando ciascun pacchetto esisteva.

Business continuity e crisis management

Piani di continuità, esiti di test, report di restore, prove di disaster recovery, lezioni apprese da esercitazioni, aggiornamenti dei contatti di crisi e decisioni di miglioramento possono diventare evidenza verificabile. La continuità non è solo dichiarazione di capacità; è storia documentata di prove e aggiornamenti.

Supply chain security

Dossier fornitori, assessment, certificazioni ricevute, report di audit, registri di subfornitura, dichiarazioni, contratti e piani di remediation possono essere attestati al momento della ricezione, della review o del rinnovo. Questo permette di ricostruire lo stato della due diligence in una data precisa.

Vulnerability handling e secure maintenance

Report di scansione, registri di remediation, accettazioni di rischio, changelog, release note, SBOM, report di patching, configurazioni pre e post intervento possono essere organizzati in manifest attestabili. Il punto non è attestare ogni vulnerabilità. È preservare l'evidenza delle decisioni e delle azioni rilevanti.

AI, automazione e agenti software

Quando l'organizzazione introduce sistemi AI o automazioni in processi di sicurezza, supporto, analisi, customer service, document management o incident response, l'ambiente di controllo può includere manifest di configurazione: versione del modello, policy attiva, strumenti abilitati, knowledge base, input e output rilevanti, approvazioni umane e dataset di riferimento. CertiSigma può attestare i manifest, lasciando i contenuti sensibili sotto controllo interno.

Questa prospettiva non intende ricondurre i sistemi AI a un obbligo specifico NIS2 in quanto tali. Evidenzia piuttosto che, quando AI e automazioni partecipano a processi rilevanti per la sicurezza, gli artefatti che ne documentano configurazione, input, output, versioni e approvazioni possono diventare parte dell'ambiente di controllo.

10. Census: dall'artefatto locale al manifest attestabile

CertiSigma diventa più utile quando l'organizzazione costruisce manifest locali prima di attestare. Il singolo hash di un file è semplice e potente, ma l'ambiente di controllo NIS2 funziona spesso per pacchetti: dossier di incidente, cartelle fornitori, release di configurazione, report trimestrali, baseline di asset, raccolte di evidenze di business continuity o pacchetti di audit.

Census si colloca nel perimetro locale dell'organizzazione come strumento di inventario, hashing, manifestazione e verifica di directory o insiemi di artefatti. Opera senza chiedere di trasferire i contenuti fuori dall'organizzazione: scansiona directory, calcola impronte SHA-256, costruisce manifest, permette controlli di integrità e prepara il materiale che può essere attestato verso CertiSigma. Il contenuto resta locale; il digest del manifest diventa il punto di contatto con lo strato esterno di prova.

Questa architettura rende concreta la formula che attraversa il documento: prova fuori, contenuto dentro, significato sotto controllo dell'organizzazione. Il controllo produce artefatti, gli artefatti entrano in un manifest locale, il manifest viene verificato o attestato e l'organizzazione conserva la possibilità di esibire il contenuto solo quando serve e a chi deve vederlo.

Dal documento isolato al pacchetto di controllo

Il singolo file attestato è utile, ma un ambiente NIS2 raramente si difende con un file isolato. Un incidente, un test di continuità, una review dei fornitori o una campagna di remediation producono insiemi di evidenze. Il valore sta nel collegare quei file tra loro: quali elementi componevano il pacchetto, quali erano inclusi, quali esclusi, quale versione era valida, quale directory è stata fotografata e quale baseline era attiva.

Census crea questo livello di collegamento attraverso il manifest. Il manifest non è una semplice lista di nomi file: associa ogni artefatto alla sua impronta, conserva il riferimento operativo necessario per ritrovarlo e permette di verificare se il contenuto disponibile oggi corrisponde ancora alla baseline registrata. Per un soggetto NIS2, questo significa poter dire non solo "questi sono i documenti", ma "questo era il pacchetto, in questa composizione, con queste impronte".

