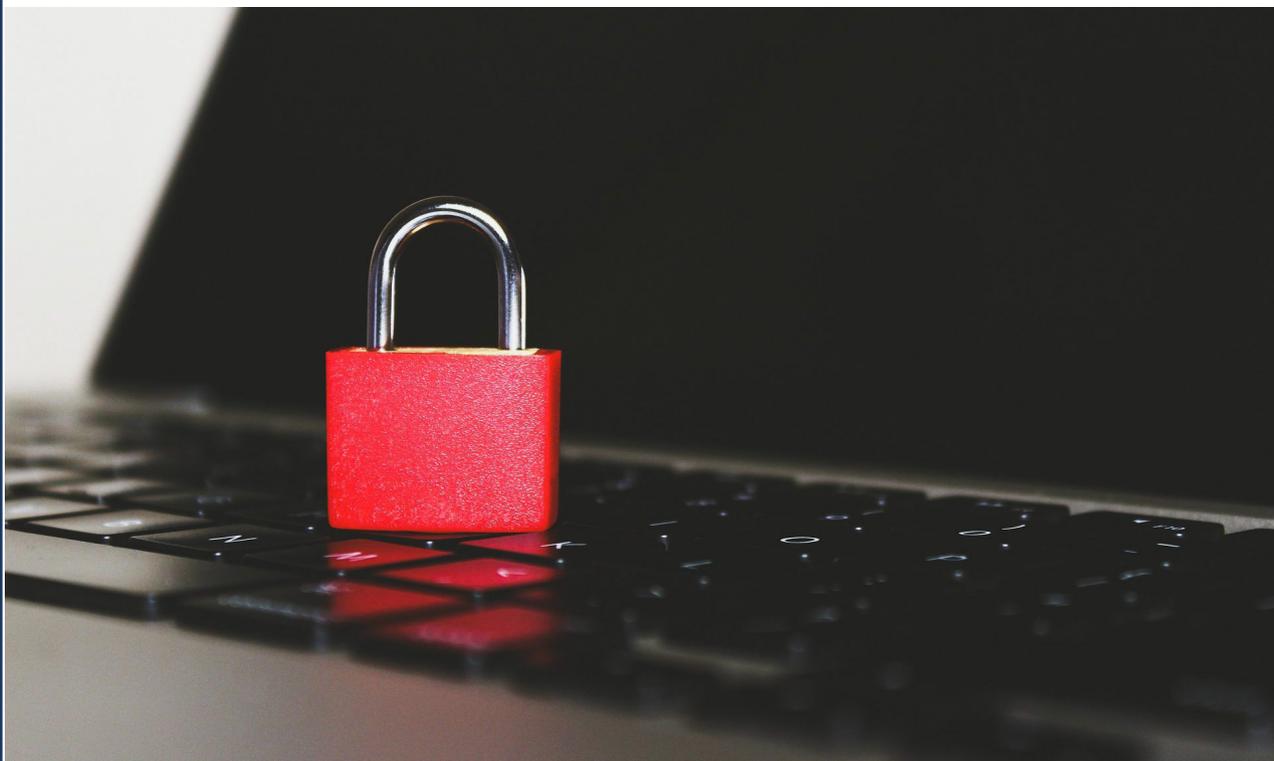
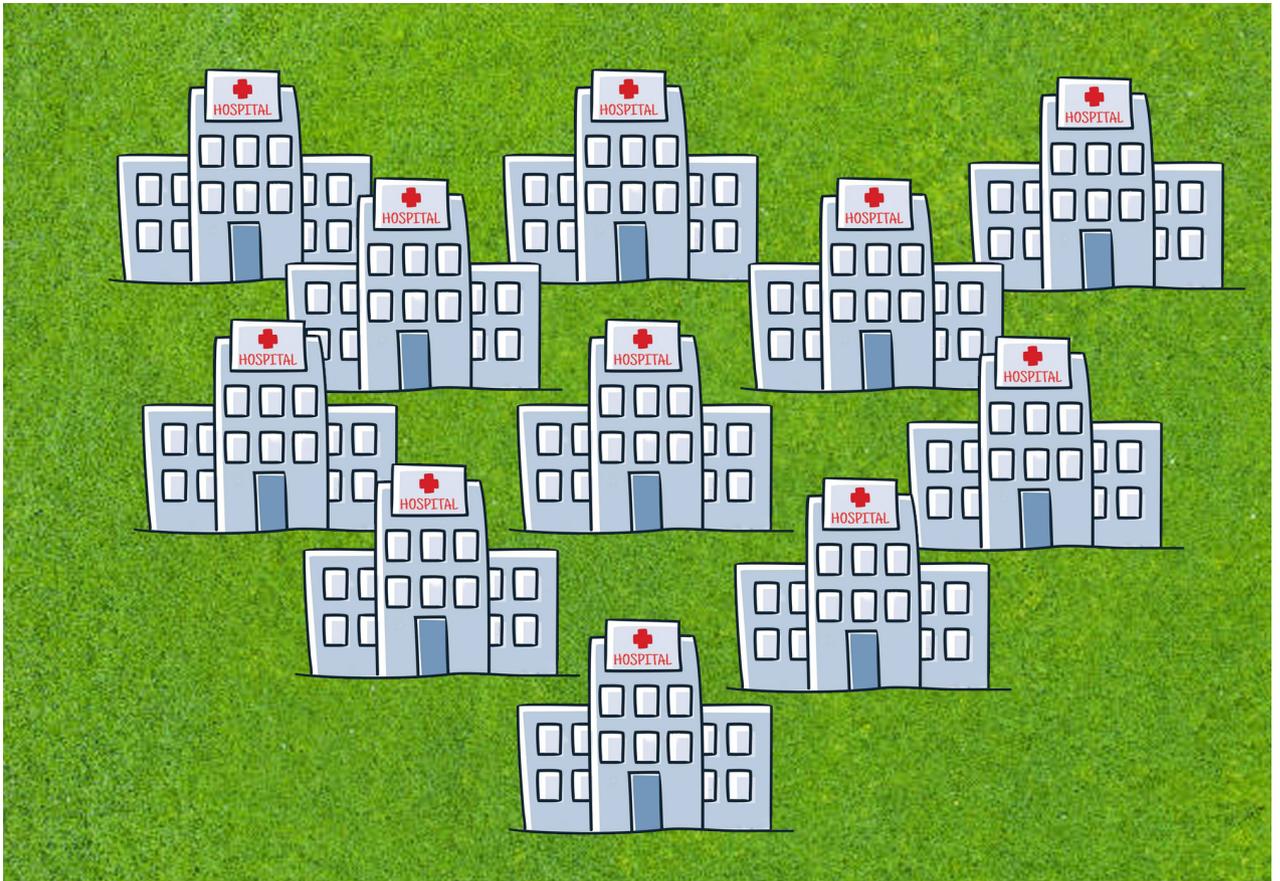


