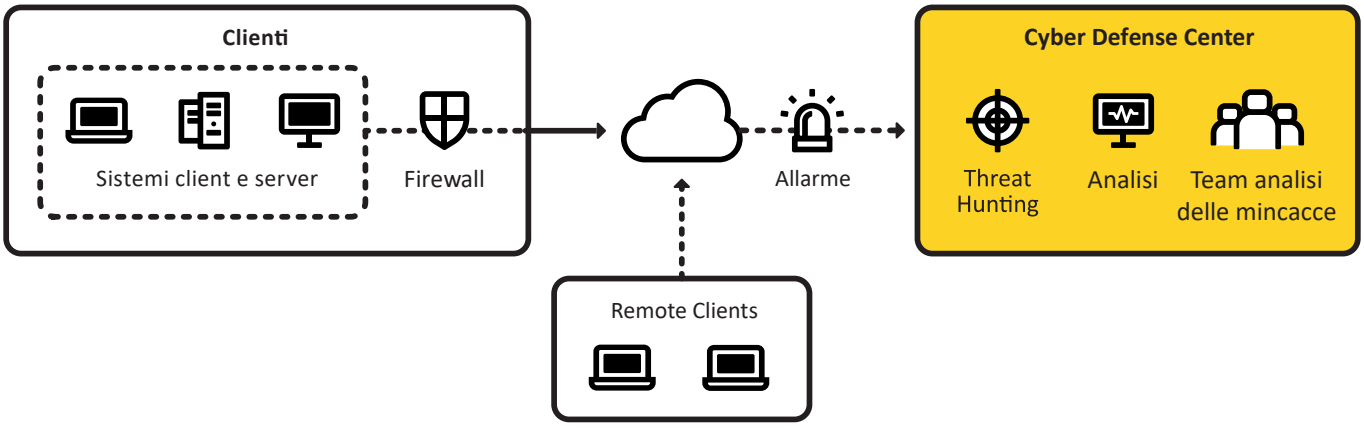
Endpoint Detection Response (EDR) as a Service

Gli endpoint rappresentano un rischio significativo per la sicurezza, poiché sono i bersagli principali degli attacchi informativi verso la rete aziendale. Tuttavia, poiché le tecnologie tradizionali endpoint non sono in grado di rilevare le minacce avanzate più recenti, non è mai stato così difficile identificare e rispondere agli attacchi che colpiscono gli endpoint stessi.

Endpoint detection and response



Con EDR as a Service di UMB potete migliorare notevolmente la visibilità degli attacchi agli endpoint grazie a un team esperto, alla più recente tecnologia EDR e all'accesso alle informazioni più aggiornate sui possibili rischi, in modo da identificare le minacce che potrebbero essere ignorate da altri controlli.

Nuovo livello di sicurezza degli endpoint
Le tecnologie di rilevamento e risposta degli endpoint portano la sicurezza di questi ultimi a un nuovo livello, migliorando la visibilità delle minacce e la risposta davanti a esse, offrendo una copertura maggiore rispetto ai tradizionali strumenti antivirus e di monitoraggio della rete. Su ogni host in cui è installato un sensore, UMB raccoglie importanti informazioni di sistema, come le modifiche al registro di sistema e ai file, e utilizza il monitoraggio del comportamento in tempo reale per rilevare attività sospette. Il rilevamento tempestivo degli attacchi agli endpoint è fondamentale, ma senza un team di professionisti della sicurezza che sfrutti le possibilità della più recente tecnologia EDR e che effettui una scansione proattiva delle minacce 24 ore su 24, è improbabile che la vostra azienda riesca a ottenere i miglioramenti nel rilevamento delle minacce che cercate.

Team di esperti di sicurezza
EDR as a Service di UMB semplifica il monitoraggio degli endpoint 24 ore su 24, 7 giorni su 7, offrendo la tecnologia più recente, un team di esperti di cybersecurity 24 ore su 24 e le informazioni più aggiornate sulle nuove possibili minacce.

Vantaggi di EDR as a Service

Meno impatto sulla vostra attività quotidiana
Identifichiamo, analizziamo e rispondiamo alla maggior parte delle minacce. In modo che voi possiate lavorare in tranquillità.

Ottimizzazione dei costi e delle risorse della sicurezza interna
Date al vostro team IT interno il tempo necessario per occuparsi degli altri problemi di sicurezza mentre UMB si occupa della protezione del vostro sistema.

Servizio di sicurezza modulare e orientato alla domanda 24 ore su 24, 7 giorni su 7
I nostri servizi modulari vi permettono di ottimizzare la vostra cybersecurity in base alle vostre esigenze, sia tecniche che finanziarie.

Opzione Shadow IT - scansione di rete senza agenti

Questa opzione esegue la scansione della rete alla ricerca di asset, anche quando non c'è un agente installato. In questo modo vengono rilevati stampanti, server, dispositivi di archiviazione e anche dispositivi mobili. Se sono disponibili i diritti di amministrazione per questi dispositivi precedentemente sconosciuti, è possibile installare un agente. Inoltre, vengono fornite raccomandazioni per aumentare il livello di protezione all'interno della rispettiva rete.

I vostri vantaggi

- Monitoraggio delle minacce 24 ore su 24, 7 giorni su 7
- Analisi e classificazione delle minacce 24 ore su 24, 7 giorni su 7
- Raccomandazioni concreti per tutti i problemi segnalati
- Raccolta di dati forensi e analisi degli endpoint interessati
- Hotline 24 ore su 24, 7 giorni su 7 con il Centro di difesa informatica
- Rapporto mensile sui servizi

Vi interessa? Contattateci!

Saremo lieti di rispondere alle vostre domande su Cybersecurity, EDR e altro ancora.

Contatti

Markus Kaegi
Team Leader Strategic Sales Consulting
markus.kaegi@umb.ch
+41 58 510 16 98
www.umb.ch