PROTEGGERE I SERVICE PROVIDER DELL'AFTERMARKET AUTOMOTIVE ITALIANO



UNIT PLUS

HWG Sababa

AKITO
IT FOR CHOICE

Unit Plus

Appartiene a Unit Holding, un'innovativa realtà che conta 160 dipendenti impegnati quotidianamente ad assistere numerosi clienti

Esperienza nel settore automotive aftermarket

Offre soluzioni innovative, altamente performanti e misurabili nel tempo

Akito

È un System Integrator specializzato nella Security e Cybersecurity

Offre tecnologie innovative e servizi, con il valore aggiunto di professionalità specifiche

Opera su tutto il territorio nazionale, per aziende del settore pubblico e privato

"Il bene più prezioso che abbiamo in mano sono i dati. La sola possibilità che questi possano essere compromessi, distrutti o resi irraggiungibili è qualcosa che non riusciamo e non vogliamo nemmeno immaginare."

Christian Olivier,
IT Manager di Unit Plus

UNIT PLUS

HWG Sababa

AKITO IT FOR CHOICE

Oggi i veicoli sono sempre più connessi ed in grado di interagire tra di loro e con il mondo esterno. Da una stima che si aggira intorno ai 24 miliardi di dollari nel 2021, il mercato globale dei veicoli connessi potrebbe raggiungere i 57,6 miliardi di dollari entro il 2026. Ma, se da un lato, la connettività garantisce una migliore esperienza di guida, dall'altro introduce potenziali vulnerabilità e punti di ingresso che gli hacker possono sfruttare, rendendo la superficie di attacco estremamente estesa.

Alla luce di questo scenario, l'industria automotive ha sviluppato delle linee guida - come l'UNECE R155-156 - volte ad integrare la sicurezza informatica lungo l'intero ciclo di vita del veicolo, dalla progettazione, alla produzione, fino alla rottamazione.

In tale contesto si inserisce il protagonista di questa storia, **Unit Plus**, un'azienda che si rapporta quotidianamente con alcuni degli attori chiave della filiera automobilistica, essendo specializzata nella fornitura di prodotti e servizi per flotte auto, OEM e molti altri protagonisti dell'automotive aftermarket.

Gestione sicura dei dati come priorità assoluta

Unit Plus vanta un ampio portfolio che spazia dalla **Business Intelligence** - finalizzata a convertire milioni di dati in informazioni indispensabili per il processo decisionale e di previsione - all'**Information Technology** - destinata alla progettazione di reti e infrastrutture hardware e software altamente personalizzate. Tecnologia e dati sono quindi due pilastri fondamentali del business dell'azienda.

"Nel corso del tempo, i nostri clienti hanno iniziato a chiedersi come venissero gestiti i loro dati e fino a che punto i servizi e i prodotti che forniamo loro fossero sicuri,"

ha commentato Christian Olivier,
IT Manager di Unit Plus,

"Per questo motivo ci siamo rivolti ad Akito - nostro partner di fiducia per la cybersecurity da molti anni - e abbiamo cercato insieme sul mercato una soluzione in grado di garantire alla nostra infrastruttura interna il livello di sicurezza richiesto dai clienti. Il nostro obiettivo era trovare un 'guardiano' esperto che fosse in grado di tenere le minacce lontane dai nostri sistemi 24x7."

Durante il processo decisionale, Unit Plus e gli esperti di Akito hanno preso in considerazione diverse opzioni. Vista la necessità di un team strutturato in grado di monitorare un'infrastruttura eterogenea, rilevare anomalie, contenere e rispondere agli attacchi informatici, la scelta è ricaduta su HWG Sababa e sul suo servizio SOC. Con un accordo quinquennale, il SOC - proprio per la sua complessità e rilevanza - è l'unico processo di sicurezza che Unit Plus ha deciso di esternalizzare.



