kaspersky BRING ON THE FUTURE

La Direttiva europea NIS 2:
nuovi obblighi e come prepararsi al cambiamento

Cos'è la direttiva NIS 2?

La Direttiva NIS 2[1] è entrata in vigore il 16 gennaio 2023 e gli Stati Membri dovranno attuarla entro il 17 ottobre 2024. Tra i vari obiettivi, la direttiva NIS 2 richiede agli operatori dei settori chiave di mettere in atto misure di sicurezza e di riportare eventuali incidenti.

Quali soggetti riguarda la NIS 2?

Un ente rientra nell'ambito di applicazione della Direttiva se opera in uno dei settori e delle tipologie di servizi elencati negli allegati della Direttiva e se ha una certa dimensione. Per tutti i dettagli, le eccezioni e le varianti riguardanti la direttiva, consultare gli articoli 2 e 3 e gli allegati I e II della Direttiva[2]. La NIS 2 stabilisce due categorie di soggetti che rientrano nel suo ambito di applicazione: enti essenziali e enti importanti. Entrambe le categorie devono rispettare gli stessi requisiti. Le differenze riguardano le misure di sorverglianza e le sanzioni.

Settori che verranno regolamentati

Settori ad alta criticità
(Soggetti essenziali)

- Energia
- Acqua potabile
- Trasporto
- Infrastrutture digitali
- Settore bancario
- Acque reflue
- Infrastrutture dei mercati finanziari
- Gestione dei servizi ICT
- Settore sanitario
- Amministrazione pubblica
- Spazio

Altri settori critici
(Soggetti importanti)

- Servizi postali e di corriere
- Produzione, trasformazione e distribuzione di alimenti
- Gestione dei rifiuti
- Industria manufatturiera
- Fabbricazione, produzione e distribuzione di sostanze chimiche
- Ricerca
- Fornitori di servizi digitali

Quali sono i requisiti di sicurezza informatica previsti dalla NIS 2?

Secondo l'articolo 21[1] della Direttiva, gli Stati Membri devono assicurare che le entità importanti e quelle essenziali prendano le adeguate e proporzionate misure tecniche, operative e organizzative per gestire i rischi relativi alla sicurezza della rete e ai sistemi informativi utilizzati per le loro operazioni o per erogare i loro servizi, per prevenire o minimizzare l'impatto degli incidenti sui destinatari dei loro servizi e su altri servizi.
Queste misure dovrebbero essere basate su un approccio che consideri tutti i rischi con lo scopo di proteggere i sistemi di rete e informativi, l'ambiente in cui operano tali sistemi e infine dovrebbe includere almeno i seguenti punti:

- Policy sull'analisi del rischio e sulla sicurezza dei sistemi informativi;
- Gestione degli incidenti;
- Continuità operativa, come gestione dei backup, disaster recovery e gestione delle crisi;
- Sicurezza della supply chain, tra cui aspetti legati alla sicurezza riguardanti il rapporto tra ogni entità e i suoi fornitori diretti o service provider;
- Sicurezza nell'acquisto, nello sviluppo e manutenzione dei sistemi di rete e informativi, inclusa la gestione e la comunicazione della vulnerabilità;
- Regole e procedure per valutare l'efficacia delle misure di sicurezza informatica relative alla gestione dei rischi;
- Pratiche di "igiene informatica" di base e formazione sul tema della sicurezza informatica;
- Policy e procedure riguardanti l'uso della crittografia e, laddove necessaria, encryption;
- Sicurezza delle risorse umane, policy di controllo degli accessi e gestione degli asset; laddove opportuno, autenticazione multi fattore o soluzioni di autenticazione continua; comunicazioni vocali, scritte e video protette; sistemi di comunicazione di emergenza protetti all'interno dell'ente.

Come cybersecurity vendor, Kaspersky sfrutta tutta la propria esperienza per aiutare le organizzazioni a costruire robuste difese informatiche ed essere conformi a NIS 2. Possiamo supportarvi con la nostra leadership soluzioni e servizi.

---

[1] Direttiva (EU) 2022/2555 del Parlamento Europeo e del Consiglio del 14 dicembre 2022 sulle misure per un elevato livello comune di sicurezza informatica in tutta l'Unione, che modifica il Regolamento No 910/2014 e la Direttiva (EU) 2018/1972, e abroga la Direttiva (EU) 2016/1148 (Direttiva NIS 2); https://eur-lex.europa.eu/eli/dir/2022/2555

[2] https://eur-lex.europa.eu/eli/dir/2022/2555

Requisiti NIS2	Soluzioni Kaspersky	Vantaggi
Capo IV, Art. 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.	 Kaspersky Security Awareness	**KASPERSKY SECURITY AWARENESS** è un approccio totalmente nuovo e differente alla formazione e alla padronanza delle competenze di sicurezza informatica. Il portafoglio di Security awareness comprende soluzioni efficaci, collaudate ed apprezzate a livello internazionale. Le soluzioni contentue all'interno del portafoglio, vengono utilizzate da organizzazioni di qualsiasi dimensione e permettono di formare i propri dipendenti grazie all'esperienza di Kaspersky, di oltre 25 anni, nel campo della sicurezza informatica. Grazie al format particolarmente coinvolgente ed efficaci, permettono alle aziende di far accrescere la consapevolezza su tematiche di cybersecurity ai propri dipendenti in modo che tutti facciano la loro parte per contribuire attivamente alla sicurezza informatica dell'organizzazione. Dato che il cambio di postura dei dipendenti richiederà sicuramente del tempo, l'approccio Kaspersky prevede la costruzione di un ciclo di formazione ed apprendimento continuativo e basato su più componenti.
	 Kaspersky Cybersecurity Training	KASPERSKY XTRAINING è una risposta al panorama delle minacce informatiche in continua evoluzione. Forniamo conoscenze aggiornate su strategie efficaci di rilevamento e mitigazione delle minacce derivanti dalle esperienze complete e ben note del Kaspersky Global Research & Analysis Team (GReAT)
	 Kaspersky ICS CERT Training	**KASPERSKY ICS CERT** è un progetto globale iniziato nel 2016, per coordinare gli sforzi dei vendor del mondo dell'automazione industriale e i proprietari ed operatori di impianti industriali. Il team del Kaspersky ICS CERT è composto da più di 30 esperti impegnati nella ricerca di minacce e vulnerabilità ICS, oltre che nella risposta ed analisi degli incidenti informatici in ambito OT. Grazie a questa esperienza, Kaspersky è in grado di fornire una formazione specifica sugli elementi essenziali della cybersecurity industriale e competenze pratiche per idagare sugli incidenti di sicurezza informatica ed eseguire ricerche sulle vulnerabilità. Tutti i nostri programmi di formazione, si basano sull'esperienza accumulata sul campo e derivata da casi reali. Il team di Kaspersky ICS CERT, offre corsi di formazione per diversi operatori della sicurezza ICS, a partire dagli operatori negli impianti fino al "C-Level", comprendendo ovviamente anche i professionisti di sicurezza informatica dedicati all'OT.

