Valutazione MITRE ATT&CK

IBM Security ReaQta offre le migliori funzionalità

Caratteristiche principali

Assicura la continuità delle operazioni aziendali liberando al contempo il team della sicurezza dall'analisi manuale delle minacce informatiche

Riduce le attività legate agli alert e semplifica la sicurezza informatica generando il numero minimo necessario di alert di minaccia

Offre una visibilità completa sui tuoi endpoint per abilitare una risposta rapida in qualsiasi fase

Informazioni sul report

ReaQta, azienda del gruppo IBM, ha creato questa valutazione MITRE ATT&CK Questo report illustra come ReaQta fornisce una copertura completa da attacchi sofisticati praticamente senza alcun intervento umano, producendo al contempo alert di alta qualità.

Cos'è una valutazione MITRE ATT&CK?

MITRE ATT&CK definisce una serie di fasi durante un attacco informatico e valuta le soluzioni in base alla loro capacità di rilevare le minacce. Ciascuna delle fasi elencate rappresenta una “strategia” nella catena d'attacco:

- Accesso iniziale
- Esecuzione
- Persistenza
- Escalation dei privilegi
- Elusione delle difese
- Accesso con credenziali
- Rilevamento
- Movimento laterale
- Raccolta
- Esfiltrazione
- Comando e controllo

Come la valutazione MITRE aiuta le organizzazioni

La valutazione non assegna punteggi e non classifica le soluzioni, ha lo scopo di aiutare le organizzazioni a identificare la soluzione più adatta che soddisfi le loro specifiche esigenze di sicurezza. Le organizzazioni devono tenere presente che la valutazione si svolge in ambienti isolati e presenta dei limiti. Ci sono casi in cui alcune funzionalità di una soluzione sono disabilitate perché non supportano una determinata infrastruttura di laboratorio, come nel caso di ReaQta NanoOS, in cui non è stato possibile utilizzare il live hypervisor per rilevare generici comportamenti dannosi. Tuttavia, la piattaforma ha funzionato bene, anche senza il suo componente principale.

MITRE si avvale di alcune tecniche identificate, ognuna delle quali appartiene a un gruppo di strategie a seconda dell'attore della minaccia selezionato per la valutazione. MITRE ha scelto APT29 per questo round di valutazione.

Compromissione

Raccolta ed elusione

Ricognizione

Espandi accesso

Esfiltrazione

Pulitura

Assicura la continuità delle operazioni aziendali liberando al contempo il tuo team di sicurezza dall'analisi manuale delle minacce informatiche

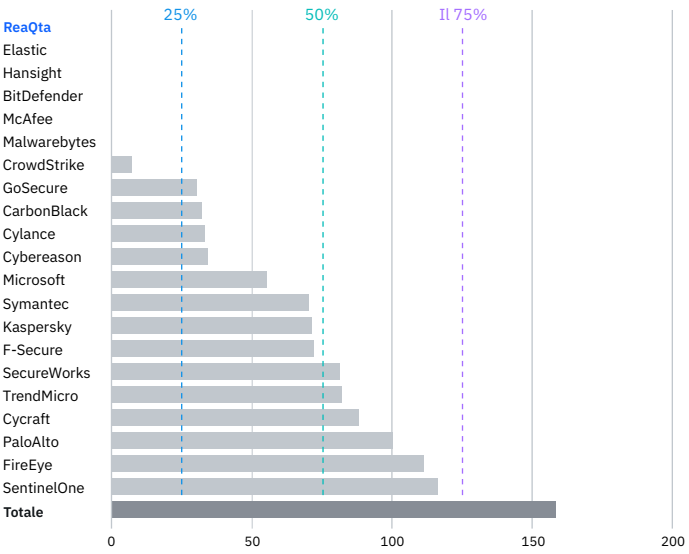
Prima di iniziare la valutazione, ReaQta ha deciso di partecipare senza un Managed Security Service Provider (MSSP), ovvero senza alcuna interazione umana durante l'attacco. MITRE è un framework di valutazione della tecnologia e quindi introdurre gli esseri umani nel processo sarebbe risultato fuorviante. Inoltre, l'utilizzo dei rilevamenti di un MSSP pregiudica pesantemente la valutazione. Il team SOC (security operations center) sa che sta avvenendo un attacco e sa esattamente dove e come viene portato.

