ɐr Insurance

Questo Questionario supplementare è applicabile alla copertura CyberEdge®. Ai fini del presente documento, per "Richiedente" si intende la Società

Nome completo del richiedente		
Fatturato/ Margine di intermediazione		

ISTRUZIONI PER LE SEGUENTI SEZIONI:
Nella colonna della risposta, a meno che la domanda non richieda specificamente un "commento" o un numero intero specifico, il menù a tendina consentirà esclusivamente la risposta "SI". Quando il Richiedente lascia una "Risposta" in bianco, questa verrà interpretata come un "no" o "controllo non presente", a meno che non vi sia un'opzione di Risposta che indichi specificamente "No", "Non so" o "Nessuno dei precedenti". Sono disponibili sezioni di commento alla fine di ogni "sezione" che consentiranno al Richiedente, se lo desidera, di fornire commenti aggiuntivi ***(Le sezioni di commento aggiuntive sono limitate a 1.000 caratteri; se è necessario ulteriore spazio, allegare un documento separato come appendice).***

PREGASI NOTARE CHE PER I QUESITI EVIDENZIATI IN VERDE OCCORRE SELEZIONARE TUTTE LE RISPOSTE APPLICABILI, MENTRE PER QUELLI EVIDENZIATI IN GIALLO OCCORRE SELEZIONARE UNA SOLA RISPOSTA

LE DOMANDE SEGUENTI SONO IMPORTANTI PER LA SOTTOSCRIZIONE DELLA COPERTURA PER IL RICHIEDENTE. IL PRESENTE QUESTIONARIO DEVE ESSERE COMPLETATO DA, O CON L'ASSISTENZA DELLA PERSONA O PERSONE RESPONSABILI DELLA SICUREZZA DEI SISTEMI INFORMATIVI DEL RICHIEDENTE. SE LA SICUREZZA DELLE INFORMAZIONI VENISSE ESTERNALIZZATA A

Data Security & Business Continuity

	Domanda	Risposta
DS/BC #1	***Seleziona una risposta:*** come è centralizzato il programma di sicurezza delle informazioni del Richiedente?	
	La sicurezza delle informazioni presso il Richiedente è gestita centralmente e le politiche si applicano a tutte le attività. Laddove vengono fatte eccezioni, è solo per asset (al contrario di "per operazione" / "persona giuridica").	
	La sicurezza delle informazioni presso il Richiedente è gestita centralmente, ma vengono fatte eccezioni per determinate attività / persone giuridiche. I controlli descritti di seguito si applicano ad almeno o più del 98% del totale degli endpoint.	
	La sicurezza delle informazioni presso il Richiedente è gestita centralmente, ma vengono fatte eccezioni per determinate attività / persone giuridiche. I controlli come delineati di seguito si applicano a meno del 98% del totale degli endpoint.	SI
	La sicurezza delle informazioni presso il Richiedente è federata; i controlli descritti di seguito si applicano ad almeno o più del 98% del totale degli endpoint.	
	La sicurezza delle informazioni presso il Richiedente è federata; i controlli descritti di seguito si applicano a più del 50% ma meno del 98% del totale degli endpoint.	
	La sicurezza delle informazioni è gestita da singole persone giuridiche o unità operative. I controlli riportati di seguito si basano su un'indagine su tutte le entità e le unità operative.	
	Altro (rispondere "Si" a destra e fornire maggiori dettagli nella sezione commenti alla fine della presente sezione Data Security & Business Continuity).	
	Non lo so.	
DS/BC # 2	***Seleziona tutte le risposte che sono vere*** **:** Per quanto riguarda la gestione da parte del Richiedente degli asset informatici (hardware e software):	
	Il Richiedente dispone di un inventario di tutte le risorse hardware aziendali - inclusi dispositivi "utente finale", dispositivi di rete, apparecchi, dispositivi IoT e server - che include l'indirizzo di rete (se statico), l'indirizzo hardware, il nome macchina e il titolare dell'asset aziendale e lo aggiorna almeno due volte l'anno.	
	Il Richiedente dispone di un inventario di tutte le risorse hardware aziendali, inclusi dispositivi dell'utente finale, dispositivi di rete, apparecchi, dispositivi IoT e server, che include l'indirizzo di rete (se statico), l'indirizzo hardware, il nome macchina e il proprietario dell'asset aziendale e lo aggiorna almeno annualmente.	
	Il Richiedente ha un processo per scoprire e identificare le risorse hardware sulla sua rete e lo fa almeno quotidianamente.	
	Il Richiedente ha un processo per scoprire e identificare le risorse hardware sulla sua rete e lo fa almeno settimanalmente.	
	Il Richiedente dispone di un processo per aggiornare l'inventario delle risorse hardware almeno settimanalmente basato su strumenti di individuazione o software per la gestione degli indirizzi IP (IPAM).	SI
	Il Richiedente dispone di un inventario di tutto il software concesso in licenza installato sulle risorse aziendali e lo aggiorna almeno due volte all'anno.	
	Il Richiedente ha un processo per verificare/garantire che tutto il software sia o supportato o qualsiasi eccezione sia documentata con l'implementazione di controlli per mitigare il conseguente rischio; il processo è ripetuto almeno mensilmente.	
	Nessuno dei precedenti.	

