SOLUZIONI DI CYBER RESILIENCE DI IBM: Safeguarded Copy, Security QRadar EDR, Security Guardium Data Protection

Progetto realizzato per SILC SPA

mauden
A RICOH Company

DOCUMENTO CONFIDENZIALE

SILC SPA IN BREVE

SILC SPA – Società Italiana Lavorazione Cellulosa

SILC SPA, azienda italiana nata nel 1972 con headquarter a Trescore Cremasco (CR), è specializzata nella produzione di prodotti assorbenti e per l'igiene della persona. Si contraddistingue per la completezza della gamma, in grado di coprire l'intera categoria dei prodotti assorbenti ed igienici destinati a bambini, donne, anziani ed animali da compagnia.

L'attività produttiva si sviluppa su un'area di circa 60.000 m², di cui 30.000 coperti, grazie a 23 linee di produzione e più di 300 addetti ed 80 agenti. Oltre agli impianti produttivi, SILC SPA dispone di spazi – dedicati soprattutto alla logistica – a Trescore, Vaiano Cremasco, Casaletto Vaprio (CR), Melegnano ed Origgio (VA).

L'azienda da anni si impegna attivamente nella riduzione dell'impronta ecologica, promuovendo iniziative e scelte produttive volte al miglioramento continuo. Questo impegno è sostenuto da un rating ESG e da un costante monitoraggio delle tematiche ambientali, sociali, di genere, di inclusione e di governance.

SILC SPA – LE ESIGENZE

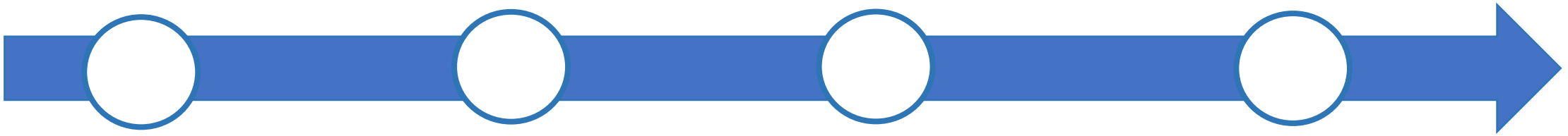
SILC SPA è consapevole della necessità di proteggere la propria rete, in quanto sarebbe un errore pensare all'infrastruttura IT come un sistema isolato e separato rispetto al business aziendale.

La rete di distribuzione dei prodotti di SILC SPA (es. pannoloni, dispositivi e presidi medici, …) include anche il servizio di fornitura domiciliale a migliaia pazienti, le attività di e-commerce anche su piattaforma interna, la distribuzione ai supermercati, 3000 farmacie dirette e centinaia di case di riposo. Gestisce oltre 7.000 posizioni dotate di rating, di cui oltre 5.000 con anche informazioni di antiriciclaggio, in una logica di presidio del rischio non per obblighi di legge. Quotidianamente l'azienda accede, quindi, ad un ammontare importante di dati sensibili, di diversa origine e tipologia e concede l'accesso in modo sicuro anche a centinaia di utenti esterni che operano per conto degli enti con cui esistono contratti di appalto.

Per SILC SPA è strategico aumentare il livello di sicurezza dei propri sistemi IT, all'interno di un percorso di modernizzazione avviato da tempo. Nel dettaglio, l'obiettivo del cliente è di implementare la cyber resilience della sua infrastruttura disponendo di copie affidabili, immutate, isolate e granulari dei dati di produzione in caso di attacchi ransomware o di altre criticità. Inoltre, monitorare l'accesso ai dati sensibili in tutti gli stati e in tutti gli ambienti, controllare costantemente gli endpoint aziendali.

SILC SPA ha scelto **IBM Safeguarded Copy** per la parte Storage DS8910, **IBM Guardium Data Protection** per il monitoraggio dell'accesso ai dati, e **IBM Security QRadar EDR** per il controllo degli endpoint.

