SOPHOS

La Direttiva NIS 2

La prima direttiva UE sulla sicurezza delle reti e dell'informazione (NIS), entrata in vigore nel 2016, è stata la prima legge UE sulla cybersecurity. Tuttavia, per ovviare alle limitazioni identificate nel quadro attuale e per rispondere alla crescita costante delle minacce informatiche all'interno dell'UE nell'era post-digitalizzazione e post-Covid-19, la Commissione europea ha sostituito la Direttiva NIS con la Direttiva NIS 2, che introduce misure di vigilanza più rigide per le autorità nazionali e requisiti di implementazione più severi. Inoltre, si prefigge di armonizzare i regimi sanzionatori negli Stati membri. La Direttiva NIS 2 è entrata in vigore il 16 gennaio 2023 e gli Stati membri hanno 21 mesi, ovvero fino al 17 ottobre 2024, per attuarla nella legislazione nazionale.

Lo scopo della Direttiva NIS 2 è incrementare i requisiti di sicurezza nell'UE per mezzo dei seguenti provvedimenti: estensione dell'ambito di applicazione a più settori e soggetti; considerazione di misure come criteri di sicurezza per l'analisi del rischio e la sicurezza dei sistemi informativi, gestione degli incidenti e protezione della catena di approvvigionamento; semplificazione degli obblighi di segnalazione, e altro. In caso di mancata conformità, la NIS 2 richiede che gli Stati membri infliggano penalità molto severe: 10 milioni di € o il 2% del fatturato annuo globale (a seconda di quale sia più elevato) per i soggetti essenziali, e 7 milioni di € o l'1,4% del fatturato annuo globale (a seconda di quale sia più elevato) per i soggetti importanti. La NIS 2 impone agli organi di gestione l'obbligo diretto di implementare e supervisionare la conformità della loro organizzazione con la legge. Una mancanza di conformità potrebbe potenzialmente portare all'imposizione di un divieto provvisorio di svolgere funzioni dirigenziali a livello di alta dirigenza del soggetto, anche per i dirigenti superiori.

Questo documento descrive come le soluzioni Sophos offrono strumenti efficaci per assistere le organizzazioni nell'ottemperare al Capo IV della direttiva NIS 2 (Misure di gestione del rischio di cibersicurezza e obblighi di segnalazione) e in ultima analisi aiutarle a soddisfare i requisiti della direttiva NIS 2.

Direttiva NIS 2 - Capo IV, Misure di gestione del rischio di cibersicurezza e obblighi di segnalazione