DS/BC # 3	***Seleziona tutte le risposte che sono vere*** **:** Per quanto riguarda la gestione del Richiedente di "Assets Vitali": gli "**Assets vitali"** sono le risorse fondamentali per il successo e il funzionamento dell'organizzazione, incluse, a titolo esemplificativo ma non esaustivo, le applicazioni che supportano la produzione aziendale, le applicazioni che memorizzano dati business critical e/o sensibili e i servizi tecnologici di base come la directory servizi, archivi di documenti ed e-mail.	
	Il Richiedente dispone di un inventario di tutti gli archivi di dati, incluso il proprietario dei dati, l'asset su cui è memorizzato, la sensibilità, i limiti di conservazione e lo smaltimento requisiti - per almeno tutti i dati sensibili e li aggiorna almeno una volta all'anno.	
	Il Richiedente ha definito e documentato tutti gli "Assets Vitali".	
	Il Richiedente ha un processo per identificare attivamente "Assets Vitali" e aggiornare l'inventario di "Assets Vitali" almeno trimestralmente.	
	Il Richiedente dà la priorità agli "Assets Vitali" in base all'importanza delle operazioni aziendali.	
	Nessuno dei precedenti.	SI
DS/BC # 4	***Qual'è il "Recovery Time Objective" (RTO) per "Assets Vitali"?*** *"RTO" indica la quantità di tempo in cui si prevede che gli "Assets Vitali" siano ripristinati da un'organizzazione dopo un disastro/interruzione.*	
	< 5 ore.	
	5-12 ore.	
	12-24 ore.	
	1-7 giorni.	SI
	> 7 giorn.	
	Nessun RTO è definito/Non so rispondere.	
DS/BC # 5	***Seleziona tutte le risposte vere:*** rispetto alle capacità di **disaster recovery** del Richiedente:	
	Esiste un processo per la creazione di backup (anche se non documentato e/o ad hoc).	SI
	La politica di disaster recovery documentata del Richiedente richiede backup automatici settimanali o più frequenti e degli standard per i backup basati sulla criticità delle informazioni.	
	Almeno trimestralmente, il Richiedente testa la sua capacità di ripristinare diversi " Assets Vitali" in conformità con il Recovery Time Objective (RTO).	
	Nessuno dei precedenti / Non lo so.	
DS/BC # 6	***Seleziona tutte le risposte vere:*** rispetto alle funzionalità di backup del Richiedente:	
	La strategia di backup del Richiedente include backup offline (archivio) conservati in loco.	SI
	La strategia di backup del Richiedente include backup offline (archivio) conservati fuori sede.	SI
	La strategia di backup del Richiedente include backup in loco regolari.	SI
	La strategia di backup del Richiedente include backup fuori sede regolari (Cloud o Continuity del Sito Operativo/Operations Site).	SI
	I backup del Richiedente sono isolati e separati dal dominio di produzione (*cioè, sono accessibili tramite un meccanismo di autenticazione esterno all'Active Directory o sono in altro modo disponibili anche se il dominio di produzione è compromesso*) o sono immutabili.	SI
	Nessuno dei precedenti / Non lo so.	

DS/BC # 7	***Seleziona tutte le risposte che sono vere:*** Rispetto alle politiche del Richiedente per l'uso della crittografia per la protezione dei dati:	
	Il Richiedente richiede che tutti i dati sui dispositivi portatili - inclusi telefoni, tablet e laptop - siano crittografati (utilizzando la crittografia completa del disco o crittografia "basata sul file")	
	Il Richiedente richiede che tutti i dispositivi dell'utente finale - anche se non portatili - contenenti dati sensibili debbano utilizzare la crittografia completa del disco.	
	Il Richiedente richiede che tutti i supporti rimovibili - chiavette USB, CD, ecc. - siano crittografati	
	Il Richiedente richiede che tutti i dati sensibili "conservati/at rest" siano crittografati (a livello di archiviazione o a livello di applicazione).	
	Nessuno dei precedenti / Non lo so.	SI
DS/BC # 8	***Seleziona tutte le risposte che sono vere***: Rispetto al monitoraggio del Richiedente di "Assets Vitali":	
	Il Richiedente ha una funzione, interna e/o esternalizzata a un Managed Security Service Provider ("MSSP"), incaricata di monitorare gli "avvisi/alert" di eventi di sicurezza, inclusi gli avvisi su "Assets Vitali" (un c.d. "Security Operations Center" o "SOC").	
	Al SOC/MSSP del Richiedente viene fornito un elenco aggiornato degli "Assets Vitali" almeno trimestralmente.	
	Il SOC/MSSP del Richiedente utilizza una soluzione SIEM (Security Information and Event Monitoring) per automatizzare la raccolta dei log dagli "Assets Vitali".	
	Nessuno dei precedenti / Non lo so.	SI
	Se il Richiedente ha commenti aggiuntivi su qualsiasi domanda o risposta specifica in questa sezione, si prega di fornirli di seguito:	

Identity, Credential, and Access Management Security

	Domanda	Risposta
ICA # 1	***Selezionare tutte le risposte vere:*** quale dei seguenti strumenti utilizza il Richiedente per i servizi directory, i provider di identità (IdP), la federazione *e/o la gestione dei diritti?*	
	Microsoft Active Directory (Active Directory)	SI
	Azure Active Directory (Azure AD)	
	Okta	
	Ping	
	Active Directory Federation Services	
	Google Workspaces	SI
	Altro (sono richiesti dettagli – pregasi fornire nella riga successiva)	
	Accesso alla rete wirelwss di ateneo mediante autenticazione federata Eduroam.	
	Nessuno dei precedenti / Non so.	
ICA # 2	***Seleziona una risposta*** : qual è lo strumento di identificazione per la maggior parte degli utenti del Richiedente?	
	Microsoft Active Directory (Active Directory)	
	Azure Active Directory (Azure AD)	
	Active Directory and Azure AD (Active Directory è autorevole)	
	Azure AD and Active Directory (Azure AD è autorevole)	