IBM SAFEGUARDED COPY – COPIE PROTETTE



Una **sessione di copia protetta** crea un gruppo di coerenza tra i volumi di origine per avere un **backup protetto**

La **capacità di backup** memorizza i dati richiesti secondo la frequenza desiderata

I **sistemi di produzione** possono continuare a funzionare, mentre accedono alla copia di backup sul volume di ripristino

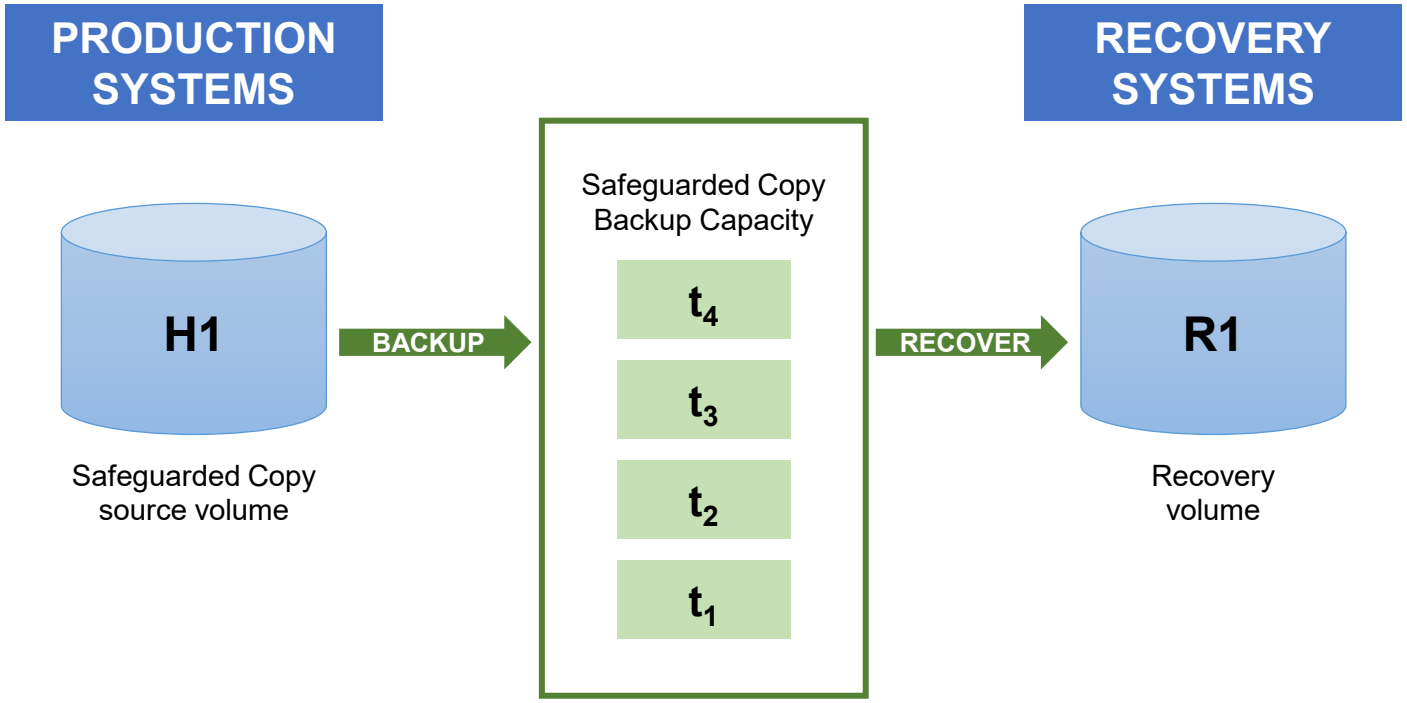
La **copia in background opzionale** assicura che tutti i dati necessari vengano copiati dalla capacità di backup

IBM Safeguarded Copy permette di allocare la capacità di backup con spazio sufficiente a soddisfare gli accordi sul livello di servizio (SLA) per la frequenza e la conservazione dei backup.

L'utilizzo di un pianificatore interno in **Copy Services Manager** consente di eseguire i backup alla frequenza desiderata. Per SILC SPA sono previste 3 copie giornaliere per 7 giorni lavorativi di retention del dato, per un totale di 21 snapshot settimanali. Il volume di origine per le relazioni di copia protetta è situato nello stesso sottosistema disco DS8910F.

IBM SAFEGUARDED COPY – BACKUP E RIPRISTINO

- i **dati di backup** possono essere utilizzati solo dopo il loro ripristino, da effettuare soltanto su un volume di ripristino separato
- il **volume di ripristino separato** fornisce una protezione aggiuntiva, per evitare che i volumi di backup vengano compromessi
- non è possibile eseguire un ripristino direttamente sul volume di origine della copia protetta



IBM SECURITY GUARDIUM DATA PROTECTION

SILC SPA ha tra le sue divisioni una che si interagisce con il settore pubblico per la fornitura di prodotti a strutture sanitarie e consegne domiciliari presso i pazienti, tramite gare d'appalto. Questa attività implica la gestione di dati sensibili da proteggere e governare con il massimo livello di sicurezza.