Requisiti NIS2	Soluzioni Kaspersky	Vantaggi
Capo IV, Art. 21, Misure di gestione dei rischi di cybersicurezza		
1.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 che tali soggetti utilizzano nelle loro attività o nella fornitura dei loro servizi, nonché per prevenire o ridurre al minimo l'impatto degli incidenti per i destinatari dei loro servizi e per altri servizi. Tenuto conto delle conoscenze più aggiornate in materia e, se del caso, delle pertinenti norme europee e internazionali, nonché dei costi di attuazione, le misure di cui al primo comma assicurano un livello di sicurezza dei sistemi informativi e di rete adeguato ai rischi esistenti. Nel valutare la proporzionalità di tali misure, si tiene debitamente conto del grado di esposizione del soggetto a rischi, delle dimensioni del soggetto e della probabilità che si verifichino incidenti, nonché della loro gravità, compreso il loro impatto sociale ed economico.	**Kaspersky Next**	**KASPERSKY NEXT** è la soluzione per proteggere le infrastrutture dalle minacce informatiche complesse ed avasive. Ogni livello di protezione, fornisce funzionalità EDR personalizzate in base alle esigenze e alle risorse a disposizione. Le nostre tecnologie di EDR e XDR si basano tutte sulla pluripremiata protezione degli endpoint unita ai controlli di livello enterprise. Grazie all'automazione di attività anche complesse e alle risposte guidate, si potrà ottenere una nuova efficienza grazie soprattutto all'automazione che permetterà di ridurre le risorse necessarie per gestire la cybersecurity aziendale. Infine, la possibilità di adottare le soluzioni sia in modalità cloud che on-prem vi permetterà di essere quanto più flessibili possibile, adattando le soluzioni alle vostre esigenze. Quando poi sarà il momento, si potrà controllare l'intera infrastruttura di cybesecurity adottata grazie alla soluzione Kaspersky OpenXDR.
	Kaspersky Managed Detection and Response Optimum	**KASPERSKY MANAGED DETECTION AND RESPONSE** offre un servizio totalmente gestito da Kaspersky che, grazie ad un monitoraggio 24/7 è in grado di rilevare e prioritizzare qualsiasi tipologia di incidente informatico, garantendo così un'indagine e una ripsosta continua. Gli analisti del SOC Kaspersky, grazie ad un'analisi approfondita della telemetria e degli eventi, sono in grado di rilevare ogni tipologia di minaccia informatica, qualsiasi sia la fase di un attacco, notificano prontamente al cliente qualsiasi attività dannosa, sia prima dell'effettiva compromissione che dopo che gli attaccanti sono riusciti a entrare all'interno dell'infrastruttura aziendale. In ogni momento, il cliente verrà guidato nell'analisi dell'incidente e riceverà risposte guidate e consigli per ottimizzare e gestire al meglio ogni incidente di sicurezza.
	Kaspersky Extended Detection and Response	**KASPERSKY XDR** è una piattaforma aperta, uno strumento universale per creare un ecosistema unificato di prodotti di cybersecurity. la piattaforma agisce come una soluzione Anti APT ALL-In-One potenziata dalla Kaspersky Threat Intelligence che controlla tutti i potenziali punti di ingresso dei cybercriminali, correlando le informazioni e orchestrando tutti i componenti di protezione dell'infrastruttura. Kaspersky XDR include un'ampia gamma di integrazioni pronte all'uso, con prodotti Kaspersky e di terze parti
	Kaspersky Industrial CyberSecurity	**KASPERSKY INDUSTRIAL CYBERSECURITY (KICS)** è una piattaforma nativa di Extended Detection and Response (XDR), appositamente progettata e certificata per proteggere le apparecchiature, gli asset e le reti OT dalle minacce informatiche. La piattaforma comprende tecnologie integrate che proteggono i componenti fondamentali dei sistemi di automazione e controllo industriale a tutti i livelli. KICS for Nodes è un software di protezione con funzionalità EDR e di controllo di conformità, dedicato agli endpoint di un impianto. KICS for Networks è progettato per l'analisi, il rilevamento e la risposta del traffico di rete OT. La funzione di gestione centralizzata a livello di sito, essenziale per scalare le operazioni di sicurezza OT a un volume elevato di infrastrutture industriali grandi, diverse e geo-distribuite, è integrata nella piattaforma. La perfetta integrazione tra i componenti della piattaforma offre una visibilità completa degli impianti OT e dei sistemi di automazione anche se distribuiti geograficamente, migliorando quindi l'esperienza del cliente, la consapevolezza della situazione e la flessibilità di implementazione. Grazie alle funzionalità native di Extended Detection and Response, la piattaforma KICS consente la convergenza IT-OT e offre numerosi vantaggi a un unico fornitore.

Requisiti NIS2	Soluzioni Kaspersky	Vantaggi
Capo IV, Art. 21, Misure di gestione dei rischi di cibersicurezza		
1.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 che tali soggetti utilizzano nelle loro attività o nella fornitura dei loro servizi, nonché per prevenire o ridurre al minimo l'impatto degli incidenti per i destinatari dei loro servizi e per altri servizi. Tenuto conto delle conoscenze più aggiornate in materia e, se del caso, delle pertinenti norme europee e internazionali, nonché dei costi di attuazione, le misure di cui al primo comma assicurano un livello di sicurezza dei sistemi informativi e di rete adeguato ai rischi esistenti. Nel valutare la proporzionalità di tali misure, si tiene debitamente conto del grado di esposizione del soggetto a rischi, delle dimensioni del soggetto e della probabilità che si verifichino incidenti, nonché della loro gravità, compreso il loro impatto sociale ed economico.	Kaspersky Container Security	**KASPERSKY CONTAINER SECURITY (KCS)** è una soluzione di sicurezza che copre ogni fase del ciclo di vita di un'applicazione containerizzata, dal suo sviluppo al funzionamento. Proteggendo i processi aziendali, in linea con gli standard e le normative di sicurezza, permette di implementare correttamente l'approccio DevSecOps. Kaspersky Container Security offre una protezione completa dalle minacce informatiche più recenti e automatizza gli audit di conformità, liberando le risorse del team di sicurezza informatica, facendole concentrare su altre attività, e riducendo il time to market del proprio applicativo. Kaspersky Container Security è stato sviluppato specificamente per gli ambienti containerizzati, garantendo una protezione a diversi livelli, dall'immagine del container al sistema operativo dell'host.
	Kaspersky Threat Intelligence	La **THREAT INTELLIGENCE KASPERSKY**, permette di accedere a tutte le informazioni necessarie per contrastare o mitigare le minacce informatiche. La profonda conoscenza e l'esperienza che Kaspersky ha acquisito, ottenute in particolare da team composti da ricercatori e analisti leader a livello mondiale, ci hanno reso il partner di fiducia delle principali forze dell'ordine e agenzie governative del mondo, tra cui INTERPOL e i principali CERT. Kaspersky Threat Intelligence offre accesso immediato a informazioni tattiche, operative e strategiche sulle minacce informatiche, permettendo di identificare e prevenire le minacce in modo proattivo, tenendo informati sui rischi e le vulnerabilità più recenti e consentendo di adottare misure proattive per proteggere i vostri sistemi prima che si verifichi un attacco informatico.
	Kaspersky Web Traffic Security	**KASPERSKY WEB TRAFFIC SECURITY (KWTS)** è una soluzione progettata per proteggere il traffico HTTP, HTTPS e FTP. L'applicazione protegge gli utenti di una rete aziendale quando accedono a qualsiasi risorsa web. Ad esempio si è in grado di eliminare del malware e altre minacce informatiche inserite all'interno dei flussi di dati che entra nella rete aziendale, attraverso i protocolli HTTP(S) e FTP; KWTS è in grado anche di bloccare preventivamente i siti web infetti e di phishing, controllando l'accesso alle risorse web da parte degli utenti, in base alle categorie e ai tipi di contenuto delle risorse web.
	Kaspersky Security for Mail Servers	**KASPERSKY SECURITY FOR MAIL SERVER (KSMS)** aiuta a creare una protezione solida verso tutti gli attacchi basati sulla posta elettronica. KSMS identifica e filtra la posta sospetta o indesiderata a livello gateway, rafforzando quindi la resilienza aziendale, rilevando e intercettando gli attacchi proprio all'inizio della killchain, prima che possano violare il perimetro e dirigersi quindi verso gli endpoint e gli utenti. Grazie ad una elaborazione rapida ed accurata delle email, si garantisce che tutte le comunicazioni legittime non siano mai ostacolate. Kaspersky Security for Mail Server offre le tecnologie di protezione più efficaci del settore, in modo da contrastare efficacemente qualsiasi tenica messa in campo da un'attaccante; dalle e-mail di phishing e spam agli attacchi BEC (Business Email Compromise) e ransomware, con quasi zero falsi positivi, consentendo alle e-mail legittime di essere recepite senza interruzioni. Kaspersky Security for Mail Server è in grado di proteggere anche oltre il gateway, andando a lavorare anche sulle singole caselle di posta di Microsoft Exchange Server o di Microsoft Exchange Online, così che anche attacchi di phishing ritardati o progettati per eludere le contromisure a livello di gateway. Tutto questo può essere identificato ed eliminato, rendendo la protezione delle caselle di posta del server un "must-have".