ICA # 2	Un provider di identità ("IdP"; e.g., Okta or Ping)	
	Collaborazione basata su cloud (e.g., Google Workspaces)	
	Altro (dettagli richiesti – fornire nella riga successiva)	
	Sistema di autenticazione di Ateneo basato su LDAP con progressiva migrazione verso frontend di autenticazione basati su Shibboleth	
	Nessuna gestione centralizzata delle identità o non so.	
ICA # 3	***Seleziona tutte le risposte vere*** : Rispetto alla gestione dell'account del Richiedente:	
	Il Richiedente dispone di un inventario di tutti gli account utente e amministrativi.	SI
	L'inventario degli account del Richiedente include il nome dell'individuo, il nome utente, le date di inizio / fine e il dipartimento.	SI
	Il Richiedente, almeno una volta all'anno, verifica che tutti gli account attivi siano autorizzati.	
	Il Richiedente, almeno trimestralmente, verifica che tutti gli account attivi siano autorizzati.	
	Nessuno dei precedenti.	
ICA # 4	***Seleziona tutte le risposte che sono vere*** **:** Rispetto alle politiche del Richiedente e ai controlli tecnici sulle password:	
	Il Richiedente fa formazione agli utenti sui rischi del riutilizzo della password e ha una politica contro di essa.	SI
	Il Richiedente ha una soluzione per impedire agli utenti di impostare password comuni e con violazioni note, anche se soddisfano i requisiti di complessità (per esempio "1q2w3e4r5t" e "Passw0rd!").	SI
	Il Richiedente fornisce un software per la "gestione delle password" ai propri dipendenti.	
	Il Richiedente con riferimento agli account "amministratore locale" ha implementato una soluzione per impostare password diverse e casuali su tutti i computer collegati al dominio (ad esempio, Local Administrator Password Solution - Riferimento: https://support.microsoft.com/en-us/topic/microsoft-security-advisory-local-administrator-password-solution-laps-now-available-may-1-2015-404369c3-ea1e-80ff-1e14-5caafb832f53).	
	Nessuno dei precedenti.	
ICA # 5	***Selezionare tutte le risposte vere:*** per quanto riguarda il modo in cui il Richiedente protegge gli account "utente" con privilegi amministrativi di dominio ("Account amministratore di dominio"): Per "**Account amministratore di dominio**" si intendono gli account utente - esclusi gli "Account di servizio" - che possono modificare le informazioni in qualsiasi soluzione utilizzata dal Richiedente per i servizi di directory, il provider di identità (IdP), la gestione dei diritti, ecc. In un ambiente Active Directory, ciò	
	Gli amministratori di sistema del Richiedente dispongono di una credenziale univoca e privilegiata per le attività amministrative (separata dalle credenziali utente per l'accesso quotidiano, la posta elettronica, ecc.).	
	Gli "Account amministratore di dominio" richiedono l'autenticazione a più fattori.	
	Gli "Account amministratore di dominio" sono gestiti e monitorati tramite accesso "just-in-time", sono limitati nel tempo e richiedono approvazioni per fornire accesso privilegiato.	
	Le credenziali degli "Account amministratore di dominio" sono conservate con una password sicura che richiede all'utente di "estrarre" le stesse credenziali (che vengono ruotate in seguito).	
	Oltre ad essere conservati con una password sicura, gli "Account amministratore di dominio" non vengono esposti all'utente amministratore quando vengono "estratti" e l'accesso viene registrato tramite un gestore di sessione.	
	Gli "Account amministratore di dominio" possono essere utilizzati solo da workstation con accesso privilegiato (workstation che non hanno accesso a Internet o e-mail).	
	Esiste un registro di tutte le azioni da parte di "Account amministratore di dominio" per almeno gli ultimi trenta giorni.	
	Nessuno dei precedenti / Non so.	SI
ICA # 6	***Seleziona una risposta:*** in che modo i dipendenti del Richiedente si autenticano per accedere in remoto alla rete aziendale?	
	L'accesso remoto alla rete aziendale richiede in genere solo un nome utente e una password validi (**autenticazione a fattore singolo**).	
	L'autenticazione a più fattori (**MFA**) è richiesta **per alcuni** tipi di accesso remoto alla rete aziendale, **ma non per tutti** .	SI
	L'autenticazione a più fattori (**MFA**) è richiesta dai criteri **per tutti** gli accessi remoti alla rete aziendale e **tutte le eccezioni** al criterio **sono documentate** .	