Il cliente ha scelto **IBM Security Guardium**, che monitora l'accesso ai dati sensibili in tutti gli stati e in tutti gli ambienti: file, database e applicazioni. La soluzione garantisce protezione dei dati evitando l'accesso da parte di soggetti non autorizzati.

PRINCIPALI FUNZIONALITA'

- Rilevamento e classificazione automatizzati dei dati
- Monitoraggio delle attività e protezione del dato
- Conformità più rapida
- Applicazione delle politiche di sicurezza in tempo quasi reale
- Comprensione dei rischi e priorità alle indagini
- Riduzione dei tempi di risposta

IBM SECURITY QRADAR EDR

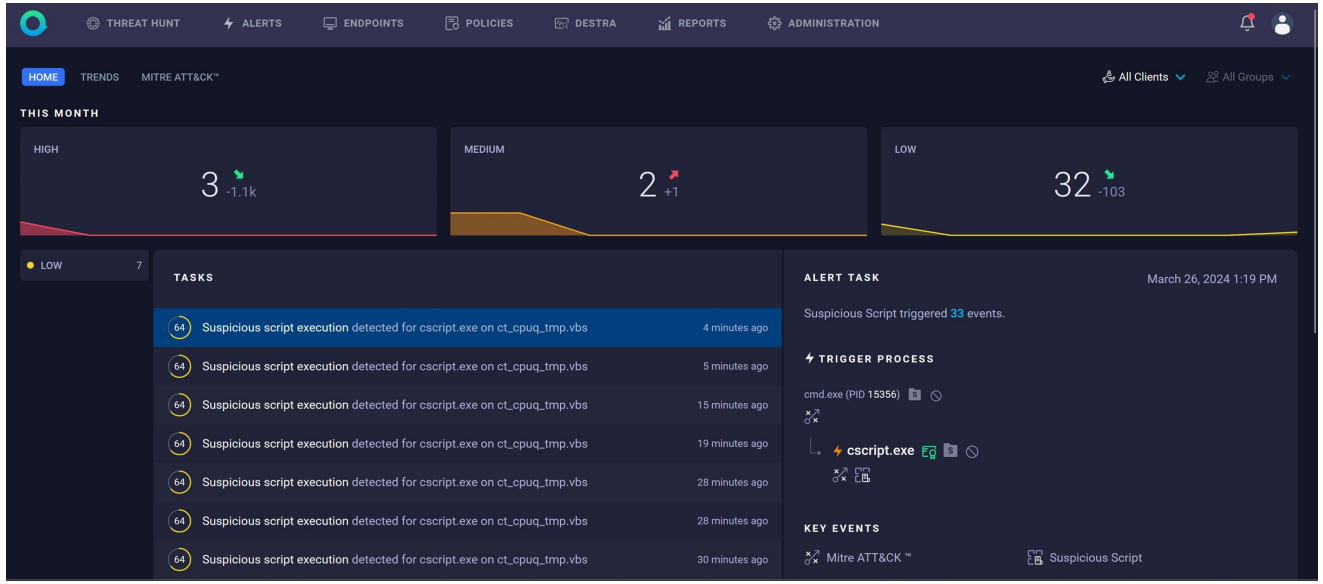
IBM Security QRadar EDR è la soluzione che consente di proteggere i device da attacchi informatici, rilevando comportamenti anomali e correggendoli in tempo quasi reale.

