Panoramica di settore 2020: manufacturing

Poiché le minacce che riguardano gli ambienti OT sono sempre maggiori e più sofisticate e le supply chain sono più che mai sotto pressione, un'approccio unificato alla sicurezza sia per gli ambienti IT che per quelli OT è diventato di estrema importanza.

Vantaggi chiave

- ✔ Protocol-agnostic e technology-agnostic, senza alcun riferimento fisso
- ✔ Protezione unificata all'interno di IT, OT e IoT
- ✔ Rilevamento di nuove minacce in tempo reale non appena emergono
- ✔ Comprensione di tutte le comunicazioni all'interno di un ambiente, dal normale traffico PLC a reti di sensori IIoT distribuite

2020: la nuova era degli attacchi OT

Nel mese di giugno 2020, EKANS, una nuova e sofisticata specie di ransomware, ha colpito numerosi stabilimenti di produzione Honda in tutto il mondo. Ha causato il blocco delle operazioni in numerosi paesi, comportando una notevole perdita di ore di produzione e retribuzioni per i dipendenti, nonché i costi necessari a ripristinare i sistemi e a riavviare le operazioni senza dover arrendersi e pagare un riscatto.

Ciò che rendeva EKANS differente era la modalità di attacco, che mirava direttamente alle vulnerabilità ICS, anziché sfruttare software IT senza patch da utilizzare come gateway. Grazie alla propria kill chain (procedura d'attacco) in grado di colpire 64 meccanismi ICS, EKANS rappresenta una nuova frontiera nel futuro degli attacchi informatici OT.

Inoltre, in un momento in cui i produttori sono sotto pressione per riuscire a soddisfare la domanda globale e sostenere le supply chain che alimentano il commercio globale, è fondamentale prioritizzare la sicurezza delle tecnologie OT. Nella primavera 2020, numerosi produttori hanno dovuto improvvisamente modificare le proprie operazioni e avviare la produzione di beni mai prodotti prima, riorganizzando le proprie linee di produzione e implementando nuove tecnologie, e molte di queste trasformazioni sono destinate a rimanere attive per molto tempo.

> "Dieci anni fa il termine "cyber security" significava solo un firewall. Oggi, grazie al 5G e al lavoro da remoto, le aziende sono più esposte alle minacce. Ed è qui che entra in azione Darktrace."
>
> Frédéric Carricaburu, CIO, Saniflo

> "Cyber AI Analyst di Darktrace è rivoluzionario perché anziché mantenere le persone davanti ad un monitor consente davvero di iniziare subito a lavorare per risolvere il problema e riduce il tempo necessario all'analisi dei problemi."
>
> Laura Tibodeau, CIO, AmSty

Un "sistema immunitario" per il settore della produzione

L'Industrial Immune System di Darktrace sfrutta la tecnologia basata sull'AI per proteggere gli ambienti cyber-fisici fondamentali e complessi di centinaia di produttori in tutto il mondo. La tecnologia dell'Immune System di Darktrace è in grado di riorganizzarsi e proteggere macchinari, configurazioni e ambienti eterogenei. Usando il machine learning sia supervisionato che non supervisionato, l'AI di Darktrace non è limitata solo ad un particolare formato digitale, ma è invece in grado di apprendere autonomamente in termini di velocità e portata.

Realizzato sul modello del sistema immunitario del corpo umano, l'Industrial Immune System di Darktrace è in grado di comprendere come sono collegati dispositivi cyber-fisici e tecnologie operative, nonché come utenti e sistemi IT operano ed interagiscono all'interno di infrastrutture digitali cyber-fisiche di grandi dimensioni.

L'AI di Darktrace sviluppa un "pattern of life" mentre elabora informazioni "in corso d'opera" e ciò significa nessuna necessità di formazione supplementare o aggiunta di set di dati. Inoltre, Darktrace è in grado di riconoscere immediatamente attività pericolose ovunque e ogniqualvolta si presentano, dall'ambiente di produzione alla casella di posta in arrivo di un dipendente, e il tutto in tempo reale.

IP colpito da un malware evoluto in un'azienda di produzione medicale

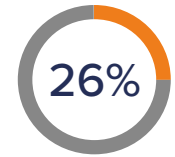
Presso un'azienda di produzione medicale europea, un'assistente amministrativa ha ricevuto un'e-mail di phishing mirata in relazione al pagamento di una fattura allegata. Credendo che l'allegato fosse autentico, ha fatto clic su di esso scaricando involontariamente un malware ad azione rapida, che ha bypassato tutti gli altri controlli di sicurezza.

Questo malware sofisticato aveva come obiettivo le proprietà intellettuali dell'azienda, che includevano formule mediche estremamente riservate. Se questi asset fossero stati compromessi, l'azienda sarebbe stata esposta ad un rischio significativo in termini di competitività e reputazione.

Una volta scaricato il malware, il dispositivo ha iniziato rapidamente a collegarsi ad una rara destinazione esterna, mentre provava a muoversi lateralmente in altri ambienti. In soli due secondi, l'AI di Darktrace ha identificato la presenza estranea.

> "Il machine learning è in grado di rilevare cose che non possiamo predire e definire. È come trovare un ago in un enorme pagliaio."
>
> **Stuart Berman, Information Security Architect, Steelcase**

Dati sulla sicurezza nella produzione



delle aziende non dispone di un reparto che supervisiona la sicurezza dei sistemi di gestione aziendale.

Nell'estate 2020 Darktrace ha rilevato più di 6.500 istanze sospette relative all'uso di protocolli ICS in più di 1.000 ambienti nelle reti IT dei propri clienti.

La dashboard OT Engineer di Darktrace mostra solo gli avvisi più rilevanti dal punto di vista operative