Baseline, integrità e cambiamento

NIS2 non chiede ambienti immobili. Chiede ambienti governati. Policy, configurazioni, asset, fornitori e sistemi cambiano continuamente; il problema è distinguere tra cambiamento autorizzato, cambiamento non documentato, drift operativo e alterazione potenzialmente rilevante.

Census consente di censire una baseline, confrontare versioni successive e rendere visibili aggiunte, rimozioni o modifiche. Un controllo di integrità può essere eseguito localmente, senza chiamare l'API e senza esporre contenuti. Se un report di vulnerabilità viene rigenerato, se una procedura viene aggiornata, se un export SIEM viene ricreato o se un contratto fornitore cambia, il manifest rende evidente che non si tratta più dello stesso oggetto digitale. Non dice se il cambiamento sia buono o cattivo; impedisce però di trattarlo come invisibile.

Incident response e ricostruzione forense

Durante un incidente, l'organizzazione produce evidenza in condizioni imperfette: informazioni incomplete, versioni che cambiano, team paralleli e sistemi che possono essere parte dell'ambiente compromesso. Census può funzionare come strumento di ordine locale: raccoglie impronte, costruisce manifest, consente confronti e prepara pacchetti verificabili.

La funzione di confronto è particolarmente rilevante per scenari di esfiltrazione o sospetta diffusione di file. Un set di file sospetti può essere confrontato con un manifest o con il registro delle impronte senza spostare l'intero archivio. Se emerge una corrispondenza, l'organizzazione ottiene un punto di contatto verificabile tra un artefatto osservato e una baseline precedente. Questo non sostituisce l'analisi forense, ma le fornisce un riferimento più solido.

Census prevede inoltre funzioni orientate alla timeline forense e alla produzione di report o evidence bundle. In una logica NIS2, ciò consente di collegare gli artefatti tecnici alla sequenza dell'incidente: quando è stato osservato un file, quando è stata prodotta una timeline, quali evidenze componevano il pacchetto, quale manifest le legava e quale attestazione esterna ne rafforzava l'integrità temporale.

Supply chain, SBOM e provenienza software

La supply chain NIS2 non riguarda soltanto contratti e questionari. Nei contesti software, cloud, OT e managed services riguarda anche componenti, dipendenze, release, SBOM, pipeline, artefatti di build e provenienza. Il soggetto NIS2 deve poter ricevere, conservare e, se necessario, verificare questi elementi.

Census può operare come strumento di inventario e attestazione di artefatti software. La documentazione Census include funzioni per SBOM in formati SPDX e CycloneDX, generazione o verifica di provenance SLSA, integrazione con ambienti CI/CD, attestazione automatica collegata a commit e produzione di output leggibili da sistemi di sicurezza. Questo non trasforma automaticamente una supply chain in una supply chain sicura, ma rende più facile costruire una memoria crittografica delle versioni, dei componenti e dei pacchetti consegnati.

Dossier fornitori e confidential matching

Il soggetto NIS2 riceve dossier, report, dichiarazioni, certificazioni, export, allegati e pacchetti documentali. Il problema non è soltanto archiviarli: è sapere quale versione è stata ricevuta, quando, da chi, per quale perimetro di servizio e con quale relazione rispetto alla valutazione del rischio.

Census può censire localmente i dossier ricevuti e trasformarli in manifest; CertiSigma può attestare il manifest o gli hash degli elementi rilevanti. Una due diligence fornitore non resta così una cartella statica, ma diventa una baseline verificabile. Se il fornitore aggiorna il pacchetto, il cambiamento diventa leggibile; se un audit chiede quale evidenza fosse disponibile in una certa data, l'organizzazione può ricostruire la composizione del dossier.

La logica può estendersi anche al confidential matching. Derived lists e capacità HMAC consentono di costruire superfici di confronto controllate: un soggetto può verificare se determinati artefatti o indicatori toccano un inventario senza consegnare l'inventario stesso. In contesti di leak detection, antifrode, indicatori cyber, componenti software o seriali, questa capacità è coerente con la tensione NIS2 tra cooperazione e riservatezza, purché sia governata con scope, revoca, logging, rate limit e valutazione del rischio sugli input.

