WIIT S.p.A.

Si prega di compilare la scheda rispettando il limite massimo di 5000 caratteri, spazi inclusi

Descrizione della problematica o del bisogno nell'azienda o pubblica amministrazione utente.

Il nostro cliente opera nel settore Oil&Gas con terminali offshore nel mare Adriatico e fa parte di un gruppo internazionale attivo su tutta la filiera estrattiva . Il gruppo rappresenta la **più grande company Oil&Gas del mondo con un fatturato di 237 miliardi di dollari e 70.000 dipendenti** e controlla **il 3%** dell'attività estrattiva di idrocarburi del pianeta.

Le attività di business del gruppo sono basate su asset a valore propri (know-how, siti di estrazione, processi) e costituiscono uno dei più importanti vantaggi competitivi all'interno settore.
L'attenzione alla security è quindi una delle priorità del gruppo e ricade su tutte le controllate.
Oltre a questo, il nostro cliente, operando con dati europei, è soggetto alla nuova normativa in materia di "data protection" (GDPR).
Mettendo a fattor comune le due esigenze, il cliente ci ha chiesto di analizzare i requisiti di security e gli aspetti GDPR, ponendoci la sfida di proporgli una **roadmap di enforcement della security** che tenesse conto dei due aspetti e mettesse a fattor comune i processi e le tecnologie.

Wiit ha proposto il proprio approccio alla cybersecurity costituito da un **framework di analisi** e dall'implementazione di una **piattaforma integrata** di **Threat Intelligence** per la **gestione orchestrata degli eventi di security**. Riteniamo che ad oggi questo approccio sia l'unico efficace, in quanto gli attacchi moderni utilizzano vettori complessi che mirano alla compromissione contemporanea di più elementi IT della vittima.

Descrizione della soluzione tecnologica (tecnologie usate, architettura, ecc.).

Nell'ambito della **Cyber Security**, WIIT ha sviluppato il **Wiit Security Univese (WSU Figura 1)**, un **framework metodologico e tecnologico completo e coerente con i principali standard mondiali (NIST).**
Tale framework si basa su cinque pillar:

1. **Network**: in quest'ambito rientrano le tecnologie atte a ispezionare il traffico da e verso internet ed all'interno del parco applicativo del Cliente
2. **Vulnerability and Security Management**: in questo ambito rientrano tutte quelle tecnologie mirate a permettere di effettuare azioni di audit e compliance sui sistemi
3. **Endpoint Protection**: quest'ambito contiene quelle tecnologie che proteggono l'Endpoint (Server, PC, Mobile)
4. **Identity Access Management**: quest'ambito prende in considerazione quegli strumenti che servono a gestire tutte le identità aziendali con particolare attenzione alle utenze privilegiate (Amministratori di Sistema)
5. **Messaging Security**: in quest'ambito rientrano quegli strumenti che ispezionano e proteggono le informazioni "in volo" come i messaggi di posta elettronica