REQUISITI DELLA DIRETTIVA NIS 2	SOLUZIONE SOPHOS	PERCHÉ È UTILE
Capo IV, Articolo 20, Governance		
2. Gli Stati membri provvedono affinché i membri dell'organo di gestione dei soggetti essenziali e importanti siano tenuti a seguire una formazione e incoraggiano i soggetti essenziali e importanti a offrire periodicamente una formazione analoga ai loro dipendenti, per far sì che questi acquisiscano conoscenze e competenze sufficienti al fine di individuare i rischi e valutare le pratiche di gestione dei rischi di cibersicurezza e il loro impatto sui servizi offerti dal soggetto.	Sophos Phish Threat	Offre simulazioni di attacchi informatici di phishing e corsi di formazione e sensibilizzazione per gli utenti finali delle organizzazioni. I corsi trattano un'ampia scelta di argomenti, da lezioni introduttive su phishing e cybersecurity, fino a informazioni importanti sulla prevenzione della perdita dei dati, sulla protezione con password e molto di più.
	Formazione e certificazioni Sophos	I corsi di formazione e le certificazioni aiutano Partner e Clienti a ottenere tutti i vantaggi delle implementazioni di sicurezza Sophos; offrono inoltre accesso a personale esperto, dotato di competenze e conoscenze aggiornate in materia di best practice di sicurezza.
Capo IV , Articolo 21, Misure di gestione dei rischi di cibersicurezza		
2. Gli Stati membri provvedono affinché i soggetti essenziali e importanti adottino misure tecniche, operative e organizzative adeguate e proporzionate per gestire i rischi posti alla sicurezza dei sistemi informativi e di rete... in base a a) politiche di analisi dei rischi e di sicurezza dei sistemi informativi;	Sophos Endpoint	Garantisce una protezione imbattibile contro ransomware e violazioni. Funzionalità di protezione innovative, inclusi deep learning basato sull'IA, antiexploit, protezione antiransomware impenetrabile con ripristino automatico dei file crittografati, e difese adattive che sono in grado di rispondere automaticamente ai cybercriminali e bloccare anche gli attacchi più avanzati.
	Sophos Firewall	Offre una protezione della rete leader di settore, ottimizzata per i requisiti della moderna Internet crittografata e per una base di utenti distribuita. Le funzionalità SD-WAN complete connettono in maniera sicura sedi e uffici distribuiti, mentre il sistema ZTNA integrato garantisce accesso sicuro e basato sugli utenti da qualsiasi luogo. Sophos Firewall si integra con Sophos Endpoint, Sophos ZTNA, i Sophos Switch e i Wireless Access Point, nonché con Sophos XDR e Sophos MDR, per rispondere automaticamente alle minacce, bloccando gli attacchi prima che riescano a diffondersi. Gli host compromessi vengono isolati automaticamente, prevenendo i tentativi di movimento laterale e le comunicazioni esterne, fino a quando non sia possibile svolgere le dovute indagini e rimuovere la minaccia.
	Sophos Managed Detection and Response (MDR)	Monitora costantemente i segnali provenienti dall'intero ambiente di sicurezza, incluse le tecnologie per rete, e-mail, firewall, gestione delle identità, endpoint e cloud, rilevando e rispondendo in maniera tempestiva e precisa ai potenziali eventi di cybersecurity. Il threat hunting proattivo identifica le minacce prima che possano avere effetti negativi sull'organizzazione.

REQUISITI DELLA DIRETTIVA NIS 2	SOLUZIONE SOPHOS	PERCHÉ È UTILE
	Sophos Network Detection and Response (NDR)	Analizza ininterrottamente il traffico, per individuare pattern sospetti. Agisce in insieme ai firewall e agli endpoint gestiti con Sophos per monitorare l'attività della rete alla ricerca di schemi sospetti e pericolosi. Analizza le parti più nascoste della rete per rilevare i flussi di traffico anomali che vengono generati da sistemi e dispositivi IoT non gestiti, da risorse non autorizzate, da minacce interne, da attacchi zero-day mai osservati prima e da pattern insoliti.
	Sophos Cloud Optix	Permette alle organizzazioni di progettare ambienti cloud pubblici per soddisfare i requisiti e mantenere gli standard e le best practice sulla sicurezza di Amazon Web Services, Microsoft Azure e Google Cloud Platform. Monitora e rileva continuamente la presenza di deviazioni dagli standard di configurazione, prevenendo, rilevando e correggendo automaticamente le modifiche accidentali o intenzionalmente malevole della configurazione delle risorse.
	Funzionalità Synchronized Security nei prodotti Sophos	Condivide dati sulla telemetria e sullo stato di integrità, rendendo possibile l'isolamento coordinato dei dispositivi infetti e abilitando il rilevamento del malware e la correzione dei problemi su server, endpoint e firewall. Questa sinergia consente di bloccare anche gli attacchi più avanzati.
2. b) gestione degli incidenti;	Sophos Endpoint	Rileva e blocca automaticamente il 99,98% degli attacchi. Fornisce opzioni dettagliate di correzione, grazie alla capacità di eliminare codice malevolo e annullare le modifiche dannose applicate dal malware alla chiave di registro.
	Sophos Firewall	I suoi strumenti completi per la compilazione di log e report nell'appliance e nel cloud offrono dati pratici per orientare e velocizzare la risposta agli incidenti. Includono dati di intelligence dettagliati sull'attività della rete e facile accesso ai log per le analisi approfondite. L'Automated Threat Response, insieme ad altri prodotti Sophos, riduce i tempi di risposta e li porta da qualche minuto a una manciata di secondi, bloccando gli attacchi prima che possano diffondersi.
	Sophos Managed Detection and Response (MDR) Complete	Include Incident Response a 360 gradi come componente standard, garantendo monitoraggio e protezione 24/7 a cura dei nostri esperti di incident response. Include reportistica e Root Cause Analysis complete. Il nostro tempo medio necessario per rilevare, indagare e rispondere alle minacce è di soli 38 minuti.
	Sophos Network Detection and Response (NDR)	Non appena Sophos NDR identifica un indicatore di compromissione, una minaccia attiva o un active adversary, lo segnala immediatamente agli analisti, che possono quindi inviare un feed sulle minacce a Sophos Firewall per attivare la risposta automatica e isolare l'host compromesso.