	Il Richiedente **non fornisce l'accesso remoto** a nessun dipendente.	
ICA # 7	***Seleziona una risposta*** : Come si autenticano i fornitori del Richiedente per accedere in remoto alla rete aziendale?	
	L'accesso remoto alla rete aziendale richiede in genere solo un nome utente e una password validi (**autenticazione a fattore singolo**).	SI
	L'autenticazione a più fattori (**MFA**) è richiesta **per alcuni** tipi di accesso remoto alla rete aziendale, **ma non per tutti** .	
	L'autenticazione a più fattori (**MFA**) è richiesta dai criteri **per tutti** gli accessi remoti alla rete aziendale e **tutte le eccezioni** al criterio sono documentate.	
	Il Richiedente **non fornisce l'accesso remoto** a nessun fornitore.	
ICA # 8	***Seleziona una risposta:*** in che modo dipendenti e fornitori del Richiedente si autenticano ad applicazioni ospitate in SaaS o di terze parti che possano essere considerati Assets Vitali?	
	L'accesso ad Assets Vitali ospitati esternamente richiede generalmente solo un nome utente e una password validi (**autenticazione a fattore singolo**).	
	L'autenticazione a più fattori è richiesta (MFA) **per alcuni** tipi di accesso a Assets Vitali ospitati esternamente, **ma non per tutti** .	SI
	L'autenticazione a più fattori è richiesta (MFA) **per tutti** gli accessi alle Assets Vitali ospitate esternamente e **tutte le eccezioni** alla politica sono documentate.	
	Il Richiedente non utilizza applicazioni ospitate in SaaS o di terze parti che possano essere considerati Assets Vitali.	
ICA # 9	***Seleziona tutte le risposte vere*** : Per quanto riguarda il modo in cui il Richiedente protegge gli "**Account di servizio privilegiati**": Gli "**account di servizio**" sono account utilizzati per l'esecuzione di applicazioni e altri processi; in genere non vengono utilizzati da persone fisiche salvo che per la risoluzione dei problemi agli stessi inerenti. "Privilegiato" significa che ha privilegi elevati e, in un ambiente Active Directory, la definizione include, ma non è limitata a, Enterprise Admins, Amministratori di Dominio e	
	Esiste un inventario di tutti gli "Account di servizio privilegiati" e viene aggiornato almeno trimestralmente.	
	Gli "Account di servizio" "privilegiati" hanno una lunghezza della password di almeno 25 caratteri.	
	Gli "Account di servizio" "privilegiati" hanno le password ruotate almeno una volta all'anno.	
	Gli "Account di servizio" "privilegiati" hanno le loro password ruotate almeno trimestralmente.	
	Gli "account di servizio" sono suddivisi in livelli (TIER) in modo tale che account diversi vengano utilizzati per interagire con workstation, server e server di autenticazione, anche per lo stesso servizio.	
	Esiste un processo per rivedere almeno una volta all'anno la necessità corrente di ciascun servizio associato agli "Account di servizio privilegiati" e per verificare che il servizio richieda ancora le autorizzazioni di cui dispone l'account del servizio (in caso contrario, è previsto il depotenziamento/perdita dei privilegi).	
	Nessuno dei precedenti / Non lo so.	SI
ICA # 10	***Selezionare una risposta:*** qual è l'**Authenticator Assurance Level (AAL)** che meglio rappresenta le soluzioni di autenticazione del Richiedente. *Pregasi fare riferimento alla pubblicazione speciale NIST 800-63B che definisce i Livelli di garanzia dell'autenticatore NIST (AAL).*	
	AAL1	SI
	AAL2	
	AAL3	
	Non lo so.	
ICA # 11	***Fornire il numero di account attivi che il Richiedente ha per le seguenti categori***e. Gli account non devono includere account inattivi, ma devono includere tutti gli account nidificati aggregati in tutti i domini/foreste.	
	Numero di "Account amministratore di dominio":	5
	Numero di "Account di servizi privilegiati":	15
	NOTA: per ogni "Account di servizio" con "privilegi", utilizzare la tabella fornita alla fine del supplemento per indicare i) il nome dell'account, ii) i privilegi di cui dispone, iii) il software che supporta, iv) a cosa ospita l'account del servizio e v) perché tali diritti sono richiesti/necessari.	
	Seleziona una risposta : quale definizione di seguito riflette meglio la posizione del Richiedente rispetto ai controlli di accesso per la workstation di ciascun utente? Ai fini della presente domanda, quando il Richiedente utilizza una soluzione per la "gestione dei privilegi dell'endpoint" o altra tecnologia simile per consentire agli utenti di richiedere temporaneamente l'accesso amministrativo per determinate attività, queste non devono essere considerate come "Accesso Amministratore".	
	Nessun account regolare, giornaliero, dell'utente è nel gruppo dell'amministratore o ha accesso come amministratore locale alla propria workstation.	

ICA # 12	La politica del Richiedente è che i dipendenti per impostazione predefinita non sono nel gruppo Amministratori e non hanno accesso amministrativo locale; tutte le eccezioni al criterio sono documentati.	
	Alcuni dei dipendenti del Richiedente fanno parte del gruppo Amministratori o sono amministratori locali.	SI
	Non lo so.	
ICA # 13	***Seleziona una risposta:*** quale descrizione riflette meglio la posizione del Richiedente rispetto ai controlli di accesso per i server membri? *Questa domanda riguarda gli account utente quotidiani dei dipendenti; quando il Richiedente fornisce ai dipendenti credenziali separate per accesso amministrativo, tali account non dovrebbero essere presi in considerazione ai fini della presente Domanda.*	
	Nessun dipendente fa parte del gruppo dell'amministratore o ha accesso amministrativo locale ai server membri.	
	La politica del Richiedente è che i dipendenti per impostazione predefinita non sono nel gruppo Amministratori e non hanno accesso amministrativo locale; tutte le eccezioni al criterio	
	sono documentate.	
	Alcuni dei dipendenti del Richiedente fanno parte del gruppo Amministratori o sono amministratori locali.	SI
	Non lo so.	
ICA # 14	***Quanti utenti del Richiedente hanno accesso amministrativo persistente a server e/o postazioni di lavoro diversi dal proprio?*** Ai fini della presente domanda, per "accesso amministrativo" si intendono i diritti di configurare, gestire e supportare in altro modo tali endpoint, anche attraverso l'uso di un account amministrativo univoco (separato dal proprio account utente quotidiano). Utenti che devono "estrarre" le credenziali per l'amministrazione *l'accesso non deve essere incluso.*	
	Inserisci un numero intero:	50
ICA # 15	***Il Richiedente raccoglie i registri di sicurezza da tutti i controller di dominio nella propria soluzione SIEM per l'analisi?***	
	Si	
	No: il Richiedente non dispone di un SIEM o non inserisce i registri di sicurezza in un SIEM	SI
	Non applicabile - non utilizza servizi directory, IdP, rights management.	
ICA # 16	***Selezionare tutte le risposte vere:*** quali criteri di controllo ha abilitato il Richiedente nei controller di dominio?	
	Convalida delle ***credenziali di controllo*** (esito negativo)	SI
	Creazione del processo di ***audit/controllo*** (esito positivo)	SI
	Controllo della Gestione del ***Gruppo di Sicurezza*** (esito positivo e negativo)	SI
	Controllo della gestione dell' ***account utente*** (esito positivo e negativo)	SI
	Controllo della gestione ***eventi di altri account*** (esito positivo e negativo)	
	Controllo dell' ***utilizzo dei privilegi sensibili*** (esito positivo e negativo)	
	Controllo degli ***Accessi*** (esito positivo e negativo)	SI
	Controllo delle modalità di ***Accesso speciale*** (esito positivo)	
	Nessuno dei precedenti / Non lo so.	
	Non applicabile (non utilizza Active Directory).	