Requisiti NIS2	Soluzioni Kaspersky	Vantaggi
Capo IV, Art. 21, Misure di gestione dei rischi di cibersicurezza		
	Kaspersky Incident Response	**RISPOSTA AGLI INCIDENTI:** Il servizio permette di ottenere un quadro dettagliato dell'incidente, coprendo l'intero ciclo di indagine e risposta agli incidenti: dalla risposta iniziale e la raccolta delle prove, all'identificazione di ulteriori tracce di hacking e alla preparazione di un piano di mitigazione degli attacchi.
2. Le misure di cui al paragrafo 1 sono basate su un approccio multirischio mirante a proteggere i sistemi informativi e di rete e il loro ambiente fisico da incidenti e comprendono almeno gli elementi seguenti: a) politiche di analisi dei rischi e di sicurezza dei sistemi informativi;	Kaspersky Next	**KASPERSKY NEXT** è la soluzione per proteggere le infrastrutture dalle minacce informatiche complesse ed avasive. Ogni livello di protezione, fornisce funzionalità EDR personalizzate in base alle esigenze e alle risorse a disposizione. Le nostre tecnologie di EDR e XDR si basano tutte sulla pluripremiata protezione degli endpoint unita ai controlli di livello enterprise. Grazie all'automazione di attività anche complesse e alle risposte guidate, si potrà ottenere una nuova efficienza grazie soprattutto all'automazione che permetterà di ridurre le risorse necessarie per gestire la cybersecurity aziendale. Infine, la possibilità di adottare le soluzioni sia in modalità cloud che on-prem vi permetterà di essere quanto più flessibili possibile, adattando le soluzioni alle vostre esigenze. Quando poi sarà il momento, si potrà controllare l'intera infrastruttura di cybesecurity adottata grazie alla soluzione Kaspersky OpenXDR.
	Kaspersky Industrial CyberSecurity	**KASPERSKY INDUSTRIAL CYBERSECURITY (KICS)** è una piattaforma nativa di Extended Detection and Response (XDR), appositamente progettata e certificata per proteggere le apparecchiature, gli asset e le reti OT dalle minacce informatiche. La piattaforma comprende tecnologie integrate che proteggono i componenti fondamentali dei sistemi di automazione e controllo industriale a tutti i livelli. KICS for Nodes è un software di protezione con funzionalità EDR e di controllo di conformità, dedicato agli endpoint di un impianto. KICS for Networks è progettato per l'analisi, il rilevamento e la risposta del traffico di rete OT. La funzione di gestione centralizzata a livello di sito, essenziale per scalare le operazioni di sicurezza OT a un volume elevato di infrastrutture industriali grandi, diverse e geo-distribuite, è integrata nella piattaforma. La perfetta integrazione tra i componenti della piattaforma offre una visibilità completa degli impianti OT e dei sistemi di automazione anche se distribuiti geograficamente, migliorando quindi l'esperienza del cliente, la consapevolezza della situazione e la flessibilità di implementazione. Grazie alle funzionalità native di Extended Detection and Response, la piattaforma KICS consente la convergenza IT-OT e offre numerosi vantaggi a un unico fornitore.
	Kaspersky Security Assessment	Questo servizio fornisce informazioni sulle vulnerabilità esistenti, sulle conseguenze del loro sfruttamento, valuta l'efficacia delle misure di sicurezza implementate e consente di pianificare ulteriori azioni per correggere i difetti rilevati e migliorare la sicurezza. Eseguire regolarmente la security assessment consente di comprendere chiaramente lo status della vostra cybersecurity e garantisce la conformità con le best practices del settore.
	Kaspersky Digital Footprint Intelligence	**KASPERSKY DIGITAL FOOTPRINT INTELLIGENCE** è un servizio completo di protezione dai rischi digitali che aiuta i clienti a monitorare le proprie risorse digitali e a rilevare le minacce provenienti dal Surface, dal Deep e dal Dark Web. Con avvisi in tempo reale, Kaspersky Digital Footprint Intelligence consente alle organizzazioni di rispondere in modo rapido ed efficace alle potenziali minacce. I report analitici integrano questi dati con l'intelligence completa dei nostri esperti che fornisce approfondimenti sui rischi per la sicurezza informatica e raccomandazioni su come mitigarli.

Requisiti NIS2	Soluzioni Kaspersky	Vantaggi
2. Le misure di cui al paragrafo 1 sono basate su un approccio multirischio mirante a proteggere i sistemi informativi e di rete e il loro ambiente fisico da incidenti e comprendono almeno gli elementi seguenti: a) politiche di analisi dei rischi e di sicurezza dei sistemi informativi;	 **Kaspersky Intelligence Reporting**	Grazie agli Intelligence Reporting i clienti Kaspersky potranno usufruire dell'accesso costante ed esclusivo alle analisi e ai rilevamenti, inclusi i dati tecnici completi (in un'ampia gamma di formati) sugli attori APT che prendono di mira il vostro settore e la vostra area geografica, imparate a conoscere e contrastare adeguatamente le minacce crimeware e le minacce informatiche che colpiscono le organizzazioni industriali (comprese le minacce che non verranno mai rese pubbliche). I report contengono una sintesi di informazioni immediate e rilevanti che illustrano ogni particolare dell'attacco oltre a offrire una descrizione tecnica dettagliata con le relative regole YARA e IOC, offrendo ai ricercatori di sicurezza, agli analisti malware, ai security engineer, agli analisti di sicurezza di rete e ai ricercatori APT, dati applicabili che consentono una risposta accurata e veloce alle minacce.
	 **Kaspersky Threat Data Feeds**	Integrando nei sistemi di sicurezza esistenti, come ad esempio i sistemi SIEM, SOAR e le piattaforme di Threat Intelligence, feed di Threat Intelligence aggiornati, contenenti informazioni su IP, URL e hash di file sospetti e pericolosi, i team di sicurezza possono automatizzare il processo di triage iniziale e fornire ai relativi specialisti il contesto necessario per identificare immediatamente gli avvisi che richiedono analisi approfondite, o che vanno inoltrati ai team di incident response per ulteriori indagini e risposte. I feed di dati vengono aggregati da fonti altamente affidabili ed eterogenee, quali Kaspersky Security Network e i nostri Web Crawler, il servizio di monitoraggio botnet (monitoraggio 24 ore su 24, 7 giorni su 7, 365 giorni all'anno di botnet e delle relative attività e obiettivi), spam trap, partner e team di ricerca.
	 **Kaspersky Unified Monitoring and Analysis Platform**	**KASPERSKY UNIFIED MONITORING AND ANALYSIS PLATFORM (KUMA)** è una soluzione SIEM avanzata per la gestione di dati ed eventi di sicurezza. KUMA analizza gli eventi di sicurezza in tempo reale, aumentando in modo significativo la consapevolezza di quanto sta avvenendo all'interno dell'infrastruttura. KUMA riceve eventi di sicurezza da varie fonti, tra cui prodotti Kaspersky, sistemi operativi, applicazioni di terze parti e strumenti di sicurezza; è in grado di mettere in relazione questi eventi tra loro e con i feed di threat intelligence può arricchire e identificare attività sospette all'interno della rete aziendale e fornire una notifica tempestiva degli incidenti di sicurezza.
	 Kaspersky Container Security	**KASPERSKY CONTAINER SECURITY (KCS)** è una soluzione di sicurezza che copre ogni fase del ciclo di vita di un'applicazione containerizzata, dal suo sviluppo al funzionamento. Proteggendo i processi aziendali, in linea con gli standard e le normative di sicurezza, permette di implementare correttamente l'approccio DevSecOps. Kaspersky Container Security offre una protezione completa dalle minacce informatiche più recenti e automatizza gli audit di conformità, liberando le risorse del team di sicurezza informatica, facendole concentrare su altre attività, e riducendo il time to market del proprio applicativo. Kaspersky Container Security è stato sviluppato specificamente per gli ambienti containerizzati, garantendo una protezione a diversi livelli, dall'immagine del container al sistema operativo dell'host.