REQUISITI DELLA DIRETTIVA NIS 2	SOLUZIONE SOPHOS	PERCHÉ È UTILE
	Sophos XDR	Permette agli analisti di rilevare gli incidenti, svolgere indagini e avviare una risposta sulle principali superfici di attacco, sfruttando le soluzioni di sicurezza (Sophos e non Sophos) già presenti nell'infrastruttura di un'azienda. Sophos XDR memorizza 90 giorni di telemetria di sicurezza nel Sophos Data Lake per semplificare la gestione degli incidenti. Allo stesso tempo, i flussi di lavoro ottimizzati e le opzioni basate sull'IA velocizzano le indagini e la risposta agli incidenti.
	Sophos Cloud Optix	Esegue la scansione delle risorse nel cloud alla ricerca di eventuali errori di configurazione, definendo gli avvisi in base al livello di rischio, per aiutare i team di sicurezza a focalizzarsi sugli ambiti con priorità più elevata; in più, fornisce consigli dettagliati per risolvere i problemi individuati.
	Servizio Sophos Rapid Response	Offre assistenza tempestiva, grazie all'azione di un team di esperti di incident response che identificano e neutralizzano le minacce attive nella tua organizzazione.
	Synchronized Security nei prodotti Sophos	Condivide dati sulla telemetria e sullo stato di integrità, rendendo possibile l'isolamento coordinato dei dispositivi infetti e abilitando il rilevamento del malware e la correzione dei problemi su server, endpoint e firewall.
2. c) continuità operativa, come la gestione del backup e il ripristino in caso di disastro, e gestione delle crisi;	Sophos Endpoint	Utilizza tecnologie di sicurezza innovative e adattive per prevenire le interruzioni del business. Include il deep learning basato sull'IA, funzionalità antiexploit e una protezione antiransomware impenetrabile, con ripristino automatico dei file allo stato pre-attacco.
	Sophos Firewall	I cluster di disponibilità elevata (HA) plug-and-play di Sophos Firewall garantiscono resilienza in caso di interruzione del business. Per una gestione più efficiente dei costi, i clienti possono usufruire della ridondanza in modalità attivo-passivo acquistando solo la licenza per il dispositivo attivo. Sophos Firewall supporta anche più connessioni Internet con failover a impatto zero, oltre al bilanciamento del carico tra LTE wireless, cavo, DSL e fibra, per garantire massima resilienza. Le opzioni estese di compilazione dei log e di report nell'appliance e nel cloud offrono dati di telemetria approfonditi e pratici per facilitare le procedure di disaster recovery.
	Sophos Managed Detection and Response (MDR)	Mitiga il rischio di interruzione del business, grazie alle opzioni di rilevamento e risposta 24/7. In caso di incidente, include un servizio di Incident Response a 360 gradi. Le integrazioni con vendor di soluzioni di backup e ripristino permettono agli analisti di identificare gli attacchi che colpiscono i backup; potranno così intervenire tempestivamente e neutralizzare i cybercriminali. Il servizio memorizza fino a un anno di dati di telemetria di sicurezza nel Sophos Data Lake, per facilitare le procedure di disaster recovery.
	Sophos XDR	Memorizza fino a 90 giorni di dati di telemetria di sicurezza nel Sophos Data Lake, per facilitare le procedure di disaster recovery. Le integrazioni con vendor di soluzioni di backup e ripristino permettono agli analisti di identificare gli attacchi che colpiscono i backup; potranno così intervenire tempestivamente e neutralizzare i cybercriminali.