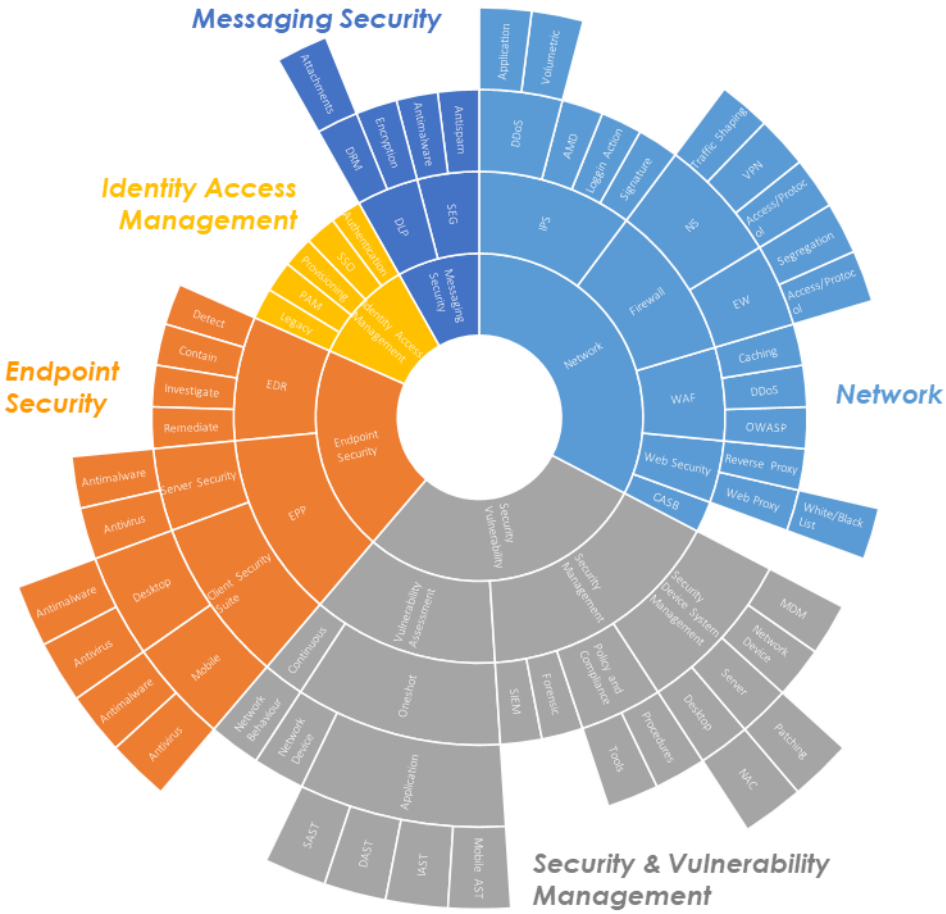


Figura 1 - Framework WSU

Abbiamo quindi realizzato un servizio continuativo di gestione delle componenti di CyberSecurity: un **Security Operating Center** as a Service che si occupa del monitoraggio, della prevenzione, della rilevazione, dell'analisi e il contenimento delle minacce.

Descrizione del progetto di implementazione - complessità, tempi, aspetti organizzativi, costi, ecc.

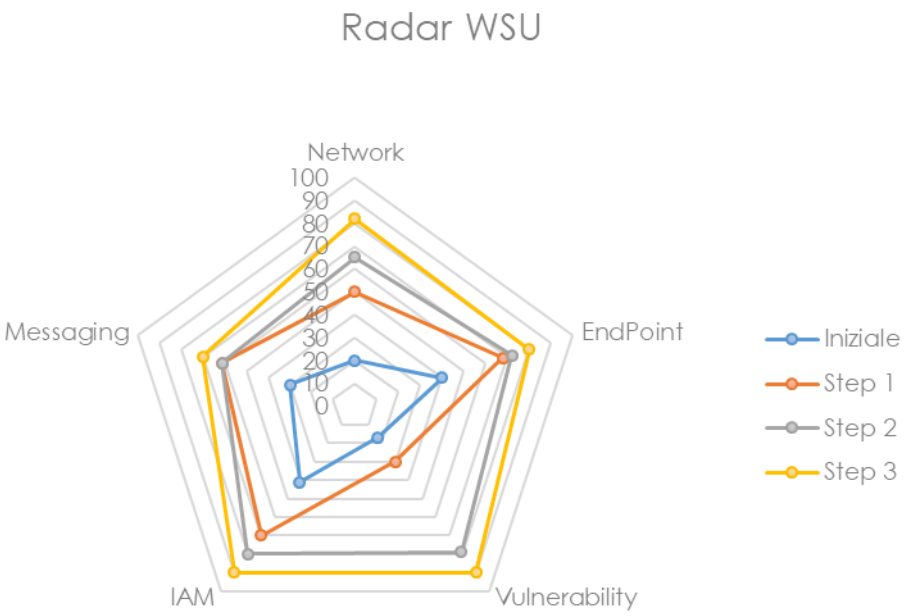
Per il cliente Wiit ha declinato il proprio framework in 3 step di applicazioni autoconsistenti che aggredissero in maniera graduale i temi di compliance GDPR ed enforcement della cybersecurity del cliente, aggiungendo ad ogni step dei Quick Win che portassero benefici immediati all'incremento dei livelli di sercurity prima e della compliance GDPR successivamente, per poi convergere alla gestione integrata della piattaforma.

- Step 1: Incremento dei livelli di sicurezza e compliance per la gestione delle utenze privilegiate (PAM), la gestione delle informazioni in volo (Sandbox Email) e l'enforcement del network di frontiera (Internet Gateway)
- Step 2: Implementazione del pacchetto GDPR (Enforcement GDPR)
- Step 3: Implementazione della piattaforma integrata di cybersecurity (Threat Intelligence).

Descrizione dei principali benefici raggiunti dall'azienda o pubblica amministrazione utente.

Ogni step di implementazione ha portato dei benefici in linea con gli obiettivi di enforcement della security, compliance GDPR e governance integrata della piattaforma di Threat Intelligence che il cliente ha richiesto a Wiit superando con lode gli strettissimi audit di compliance della capogruppo.

Nella figura di seguito è rappresentato un grafico sintetico per evidenziare il beneficio ottenuto dal cliente in termini di incremento dei livelli di security associato a ciascuno step.



Descrizione degli elementi distintivi e di reale innovatività/originalità della soluzione, anche con riferimento a soluzioni «concorrenti».

Gli elementi distintivi della soluzione risiedono nelle modalità di approccio al tema della cybersecurity in maniera integrata e corredata da una componente di servizio che rende realmente efficace la soluzione.

Le modalità di analisi dei punti di intervento sul cliente e della costruzione della soluzione sono stati effettuati utilizzando **il framework proprietario di Wiit (WSU).** Tale framework permette di indirizzare sia gli aspetti di vulnerabilità che quelli di GDPR, permettendo di costruire una piattaforma integrata e un modello di governance generale della cybersecurity. Wiit è quindi in grado, analogamente a quanto effettua per la propria piattaforma PaaS dedicata alle applicazioni critiche, anche di erogare una piattaforma di Security-as-a-Service, flessibile e scalabile per le esigenze dei propri clienti.