Controlli continui, watch mode e integrazione con SOC/SIEM

Un ambiente NIS2 non vive soltanto di verifiche periodiche. Alcuni controlli hanno bisogno di continuità: directory critiche, pacchetti di evidenza in costruzione, cartelle forensi, artefatti di build, registri esportati, baseline di configurazione. Census può essere utilizzato anche in modalità di osservazione del filesystem, con eventi di cambiamento, soglie di alert e notifiche collegate al ciclo T1/T2.

Questo non sostituisce EDR, XDR, SIEM o strumenti di monitoraggio. La funzione è diversa: aggiungere una spina dorsale di integrità e attestazione agli artefatti che il SOC o il team di sicurezza considera rilevanti. Se un file entra, cambia o scompare da una directory monitorata, l'evento può alimentare un flusso locale, essere registrato, correlato, trasformato in output JSONL, CEF o ECS, o entrare in una timeline forense.

AI, dataset e automazioni dentro l'ambiente NIS2

NIS2 non è una norma sull'intelligenza artificiale, ma molte organizzazioni soggette a NIS2 useranno AI e automazioni nei propri processi: assistenti interni, agenti per il SOC, sistemi di classificazione, pipeline di analisi, strumenti di remediation, generatori di report, knowledge base tecniche. Quando questi sistemi partecipano a processi rilevanti per la sicurezza, gli artefatti che ne documentano configurazione, input, output e versioni possono diventare parte dell'ambiente di controllo.

Census può aiutare a trattare questi oggetti come inventario verificabile: un dataset usato per addestrare, valutare o alimentare un agente può essere censito localmente; una knowledge base può avere una baseline; un set di policy o prompt può essere collegato a un manifest; un report generato da un agente può essere attestato come artefatto, senza pretendere che l'attestazione dica se il report sia corretto.

Il valore complessivo: dalla cartella al sistema di memoria

Un'organizzazione regolata possiede già molti strumenti: document management, ticketing, GRC, SIEM, EDR, vulnerability scanner, backup, repository di codice, portali fornitori. Il problema è che questi strumenti producono evidenza in luoghi diversi e con livelli diversi di robustezza. Census non li sostituisce; li attraversa come inventario crittografico locale.

Per questo si colloca bene nel racconto NIS2. CertiSigma fornisce lo strato di attestazione content-blind; Census rende praticabile il passaggio intermedio: trasformare artefatti dispersi in manifest, baseline, confronti, report e pacchetti verificabili. Il risultato non è una promessa di conformità automatica, ma una memoria tecnica più ordinata, meno dipendente dalla fiducia nel singolo sistema

e più facile da ricostruire quando servono audit, incident response, confronto con fornitori, verifica di integrità o produzione di evidenza verso l'esterno.

11. Il valore della prova content-blind

La prova content-blind risponde a una tensione tipica dei contesti regolati: dimostrare senza esporre. Un'organizzazione soggetta a NIS2 può dover dimostrare molte cose a molti interlocutori diversi: management, auditor, autorità, assicuratori, clienti, partner, fornitori, investigatori, periti. Ogni interlocutore può avere bisogno di vedere una parte diversa della storia.

Centralizzare tutto presso un fornitore di prova sarebbe spesso sproporzionato. Le evidenze possono contenere dati personali, segreti commerciali, vulnerabilità, configurazioni, log sensibili, informazioni su fornitori critici o contenuti coperti da riservatezza. D'altra parte, conservare tutto solo internamente può indebolire la capacità di dimostrare integrità e anteriorità.

Il modello content-blind separa i piani. Il piano del contenuto resta interno. Il piano della prova viene esternalizzato attraverso digest, manifest, timestamp e ancoraggi. Il piano del significato resta nelle mani dell'organizzazione: solo l'organizzazione sa se quel digest corrisponde a un report di incidente, a un file di configurazione, a un dossier fornitori o a un pacchetto di audit.