REQUISITI DELLA DIRETTIVA NIS 2	SOLUZIONE SOPHOS	PERCHÉ È UTILE
	Sophos Cloud Optix	Identifica quando non vengono eseguiti backup negli account all'interno dell'infrastruttura cloud pubblica, segnalandolo nella console di Cloud Optix, per permettere ai team di sicurezza di intraprendere l'azione necessaria.
	Servizio Sophos Rapid Response	Offre assistenza tempestiva, grazie all'azione di un team di esperti di incident response che identificano e neutralizzano le minacce attive nella tua organizzazione.
2. d) sicurezza della catena di approvvigionamento, compresi aspetti relativi alla sicurezza riguardanti i rapporti tra ciascun soggetto e i suoi diretti fornitori o fornitori di servizi;	Sophos Endpoint	Offre una difesa completa e in profondità contro le minacce che si infiltrano nei sistemi attraverso fornitori di terze parti. Le capacità di protezione includono il deep learning basato sull'IA, funzionalità antiexploit, protezione antiransomware impenetrabile con ripristino automatico dei file crittografati, e difese adattive che rispondono automaticamente ai comportamenti tipici dei cybercriminali.
	Sophos Managed Detection and Response (MDR)	Offre opzioni di threat hunting e correzione delle minacce a cura di tecnici esperti, nell'ambito di un servizio completamente gestito. Gli specialisti Sophos sono operativi 24/7 e lavorano instancabilmente per individuare, confermare e risolvere proattivamente le minacce e gli incidenti della supply chain. L'ampia selezione di integrazioni con le soluzioni di sicurezza e aziendali già in uso nell'organizzazione (incluse quelle di Microsoft e Google) ci permettono di ottenere visibilità e mitigare le minacce con la tua stessa catena di approvvigionamento tecnologica.
	Sophos XDR	Consente agli analisti di rilevare le attività sospette, di svolgere indagini e di avviare una risposta negli ambienti dei soggetti, per aiutarli a individuare e bloccare gli attacchi che colpiscono la catena di approvvigionamento. Sophos NDR (un add-on di Sophos XDR) offre rilevamento nelle parti più nascoste della rete, monitorando TUTTO il traffico di rete, per identificare le minacce che potrebbero sfuggire ad altre soluzioni, incluse quelle dei partner della catena di approvvigionamento.
	Sophos ZTNA	Difende la tua organizzazione dagli attacchi alla supply chain che cercano di sfruttare l'accesso dei fornitori ai tuoi sistemi interni, con una protezione basata su controlli estremamente granulari degli accessi. Prima di concedere l'accesso alle risorse, questa soluzione basata sul cloud convalida l'identità dell'utente, lo stato di integrità del dispositivo e la conformità ai criteri. Autentica le richieste provenienti da Partner attendibili, indipendentemente da dove siano situati.
2. e) sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informatici e di rete, compresa la gestione e la divulgazione delle vulnerabilità;	Sophos Firewall	Sophos Firewall aderisce all'iniziativa "Secure by Design" e continuiamo a impegnarci per fare in modo che diventi il firewall più difficile da compromettere per i cybercriminali. Include: › Best practice integrate per ottimizzare la sicurezza dei clienti › Protezione avanzata contro gli attacchi, con opzioni di gestione remota sicura, container, gestione rigida degli accessi, MFA e molto di più › Risposta automatizzata alla disponibilità di hotfix, con aggiornamenti over-the-air per la risoluzione dei problemi di sicurezza urgenti › Monitoraggio proattivo della base di installazione globale dei firewall › Programma efficace e trasparente di comunicazione delle vulnerabilità, con iniziative di bug bounty leader di mercato

