Servizi Darktrace Analyst

Darktrace si impegna a garantire che i propri clienti ottengano la massima qualità dalla nostra tecnologia di cyber AI di primo ordine. Per poter offrire il miglior supporto possibile, le nostre opzioni di assistenza possono essere personalizzate per migliorare e ampliare la sicurezza e i team IT del cliente.

I servizi possono essere forniti tramite i Cyber Analyst di Darktrace, esperti in analisi delle minacce e cyber intelligence, o tramite i partner certificati Darktrace. Cosa più importante, queste offerte sono personalizzate sulla base delle esperienze acquisite in aziende e settori di ogni tipo, per fornire un servizio su misura.

Proactive Threat Notification 24 ore su 24, 7 giorni su 7

I Security Operations Center (SOC) di Darktrace, con sede a Cambridge, San Francisco e Singapore forniscono un'assistenza 24 ore su 24 relativa ad incidenti significativi identificati nell'ambiente del cliente, segnalati dal sistema Darktrace utilizzato. Gestito dai Cyber Analyst di Darktrace, questo servizio fornisce avvisi in caso di attività insolite o deviazioni nei comportanti che possono essere indicativi di un attacco in corso. Questi incidenti sono rapidamente analizzati su richiesta e i nostri Cyber Analyst forniranno tutte le informazioni necessarie per agire in base agli eventi che si verificano.
Le Proactive Threat Notification (PTN) garantiscono che gli incidenti rilevati con la massima precisione, che sono chiari indicatori di un attacco emergente, siano indirizzati direttamente nel SOC di Darktrace per l'analisi e la valutazione da parte dei nostri team di Cyber Analyst esperti.

Gli allarmi monitorati da Darktrace come parte del servizio PTN possono essere identificati dal tag "Enhanced Monitoring" (monitoraggio avanzato) all'interno dell'Enterprise Immune System e possono essere visualizzati mediante filtraggio nel Threat Visualizer e nel Model Editor. Il tag Enhanced Monitoring consente anche di visualizzare esattamente quale modello di violazione è stato inoltrato a livello superiore al SOC per l'analisi.

Il nostro team di ricerca e sviluppo valuta e aggiorna continuamente il servizio PTN al fine di garantire che l'indagine sia eseguita sulle violazioni con priorità più elevata e che sia possibile rispondere rapidamente agli attacchi di ogni tipo, dalle minacce conosciute e tradizionali a quelle del tutto nuove e mai individuate in precedenza.

Una volta che un PTN viene passato di livello nel SOC di Darktrace, viene analizzato da parte di uno dei nostri Cyber Analyst mondiale. Per l'analisi dei casi più complessi, il SOC di Darktrace ha accesso ad analisti senior di Livello 3 che fanno parte del nostro gruppo di analisti mondiali. La decisione di attivare un allarme può coinvolgere numerosi analisti che collaborano per prendere una decisione informata relativa al fatto se l'organizzazione è esposta o meno ad una minaccia diretta ed immediata.

Ricordiamo che non tutti gli allarmi vengono analizzati, ma solo gli incidenti che sono altamente indicativi di un attacco sono contrassegnati con il tag Enhanced Monitoring e saranno analizzati dagli analisti PTN.

Se, durante la fase di analisi, Darktrace rileva la chiara evidenza di un attacco, il team del cliente sarà contattato immediatamente e saranno fornite le informazioni riscontrate al fine di poter intervenire immediatamente. Darktrace può suggerire che qualsiasi allarme PTN sia considerato come Priorità elevata. Gli allarmi completamente analizzati saranno crittografati utilizzando una chiave privata condivisa ed inviati per e-mail ad una lista di distribuzione denominata all'interno dell'organizzazione. È possibile anche ricevere telefonate e/o messaggi SMS automatici nel caso sia inviato un avviso di posta elettronica PTN. È possibile configurare contatti SOC e metodi di inoltro dei messaggi tramite il Customer Portal nelle preferenze dell'account.