L'approccio MSSP non avrebbe fornito ai clienti di ReaQta un'equa valutazione della tecnologia. MITRE ha ascoltato i feedback e, a partire dal Round 3, tutte le aziende verranno valutate senza il coinvolgimento umano.

Gli MSSP aggiungono un grande valore e i clienti dovrebbero essere liberi di scegliere tra MSSP e distribuzioni autonome.

Come riportato nel grafico sottostante, il numero di rilevamenti eseguiti dagli esseri umani ha avuto un enorme impatto sui rilevamenti generati. In molti casi, più del 50% dei rilevamenti, e fino al 73%, sono stati creati manualmente. Solo 6 aziende hanno deciso di partecipare senza che gli esseri umani fossero coinvolti nel processo.

Rilevamenti MSSP (generati manuale)



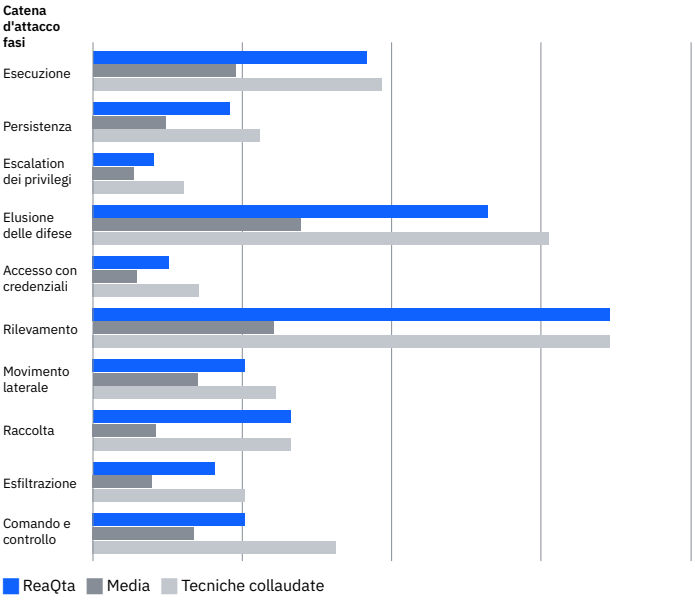
Rilevamenti manuali generati da ciascun provider

Valutazione MITRE Round 2: APT29

I fornitori sono stati testati sulla loro capacità di rilevare le tattiche e le tecniche utilizzate da APT29 (noto anche come The Dukes, Cozy Bear e CozyDuke), un sofisticato avversario di uno stato-nazione noto per il suo approccio furtivo. APT29 è ampiamente noto per essere dietro ad attacchi notevoli: il Pentagono nel 2015, il Comitato Nazionale Democratico nel 2016 e i governi norvegese e olandese nel 2017.

Il cambiamento rispetto al round precedente è stato importante: APT3 (Round 1) è un attore di minacce rumoroso, che adotta vari strumenti con molta meno attenzione al mantenimento di un basso profilo. APT29, d'altra parte, è estremamente furtivo, opera con un profilo molto basso e fa molto affidamento su LOLBins e malware senza file.

Copertura del rilevamento delle tecniche (automatizzata)



Copertura del rilevamento automatico ReaQta rispetto alla media

Risultati della valutazione di ReaQta

L'attacco si è svolto in due giorni in cui gli aggressori si sono gradualmente spostati più in profondità nella rete dopo aver ottenuto l'accesso iniziale. La stragrande maggioranza delle operazioni è stata eseguita utilizzando Microsoft PowerShell, invece di strumenti personalizzati e malware, per mantenere un basso profilo e complicare il rilevamento. L'obiettivo della valutazione è mostrare come le soluzioni testate rispondano all'attacco e che tipo di visibilità viene assicurata nel corso dell'intera catena di attacco.

Come risulta evidente dalla sintesi dei risultati della valutazione, ReaQta ha fornito una visibilità completa sull'intera catena d'attacco. ReaQta ha rilevato il 90% delle strategie e delle tecniche testate, dimostrando la sua capacità di rispondere e rimediare alle minacce in ogni fase dell'attacco.