REQUISITI DELLA DIRETTIVA NIS 2	SOLUZIONE SOPHOS	PERCHÉ È UTILE
	Sophos Managed Detection and Response (MDR)	Gli analisti esperti del team Sophos MDR monitorano ininterrottamente gli avvisi generati da tutti i prodotti installati nella rete, indagando sulle attività sospette e neutralizzando gli attacchi 24/7. Sophos NDR offre rilevamento nelle parti più nascoste della rete, monitorando TUTTO il traffico di rete, per identificare le minacce che potrebbero sfuggire ad altre soluzioni. Sophos MDR risponde proattivamente alla divulgazione delle vulnerabilità da parte del Cliente. Non appena riceve la notifica, viene avviata un'indagine completa che cerca tracce di attività di exploit. Se necessario, Sophos MDR provvede a correggere l'incidente e offre consulenza su come incrementare la sicurezza dell'ambiente e prevenire tentativi di exploit in futuro. Per rispondere all'indagine sulla divulgazione delle informazioni, viene fornito un report completo, compilato da esperti umani. Sophos Managed Risk è un servizio completamente gestito di Vulnerability Management, che identifica quando i sistemi sono esposti alle minacce e offre consulenza sull'applicazione delle patch in base al rischio. Collabora con il servizio Sophos MDR e ne estende le capacità. Sophos aderisce all'iniziativa "Secure by Design". Abbiamo implementato un programma efficace e trasparente di comunicazione delle vulnerabilità, incluse disposizioni di esenzione da responsabilità che offrono supporto ai ricercatori, nonché iniziative di bug bounty leader di mercato.
	Sophos XDR	Permette agli analisti di monitorare ininterrottamente gli avvisi generati da tutti i prodotti installati nella rete, per indagare sulle attività sospette e neutralizzare gli attacchi 24/7. Sophos NDR (un add-on di Sophos XDR) offre rilevamento nelle parti più nascoste della rete, monitorando TUTTO il traffico di rete, per identificare le minacce che potrebbero sfuggire ad altre soluzioni.
	Sophos Cloud Optix	Esegue la scansione delle risorse nel cloud alla ricerca di eventuali errori di configurazione, definendo gli avvisi in base al livello di rischio, per aiutare i team di sicurezza a focalizzarsi sugli ambiti con priorità più elevata; in più, fornisce consigli dettagliati per risolvere i problemi individuati.
	Servizio Sophos Rapid Response	Ottieni assistenza tempestiva, con l'intervento di un team di esperti di incident response che identificano e neutralizzano le minacce attive nella tua organizzazione.