Requisiti NIS2	Soluzioni Kaspersky	Vantaggi
2. b) gestione degli incidenti;	**Kaspersky Incident Response**	Risposta agli incidenti: Il servizio permette di ottenere un quadro dettagliato dell'incidente, coprendo l'intero ciclo di indagine e risposta agli incidenti: dalla risposta iniziale e la raccolta delle prove, all'identificazione di ulteriori tracce di hacking e alla preparazione di un piano di mitigazione degli attacchi.
	Kaspersky Endpoint Detection and Response	La visibilità limitata e la mancanza di risorse gioca a favore degli autori degli attacchi. **KASPERSKY ENDPOINT DETECTION AND RESPONSE (EDR)** Optimum offre un rilevamento avanzato, funzionalità di indagine semplificate e una risposta automatizzata in un pacchetto facile da usare, per proteggere la vostra azienda dalle minacce più recenti.
	Kaspersky Endpoint Detection and Response	I cyberattacchi stanno diventando sempre più sofisticati e capaci di eludere le misure di sicurezza esistenti. **Kaspersky Endpoint Detection and Response (EDR)** Expert offre visibilità completa in tutti gli endpoint della rete aziendale e offre difese di livello superiore, automatizzando le attività EDR di routine e consentendo agli analisti di rilevare, assegnare le priorità, analizzare e neutralizzare velocemente minacce complesse e attacchi di tipo APT. Kaspersky EDR Expert utilizza un singolo agente che può essere gestito sia da una singola piattaforma di gestione basata sul cloud che da una console offline in ambienti di tipo "air-gap", sfruttando tecnologie di threat intelligence e integrando strategie di rilevamento personalizzabili.
	Kaspersky Extended Detection and Response	**L' XDR** come una singola piattaforma aperta, uno strumento universale per creare un ecosistema unificato di prodotti di cybersecurity. la piattaforma agisce come una soluzione Anti APT ALL-In-One potenziata dalla Kaspersky Threat Intelligence che controlla tutti i potenziali punti di ingresso dei cybercriminali, correlando le informazioni e orchestrando tutti i componenti di protezione dell'infrastruttura. Kaspersky XDR include un'ampia gamma di integrazioni pronte all'uso, con prodotti Kaspersky e di terze parti
	Kaspersky Managed Detection and Response	**KASPERSKY MANAGED DETECTION AND RESPONSE** offre funzionalità di rilevamento, definizione delle priorità, indagine e risposta continue completamente gestite e personalizzate. Lo scopo principale del servizio MDR è rilevare le minacce in ogni fase di un attacco informatico, sia prima dell'effettiva compromissione sia dopo che gli attori malintenzionati sono penetrati nell'infrastruttura aziendale. Gli analisti SOC indagano sugli avvisi e informano il cliente dell'attività dannosa, fornendo risposte e indicazioni di mitigazione, sulla base di un monitoraggio della sicurezza 24 ore su 24, 7 giorni su 7, potenziato dalla ricerca automatizzata delle minacce, dall'indagine sugli incidenti e dalle risposte guidate e gestite
	Kaspersky Threat Lookup	**KASPERSKY THREAT LOOKUP** fornisce tutte le conoscenze acquisite da Kaspersky sulle minacce informatiche e sulle relazioni tra di esse, riunite in un unico e potente servizio Web. L'obiettivo è fornire ai team di sicurezza la maggior quantità possibile di dati, per prevenire gli attacchi informatici prima che compromettano l'organizzazione. La piattaforma recupera le informazioni dettagliate più recenti in termini di Threat Intelligence riguardo a URL, domini, indirizzi IP, hash di file, denominazioni delle minacce, dati statistici/comportamentali, dati WHOIS/DNS, attributi di file, dati di geolocalizzazione, catene di download, timestamp. Il risultato è una visibilità globale delle minacce nuove ed emergenti: ciò consente di proteggere al meglio la propria azienda, migliorando sensibilmente qualità ed efficienza delle attività di incident response.

Requisiti NIS2	Soluzioni Kaspersky	Vantaggi
2. b) gestione degli incidenti;	Kaspersky Threat Analysis	Di fronte a una potenziale minaccia informatica, decidere tempestivamente diventa fondamentale. Oltre alle tecnologie di analisi delle minacce come la sandboxing, Kaspersky Threat Analysis fornisce tecnologie di attribuzione all'avanguardia (un approccio multilivello che fornisce un'analisi efficiente delle minacce, così è possibile prendere decisioni pienamente informate per difendersi dagli attacchi anche prima che vengano lanciati). Diversi strumenti di analisi delle minacce si combinano per consentire agli operatori di analizzare la situazione da tutti gli angoli, grazie a un quadro completo del panorama delle minacce e di rispondere in modo rapido ed efficace.
	Kaspersky Threat Data Feeds	Integrando nei sistemi di sicurezza esistenti, come ad esempio i sistemi SIEM, SOAR e le piattaforme di Threat Intelligence, feed di Threat Intelligence aggiornati, contenenti informazioni su IP, URL e hash di file sospetti e pericolosi, i team di sicurezza possono automatizzare il processo di triage iniziale e fornire ai relativi specialisti il contesto necessario per identificare immediatamente gli avvisi che richiedono analisi approfondite, o che vanno inoltrati ai team di incident response per ulteriori indagini e risposte. I feed di dati vengono aggregati da fonti altamente affidabili ed eterogenee, quali Kaspersky Security Network e i nostri Web Crawler, il servizio di monitoraggio botnet (monitoraggio 24 ore su 24, 7 giorni su 7, 365 giorni all'anno di botnet e delle relative attività e obiettivi), spam trap, partner e team di ricerca.
	Kaspersky Unified Monitoring and Analysis Platform	**KASPERSKY UNIFIED MONITORING AND ANALYSIS PLATFORM** è una soluzione software integrata che include il seguente insieme di funzioni: - Ricezione, elaborazione e archiviazione di eventi di sicurezza delle informazioni. - Analisi e correlazione dei dati in ingresso. - Ricerca all'interno degli eventi ottenuti. - Creazione di notifiche al rilevamento di sintomi di minacce alla sicurezza delle informazioni. La soluzione è basata su un'architettura a microservizi. Ciò significa che è possibile creare e configurare i relativi microservizi in modo da usare KUMA sia come sistema di gestione dei log, che come sistema SIEM a tutti gli effetti. Inoltre, il routing flessibile dei flussi di dati consente di utilizzare servizi di terze parti per un'ulteriore elaborazione degli eventi.
	Kaspersky Container Security	**KASPERSKY CONTAINER SECURITY (KCS)** è una soluzione di sicurezza che copre ogni fase del ciclo di vita di un'applicazione containerizzata, dal suo sviluppo al funzionamento. Proteggendo i processi aziendali, in linea con gli standard e le normative di sicurezza, permette di implementare correttamente l'approccio DevSecOps. Kaspersky Container Security offre una protezione completa dalle minacce informatiche più recenti e automatizza gli audit di conformità, liberando le risorse del team di sicurezza informatica, facendole concentrare su altre attività, e riducendo il time to market del proprio applicativo. Kaspersky Container Security è stato sviluppato specificamente per gli ambienti containerizzati, garantendo una protezione a diversi livelli, dall'immagine del container al sistema operativo dell'host.