Questa separazione ha un valore strategico. Permette di produrre evidenza senza trasformare l'evidence provider in un nuovo centro di raccolta di informazioni sensibili. Riduce l'osservabilità del contenuto e rende più semplice inserire la prova in ambienti dove minimizzazione, riservatezza e controllo del dato sono requisiti essenziali.

12. Evidenza non significa automaticamente verità

La forza di uno strato di evidenza dipende anche dalla precisione con cui viene collocato. CertiSigma può attestare l'esistenza e l'integrità temporale di un digest o di un manifest. Questo è molto. Non serve trasformarlo in altro.

L'attestazione crittografica rafforza la prova dell'esistenza, dell'integrità e della collocazione temporale di un artefatto; non prova, da sola, che l'artefatto sia corretto, completo, sufficiente, conforme o adeguato rispetto agli obblighi NIS2.

Se un report di backup viene attestato, l'attestazione rende verificabile che quel report esisteva in una certa forma in un certo momento. La riuscita effettiva del restore dipende dal contenuto del report, dai test eseguiti e dalla valutazione tecnica. Se un dossier fornitore viene attestato, la prova conserva integrità e temporalità del pacchetto. La qualità della due diligence dipende dalla metodologia usata dall'organizzazione. Se una timeline di incidente viene attestata, la prova preserva quella versione della timeline. La correttezza forense della ricostruzione resta oggetto di analisi.

Questa distinzione non è difensiva. È il motivo per cui CertiSigma può stare bene dentro NIS2. Un'organizzazione regolata non ha bisogno di un fornitore che dichiari conformità al posto suo. Ha bisogno di componenti che svolgano funzioni chiare, verificabili e componibili. CertiSigma svolge una funzione delimitata: rafforza la memoria crittografica dell'ambiente di controllo.

La credibilità nasce proprio da questo. Governance, controlli, consulenza, audit, valutazioni legali e interlocuzione con l'autorità restano nei luoghi corretti. L'evidence layer produce una base più solida per quei luoghi.

13. Il rapporto con standard, autorità e recepimenti nazionali

NIS2 resta una direttiva europea che vive attraverso recepimenti nazionali e indicazioni delle autorità competenti. Questo significa che un'organizzazione deve sempre guardare al proprio ordinamento, al proprio settore, alla propria autorità di riferimento e agli eventuali atti tecnici applicabili. La direttiva stabilisce il quadro; il diritto nazionale e gli atti di esecuzione definiscono una parte rilevante dell'operatività.

Ogni riferimento operativo a termini, autorità competenti, registrazioni, classificazioni soggettive, misure applicabili e procedure di notifica deve quindi essere verificato nel diritto nazionale di recepimento e negli atti dell'autorità competente per il settore e la giurisdizione interessati.

Il Regolamento di esecuzione (UE) 2024/2690 ha introdotto requisiti tecnici e metodologici specifici per alcune categorie di soggetti digitali, tra cui DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers,

managed security service providers, online marketplaces, online search engines, social networking services platforms e trust service providers. ENISA ha pubblicato nel giugno 2025 una guida tecnica di implementazione collegata a tale regolamento, con esempi di evidenza e mapping dei requisiti. Tale regolamento non esaurisce l'intero universo NIS2, ma fornisce requisiti tecnici e metodologici specifici per le categorie di soggetti digitali da esso espressamente considerate.

Questi sviluppi confermano la direzione generale: il controllo cyber viene tradotto in requisiti, misure, procedure e prove. Anche quando CertiSigma non è menzionato da una norma, il suo spazio nasce dal bisogno più generale di conservare evidenze tecniche integre e verificabili. La tecnologia entra come componente dell'ambiente di controllo, non come scorciatoia rispetto al quadro regolatorio.