REQUISITI DELLA DIRETTIVA NIS 2	SOLUZIONE SOPHOS	PERCHÉ È UTILE
2. f) strategie e procedure per valutare l'efficacia delle misure di gestione dei rischi di cibersicurezza;	Sophos Endpoint	I controlli di integrità incorporati permettono alle organizzazioni di identificare e risolvere rapidamente i problemi di configurazione dei dispositivi protetti con Sophos. Se dovesse essere identificato un problema, l'opzione "Risolvi automaticamente" permette agli utenti di correggere le configurazioni non sicure con pochissimi clic.
	Sophos Firewall	I report sul profilo di sicurezza integrati consentono alle organizzazioni di valutare rapidamente la propria struttura di protezione della rete e identificare gli ambiti che richiedono miglioramenti.
	Sophos Managed Detection and Response (MDR)	Indaga e valuta 24/7 i potenziali rischi di sicurezza nell'intero ambiente, utilizzando i dati di intelligence sulle minacce leader di settore forniti da Sophos X-Ops per identificare i livelli di rischio e assegnare la giusta priorità alle attività di risposta.
2. g) pratiche di igiene informatica di base e formazione in materia di cibersicurezza;	Sophos Phish Threat	Offre simulazioni di attacchi informatici di phishing e corsi di formazione e sensibilizzazione per gli utenti finali delle organizzazioni. I corsi trattano un'ampia selezione di argomenti, da lezioni introduttive su phishing e cybersecurity, fino a informazioni importanti sulla prevenzione della perdita dei dati, sulla protezione con password e molto di più.
	Formazione e certificazioni Sophos	I corsi di formazione e le certificazioni aiutano Partner e Clienti a ottenere tutti i vantaggi delle implementazioni di sicurezza Sophos; offrono inoltre accesso a personale esperto, dotato di competenze e conoscenze aggiornate in materia di best practice di sicurezza.
2. h) politiche e procedure relative all'uso della crittografia e, se del caso, della cifratura;	Sophos Firewall	Consente di utilizzare l'autenticazione a più fattori (MFA) per le connessioni VPN, con integrazione granulare di RADIUS/TACACS. Il Sophos Cryptographic Module integrato nei sistemi Sophos Firewall offre crittografia con convalida FIPS 140-2 per la protezione delle informazioni di natura sensibile.
	Sophos Email	Sophos SPX Encryption offre crittografia dei dati in transito e inattivi. SPX Encryption è in grado di incapsulare dinamicamente i contenuti di e-mail e allegati in un PDF crittografato in maniera sicura, per garantire il rispetto della conformità.
	Sophos Wireless	Crea sessioni Wi-Fi crittografate in maniera dinamica, che proteggono le informazioni in transito sulle reti e sugli hotspot gestiti da Sophos.

REQUISITI DELLA DIRETTIVA NIS 2	SOLUZIONE SOPHOS	PERCHÉ È UTILE
2. i) sicurezza delle risorse umane, strategie di controllo dell'accesso e gestione degli attivi;	Sophos Firewall	La sensibilizzazione degli utenti in tutti gli ambiti del nostro firewall regola ogni aspetto relativo ai criteri e alla reportistica del firewall. Pertanto, garantisce pieno controllo a livello di utente sulle applicazioni e sull'uso della larghezza di banda e di altre risorse della rete. L'opzione ZTNA integrata offre accesso sicuro, in base all'utente, da qualsiasi luogo. Sono inclusi anche controlli di amministrazione basati sui ruoli, autenticazione a più fattori e controlli granulari per gli accessi.
	Sophos Managed Detection and Response (MDR)	Gli esperti di threat hunting monitorano e mettono in correlazione l'attività dei sistemi informativi nell'intero ambiente di IT security, identificando e svolgendo indagini sulle attività sospette. Inoltre, esaminano regolarmente i record di attività dei sistemi informativi, inclusi quelli relativi a sistemi HR, controllo degli accessi e risorse.
	Sophos XDR	Permette agli analisti di monitorare e mettere in correlazione l'attività dei sistemi informativi nell'intero ambiente di sicurezza, identificando e svolgendo indagini sulle attività sospette, incluse quelle che riguardano sistemi HR, controllo degli accessi e risorse.
	Sophos Central	Tiene aggiornati gli elenchi di accesso e le informazioni sui privilegi degli utenti. Applica procedure volte a garantire la revoca dei diritti di accesso qualora i singoli utenti non dovessero più soddisfare le condizioni necessarie per ottenere l'accesso (ad es. perché cambiano ruolo all'interno dell'azienda o perché si dimettono).
	Sophos Cloud Optix	Consente di gestire l'inventario quando si utilizzano provider di servizi cloud multipli, con monitoraggio continuo delle risorse e visualizzazione completa della topologia e del traffico della rete.
	Sophos ZTNA	Permette di ottenere livelli superiori di sicurezza e maggiore agilità durante i cambiamenti di ambiente, semplificando e velocizzando il processo di registrazione e rimozione delle autorizzazioni per utenti e dispositivi. Prima di garantire accesso ad applicazioni e dati, convalida continuamente l'identità dell'utente, lo stato di integrità del dispositivo e la conformità ai criteri.
2. j) uso di soluzioni di autenticazione a più fattori o di autenticazione continua, di comunicazioni vocali, video e testuali protette e di sistemi di comunicazione di emergenza protetti da parte del soggetto al proprio interno, se del caso.	Sophos Firewall	Supporta opzioni flessibili di autenticazione a più fattori (MFA), con controlli di amministrazione basati sui ruoli e servizi di directory per accedere agli ambiti più importanti del sistema. La funzionalità ZTNA integrata convalida continuamente l'identità dell'utente, lo stato di integrità del dispositivo e la conformità ai criteri, prima di garantire accesso ad applicazioni e dati. Sophos Firewall include anche controlli granulari per gestire gli accessi.
	Sophos Central	Utilizza l'autenticazione a due fattori per proteggere gli account degli amministratori e quelli con privilegi elevati.
	Sophos Cloud Optix	Monitora gli account AWS/Azure/GCP, individuando gli accessi da parte di account di utenti root e utenti IAM nei quali l'autenticazione a più fattori è disattivata, per permetterti di risolvere il problema e garantire la conformità alle normative.
	Sophos ZTNA	Prima di garantire accesso ad applicazioni e dati, convalida continuamente l'identità dell'utente, lo stato di integrità del dispositivo e la conformità ai criteri.