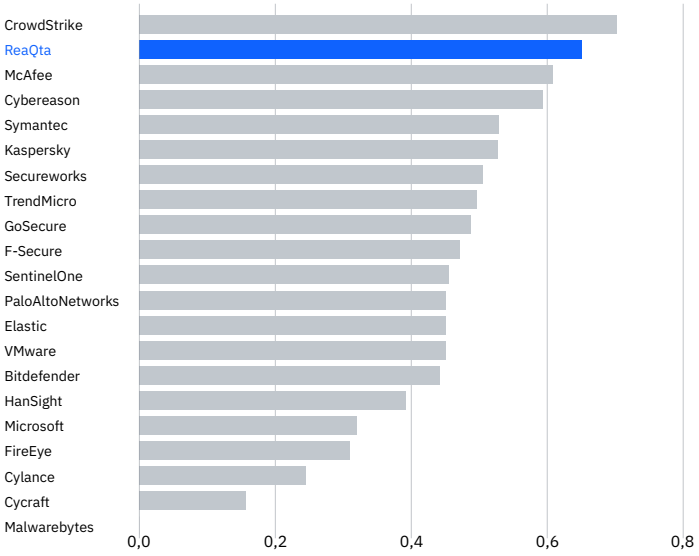
ReaQta mostra uno dei tassi d'intervento più elevati al mondo, anche se confrontato con i fornitori che si affidano ai rilevamenti manuali da parte degli MSSP.

Riduci le attività legate agli alert e semplifica la tua sicurezza informatica generando il numero minimo necessario di alert di minaccia

La piattaforma ha rilevato e generato alert fin dalle fasi di esecuzione, persistenza, escalation dei privilegi ed elusione delle difese, consentendo al team di sicurezza di tenere traccia di APT29 e delle sue azioni. Gli alert della piattaforma sono stati coerenti durante le fasi successive della catena di attacco: movimento laterale, raccolta, esfiltrazione e comando e controllo, mostrando la capacità di ReaQta di rispondere e limitare i danni anche nelle fasi finali di un attacco informatico.

Il tasso di attuabilità ha evidenziato la capacità della piattaforma di ridurre la confusione riducendo il numero di alert generati. La piattaforma ha segnalato tutte le strategie e le tecniche in pochi alert correlati, invece di inviare un alert per ciascuna strategia e tecnica, che equivarrebbe a un elevato numero di alert da esaminare e a cui rispondere, ingestibile per i team SOC.

Concretezza degli alert

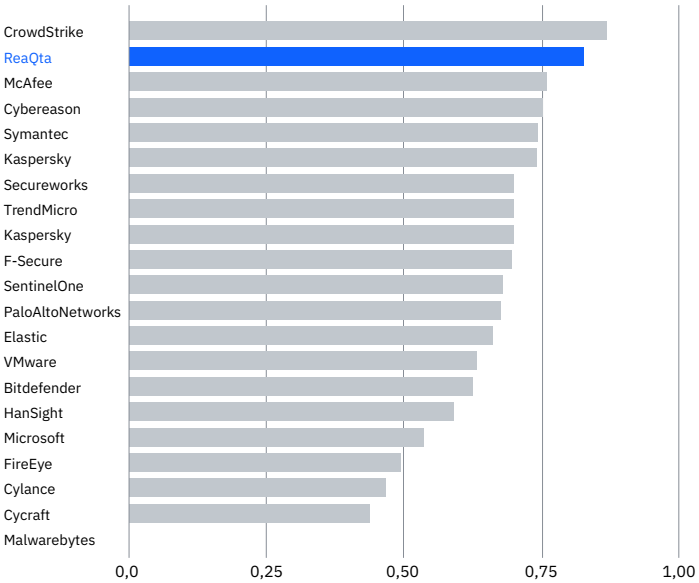


Tassi di perseguibilità (i dati includono i rilevamenti manuali per i fornitori che si affidano agli MSSP)

Ancora una volta, ReaQta fornisce alert di alta qualità senza l'intervento umano, mentre sia il primo che il terzo fornitore classificato hanno fatto affidamento sull'analisi manuale durante la valutazione.

Il livello di visibilità assicurato da ReaQta rende necessario filtrare i dati, correlarli e generare il minor numero possibile di alert, ciascuno contenente la maggior quantità di informazioni correlate. Questo è lo scopo dei motori AI di ReaQta: raccogliere, correlare e riassumere la telemetria. La qualità degli alert è confermata anche dall'analisi di Forrester nel grafico sottostante.

