

N-able EDR: RemoteOps

RemoteOps è una funzionalità aggiuntiva avanzata per le indagini sulle minacce e l'applicazione di rimedi di N-able EDR, con tecnologia SentinelOne®

Con RemoteOps, i team di risposta agli incidenti e gli analisti SOC possono condurre indagini e applicare misure da remoto per le minacce su più endpoint nell'intera organizzazione gestita. La possibilità di eseguire gli script integrati o quelli personalizzati caricati direttamente dalla console SentinelOne consente a chi si occupa di risposta agli incidenti di raccogliere prove legali, modificare gli strumenti di implementazione delle risposte agli incidenti e accelerare le indagini sulle minacce e automatizzare i flussi di lavoro circa l'applicazione di rimedi in modo semplicissimo. RemoteOps aiuta i team di sicurezza a proteggere in modo efficiente l'organizzazione dalle minacce che richiedono interventi tempestivi.

Name	Type	Status	Priority	Action	ID	Created Time	Updated At	Updated By	Scope Path
Find File by Device	Data Collection	Success	1.00	Scripted	1646545048020501	Mar 19, 2023 04:42:23	Mar 3, 2024 02:21:08	Global	Global
Move File	Action	Success	1.00	Scripted	16465450584131163	Mar 19, 2023 04:42:23	Mar 3, 2024 02:21:08	Global	Global
Roll Back Remove Installed Applicat...	Action	Success	0.01	Scripted	1537838205954902424	Oct 23, 2022 05:15:14	Mar 3, 2024 02:21:07	Global	Global
Download File (Windows)	Action	Success	1.00	Scripted	148171782875132228	Aug 14, 2022 02:42:58	Mar 3, 2024 02:21:08	Global	Global
Multi Action Script (Linux/macOS)	Action	Success	1.00	Scripted	1466645480041002346	Jul 17, 2022 10:02:45	Mar 3, 2024 02:21:09	Global	Global
Multi Action Script (Windows)	Action	Success	1.00	Scripted	1466645480000007488	Jul 17, 2022 10:02:45	Mar 3, 2024 02:21:09	Global	Global
Terminate Processes (Windows)	Action	Success	1.00	Scripted	1466645478194252344	Jul 17, 2022 10:02:45	Mar 3, 2024 02:21:09	Global	Global
Delete Files (Windows)	Action	Success	1.00	Scripted	1466645478161788222	Jul 17, 2022 10:02:45	Mar 3, 2024 02:21:09	Global	Global
Delete Files (Linux/macOS)	Action	Success	1.00	Scripted	146664547816179729	Jul 17, 2022 10:02:45	Mar 3, 2024 02:21:09	Global	Global
Terminate Processes (Linux/macOS)	Action	Success	1.00	Scripted	1466645478161791838	Jul 17, 2022 10:02:45	Mar 3, 2024 02:21:09	Global	Global
Fetch File Path (Linux/macOS)	Artifact Collection	Success	1.00	Scripted	1466645478192118005	Jul 17, 2022 10:02:45	Mar 3, 2024 02:21:09	Global	Global
Download File (Linux/macOS)	Action	Success	1.00	Scripted	14666454781622946110	Jul 17, 2022 10:02:45	Mar 3, 2024 02:21:09	Global	Global
Start Process (Linux/macOS)	Action	Success	1.00	Scripted	1466645478138220789	Jul 17, 2022 10:02:44	Mar 3, 2024 02:21:08	Global	Global
Start Process (Windows)	Action	Success	1.00	Scripted	1466645478161514327	Jul 17, 2022 10:02:44	Mar 3, 2024 02:21:08	Global	Global
Fetch File Path (Windows)	Artifact Collection	Success	1.00	Scripted	1466645472928023191	Jul 17, 2022 10:02:44	Mar 3, 2024 02:21:08	Global	Global
Get Services	Data Collection	Success	1.00	Scripted	1349732020384805187	Feb 4, 2021 02:16:19	Mar 3, 2024 02:21:08	Global	Global
Change Local Firewall	Action	Success	1.00	Scripted	1545278159421243514	May 26, 2021 07:11:21	Mar 3, 2024 02:21:08	Global	Global
Get Security Event Log	Data Collection	Success	1.00	Scripted	1545278159421243513	May 26, 2021 07:11:21	Mar 3, 2024 02:21:08	Global	Global
Get USB Media	Data Collection	Success	1.00	Scripted	154527808968216103	May 26, 2021 07:11:20	Mar 3, 2024 02:21:08	Global	Global
Get Scheduled Tasks	Data Collection	Success	1.00	Scripted	1545278089479020444	May 26, 2021 07:11:20	Mar 3, 2024 02:21:08	Global	Global