Case History
PromiGroup

Operazione Sicurezza informatica



Un importante consorzio che rappresenta diverse strutture sanitarie multispecialistiche ha dato piena fiducia a PromiGroup in tema di sicurezza, prevenendo quindi ogni possibile problematica a breve e a lungo termine, e garantendo un alto livello di sicurezza. Per il cliente la sicurezza è un tema prioritario, in quanto hanno la completa gestione di dati estremamente sensibili dei clienti.

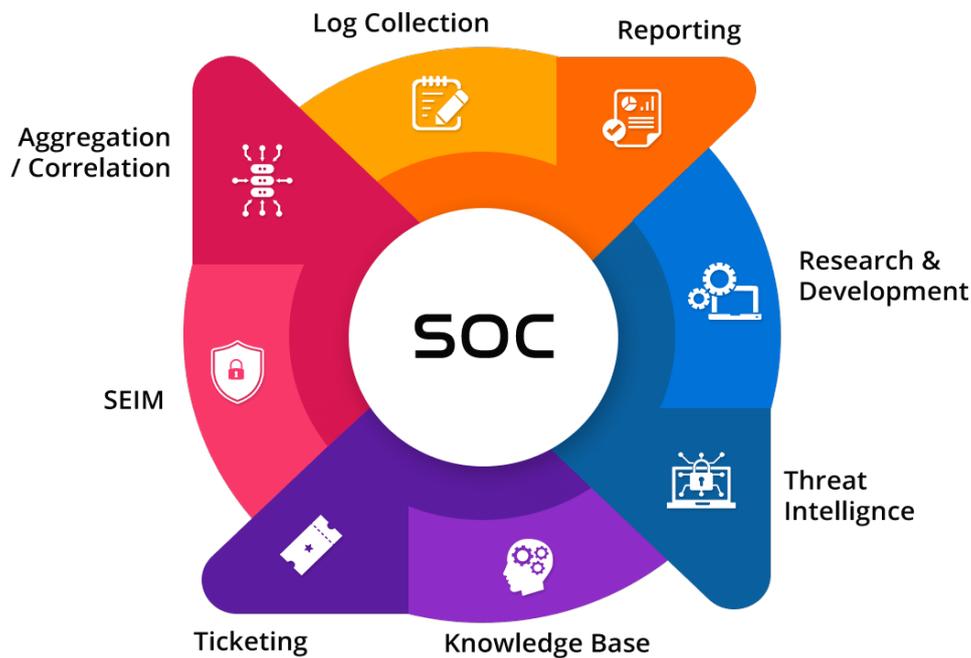


Si è quindi proceduto con un'analisi congiunta sulle criticità, per proseguire verso una soluzione di protezione totale che prevedeva la copertura degli end-point e del percorso di rete, creando così una infrastruttura di cybersecurity solida e rapida negli alert.