	Se il Richiedente ha commenti aggiuntivi su qualsiasi domanda o risposta specifica in questa sezione, si prega di fornirli di seguito:	

Security Monitoring and Incident Response

	Domanda	Risposta

SMIR # 1	***Seleziona una risposta:*** quale descrizione riflette meglio il programma per la gestione della **sicurezza operativa** del Richiedente?	
	Il Richiedente non ha nessuno (interno o esterno) dedicato al monitoraggio delle operazioni di sicurezza (un "Security Operations Center" o SOC).	
	Il Richiedente ha un SOC, ma non è 24 ore su 24, 7 giorni su 7 (può essere interno o esterno).	SI
	Il Richiedente ha un monitoraggio 24 ore su 24, 7 giorni su 7, delle operazioni di sicurezza da parte di una terza parte (per esempio un Managed Security Service Provider).	
	Il Richiedente ha un monitoraggio 24 ore su 24, 7 giorni su 7 delle operazioni di sicurezza internamente (indipendentemente dal fatto che venga utilizzata o meno anche una terza parte).	
SMIR # 2	***Seleziona tutte le risposte che sono vere:*** rispetto alle capacità di sicurezza e monitoraggio della rete del Richiedente:	
	Il Richiedente utilizza uno strumento "Security Information and Event Monitoring" c.d. SIEM per correlare l'output di più strumenti di sicurezza.	SI
	Il Richiedente monitora il traffico di rete per trasferimenti di dati anomali e potenzialmente sospetti.	SI
	Il Richiedente monitora i problemi di prestazioni e capacità di archiviazione su tutti i server (es. utilizzo elevato della memoria o del processore o nessun spazio libero su disco).	SI
	Il Richiedente ha strumenti per monitorare la perdita di dati (DLP) e sono in modalità di blocco.	
	Il Richiedente dispone di strumenti per monitorare la perdita di dati (DLP), ma non sono in modalità di blocco.	
	Nessuno dei precedenti / Non lo so.	
SMIR # 3	***Qual è stato il tempo medio del Richiedente per valutare e contenere gli incidenti di sicurezza delle workstation per l'ultimo trimestre completato?***	
	<30 minuti	
	30 minuti-2 ore	
	2-8 ore	
	8 ore-3 giorni	
	>3 giorni	
	Il Richiedente non tiene traccia di questa metrica / Non lo so.	SI
SMIR # 4	***Quale percentuale delle "Assets Vitali" del Richiedente viene registrata e inoltrata a una soluzione SIEM?***	
	0-30%	SI
	31-50%	
	51-70%	
	>= 71%	

	Non lo so	
	Non applicabile (nessun SIEM)	
SMIR # 5	***Per quanto tempo la soluzione SIEM del Richiedente conserva i registri?***	
	Meno di 30 giorni	
	30-59 giorni	
	60-89 giorni	SI
	90 giorni o più	
	Non lo so	
	Non applicabile (nessun SIEM)	
SMIR # 6	***Seleziona tutte le risposte che sono vere*** : Con riferimento alle modalità con cui il Richiedente convalida l'efficienza e l'efficacia dei controlli di sicurezza:	
	Il Richiedente utilizza software di Breach and Attack Simulation (BAS) per verificare l'efficacia dei controlli di sicurezza.	
	Il Richiedente ha un "red team" in staff per testare i controlli di sicurezza, o almeno annualmente ingaggia esperti per eseguire un test di penetrazione incentrato sui Sistemi interni.	
	Il Richiedente ha ingaggiato una parte esterna per simulare gli attori delle minacce e testare i controlli di sicurezza nell'ultimo anno.	
	Nessuno dei precedenti.	
SMIR # 7	***Seleziona tutte le risposte vere*** : rispetto al programma e alle procedure di risposta agli incidenti del Richiedente:	
	Il Richiedente ha un piano di risposta agli incidenti documentato.	SI
	Il piano di risposta agli incidenti del Richiedente include un playbook specifico per l'eventualità di un incidente ransomware presso l'organizzazione.	
	Il piano di risposta agli incidenti del Richiedente include un playbook specifico per l'eventualità di un incidente ransomware a una terza parte / MSP.	
	Il piano di risposta agli incidenti del Richiedente include informare le forze dell'ordine una volta che sia confermato un incidente ransomware.	SI
	Il piano di risposta del Richiedente include un processo per ristabilire le operazioni aziendali mediante il ripristino da c.d. backup noto come "pulito".	
	Nessuno dei precedenti.	
SMIR # 8	***Il Richiedente dispone di un processo documentato per rispondere agli incidenti di phishing (sia che si rivolga specificamente al Richiedente o ai suoi dipendenti, oppure no)?***	
	Si	
	No	SI

	Se il Richiedente ha commenti aggiuntivi su qualsiasi domanda o risposta specifica in questa sezione, si prega di fornirli di seguito:	

Risk Management

	Domanda	Risposta
RM # 1	***Il Richiedente dispone di un programma di scansione delle vulnerabilità che identifica e gestisce le vulnerabilità in "Assets Vitali"?***	
	Si	SI
	No	
RM # 2	***Selezionare tutte le risposte vere:*** in relazione ai fattori utilizzati dal Richiedente per dare priorità alle patch:	
	Common Vulnerability Scoring System (CVSS) score.	SI
	Correlazione con il fatto che la vulnerabilità influenzi gli "Assets Vitali" del Richiedente.	SI
	Threat Intelligence generica (ad esempio, che gli attori delle minacce stanno sfruttando una determinata vulnerabilità; questo include strumenti come il Known Exploited Vulnerability Catalog del CISA).	SI
	Threat Intelligence specifica per il Richiedente (compresa l'attività di intelligence su attori malevoli che potrebbero prendere di mira il Richiedente attraverso lo sfruttamento, in particolare, di una determinata vulnerabilità, o dati dall'ambiente del Richiedente che indichino dove siano concentrati gli attori malevoli).	SI
	Nessuno dei precedenti / Non lo so.	
RM # 3	***Qual è il tempo "target" che il Richiedente si è dato per distribuire le patch critiche (che hanno la massima priorità)*** ?	
	Entro 24 ore.	
	24-72 ore.	
	3-7 giorni.	
	7-29 giorni.	
	>= 30 giorni.	
	Non esiste un criterio definito che fissa entro quanto le patch devono essere distribuite/Non so.	
RM # 4	***Qual è il tasso di conformità del Richiedente ai propri standard per l'implementazione delle patch critiche nell'ultimo trimestre completato?***	
	>95%	
	90-95%	

