

CASE STUDY

“ SGBox viene utilizzato principalmente per la raccolta log di accesso degli amministratori di sistema. La grande versatilità di SGBox consente di acquisire i log a prescindere dalla fonte dati che li ha generati ”

Flavio Aime
IT Networking Eltek S.p.A.

AZIENDA

Gruppo Eltek S.p.A.

SETTORE

Manifatturiero

IMPLEMENTAZIONE

Log Management

OBIETTIVI

- Piattaforma unificata per la gestione eterogenea delle informazioni raccolte
- Compliance al D.Lgs. 196

A proposito di SGBox

SGBox è un security vendor dinamico e innovativo con oltre 10 anni di esperienza nella produzione di software in forte espansione nei mercati europei e medio-orientali. SGBox ridefinisce l'approccio alla cyber security e compliance (GDPR, ISO27001, PCI-DSS, ...) proponendo una soluzione integrata ma modulare, scalabile e di facile utilizzo in grado di adattarsi alle crescenti richieste del mercato.

AN ORGANIZATION AT YOUR SERVICE

ELTEK
GROUP

Overview

Il Gruppo Eltek è stato fondato nel 1979 dal manager Luigi Sassone ed è specializzato nella ricerca, progettazione, sviluppo e produzione di componenti meccanici ed elettronici. Tradizionalmente conosciuto per la componentistica nei settori elettrodomestico e automobilistico, recentemente ha iniziato a interessarsi anche al settore medicale e alla ricerca avanzata nel settore delle nano-biotecnologie. La sua sede storica è a Casale Monferrato, ma nei suoi quasi quarant'anni di storia ha perseguito un progetto di internazionalizzazione che gli ha permesso di aprire altre 5 sedi produttive e 2 commerciali, in 3 continenti. La sua esperienza è eterogenea: dalla progettazione e costruzione degli stampi, all'elettronica, all'ingegnerizzazione di linee produttive semiautomatiche o completamente automatiche con capacità variabili dalle piccole serie ai milioni di pezzi all'anno. Attualmente il gruppo è strutturato in tre aree (Business, Appliance, Automotive e Medical) che gli permettono di garantire forte presenza internazionale, orientamento al prodotto e ricerca e sviluppo continuo, grazie all'impiego di tecnologie sempre all'avanguardia.

Challenge

Il Gruppo Eltek era alla ricerca di una soluzione conforme alle prescrizioni del Garante della Privacy (D.Lgs. 196). Il Garante per la protezione dei dati ha disposto l'adozione di specifiche misure tecniche ed organizzative relativamente alla figura degli "amministratori di sistema", adottando un provvedimento che regola la gestione delle informazioni provenienti dai sistemi, relative alle connessioni effettuate da parte degli amministratori di sistema. I log raccolti devono essere mantenuti per un periodo di almeno 6 mesi in modalità cifrata al fine di garantirne l'inalterabilità.

Soluzione adottata

Il Gruppo Eltek ha adottato la soluzione di SGBox implementando il modulo Log Management che consente di raccogliere i log di qualsiasi formato proveniente da qualsiasi fonte di dati. I log raccolti sono processati per estrarre gli eventi associati che possono essere facilmente analizzati in tempo reale o su base storica. In questo modo è possibile raggiungere un accesso ottimale di normalizzazione, raccogliere e riconoscere eventi significativi della rete e rilevare anomalie sul numero di attacchi ricevuti dalla rete.