L'infrastruttura è stata così composta:

- SIEM (Security Infrastructure event management)
- SOC (Security operation central)
- NDR (Network Detection & Response)





SOC e SIEM

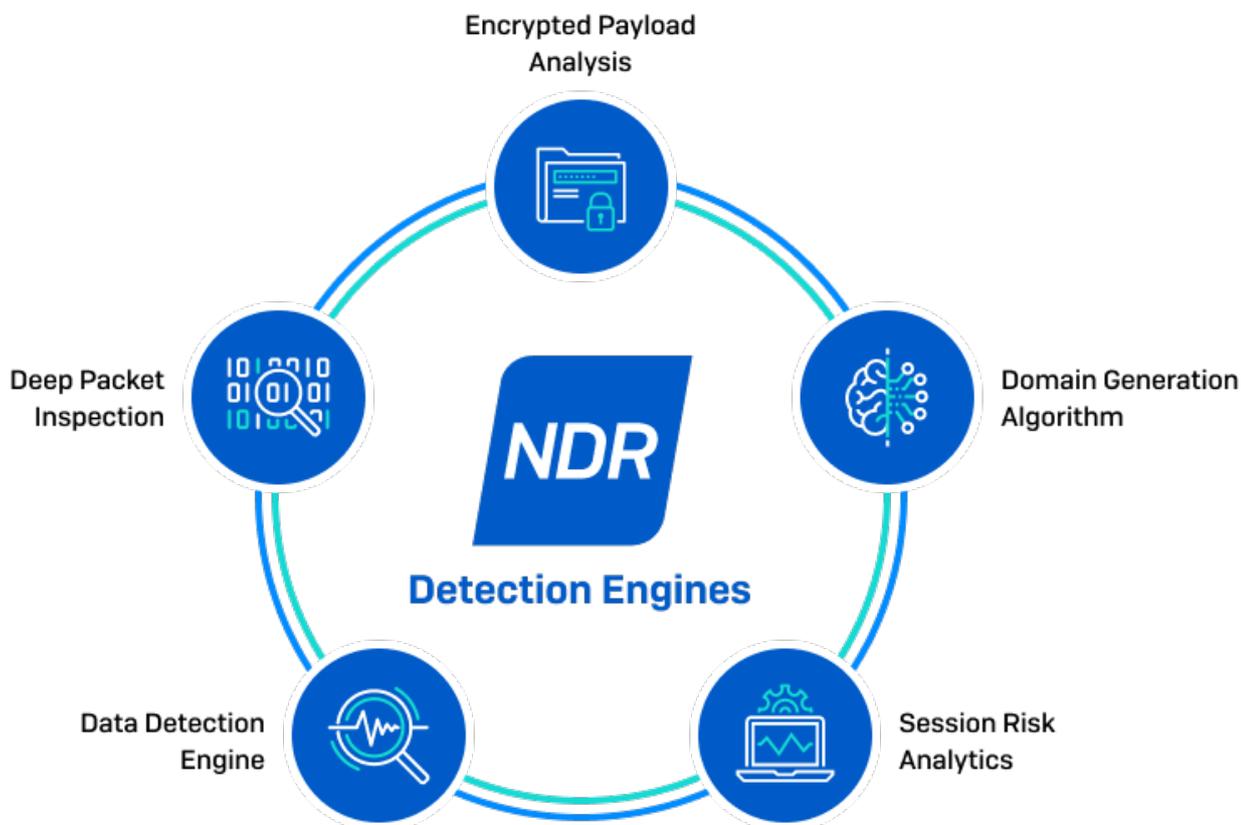
Il SOC svolge ora un compito di raccolta log dei singoli end point sui quali è stato installato un antivirus; successivamente, vengono inviati al SIEM che procede ad un'analisi dei dati supportata da un IA.

Infine, l'esito porta a scernere i dati e scovare le minacce.

Il flusso sopra descritto porta poi ad avere un preciso e puntuale allarme al gestore della rete.

NDR e SIEM

Anche la parte del network prevede una copertura completa: oltre agli end point, il sistema NDR svolge un ruolo primario grazie ad una serie di sonde, le quali, a loro volta mandano i propri log al SIEM completando così l'analisi anche del network e creando una piena copertura della protezione per i dati aziendali.



PromiGroup è riuscita a coprire ampiamente le aspettative del cliente, creando così una protezione completa della rete dell'intero consorzio.



PromiGroup