RM # 4	80-89%	
	<80%	
	Non tracciato/Non so.	SI
RM # 5	***Seleziona tutte le risposte vere:*** Rispetto alle politiche del Richiedente per l'utilizzo delle risorse IT organizzative:	
	Il Richiedente ha una "**Politica di utilizzo accettabile** " (AUP) che delinea gli obblighi e i vincoli degli utenti.	SI
	L'AUP descrive le conseguenze per le violazioni della politica.	SI
	Agli utenti non è consentito navigare su piattaforme di social media dalle risorse organizzative, tranne nei casi in cui si tratti di un'esigenza aziendale definita.	
	Agli utenti non è consentito accedere alla posta elettronica personale dalle risorse dell'organizzazione.	
	Agli amministratori è esplicitamente vietato navigare in Internet o accedere alla posta elettronica personale dai loro account privilegiati.	
	Gli utenti e gli amministratori sono responsabili di mantenere il computer e gli account al sicuro da rischi o problemi comuni.	SI
	Gli utenti e gli amministratori sono tenuti a segnalare violazioni sospette.	SI
	Nessuno dei precedenti / Non lo so.	
RM # 6	***Seleziona tutte le risposte che son o vere:*** rispetto alle capacità del Richiedente di monitorare comportamenti rischiosi e insider (soggetti con accesso a informazioni privilegiate) malintenzionati:	
	Il Richiedente ha un programma per la gestione di minacce interne.	
	Il Richiedente monitora quando un account utente o amministratore imposta una password non sicura.	SI
	Il Richiedente monitora quando gli account "privilegiati" accedono a siti Web e servizi non autorizzati.	SI
	Il Richiedente monitora l'accesso remoto non autorizzato a "Assets Vitali".	
	Il Richiedente monitora sia gli account utente che quelli amministratore che instaurino una comunicazione con siti Web noti come dannosi, indirizzi IP e altre risorse di gruppi che è notorio costituiscano una minaccia.	SI
	Nessuno dei precedenti / Non lo so.	

	Se il Richiedente ha qualsiasi commento aggiuntivo su qualsiasi domanda o risposta specifica in questa sezione, si prega di fornirli di seguito:	

Phishing Defense

	Domanda	Risposta
PhD # 1	***Seleziona tutte le risposte che sono vere*** **:** rispetto alle capacità del Richiedente per mitigare gli incidenti di phishing:	
	Il candidato fornisce una formazione sulla consapevolezza della sicurezza, compresa la formazione sulla consapevolezza del phishing, ai dipendenti almeno una volta all'anno.	SI
	Il candidato utilizza attacchi di phishing simulati per testare la consapevolezza della sicurezza informatica dei dipendenti almeno una volta all'anno.	SI
	Se il Richiedente sta conducendo attacchi di phishing simulati, il tasso di successo è stato inferiore al 15% nell'ultimo test (meno del 15% dei dipendenti sono stati oggetto di phishing con successo).	
	Il Richiedente "tagga" o contrassegna in altro modo le e-mail dall'esterno dell'organizzazione.	SI
	Il Richiedente dispone di un processo documentato per segnalare e-mail sospette a un team di sicurezza interno per indagare e pubblicare il processo agli utenti.	SI
	Nessuno dei precedenti / Non lo so.	
PhD # 2	***Seleziona tutte le risposte che sono vere:*** rispetto alle capacità del Richiedente di bloccare siti Web e / o e-mail potenzialmente dannosi:	
	Il Richiedente utilizza una soluzione di filtraggio della posta elettronica che blocca gli allegati dannosi noti e i tipi di file sospetti, inclusi gli eseguibili.	SI
	Il Richiedente utilizza una soluzione di filtraggio della posta elettronica che blocca i messaggi sospetti in base al loro contenuto o agli attributi del mittente.	SI
	Il Richiedente utilizza una soluzione di filtraggio web che impedisce ai dipendenti di visitare pagine Web dannose o sospette note.	SI
	Il Richiedente blocca i domini non categorizzati e appena registrati utilizzando proxy Web o filtri DNS.	SI
	Il Richiedente utilizza una soluzione di filtraggio Web che blocca i download dannosi o sospetti noti, inclusi gli eseguibili.	SI
	La soluzione di filtraggio della posta elettronica del Richiedente ha la capacità di eseguire allegati sospetti in una sandbox.	
	Le funzionalità di filtraggio Web del Richiedente sono efficaci su tutte le risorse dell'organizzazione, anche se la risorsa non è sulla rete dell'organizzazione (ad esempio, le risorse sono configurate per utilizzare filtri Web basati su cloud o richiedere una connessione VPN per navigare in Internet).	
	Nessuno dei precedenti / Non lo so.	