Per le organizzazioni italiane, il recepimento è avvenuto con il Decreto Legislativo 4 settembre 2024, n. 138, pubblicato nella Gazzetta Ufficiale del 1° ottobre 2024. Come in ogni recepimento, gli aspetti procedurali, la classificazione, i rapporti con l'autorità nazionale e i termini applicativi devono essere letti sul testo nazionale e sugli atti delle autorità competenti. Il livello europeo fornisce il telaio; l'implementazione concreta passa dal diritto nazionale.

14. Una architettura narrativa per spiegare CertiSigma dentro NIS2

Il modo più convincente per raccontare CertiSigma in un contesto NIS2 non è partire dal prodotto. È partire dal bisogno. NIS2 chiede governance, risk management, incident reporting e supply chain security. Tutti questi elementi generano evidenze. Le evidenze devono essere integre, ricostruibili, proporzionate e, quando serve, verificabili da terzi. Alcune evidenze sono troppo sensibili per essere trasferite fuori dall'organizzazione. Da qui nasce lo spazio di una prova content-blind.

Il racconto diventa lineare: la direttiva aumenta il bisogno di controllo; il controllo aumenta il bisogno di evidenza; l'evidenza aumenta il bisogno di integrità; l'integrità, se costruita male, può aumentare l'esposizione; CertiSigma separa prova e contenuto, permettendo di attestare impronte e manifest senza spostare il materiale sostantivo.

Questa narrazione evita due errori opposti. Il primo è presentare CertiSigma come soluzione totale alla NIS2. Il secondo è ridurlo a un disclaimer tecnico. CertiSigma è più interessante se collocato nel mezzo: una primitiva infrastrutturale per rendere più solida la memoria dell'ambiente di controllo.

In questa posizione, il servizio parla a CISO, risk manager, responsabili compliance, legal, auditor interni, responsabili supply chain, responsabili IT e management. Non dice loro come fare il proprio mestiere. Offre un modo per rendere più verificabile il materiale che quel mestiere produce.

15. Dalla conformità dichiarata alla memoria verificabile

NIS2 non può essere ridotta a modulistica, né a tecnologia. È un cambiamento di responsabilità. Chiede alle organizzazioni di governare la cybersicurezza come rischio operativo, di coinvolgere il management, di proteggere la supply chain, di prepararsi agli incidenti e di dimostrare che le misure adottate sono appropriate e proporzionate.

Il punto di incontro tra NIS2 e CertiSigma non è la promessa di conformità. È la memoria verificabile. Ogni ambiente di controllo produce una storia: decisioni, policy, evidenze, report, eccezioni, fornitori valutati, incidenti gestiti, vulnerabilità corrette, esercitazioni, backup testati, configurazioni congelate, dossier aggiornati. Questa storia diventa più forte se i suoi artefatti critici possono essere collegati a impronte temporali verificabili.

CertiSigma offre a questa storia uno strato di prova esterno e content-blind. Non porta fuori il contenuto. Non pretende di conoscere il significato degli artefatti. Non sostituisce il giudizio qualificato. Ma permette all'organizzazione di dire, quando serve: questo pacchetto esisteva, questa era la sua forma, questa era la sua impronta, questa è la catena che lo collega a una prova indipendentemente verificabile.

Nel mondo NIS2, questa capacità può diventare parte naturale della maturità operativa. Non perché risolva tutto. Perché rafforza il punto su cui tutto, alla fine, si appoggia: la capacità di dimostrare.

Riferimenti essenziali

- Direttiva (UE) 2022/2555, NIS2 Directive, EUR-Lex: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng
- Regolamento di esecuzione (UE) 2024/2690, EUR-Lex: https://eur-lex.europa.eu/eli/reg_impl/2024/2690/oj/eng
- ENISA, NIS2 Technical Implementation Guidance, 26 giugno 2025: https://www.enisa.europa.eu/publications/nis2-technical-implementation-guidance
- Recepimento italiano: Decreto Legislativo 4 settembre 2024, n. 138, Gazzetta Ufficiale: https://www.gazzettaufficiale.it/eli/id/2024/10/01/24G00155/SG
- CertiSigma Census — CLI Documentation: https://developers.certisigma.ch/census

https://certisigma.ch/legal/imprint