Requisiti NIS2	Soluzioni Kaspersky	Vantaggi
2. c) continuità operativa, come la gestione del backup e il ripristino in caso di disastro, e gestione delle crisi;	Kaspersky Next	**KASPERSKY NEXT** è la soluzione ideale per proteggere l' infrastruttura da ransomware, malware, minacce evasive e complesse. Sono disponibili funzionalità EDR in ogni livello, personalizzate in base alle tue esigenze e risorse. Le nostre tecnologie EDR e XDR si basano sulla pluripremiata protezione degli endpoint e sui controlli di livello aziendale. Kaspersky Next garantisce una ritrovata efficienza con l'automazione di attività semplici e complesse, insieme alla risposta guidata per aumentare la velocità di risposta agli incidenti e ridurre le risorse necessarie per gestire la sicurezza informatica dell'azienda. Le opzioni cloud e on-premise si adattano a tutti i requisiti delle diverse infrastrutture aziendali.
	Kaspersky Managed Detection and Response	**KASPERSKY MANAGED DETECTION AND RESPONSE** offre funzionalità di rilevamento, definizione delle priorità, indagine e risposta continue completamente gestite e personalizzate. Lo scopo principale del servizio MDR è rilevare le minacce in ogni fase di un attacco informatico, sia prima dell'effettiva compromissione sia dopo che gli attori malintenzionati sono penetrati nell'infrastruttura aziendale. Gli analisti SOC indagano sugli avvisi e informano il cliente dell'attività dannosa, fornendo risposte e indicazioni di mitigazione, sulla base di un monitoraggio della sicurezza 24 ore su 24, 7 giorni su 7, potenziato dalla ricerca automatizzata delle minacce, dall'indagine sugli incidenti e dalle risposte guidate e gestite
	Kaspersky Incident Response	Risposta agli incidenti: Il servizio permette di ottenere un quadro dettagliato dell'incidente, coprendo l'intero ciclo di indagine e risposta agli incidenti: dalla risposta iniziale e la raccolta delle prove, all'identificazione di ulteriori tracce di hacking e alla preparazione di un piano di mitigazione degli attacchi.
	Kaspersky Incident Communications	Dal momento in cui viene scoperto un incidente informatico, ogni azione conta. Il modo in cui vengono gestite le comunicazioni, esternamente e internamente, è fondamentale, in particolare quando si ha a che fare con vettori di attacco sconosciuti e minacce persistenti avanzate (APT). Kaspersky ha sviluppato una formazione all'avanguardia che consente al top management, ai professionisti della sicurezza informatica e delle comunicazioni aziendali di gestire le comunicazioni di crisi, compreso lo sviluppo e l'utilizzo di risorse adeguate, durante l'attacco di un incidente informatico sconosciuto o di una minaccia persistente avanzata (APT).

Requisiti NIS2	Soluzioni Kaspersky	Vantaggi
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;	 **Kaspersky SD-WAN**	**KASPERSKY SD-WAN** è progettato per creare reti sicure e tolleranti ai guasti con gestione unificata, essenziali per le aziende distribuite di oggi. La soluzione consente di utilizzare diversi canali di comunicazione, ottimizzare le connessioni cloud, aumentare la sicurezza e migliorare le prestazioni delle applicazioni e accelerare l'implementazione di nuovi servizi.
	 Kaspersky Threat Intelligence	**La THREAT INTELLIGENCE KASPERSKY**, permette di accedere a tutte le informazioni necessarie per contrastare o mitigare le minacce informatiche. La profonda conoscenza e l'esperienza che Kaspersky ha acquisito, ottenute in particolare da team composti da ricercatori e analisti leader a livello mondiale, ci hanno reso il partner di fiducia delle principali forze dell'ordine e agenzie governative del mondo, tra cui INTERPOL e i principali CERT. Kaspersky Threat Intelligence offre accesso immediato a informazioni tattiche, operative e strategiche sulle minacce informatiche, permettendo di identificare e prevenire le minacce in modo proattivo, tenendo informati sui rischi e le vulnerabilità più recenti e consentendo di adottare misure proattive per proteggere i vostri sistemi prima che si verifichi un attacco informatico.
	 Kaspersky Managed Detection and Response	**KASPERSKY MANAGED DETECTION AND RESPONSE** offre funzionalità di rilevamento, definizione delle priorità, indagine e risposta continue completamente gestite e personalizzate. Lo scopo principale del servizio MDR è rilevare le minacce in ogni fase di un attacco informatico, sia prima dell'effettiva compromissione sia dopo che gli attori malintenzionati sono penetrati nell'infrastruttura aziendale. Gli analisti SOC indagano sugli avvisi e informano il cliente dell'attività dannosa, fornendo risposte e indicazioni di mitigazione, sulla base di un monitoraggio della sicurezza 24 ore su 24, 7 giorni su 7, potenziato dalla ricerca automatizzata delle minacce, dall'indagine sugli incidenti e dalle risposte guidate e gestite
	 **Kaspersky Scan Engine**	**KASPERSKY SCAN ENGINE (KSEN)** fornisce una protezione completa per portali e applicazioni Web, server proxy, storage collegato in rete e gateway di posta. È facile da gestire e distribuire tramite HTTP e ICAP come servizio autonomo, cluster scalabile o contenitore Docker. KSE utilizza i metodi di rilevamento più recenti per rilevare e rimuovere malware tra cui trojan, minacce di phishing, worm, rootkit, spyware e adware.