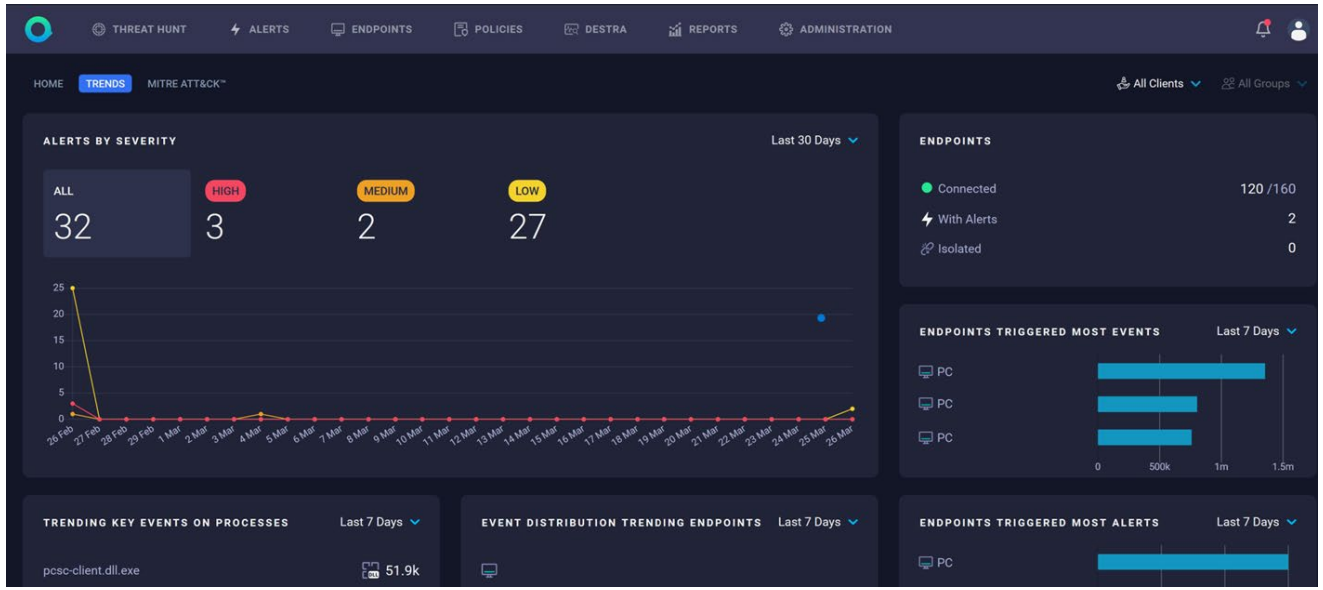
Un agent installato sui client device di SILC SPA svolge un ruolo di sentinella, generando eventi lato security ed inviando, in maniera automatizzata, continui report sugli endpoint ad una dashboard centrale.

PRINCIPALI CARATTERISTICHE

- Rimedia alle minacce degli endpoint quasi in tempo reale con un'automazione intelligente
- Consente di prendere decisioni informate grazie agli storyboard di visualizzazione degli attacchi
- Automatizza la gestione degli avvisi per ridurre l'affaticamento degli analisti e concentrarsi sulle minacce più importanti
- Fornisce al personale la possibilità di salvaguardare la continuità aziendale grazie a funzionalità avanzate di apprendimento continuo AI e a un'interfaccia di facile utilizzo