	Se il Richiedente ha commenti aggiuntivi su qualsiasi domanda o risposta specifica in questa sezione, si prega di fornirli di seguito:	
	La prima simulazione di phishing è stata prigrammata ma non ancora completata per cui i risultati non sono ancora disponibili	

Malware defense

	Domanda	Risposta
	Seleziona tutte le risposte vere: rispetto alle funzionalità dello strumento di sicurezza degli endpoint del Richiedente:	

Mal # 1	La soluzione di sicurezza degli endpoint del Richiedente include antivirus con funzionalità euristiche.	SI
	Il Richiedente utilizza strumenti di sicurezza degli endpoint con funzionalità di rilevamento comportamentale e mitigazione degli exploit.	
	Il Richiedente utilizza uno strumento di rilevamento e risposta alle minacce endpoint (ETDR o EDR) che esegue tutte le seguenti operazioni: monitora gli indicatori di minaccia; identifica i modelli che corrispondono alle minacce note; risponde automaticamente rimuovendo o contenendo minacce; avvisa il personale di sicurezza di incidenti; fornisce funzionalità forensi e di analisi per consentire agli analisti di eseguire attività di caccia alle minacce.	
	Il Richiedente implementa i controlli delle applicazioni su tutte le workstation per consentire solo l'esecuzione di applicazioni autorizzate. Le applicazioni non autorizzate vengono bloccate e l'elenco delle applicazioni autorizzate viene rivalutato almenodue volte all'anno.	
	Il Richiedente ha un gruppo interno e/o MSSP che monitora l'output degli strumenti di sicurezza degli endpoint e indaga su eventuali anomalie.	
	Nessuno dei precedenti / Non lo so.	
Mal # 2	***Selezionare tutte le risposte vere:*** in relazione alla distribuzione da parte del Richiedente dei propri strumenti di sicurezza degli endpoint (come descritto sopra):	
	Gli strumenti di sicurezza degli endpoint del Richiedente sono distribuiti su tutte le workstation e laptop; tutte le eccezioni sono documentate.	
	Gli strumenti di sicurezza degli endpoint del Richiedente sono distribuiti su tutti i server (esclusi gli host hypervisor); tutte le eccezioni sono documentate.	SI
	Gli strumenti di sicurezza degli endpoint del Richiedente sono distribuiti su tutti i dispositivi mobili (inclusi tablet, telefoni, ecc., ma escludono i laptop); tutte le eccezioni sono documentate.	
	Nessuno dei precedenti / Non lo so.	
Mal # 3	***Seleziona tutte le risposte che sono vere*** **:** rispetto alla configurazione del Richiedente dei suoi strumenti di sicurezza degli endpoint (come descritto sopra):	
	Per quegli strumenti che richiedono definizioni aggiornate, tali strumenti sono aggiornati almeno quotidianamente.	SI
	Gli strumenti sono configurati per bloccare (anziché notificare) processi/file sospetti dannosi.	SI
	Gli strumenti sono configurati per trovare risorse non gestite, che vengono affrontate almeno settimanalmente.	
	Le funzioni anti-manomissione sono abilitate.	
	Nessuno dei precedenti / Non lo so.	
Mal # 4	***Identificare gli strumenti di sicurezza utilizzati sugli endpoint (si prega di essere il più specifici possibile, ad esempio "Falcon Prevent, Insight and Overwatch", non genericamente "CrowdStrike"):***	
	Sophos Cloud Antivirus installato solo su circa un terzo delle workstation globali che accedono alla rete di ateneo	
Mal # 5	***Seleziona tutte le risposte che sono vere*** **:** Rispetto alle capacità del Richiedente di limitare il movimento laterale:	
	Il Richiedente ha segmentato la rete in base all'area geografica (ad esempio, il traffico tra uffici in località diverse è negato a meno che non sia richiesto per supportare un requisito aziendale specifico).	
	Il Richiedente ha segmentato la rete per funzione aziendale (cioè, traffico tra asset che supportano diverse funzioni - HR e Finance per esempio - viene negato a meno che non sia necessario per supportare un requisito aziendale specifico).	
	Il Richiedente ha implementato regole firewall host che impediscono l'uso di RDP per accedere alle workstation.	SI
	Il Richiedente ha configurato tutti gli account di servizio per negare gli accessi interattivi.	

	Nessuno dei precedenti / Non lo so.	
Mal # 6	***Il Richiedente ha condotto un esercizio che simula le tattiche, le tecniche e le procedure degli attori del ransomware nell'ultimo anno ?***	
	Si	
	No	SI

	Se il Richiedente ha commenti aggiuntivi su qualsiasi domanda o risposta specifica in questa sezione, si prega di fornirli di seguito:	

Third Parties & Managed Service Providers Defense

	Domanda	Risposta
TP & MSP # 1	***Selezionare tutte le risposte vere :*** rispetto ai ruoli di terze parti o Managed Service Provider (MSP) per la rete del Richiedente, incluso l'accesso remoto a risorse come cloud e VPN.	
	Il Richiedente utilizza un MSP per l'amministrazione di "Assets Vitali".	
	Il Richiedente utilizza un MSP per le operazioni di sicurezza.	
	Il Richiedente utilizza un MSP per il backup e il ripristino dei dati.	
	Il Richiedente utilizza un MSP per la trasformazione verso il cloud (cloud transformation).	
	Il Richiedente utilizza un MSP per lo sviluppo del software.	
	Il Richiedente fornisce a terzi un accesso persistente ("sempre attivo") alle risorse aziendali (l'accesso non richiede l'autorizzazione del Richiedente).	SI
	Nessuno dei precedenti / Non lo so.	
TP & MSP # 2	***Il Richiedente dispone di un processo o di una soluzione tecnica per identificare, valutare, gestire, monitorare e ridurre i rischi derivanti da MSP e terze parti?***	
	Si	
	No	SI

	Se il Richiedente ha commenti aggiuntivi su qualsiasi domanda o risposta specifica in questa sezione, si prega di fornirli di seguito:	