Requisiti NIS2	Soluzioni Kaspersky	Vantaggi
2. e) sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informativi e di rete, compresa la gestione e la divulgazione delle vulnerabilità;	**Kaspersky Security Assessment**	Questo servizio fornisce informazioni sulle vulnerabilità esistenti, sulle conseguenze del loro sfruttamento, valuta l'efficacia delle misure di sicurezza implementate e consente di pianificare ulteriori azioni per correggere i difetti rilevati e migliorare la sicurezza. Eseguire regolarmente la security assessment consente di comprendere chiaramente lo status della vostra cybersecurity e garantisce la conformità con le best practices del settore.
	Kaspersky Threat Data Feeds	Integrando nei sistemi di sicurezza esistenti, come ad esempio i sistemi SIEM, SOAR e le piattaforme di Threat Intelligence, feed di Threat Intelligence aggiornati, contenenti informazioni su IP, URL e hash di file sospetti e pericolosi, i team di sicurezza possono automatizzare il processo di triage iniziale e fornire ai relativi specialisti il contesto necessario per identificare immediatamente gli avvisi che richiedono analisi approfondite, o che vanno inoltrati ai team di incident response per ulteriori indagini e risposte. I feed di dati vengono aggregati da fonti altamente affidabili ed eterogenee, quali Kaspersky Security Network e i nostri Web Crawler, il servizio di monitoraggio botnet (monitoraggio 24 ore su 24, 7 giorni su 7, 365 giorni all'anno di botnet e delle relative attività e obiettivi), spam trap, partner e team di ricerca.
	Kaspersky Next	**KASPERSKY NEXT** è la soluzione ideale per proteggere l' infrastruttura da ransomware, malware, minacce evasive e complesse. Sono disponibili funzionalità EDR in ogni livello, personalizzate in base alle tue esigenze e risorse. Le nostre tecnologie EDR e XDR si basano sulla pluripremiata protezione degli endpoint e sui controlli di livello aziendale. Kaspersky Next garantisce una ritrovata efficienza con l'automazione di attività semplici e complesse, insieme alla risposta guidata per aumentare la velocità di risposta agli incidenti e ridurre le risorse necessarie per gestire la sicurezza informatica dell'azienda. Le opzioni cloud e on-premise si adattano a tutti i requisiti delle diverse infrastrutture aziendali.
	Kaspersky Industrial CyberSecurity	**KASPERSKY INDUSTRIAL CYBERSECURITY (KICS)** è una piattaforma nativa di Extended Detection and Response (XDR), appositamente progettata e certificata per proteggere le apparecchiature, gli asset e le reti OT dalle minacce informatiche. La piattaforma comprende tecnologie integrate che proteggono i componenti fondamentali dei sistemi di automazione e controllo industriale a tutti i livelli. KICS for Nodes è un software di protezione con funzionalità EDR e di controllo di conformità, dedicato agli endpoint di un impianto. KICS for Networks è progettato per l'analisi, il rilevamento e la risposta del traffico di rete OT. La funzione di gestione centralizzata a livello di sito, essenziale per scalare le operazioni di sicurezza OT a un volume elevato di infrastrutture industriali grandi, diverse e geo-distribuite, è integrata nella piattaforma. La perfetta integrazione tra i componenti della piattaforma offre una visibilità completa degli impianti OT e dei sistemi di automazione anche se distribuiti geograficamente, migliorando quindi l'esperienza del cliente, la consapevolezza della situazione e la flessibilità di implementazione. Grazie alle funzionalità native di Extended Detection and Response, la piattaforma KICS consente la convergenza IT-OT e offre numerosi vantaggi a un unico fornitore.
	Kaspersky Digital Footprint Intelligence	Questo servizio fornisce informazioni sulle vulnerabilità esistenti, sulle conseguenze del loro sfruttamento, valuta l'efficacia delle misure di sicurezza implementate e consente di pianificare ulteriori azioni per correggere i difetti rilevati e migliorare la sicurezza. Eseguire regolarmente la security assessment consente di comprendere chiaramente lo status della vostra cybersecurity e garantisce la conformità con le best practices del settore.
	Kaspersky Managed Detection and Response	Integrando nei sistemi di sicurezza esistenti, come ad esempio i sistemi SIEM, SOAR e le piattaforme di Threat Intelligence, feed di Threat Intelligence aggiornati, contenenti informazioni su IP, URL e hash di file sospetti e pericolosi, i team di sicurezza possono automatizzare il processo di triage iniziale e fornire ai relativi specialisti il contesto necessario per identificare immediatamente gli avvisi che richiedono analisi approfondite, o che vanno inoltrati ai team di incident response per ulteriori indagini e risposte. I feed di dati vengono aggregati da fonti altamente affidabili ed eterogenee, quali Kaspersky Security Network e i nostri Web Crawler, il servizio di monitoraggio botnet (monitoraggio 24 ore su 24, 7 giorni su 7, 365 giorni all'anno di botnet e delle relative attività e obiettivi), spam trap, partner e team di ricerca.

Requisiti NIS2	Soluzioni Kaspersky	Vantaggi
2. f) strategie e procedure per valutare l'efficacia delle misure di gestione dei rischi di cibersicurezza;	 Kaspersky Digital Footprint Intelligence	**KASPERSKY DIGITAL FOOTPRINT INTELLIGENCE** è un servizio completo di protezione dai rischi digitali che aiuta i clienti a monitorare le proprie risorse digitali e a rilevare le minacce provenienti dal Surface, dal Deep e dal Dark Web. Con avvisi in tempo reale, Kaspersky Digital Footprint Intelligence consente alle organizzazioni di rispondere in modo rapido ed efficace alle potenziali minacce. I report analitici integrano questi dati con l'intelligence completa dei nostri esperti che fornisce approfondimenti sui rischi per la sicurezza informatica e raccomandazioni su come mitigarli.
	 Kaspersky Next	**KASPERSKY NEXT** è la soluzione ideale per proteggere l' infrastruttura da ransomware, malware, minacce evasive e complesse. Sono disponibili funzionalità EDR in ogni livello, personalizzate in base alle tue esigenze e risorse. Le nostre tecnologie EDR e XDR si basano sulla pluripremiata protezione degli endpoint e sui controlli di livello aziendale. Kaspersky Next garantisce una ritrovata efficienza con l'automazione di attività semplici e complesse, insieme alla risposta guidata per aumentare la velocità di risposta agli incidenti e ridurre le risorse necessarie per gestire la sicurezza informatica dell'azienda. Le opzioni cloud e on-premise si adattano a tutti i requisiti delle diverse infrastrutture aziendali.
	 Kaspersky Security Assessment	Questo servizio fornisce informazioni sulle vulnerabilità esistenti, sulle conseguenze del loro sfruttamento, valuta l'efficacia delle misure di sicurezza implementate e consente di pianificare ulteriori azioni per correggere i difetti rilevati e migliorare la sicurezza. Eseguire regolarmente la security assessment consente di comprendere chiaramente lo status della vostra cybersecurity e garantisce la conformità con le best practices del settore.
	 Kaspersky Threat Data Feeds	Integrando nei sistemi di sicurezza esistenti, come ad esempio i sistemi SIEM, SOAR e le piattaforme di Threat Intelligence, feed di Threat Intelligence aggiornati, contenenti informazioni su IP, URL e hash di file sospetti e pericolosi, i team di sicurezza possono automatizzare il processo di triage iniziale e fornire ai relativi specialisti il contesto necessario per identificare immediatamente gli avvisi che richiedono analisi approfondite, o che vanno inoltrati ai team di incident response per ulteriori indagini e risposte. I feed di dati vengono aggregati da fonti altamente affidabili ed eterogenee, quali Kaspersky Security Network e i nostri Web Crawler, il servizio di monitoraggio botnet (monitoraggio 24 ore su 24, 7 giorni su 7, 365 giorni all'anno di botnet e delle relative attività e obiettivi), spam trap, partner e team di ricerca.
	 Kaspersky Industrial CyberSecurity	**KASPERSKY INDUSTRIAL CYBERSECURITY (KICS)** è una piattaforma nativa di Extended Detection and Response (XDR), appositamente progettata e certificata per proteggere le apparecchiature, gli asset e le reti OT dalle minacce informatiche. La piattaforma comprende tecnologie integrate che proteggono i componenti fondamentali dei sistemi di automazione e controllo industriale a tutti i livelli. KICS for Nodes è un software di protezione con funzionalità EDR e di controllo di conformità, dedicato agli endpoint di un impianto. KICS for Networks è progettato per l'analisi, il rilevamento e la risposta del traffico di rete OT. La funzione di gestione centralizzata a livello di sito, essenziale per scalare le operazioni di sicurezza OT a un volume elevato di infrastrutture industriali grandi, diverse e geo-distribuite, è integrata nella piattaforma. La perfetta integrazione tra i componenti della piattaforma offre una visibilità completa degli impianti OT e dei sistemi di automazione anche se distribuiti geograficamente, migliorando quindi l'esperienza del cliente, la consapevolezza della situazione e la flessibilità di implementazione. Grazie alle funzionalità native di Extended Detection and Response, la piattaforma KICS consente la convergenza IT-OT e offre numerosi vantaggi a un unico fornitore.
	 Kaspersky Managed Detection and Response Optimum	**KASPERSKY MANAGED DETECTION AND RESPONSE** offre funzionalità di rilevamento, definizione delle priorità, indagine e risposta continue completamente gestite e personalizzate. Lo scopo principale del servizio MDR è rilevare le minacce in ogni fase di un attacco informatico, sia prima dell'effettiva compromissione sia dopo che gli attori malintenzionati sono penetrati nell'infrastruttura aziendale. Gli analisti SOC indagano sugli avvisi e informano il cliente dell'attività dannosa, fornendo risposte e indicazioni di mitigazione, sulla base di un monitoraggio della sicurezza 24 ore su 24, 7 giorni su 7, potenziato dalla ricerca automatizzata delle minacce, dall'indagine sugli incidenti e dalle risposte guidate e gestite