Nonostante l'infrastruttura molto diversificata di Unit Plus - composta da server, switchboard, firewall, piattaforme e molto altro - il processo di onboarding è stato fluido. L'elemento più complesso di questa fase è stato proprio l'inventario, indispensabile per consentire agli analisti del SOC di accedere alle informazioni dei singoli nodi e attivare correttamente le sonde di monitoraggio. Una volta terminato l'onboarding, è iniziato il monitoring vero e proprio, finalizzato a stroncare sul nascere qualsiasi tentativo di attacco.

Il servizio SOC in dettaglio

HWG Sababa offre un servizio SOC di livello 1, 2 e 3 che soddisfa le esigenze di sicurezza di ambienti IT e OT, sfruttando tecnologie avanzate - come SIEM, SOAR, Threat Intelligence - e fornendo soluzioni personalizzate per diversi settori e industrie.

In grado di monitorare, rilevare, analizzare e rispondere agli incidenti e alle minacce cyber 24 ore su 24, il SOC è composto da 70 cybersecurity analyst certificati, che di fatto rappresentano il vero valore aggiunto del servizio.

L'organizzazione interna del SOC è la seguente:

- **Security Manager.** È il principale interlocutore per il cliente, con una visione completa e la piena responsabilità dello stato del servizio. Questo profilo è coinvolto nelle fasi di incident management e nei review meeting.

- **Proactive Detection Team (livello 1 e livello 2).** Team di analisti di sicurezza che identifica le minacce indirizzate all'infrastruttura digitale, monitorando continuamente l'alert queue, eseguendo il triage degli avvisi di sicurezza e svolgendo un'analisi approfondita degli attacchi. Il team gestisce gli incidenti di sicurezza, determinando se un sistema o un set di dati critici è stato colpito, occupandosi della remediation e fornendo supporto nello sviluppo di nuovi metodi analitici di rilevamento delle minacce.

- **Competence Center (livello 3).** Disponendo di conoscenze approfondite su rete, endpoint, threat intelligence, analisi forense, reverse engineering, nonché sul funzionamento di applicazioni specifiche, il Competence Center agisce come "cacciatore" di incidenti. Essendo attivamente coinvolto nello sviluppo, nella messa a punto e nell'implementazione di metodi analitici di rilevamento delle minacce, esso aiuta a risolvere gli eventi di sicurezza più complessi.

La **reportistica** è un'altra componente chiave del servizio.
Giornalmente sono disponibili report generati automaticamente,
mentre gli analisti di HWG Sababa forniscono in aggiunta quanto segue:

- **Report settimanale:**
descrizione dettagliata degli avvisi settimanali e report personalizzati richiesti

- **Report mensile:**
overview mensile del servizio, che include anche una sezione sugli executive members

- **Report annuale:**
overview annuale del servizio

Risultati

Il progetto è in corso dal 2021 con nessun incidente riscontrato sino ad ora, ma un livello di attenzione sempre altissimo.

"Sappiamo tutti che non si tratta più di stabilire se un attacco avverrà, ma quando. Il mio obiettivo è proprio quello di rimandare il più possibile questo momento e, allo stesso tempo, avere gli strumenti necessari per rispondere nel caso in cui venissimo colti di sorpresa", ha commentato **Christian Olivier.**

"Il monitoraggio continuo ha sicuramente aumentato il nostro livello di sicurezza e garantisce una risposta proattiva ai tentativi di attacco. Il feedback è positivo, siamo molto soddisfatti di questa collaborazione."

Inoltre, su base mensile, Unit Plus riceve report con azioni correttive da implementare per ridurre il rischio di minacce o vulnerabilità.

"Il report mensile è sicuramente un aspetto che apprezzo molto del servizio e lo considero uno strumento molto utile poiché ci permette di tenere sotto controllo strumenti e sistemi critici." ha concluso Christian.

HWG Sababa

AKITO
IT FOR CHOICE

UNIT
PLUS

Follow us on:

HWG Sababa
www.hwgsababa.com

Akito
www.akito.it