Qualità degli alert



Qualità degli alert (i dati includono i rilevamenti manuali per i fornitori che si affidano agli MSSP)

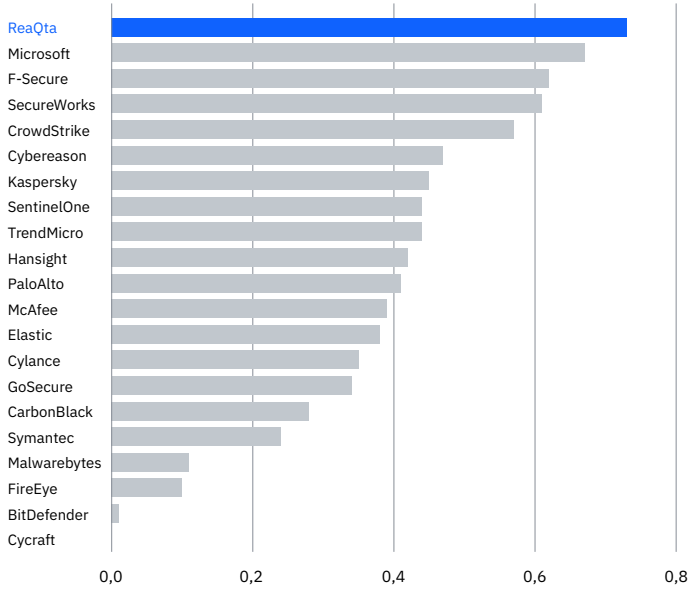
“La concretezza di un avviso è data dal prodotto della sua efficienza per la sua qualità [...] l'efficienza degli alert (non troppi) e la qualità degli alert (quanto consentono di comprendere ciò che accade) sono entrambi correlati e fondamentali per capire quanto ‘concreto’ sarà un determinato avviso”.

Forrester[2]

Fornire alert completi ed affidabili è il criterio che distingue una buona piattaforma dai semplici generatori di rumore.

Il grafico seguente mostra come si è comportato ReaQta rispetto ad altre soluzioni quando sono stati rimossi i rilevamenti manuali. Ciascuna barra rappresenta la quantità di informazioni relative all'incidente acquisite in ciascun avviso generato. I motori di ReaQta hanno catturato la maggior quantità di informazioni, il che si traduce in una considerevole riduzione del carico di lavoro in ambienti reali.

Copertura dell'attacco per avviso generato (rapporto signal-to-noise)



Percentuale di copertura dell'attacco fornita per avviso

ReaQta ha generato solo 25 alert e in ciascuno si essi ha raccolto correttamente tutte le informazioni necessarie per tracciare gli aggressori, invece di creare 158 alert, uno per tecnica verificata.

La capacità di fornire un flusso di lavoro unificato per la risoluzione degli incidenti è fondamentale per ridurre le attività legate agli alert.

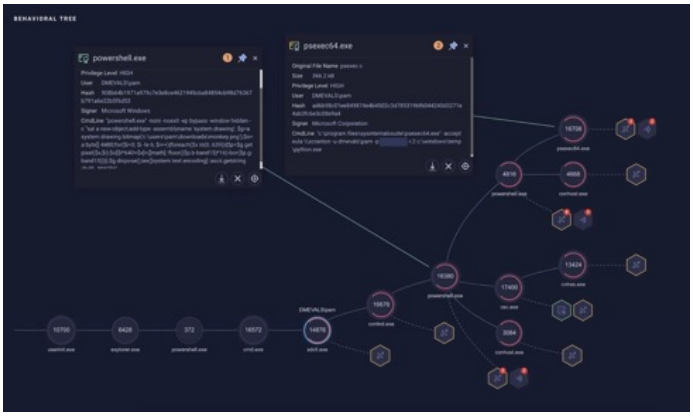
ReaQta ha correlato gli eventi durante la valutazione di MITRE. Ciò ha consentito agli analisti di rilevare e studiare facilmente un aggressore attivo, senza la distrazione di centinaia di alert generati senza alcuna correlazione diretta con l'incidente originale. Questo sarebbe stato molto più difficile da gestire durante un'analisi reale.

L'approccio ReaQta ha ridotto le attività legate agli alert dell'85% preservando la completa visibilità sull'intero attacco. ReaQta è specificamente progettato per generare il minor numero di alert per incidente, dando luogo ad un'esperienza di analisi fluida e senza interruzioni. La possibilità di racchiudere tutte le informazioni in un'unica visualizzazione aiuta gli analisti a rispondere più rapidamente, senza dover passare attraverso la visualizzazione di schermate diverse per ottenere una comprensione completa degli eventi.