Perimeter and Internet Defense

	Domanda	Risposta
Perimeter # 1	***Seleziona tutte le risposte che sono* vere:** rispetto alle capacità del Richiedente di proteggere i sistemi esposti verso l'esterno, inclusi i sistemi esposti su Internet:	
	Il Richiedente mantiene un inventario degli Assets esposti verso l'esterno.	SI
	Il Richiedente esegue scansioni di vulnerabilità regolari degli Assets esposti verso l'esterno.	SI
	Il Richiedente dispone di un Web Application Firewall (WAF) per tutte le applicazioni esposte verso l'esterno ed è in modalità di blocco.	
	Il Richiedente esegue la scansione delle risorse esposte verso l'esterno alla ricerca di vulnerabilità almeno una volta al mese.	
	Il Richiedente utilizza un servizio esterno per monitorare la sua superficie di attacco (sistemi connessi a Internet).	SI
	Il Richiedente disabilita o blocca sui sistemi esposti verso l'esterno quelle porte, servizi e protocolli noti per consentire la diffusione di ransomware, inclusi, a titolo esemplificativo ma non esaustivo, RDP, SMBv1 e SMBv2.	SI
	Gli Asset del Richiedente esposti verso l'esterno sono segmentati all'interno di una zona demilitarizzata (DMZ); la DMZ non è direttamente indirizzabile alla rete della società. Gli utenti che richiedono l'accesso ai servizi DMZ vengono indirizzati su Internet per l'accesso.	SI
	Il Richiedente può rilevare e rispondere alle minacce attraverso soluzioni di monitoraggio degli endpoint e delle reti.	
	Nessuno dei precedenti / Non so.	

	Se il Richiedente ha commenti aggiuntivi su qualsiasi domanda o risposta specifica in questa sezione, si prega di fornirli di seguito:	

"Privileged" "Service Account" Appendix (if applicable)

Per ogni "Account di servizio privilegiato", utilizzare la tabella fornita per indicare:

Appendice "Account di servizio" "Privilegiato"

Nome dell'account	Privilegi che ha	Prodotto software supportato	Su quale HOST si Autentica	Perché questi diritti sono richiesti
SOLO A TITOLO DI ESEMPIO svc_cyberark	*SOLO A TITOLO DI* ESEMPIO: *Amministratore di dominio*	*SOLO A TITOLO DI ESEMPIO CyberArk Privileged Access Manager*	*SOLO A TITOLO DI ESEMPIO Esclusivamente controller di dominio*	*SOLO A TITOLO DI ESEMPIO DA richiesto per modificare le password degli account sensibili*
	Choose an item.		Choose an item.	
	Choose an item.		Choose an item.	
	Choose an item.		Choose an item.	
	Choose an item.		Choose an item.	
	Choose an item.		Choose an item.	

	Choose an item.		Choose an item.	
	Choose an item.		Choose an item.	
	Choose an item.		Choose an item.	
	Choose an item.		Choose an item.	
	Choose an item.		Choose an item.	
	Choose an item.		Choose an item.	
	Choose an item.		Choose an item.	
	Choose an item.		Choose an item.	
	Choose an item.		Choose an item.	
	Choose an item.		Choose an item.	
	Choose an item.		Choose an item.	
	Choose an item.		Choose an item.	
	Choose an item.		Choose an item.	
	Choose an item.		Choose an item.	
	Choose an item.		Choose an item.	
	Choose an item.		Choose an item.	
	Choose an item.		Choose an item.	
	Choose an item.		Choose an item.	
	Choose an item.		Choose an item.	
	Choose an item.		Choose an item.	
	Choose an item.		Choose an item.	
	Choose an item.		Choose an item.	
	Choose an item.		Choose an item.	
	Choose an item.		Choose an item.	
	Choose an item.		Choose an item.	

QUESTO QUESTIONARIO SUPPLEMENTARE È DA INTENDERSI INCORPORATO E PARTE INTEGRANTE DEL QUESTIONARIO CYBEREDGE COMPILATO DAL RICHIEDENTE.

TUTTE LE DICHIARAZIONI E LE GARANZIE RESE DAL RICHIEDENTE IN RELAZIONE AL QUESTIONARIO CYBEREDGESI INTENDONO RIFERITE ANCHE ALLE INFORMAZIONI FORNITE NEL PRESENTE QUESTIONARIO SUPPLEMENTARE.

IL RICHIEDENTE È CONSAPEVOLE CHE QUALSIASI POLIZZA EMESSA DALL'ASSICURATORE SI BASA SULLE DICHIARAZIONI CONTENUTE NEL PRESENTE QUESTIONARIO SUPPLEMENTARE IL QUALE POTRÀ ESSERE INCORPORATO PER RIFERIMENTO NELLA POLIZZA.

LE RISPOSTE RELATIVE ALLE DOMANDE CONTENUTE NEL PRESENTE QUESTIONARIO SUPPLEMENTARE SONO CONSIDERATE DI PRIMARIA IMPORTANZA PER LA COMPAGNIA DI ASSICURAZIONE, SIA NELL'IPOTESI IN CUI IL PRESENTE QUESTIONARIO SIA INCORPORATO NELLA POLIZZA SIA IN OGNI ALTRO CASO.

A TALI DOMANDE DOVRÀ QUINDI ESSERE DATA RISPOSTA SOLO DOPO AVER ESPERITO UN ATTENTO E COMPLETO ESAME DELLA PROPRIA ATTIVITÀ. SI PREGA PERTANTO DI INDICARE QUALSIASI FATTO O CIRCOSTANZA CHE POSSA ASSUMERE RILEVANZA AI FINI DELLA VALUTAZIONE DEL RISCHIO DA PARTE DEGLI ASSICURATORI IN QUANTO, AI SENSI E PER GLI EFFETTI DEGLI ARTT. 1892, 1893 E 1894 DEL CODICE CIVILE, LE DICHIARAZIONI INESATTE O INCOMPLETE E LE RETICENZE IN MERITO AL RISCHIO OGGETTO DI ASSICURAZIONE, POSSONO COMPORTARE L'ANNULLAMENTO DEL CONTRATTO O, COMUNQUE, LA PERDITA PARZIALE O TOTALE DELL'INENNIZZO DA PARTE DEL RICHIEDENTE.

IL SOTTOSCRITTO DICHIARA DI ESSERE UN RAPPRESENTANTE DEBITAMENTE AUTORIZZATO DEL RICHIEDENTE E DI ESSERE PIENAMENTE AUTORIZZATO A RISPONDERE ED A RILASCIAREAFFERMAZIONI E DICHIARAZIONI IN NOME E PER CONTO DEL RICHIEDENTE.