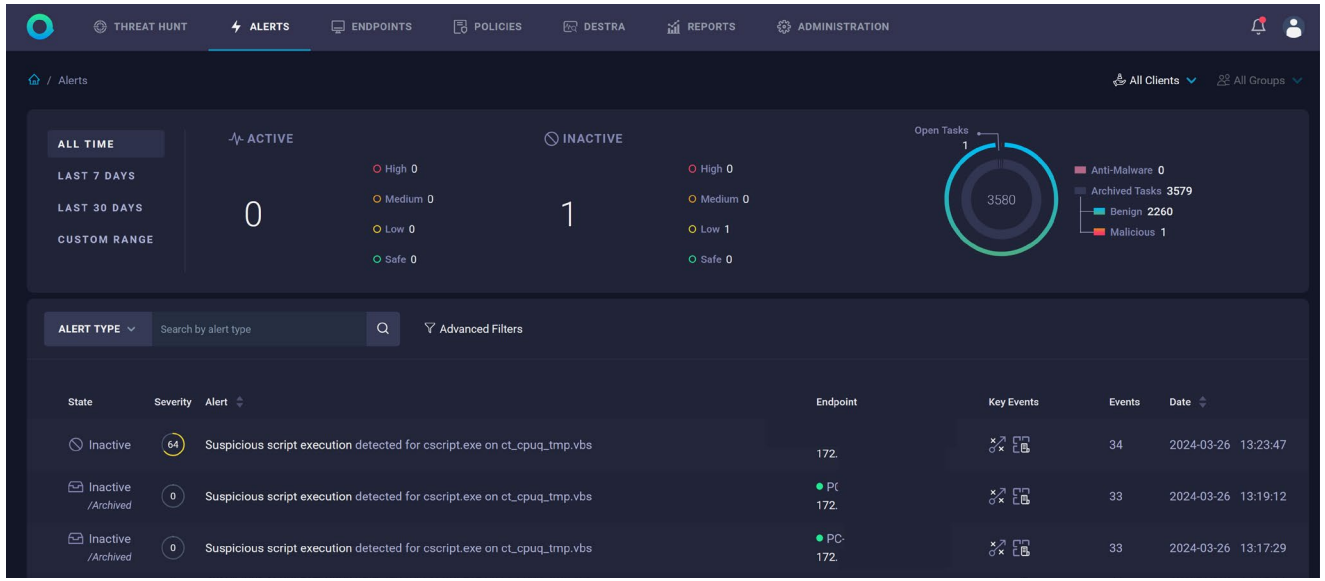
IBM SECURITY QRADAR EDR – DASHBOARD





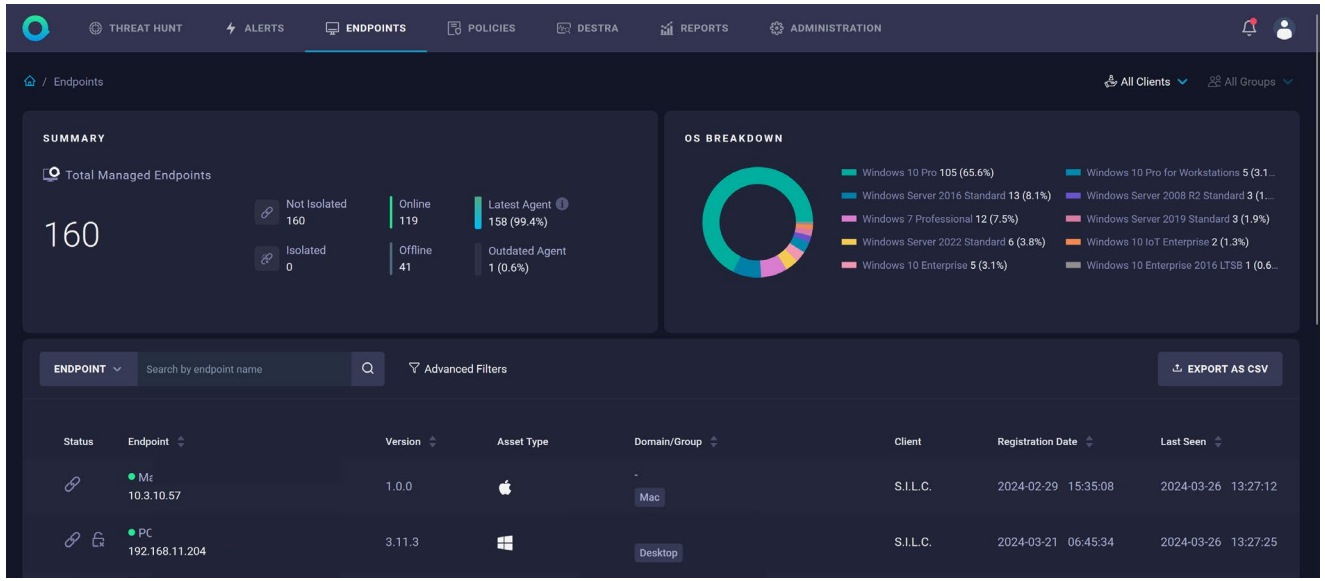
Una dashboard, a disposizione di SILC SPA, fornisce una panoramica riassuntiva del mese di IBM Security QRadar EDR e rileva le anomalie e i comportamenti sugli endpoint.

IBM SECURITY QRADAR – EDR E ALERT



Una panoramica dei dettagli e degli avvisi a disposizione di SILC SPA. Per ogni comportamento è possibile visualizzare un albero comportamentale di facile comprensione.

Questa è una delle funzioni più caratterizzanti di IBM Security QRadar EDR.



Questa immagine è un esempio di overview sugli endpoint presenti in SILC SPA. La soluzione offre la possibilità di isolare i singoli endpoint a fronte del rilevamento di comportamenti anomali.

Via Giorgio Stephenson 43/a, 20157 - Milano

Via Mario Bianchini 13-15, 00142 - Roma

Via Pavia 9/A1, 10098 - Rivoli (TO)

www.mauden.com info@mauden.com