REQUISITI DELLA DIRETTIVA NIS 2	SOLUZIONE SOPHOS	PERCHÉ È UTILE
Capo IV, Articolo 23, Obblighi di segnalazione		
4. Gli Stati membri provvedono affinché, ai fini della notifica a norma del paragrafo 1, i soggetti interessati trasmettano al CSIRT o, se opportuno, all'autorità competente: d) una relazione finale entro un mese dalla trasmissione della notifica dell'incidente di cui alla lettera b), che comprenda: (i) una descrizione dettagliata dell'incidente, comprensiva della sua gravità e del suo impatto;	Sophos Managed Detection and Response (MDR)	Include Incident Response a 360 gradi e analisi della root cause. Gli esperti di Sophos correggono i danni causati dall'incidente e offrono un report compilato interamente da esseri umani, che include i dettagli di come si è svolto l'attacco e offre consulenza su come potenziare i sistemi di sicurezza dell'ambiente, per proteggerlo da tentativi futuri di exploit.
	Sophos XDR	Permette agli analisti di identificare e compilare report su tutte le fasi della catena di attacco, fornendo una descrizione dettagliata dell'incidente e della root cause dell'attacco.
4. Gli Stati membri provvedono affinché, ai fini della notifica a norma del paragrafo 1, i soggetti interessati trasmettano al CSIRT o, se opportuno, all'autorità competente: d) una relazione finale entro un mese dalla trasmissione della notifica dell'incidente di cui alla lettera b), che comprenda: (ii) il tipo di minaccia o la causa di fondo che ha probabilmente innescato l'incidente;	Sophos Managed Detection and Response (MDR)	Include Incident Response a 360 gradi e analisi della root cause. Gli esperti di Sophos correggono i danni causati dall'incidente e offrono un report compilato interamente da esseri umani, che include i dettagli di come si è svolto l'attacco e offre consulenza su come potenziare i sistemi di sicurezza dell'ambiente, per proteggerlo da tentativi futuri di exploit.
	Sophos XDR	Permette agli analisti di identificare e compilare report su tutte le fasi della catena di attacco, fornendo una descrizione dettagliata dell'incidente e della root cause dell'attacco.

2024-08-26 (WP-NP)

SOPHOS