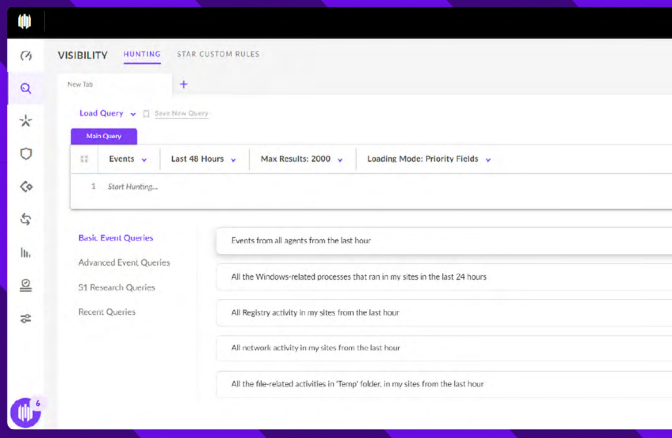
N-ABLE™ Scheda delle funzionalità

Threat Hunting

Una funzionalità avanzata di N-able EDR

Threat Hunting, disponibile in N-able EDR, è una funzionalità avanzata che consente a MSP e reparti IT di individuare minacce informatiche nascoste e di rispondere a eventuali incidenti più rapidamente. Grazie all'elevato livello di visibilità sugli endpoint, i professionisti della sicurezza possono cercare indicatori di compromissione, recuperare tutti i dettagli di una minaccia in base alla correlazione in tempo reale dei dati dell'endpoint, identificare comportamenti sospetti prima che venga sferrato un vero e proprio attacco e prendere misure appropriate.



Vantaggi chiave e funzionalità

- Individua eventuali indicatori di compromissione, di attacco o gli indicatori comportamentali MITRE Engenuity™ ATT&CK®
- Usa l'estensione di ricerca per il browser per cercare sul web gli indicatori che ti interessano e rintracciarli nel tuo ambiente
- Crea query di ricerca personalizzate o utilizza la libreria di query per la ricerca esistenti

Riduci le attività del Security Operation Center con l'automazione

- Migliora le risorse del Security Operation Center grazie alle regole di ricerca automatizzate, alla correlazione dei dati e all'applicazione di rimedi con un solo clic
- Trasforma le query personalizzate in regole automatizzate di ricerca minacce grazie a Storyline Active Response™ (STAR)
- Riduci le tempistiche legate alle indagini manuali e il fastidio degli avvisi

Approfitta della visibilità completa sugli endpoint e delle informazioni fruibili

- Scopri cosa è successo all'ambiente grazie alla correlazione dei dati in tempo reale basata su IA e a Storyline™
- Sfrutta la conservazione dei dati innocui per analisi complete

N-able EDR dispone della tecnologia SentinelOne®, leader di settore per:

- Valutazione MITRE Engenuity™ ATT&CK®
- Report Gartner® Magic Quadrant™

Conduci indagini rapide e accurate

- Visualizza l'attività delle minacce (la catena completa degli eventi che hanno portato a un attacco) per comprendere rapidamente il contesto, la causa scatenante e i lateral movement
- Esegui query e valutazioni su elevati volumi di telemetria EDR

Collegati senza intoppi ai sistemi di terze parti

- Semplifica gli eventi syslog per il SIEM
- Usa le notifiche granulari per assegnare la priorità e instradare i ticket tramite il sistema di gestione di ticket PSA
- Utilizza i servizi API

N-ABLE™

In N-able, la nostra mission è proteggere le attività dalle minacce informatiche in evoluzione con una piattaforma unificata di resilienza informatica per gestione, messa in sicurezza e ripristino. La nostra infrastruttura tecnologica scalabile include funzionalità basate su IA, integrazioni di terze parti leader del settore e la flessibilità necessaria per utilizzare le tecnologie di preferenza al fine di trasformare i flussi di lavoro e di produrre risultati di sicurezza critici. Il nostro approccio incentrato sui partner combina prodotti, esperti, formazione ed eventi tenuti da colleghi che consentono ai nostri clienti di stare al sicuro, essere resilienti e avere successo. n-able.com/it

---