Acquisisci una visibilità completa sui tuoi endpoint per abilitare una risposta rapida in qualsiasi fase

La piattaforma è stata in grado di mantenere la correlazione tra le azioni in tutte le fasi della catena di attacco di ATT&CK. La correlazione automatica degli eventi riduce il tempo necessario per mettere insieme i diversi interventi degli aggressori e, in definitiva, riduce il tempo di risposta in caso di attacchi reali.

Struttura comportamentale



ReaQta ha legato gli eventi durante la valutazione di MITRE.

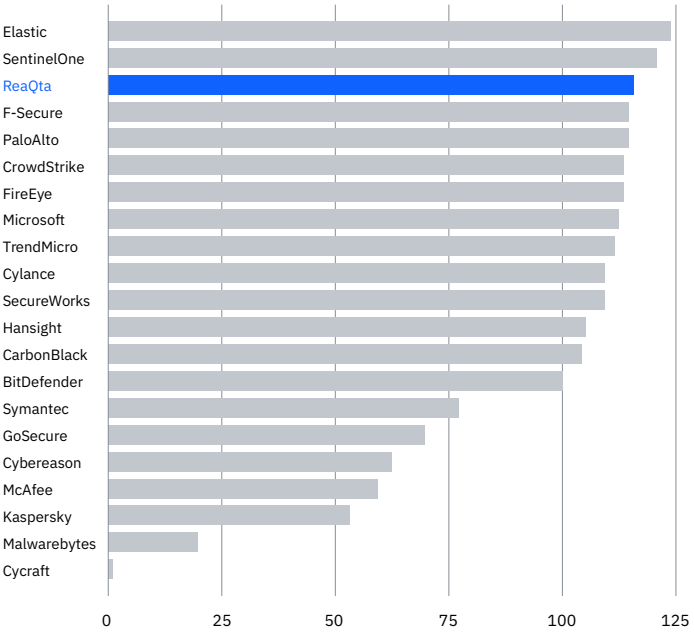
Per fornire un esempio relativo alla valutazione, il grafico precedente mostra come un'intera fase dell'attacco sia stata catturata all'interno di un singolo avviso. ReaQta ha messo in correlazione tutte le informazioni in una trama facilmente comprensibile, fornendo così a un team SOC tutte le informazioni per un triage tempestivo. Non è stata richiesta alcuna interazione umana e l'attacco è stato spiegato chiaramente e il suo rischio è stato valutato, senza richiedere alcuna attività manuale.

Analizzando più nel dettaglio il rilevamento delle strategie e delle tecniche dell'APT29, ReaQta ha assicurato visibilità dalle prime fasi della catena di attacco fino alle fasi più sofisticate, che sono spesso più difficili da rilevare. Ciò che è degno di nota è la capacità della piattaforma di rilevare in modo uniforme le minacce in ogni fase, fornendo così opportunità di risposta e correzione ad ogni stadio.

ReaQta ha evidenziato una delle migliori telemetrie, combinata con un impressionante motore di AI in grado di condensare informazioni e valutare il rischio. Si rivelerà un potente strumento nelle mani di qualsiasi SOC o team che desidera dedicare tempo alla ricerca delle minacce invece di gestire costantemente gli alert.

ReaQta ha evidenziato una delle migliori telemetrie.

Telemetria



Quantità di telemetria fornita da ReaQta

Conclusioni

La piattaforma basata sull'AI di ReaQta fornisce ai team di sicurezza funzionalità avanzate di rilevamento e risposta rapida, riducendo al minimo l'intervento umano, semplificando l'intero processo di sicurezza informatica e promuovendo la continuità aziendale per le organizzazioni di tutte le dimensioni.

Questa valutazione ha confermato la validità dell'approccio di ReaQta al rilevamento di sofisticati attori di minacce. ReaQta continuerà in futuro a partecipare a test di terze parti indipendenti.

ReaQta apprezza l'impegno di MITRE nell'aiutare le organizzazioni a prendere decisioni informate grazie a queste valutazioni.

Per maggiori informazioni, visita:
ibm.com/products/reaqta

IBM Italia S.p.A.
Circonvallazione Idroscalo
20090 Segrate (Milano)
Italia

Prodotto negli Stati Uniti d'America
Marzo 2022

1 MITRE ATT&CK evaluation, The MITRE Corporation and MITRE Engenuity, 2020.
2 Further Down the Rabbit Hole With MITRE’s ATT&CK Eval Data, blog di Forrester, 4 maggio 2020.