Funzionalità principali

- Esegui script per la raccolta dati dalla libreria di script integrata
- Esegui operazioni integrate e script per la raccolta di prove
- Carica ed esegui script personalizzati quando necessario
- Esegui script direttamente dalla console SentinelOne
- Conduci indagini e analizza i risultati su ampia scala
- Automatizza le risposte ad avvisi e minacce
- Supporto per dispositivi Windows, macOS e Linux tramite interfaccia utente/API

Indagini forensi su ampia scala accelerate

- Conduci indagini da remoto sulle minacce nell'intera organizzazione
- Esegui diversi script forensi e strumenti per la risposta agli incidenti su migliaia di endpoint
- Raccogli prove legali in tempo reale per condurre indagini più avanzate
- Accelera la classificazione e l'implementazione di risposte grazie alla libreria di script di RemoteOps

Ottimizzazione delle tempistiche medie di risposta

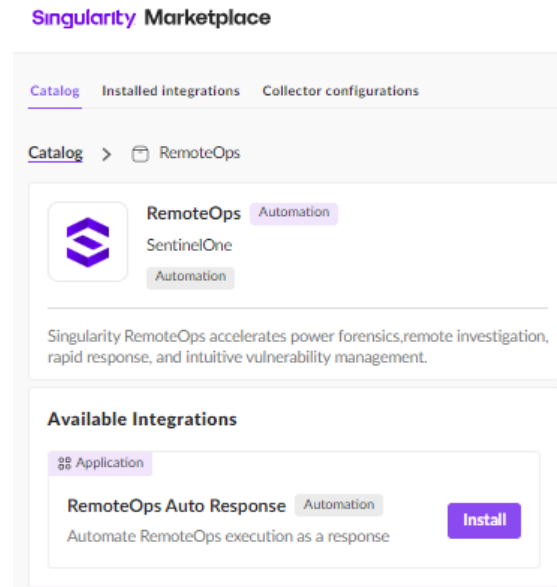
- Adotta misure immediate di risposta per contenere le minacce in tempo reale
- Rispondi alle minacce su più endpoint contemporaneamente
- Identifica potenziali falle per la sicurezza prima che si verifichi un incidente
- Agisci tempestivamente in caso di attacchi tramite un'interfaccia utente semplificata e/o API

Gestione semplificata di vulnerabilità e configurazioni

- Identifica senza difficoltà eventuali vulnerabilità e configurazioni errate per l'intera organizzazione
- Proteggi al massimo gli endpoint implementando pacchetti tramite script personalizzati
- Unifica le attività di gestione con un singolo agent e una sola console

RemoteOps Auto Response

RemoteOps Auto Response, disponibile in SentinelOne Singularity Marketplace, è un'integrazione gratuita che consente agli utenti di ampliare la mitigazione delle minacce impostando l'attivazione automatica di uno script di RemoteOps. È possibile configurare l'integrazione perché risponda ad avvisi e minacce quando si verifica un determinato evento o vengono soddisfatte le condizioni configurate ed esegua immediatamente la raccolta di dati, di prove e/o gli script operazione automatici sull'endpoint sospetto o infetto.



N-able offre ai provider di servizi IT potenti soluzioni software per monitorare, gestire e mettere in sicurezza sistemi, dati e reti dei relativi clienti. Grazie alla piattaforma scalabile su cui si basano i nostri prodotti, offriamo un'infrastruttura sicura e strumenti adeguati per semplificare ecosistemi complessi e le risorse per stare al passo con le esigenze IT in continua evoluzione. Aiutiamo i nostri partner in ogni fase del loro percorso a proteggere i clienti e a espandere la propria offerta di servizi, grazie a un portafoglio flessibile e in continua crescita di integrazioni fornite dai provider di tecnologie leader del settore. n-able.com/it

Il presente documento viene fornito per puro scopo informativo e i suoi contenuti non vanno considerati come una consulenza legale. N-able non rilascia alcuna garanzia, esplicita o implicita, né si assume alcuna responsabilità legale per le informazioni qui contenute, per l'accuratezza, la completezza o l'utilità dei dati qui inclusi.

I marchi registrati, i marchi di servizio e i loghi di N-able sono di esclusiva proprietà di N-able Solutions ULC e N-able Technologies Ltd. Tutti gli altri marchi registrati sono di proprietà dei rispettivi titolari.

© 2024 N-able Solutions ULC e N-able Technologies Ltd. Tutti i diritti riservati.