> "La nostra squadra può spesso essere ridotta al minimo. Le e-mail e le chiamate dirette che abbiamo ricevuto da quando ci siamo abbonati al servizio PTN di Darktrace ci hanno fornito le informazioni necessarie per agire immediatamente."
>
> CISO, Better.com

Ask the Expert, 24 ore su 24, 7 giorni su 7

Accessibile direttamente dal Threat Visualizer e dal Customer Portal, Ask the Expert (ATE) è una funzione attivabile che consente al cliente e al suo team della sicurezza di inviare domande ai Cyber Analyst di Darktrace e per ricevere assistenza da parte di esperti durante le indagini sulle minacce in tempo reale. Il cliente riceverà rapidi feedback relativi a minacce nuove o evolute relative al proprio ambiente.

L'accesso all'ATE tramite il Threat Visualizer consente di trascinare la selezione di grafici e dati sul flusso di traffico direttamente nelle richieste inviate. Questo metodo di assistenza consente ai team della sicurezza di collaborare attivamente con i Darktrace Analyst su un'ampia gamma di argomenti. Quando i Cyber Analyst rispondono ad una richiesta ATE, la risposta sarà disponibile nella sezione "Aiuto -> Visualizza domande" nel menu a discesa. Le risposte sono visibili anche nel Customer Portal.

Non c'è alcun limite al numero di richieste che è possibile generare con l'ATE, ma a volte i Cyber Analyst possono reindirizzare il cliente ai team di formazione interna o tecnici operativi se la domanda riguarda maggiormente le funzionalità software e meno l'analisi. I servizi di assistenza software/hardware e le richieste relative alle funzionalità possono sempre essere inoltrate tramite il Customer Portal.

Tutte le richieste ATE sono accodate per l'accesso al team di Cyber Analyst globale di Darktrace, quindi anche se l'ATE non è una funzione di chat diretta, in caso di attacco real-time Darktrace prioritizzerà l'accesso al SOC e fornirà un supporto diretto e feedback rapidi nel corso dell'indagine iniziale, al fine di garantire che il cliente acceda a dati e informazioni generati dalla Cyber AI Platform di Darktrace.

> “Il personale è super disponibile e ben informato... il loro fantastico team di supporto è sempre pronto ad aiutare e rispondere a qualsiasi domanda.”
>
> Specialista IT senior, Media

Fornitura del servizio e dati del cliente

I servizi di Darktrace sono forniti da un team interno di Cyber Analyst che fanno parte del nostro team SOC globale. L'accesso ai nostri servizi disponibili 24 ore su 24, 7 giorni su 7 dipenderà dagli accordi sottoscritti dal cliente nel contratto. Il servizio PTN richiede un collegamento Call Home standard dal dispositivo principale del cliente verso il Management Center Darktrace a Cambridge, Regno Unito. Darktrace provvede e monitora le registrazioni di controllo complete dal Management Center Darktrace, al fine di registrare le azioni completate dai dipendenti Darktrace nel corso dell'esecuzione dei servizi stabiliti dal contratto. I dipendenti Darktrace devono fornire motivazioni verificate sul perché accedono ad un determinato account prima che venga loro concesso un token di accesso.

L'offerta di servizi disponibili richiede che analisi e segnalazione siano eseguiti esternamente alla piattaforma di Darktrace.

Tutti i dati inseriti in Ask The Expert, sia dal cliente che dal team di Cyber Analyst di Darktrace, sono archiviati nel Customer Portal di Darktrace, ospitato da Darktrace nel Management Center di Darktrace. I ticket chiusi rimangono nell'archivio del portale per poter essere riesaminati dal cliente.

I dati di violazione del modello "Enhanced Monitoring" per la Proactive Threat Notification saranno rinviati al Management Center di Darktrace e visualizzati nella SOC di Darktrace. Gli analisti riesamineranno questi dati e accederanno all'installazione del cliente per eseguire ulteriori analisi. Se una violazione giustifica un allarme minaccia immediato, l'analista invierà i propri risultati al cliente, come dettagliato in precedenza. I dati di violazione del modello associati all'allarme e i report inviati al cliente sono conservati nel SOC di Darktrace per poter essere riesaminati dal cliente.