Le violazioni accadono: l’importante è essere preparati

Author : Redazione

Date : 2 Ottobre 2019

Unire la rilevazione e risposta con la continuos response

L’idea che sta dietro al concetto di Managed Detection and Response (MDR) è semplice. “Managed” sta per gestito: il servizio di rilevazione e risposta alle cyber-minacce viene completamente eseguito da un partner esterno, che richiede pochissimi input al team IT interno. “Detection and response” fa riferimento al principio di funzionamento del servizio: inserendo sensori sofisticati sulla rete e gli endpoint di un’azienda viene fornita completa visibilità sull’ambiente IT.

Il risultato qual è? Una soluzione che può rilevare violazioni di dati basandosi sul *comportamento*, invece che sui tradizionali segnali di attività malevola, consentendo azioni di risposta rapide ed efficaci, supportate dall'automazione o dall'esperienza umana.

In F-Secure questo servizio MDR si chiama **Countercept.** Si tratta di un servizio di threat hunting completamente gestito che rileva gli attaccanti più esperti in pochi minuti.

In molte società, la ‘rilevazione’ e ‘risposta’ alle minacce sono trattate come funzioni separate. Un fornitore di servizi MDR efficace, invece, mette insieme gli skillset e i processi che tradizionalmente restavano separati tra threat hunter e incident responder, creando un team che rileva e risponde velocemente agli attacchi prima di un impatto sul business. Questo approccio in F-Secure viene chiamato **Continuous Response**. La metodologia Continuous Response prevede tre momenti, individuabili in tre parole chiave: Collaborazione, Contesto e Controllo.

Per *Collaborazione* si intende la capacità di attivarsi e coordinarsi velocemente, attraverso ruoli chiari, compiti e responsabilità assegnati sia al team interno che a quello esterno all’azienda, così che quando un attacco viene rilevato entrambi i team possano attivarsi velocemente.

Il Contesto indica l’accesso alle risorse di intelligenza più pertinenti per fornire più informazioni possibili sull’incidente.

Il *Controllo* comprende le attività di investigazione, contenimento, e rimedio che permettono la Continuous Response durante un attacco, incluse azioni che rallentano gli attaccanti senza che si accorgano della presenza degli specialisti F-Secure.

È chiaro che la velocità di risposta all’interno di una ristretta finestra di opportunità può cambiare radicalmente il modo in cui un’azienda si riprende da una violazione.

Per maggiori informazioni: https://blog.f-secure.com/continuous-response/