Requisiti NIS2	Soluzioni Kaspersky	Vantaggi
2. g) pratiche di igiene informatica di base e formazione in materia di cibersicurezza;	Kaspersky Security Awareness	**KASPERSKY SECURITY AWARENESS** è un approccio totalmente nuovo e differente alla formazione e alla padronanza delle competenze di sicurezza informatica. Il portafoglio di Security awareness comprende soluzioni efficaci, collaudate ed apprezzate a livello internazionale. Le soluzioni contentue all'interno del portafoglio, vengono utilizzate da organizzazioni di qualsiasi dimensione e permettono di formare i propri dipendenti grazie all'esperienza di Kaspersky, di oltre 25 anni, nel campo della sicurezza informatica. Grazie al format particolarmente coinvolgente ed efficaci, permettono alle aziende di far accrescere la consapevolezza su tematiche di cybersecurity ai propri dipendenti in modo che tutti facciano la loro parte per contribuire attivamente alla sicurezza informatica dell'organizzazione. Dato che il cambio di postura dei dipendenti richiederà sicuramente del tempo, l'approccio Kaspersky prevede la costruzione di un ciclo di formazione ed apprendimento continuativo e basato su più componenti.
	Kaspersky Cybersecurity Training	**KASPERSKY X TRAINING** è una risposta al panorama delle minacce informatiche in continua evoluzione. Forniamo conoscenze aggiornate su strategie efficaci di rilevamento e mitigazione delle minacce derivanti dalle esperienze complete e ben note del Kaspersky Global Research & Analysis Team (GReAT)
	Kaspersky ICS CERT Training	**KASPERSKY ICS CERT** is a global project established in 2016 to coordinate the efforts of industrial automation system vendors and industrial facility owners and operators. The team includes more than 30 experts in ICS threat and vulnerability research, incident response and security analysis. We provide training in industrial cybersecurity essentials and practical skills to investigate cybersecurity incidents and perform vulnerability research. Our programs are based on the practical experience and real-life cases.The Kaspersky ICS CERT team delivers trainings for different operators of the ICS secotr, starting from field operators up to C-Level, including Cybersecurity professionals dedicated to the OT.
2. h) politiche e procedure relative all'uso della crittografia e, se del caso, della cifratura;	Kaspersky Next	**KASPERSKY NEXT** è la soluzione ideale per proteggere l' infrastruttura da ransomware, malware, minacce evasive e complesse. Sono disponibili funzionalità EDR in ogni livello, personalizzate in base alle tue esigenze e risorse. Le nostre tecnologie EDR e XDR si basano sulla pluripremiata protezione degli endpoint e sui controlli di livello aziendale. Kaspersky Next consente anche la gestione della crittografia dei sistemi Windows, MacOS, attraverso la console di management sia in-Cloud che On-Prem.
2. i) sicurezza delle risorse umane, strategie di controllo dell'accesso e gestione degli attivi;	Kaspersky Managed Detection and Response	**KASPERSKY MANAGED DETECTION AND RESPONSE** offre funzionalità di rilevamento, definizione delle priorità, indagine e risposta continue completamente gestite e personalizzate. Lo scopo principale del servizio MDR è rilevare le minacce in ogni fase di un attacco informatico, sia prima dell'effettiva compromissione sia dopo che gli attori malintenzionati sono penetrati nell'infrastruttura aziendale. Gli analisti SOC indagano sugli avvisi e informano il cliente dell'attività dannosa, fornendo risposte e indicazioni di mitigazione, sulla base di un monitoraggio della sicurezza 24 ore su 24, 7 giorni su 7, potenziato dalla ricerca automatizzata delle minacce, dall'indagine sugli incidenti e dalle risposte guidate e gestite. Tra gli attacchi identificati dal servizio MDR ci sono: i tentativi di brute force sulle credenziali, l'abuso di credenziali amministrative, l'identificazione di sfruttamento di vulnerabilità volte a sottrarre credenziali e il loro utilizzo illecito.
	Kaspersky Digital Footprint Intelligence	**KASPERSKY DIGITAL FOOTPRINT INTELLIGENCE** è un servizio completo di protezione dai rischi digitali che aiuta i clienti a monitorare le proprie risorse digitali e a rilevare le minacce provenienti dal Surface, dal Deep e dal Dark Web. Con avvisi in tempo reale, Kaspersky Digital Footprint Intelligence consente alle organizzazioni di rispondere in modo rapido ed efficace alle potenziali minacce. I report analitici integrano questi dati con l'intelligence completa dei nostri esperti che fornisce approfondimenti sui rischi per la sicurezza informatica e raccomandazioni su come mitigarli. Il servizio monitora i principali forum e mercati del Dark Web allo scopo di intercettare la messa in vendita di credenziali appartenenti all'infrastruttura monitorata, sottratte attraverso compromissioni di varia natura (infostealer, phishing, sfruttamento di vulnerabilità,etc...), in modo da consentire la mitigazione del rischio di un potenziale attacco informatico.

