www.sangfor.it
francesco.addesi@sangfor.com,
giulia.bianchi@sangfor.com

ASST VALLE OLONA

Caso di Successo

Sistema Socio Sanitario
Regione Lombardia
ASST Valle Olona

PANORAMICA

L'Azienda Socio Sanitaria Territoriale (ASST) della Valle Olona nasce l'1 gennaio 2016. Ora è una realtà ben radicata nel medesimo territorio e copre il fabbisogno di prestazioni sanitarie e sociosanitarie di ben 32 Comuni.
Le attività sono svolte nei 4 presidi ospedalieri di Busto Arsizio, Gallarate, Saronno e Somma Lombardo.

LA SFIDA

Il sistema di antivirus in essere era un sistema tradizionale che non dava garanzie in materia di protezione da attacchi complessi. Era necessario aggiornarsi e passare ad una tecnologia più recente, che analizzasse i comportamenti sospetti riconducibili a virus tramite Intelligenza Artificiale (AI).

I recenti attacchi alle aziende sanitarie milanesi hanno fatto alzare il livello di interesse sulla cybersecurity. «I sistemi di prevenzione tradizionali non riescono più a tenere le organizzazioni al sicuro, è tempo di evolversi e cambiare mentalità». Questo è ciò che hanno pensato in Valle Olona, quando ci hanno chiesto di mettere al sicuro i loro asset aziendali.

SOMMARIO

- Settore Ospedaliero
- Location: Valle Olona, Italia

SOLUZIONE SANGFOR

È stata messa in sicurezza la rete informatica combinando ENDPOINT SECURE con CYBER COMMAND, per una protezione estesa e multilayer del network. Un nuovo approccio alla cybersecurity per una visibilità a 360° su asset, vulnerabilità, traffico e comportamenti anomali con lo scopo di rilevare le minacce nascoste nella rete e risolvere i problemi di sicurezza sul nascere prima che diventino gravi incidenti.
La correlazione tra i due prodotti ha permesso di automatizzare le operazioni di sicurezza senza dover necessariamente ricorrere ad un SOC.
Le azioni che vengono svolte si possono riassumere in:
- Identificazione automatica degli asset e relativo inventario (server, workstation, software, porte e servizi esposti o vulnerabili)
- Analisi del rischio attuale e potenziale basato su indicatori di compromissione e attacco per ogni singolo asset
- Visibilità completa sugli eventi di sicurezza e la loro evoluzione nel tempo, monitoraggio attivo 24/7 per mezzo di Intelligenza Artificiale
- Detection & Response automatica sia a livello network che a livello endpoint