Requisiti NIS2	Soluzioni Kaspersky	Vantaggi
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.	Kaspersky Next	**KASPERSKY NEXT** è la soluzione ideale per proteggere l' infrastruttura da ransomware, malware, minacce evasive e complesse. Sono disponibili funzionalità EDR in ogni livello, personalizzate in base alle tue esigenze e risorse. Le nostre tecnologie EDR e XDR si basano sulla pluripremiata protezione degli endpoint e sui controlli di livello aziendale. Kaspersky Next consente anche la gestione della crittografia dei sistemi Windows, MacOS, attraverso la console di management sia in-Cloud che On-Prem.
	Kaspersky Threat Intelligence	**IL THREAT INTELLIGENCE PORTAL** prevede l'accesso alla piattaforma web e quello tramite Open API
Capo IV, Art. 23, Obblighi di segnalazione		
4. 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; ii) il tipo di minaccia o la causa di fondo che ha probabilmente innescato l'incidente;	Kaspersky Incident Response	Risposta agli incidenti: Il servizio permette di ottenere un quadro dettagliato dell'incidente, coprendo l'intero ciclo di indagine e risposta agli incidenti: dalla risposta iniziale e la raccolta delle prove, all'identificazione di ulteriori tracce di hacking e alla preparazione di un piano di mitigazione degli attacchi.
	Kaspersky Intelligence Reporting	Grazie agli Intelligence Reporting i clienti Kaspersky potranno usufruire dell'accesso costante ed esclusivo alle analisi e ai rilevamenti, inclusi i dati tecnici completi (in un'ampia gamma di formati) sugli attori APT che prendono di mira il vostro settore e la vostra area geografica, imparate a conoscere e contrastare adeguatamente le minacce crimeware e le minacce informatiche che colpiscono le organizzazioni industriali (comprese le minacce che non verranno mai rese pubbliche). I report contengono una sintesi di informazioni immediate e rilevanti che illustrano ogni particolare dell'attacco oltre a offrire una descrizione tecnica dettagliata con le relative regole YARA e IOC, offrendo ai ricercatori di sicurezza, agli analisti malware, ai security engineer, agli analisti di sicurezza di rete e ai ricercatori APT, dati applicabili che consentono una risposta accurata e veloce alle minacce.
	Kaspersky Threat Lookup	**KASPERSKY THREAT LOOKUP** fornisce tutte le conoscenze acquisite da Kaspersky sulle minacce informatiche e sulle relazioni tra di esse, riunite in un unico e potente servizio Web. L'obiettivo è fornire ai team di sicurezza la maggior quantità possibile di dati, per prevenire gli attacchi informatici prima che compromettano l'organizzazione. La piattaforma recupera le informazioni dettagliate più recenti in termini di Threat Intelligence riguardo a URL, domini, indirizzi IP, hash di file, denominazioni delle minacce, dati statistici/comportamentali, dati WHOIS/DNS, attributi di file, dati di geolocalizzazione, catene di download, timestamp. Il risultato è una visibilità globale delle minacce nuove ed emergenti: ciò consente di proteggere al meglio la propria azienda, migliorando sensibilmente qualità ed efficienza delle attività di incident response.
	Kaspersky Threat Analysis	Di fronte a una potenziale minaccia informatica, decidere tempestivamente diventa fondamentale. Oltre alle tecnologie di analisi delle minacce come la sandboxing, **KASPERSKY THREAT ANALYSIS** fornisce tecnologie di attribuzione all'avanguardia (un approccio multilivello che fornisce un'analisi efficiente delle minacce, così è possibile prendere decisioni pienamente informate per difendersi dagli attacchi anche prima che vengano lanciati). Diversi strumenti di analisi delle minacce si combinano per consentire a voi e al vostro team di analizzare la situazione da tutti gli angoli, grazie a un quadro completo del panorama delle minacce e di rispondere in modo rapido ed efficace.

Requisiti NIS2	Soluzioni Kaspersky	Vantaggi
4. 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; ii) il tipo di minaccia o la causa di fondo che ha probabilmente innescato l'incidente;	 Kaspersky Managed Detection and Response	**KASPERSKY MANAGED DETECTION AND RESPONSE** offre funzionalità di rilevamento, definizione delle priorità, indagine e risposta continue completamente gestite e personalizzate. Lo scopo principale del servizio MDR è rilevare le minacce in ogni fase di un attacco informatico, sia prima dell'effettiva compromissione sia dopo che gli attori malintenzionati sono penetrati nell'infrastruttura aziendale. Gli analisti SOC indagano sugli avvisi e informano il cliente dell'attività dannosa, fornendo risposte e indicazioni di mitigazione, sulla base di un monitoraggio della sicurezza 24 ore su 24, 7 giorni su 7, potenziato dalla ricerca automatizzata delle minacce, dall'indagine sugli incidenti e dalle risposte guidate e gestite
	 Kaspersky Endpoint Security and Response	La visibilità limitata e la mancanza di risorse gioca a favore degli autori degli attacchi. Kaspersky Endpoint Detection and Response (EDR) Optimum offre un rilevamento avanzato, funzionalità di indagine semplificate e una risposta automatizzata in un pacchetto facile da usare, per proteggere la vostra azienda dalle minacce più recenti.
	 Kaspersky Endpoint Security and Response	I cyberattacchi stanno diventando sempre più sofisticati e capaci di eludere le misure di sicurezza esistenti. **KASPERSKY ENDPOINT DETECTION AND RESPONSE (EDR)** Expert offre visibilità completa in tutti gli endpoint della rete aziendale e offre difese di livello superiore, automatizzando le attività EDR di routine e consentendo agli analisti di rilevare, assegnare le priorità, analizzare e neutralizzare velocemente minacce complesse e attacchi di tipo APT. Kaspersky EDR Expert utilizza un singolo agente che può essere gestito sia da una singola piattaforma di gestione basata sul cloud che da una console offline in ambienti di tipo "air-gap", sfruttando tecnologie di threat intelligence e integrando strategie di rilevamento personalizzabili.
	 **Kaspersky Extended Detection and Response**	**L' XDR** come una singola piattaforma aperta, uno strumento universale per creare un ecosistema unificato di prodotti di cybersecurity. la piattaforma agisce come una soluzione Anti APT ALL-In-One potenziata dalla Kaspersky Threat Intelligence che controlla tutti i potenziali punti di ingresso dei cybercriminali, correlando le informazioni e orchestrando tutti i componenti di protezione dell'infrastruttura. Kaspersky XDR include un'ampia gamma di integrazioni pronte all'uso, con prodotti Kaspersky e di terze parti
	 Kaspersky Industrial CyberSecurity	**KASPERSKY INDUSTRIAL CYBERSECURITY (KICS)** è una piattaforma nativa di Extended Detection and Response (XDR), appositamente progettata e certificata per proteggere le apparecchiature, gli asset e le reti OT dalle minacce informatiche. La piattaforma comprende tecnologie integrate che proteggono i componenti fondamentali dei sistemi di automazione e controllo industriale a tutti i livelli. KICS for Nodes è un software di protezione con funzionalità EDR e di controllo di conformità, dedicato agli endpoint di un impianto. KICS for Networks è progettato per l'analisi, il rilevamento e la risposta del traffico di rete OT. La funzione di gestione centralizzata a livello di sito, essenziale per scalare le operazioni di sicurezza OT a un volume elevato di infrastrutture industriali grandi, diverse e geo-distribuite, è integrata nella piattaforma. La perfetta integrazione tra i componenti della piattaforma offre una visibilità completa degli impianti OT e dei sistemi di automazione anche se distribuiti geograficamente, migliorando quindi l'esperienza del cliente, la consapevolezza della situazione e la flessibilità di implementazione. Grazie alle funzionalità native di Extended Detection and Response, la piattaforma KICS consente la convergenza IT-OT e offre numerosi vantaggi a un unico fornitore.
	 Kaspersky Container Security	**KASPERSKY CONTAINER SECURITY (KCS)** è una soluzione di sicurezza che copre ogni fase del ciclo di vita di un'app containerizzata, dallo sviluppo al funzionamento. Protegge i processi aziendali della tua organizzazione in linea con gli standard e le normative di sicurezza e supporta l'implementazione dell'approccio DevSecOps. Kaspersky Container Security offre una protezione completa dalle minacce informatiche più recenti e automatizza i controlli di conformità, liberando le risorse del team di sicurezza delle informazioni per concentrarsi su altre attività e riducendo il time-to-market. Kaspersky Container Security è stato sviluppato specificatamente per ambienti containerizzati, garantendo protezione a diversi livelli, dall'immagine del container al sistema operativo host.