Seqrite **EDR Cloud**

Da qualche anno gli attacchi informatici furtivi ed elusivi contro gli endpoint aziendali sono in costante aumento.Le soluzioni di rilevamento e risposta tradizionali sono ormai inadeguate e insufficienti, perché non sono in grado di reperire efficacemente i dati necessari per rilevare e rispondere a queste attività insolite.

Seqrite EDR Cloud è una solida soluzione di rilevamento e risposta che riesce a far fronte a questo problema perché offre, continuativamente, massima visibilità sui dati e una maggiore possibilità di controllo sugli hardware, sui sistemi operativi e sulle applicazioni. Consente di esaminare gli alert ed eventi passati, interrogare il sistema per ricavarne i dati più recenti ed eseguire attività di risposta e ripristino (sia manuali che automatiche) in tempo reale.

Caratteristiche di Seqrite EDR Cloud:

Verifica in più fasi

Esamina tutti gli eventi di sistema attraverso più livelli di sicurezza: analisi comportamentale, comparazione delle firme e rilevamento basato su machine learning (ML).

Supporto per reti offline e air-gapped

Seqrite EDR offre il supporto più avanzato per le reti air-gapped. Può aggiornare le regole di comportamento e gli IOC (Indicatori di compromissione) e ha capacità di risposta autonoma offline in ambienti aziendali di questo tipo.

Ricerca automatizzata e manuale degli IOC

Effettua ricerche automatizzate e manuali degli Indicatori di Compromissione (IOC) sui dati storici, utilizzando IOC provenienti dalle più recenti informazioni di Threat Intelligence fornite dal team Seqrite Threat Intelligence e da altre fonti.

Sistema di notifiche avanzato

Si integra perfettamente con tutte le soluzioni SIEM e invia alert tramite SMS o email.

Dashboard e widget

Fornisce resoconti completi sullo stato del sistema, inclusi incidenti principali, sintesi generali, eventi di sicurezza più interessanti e il tasso di falsi positivi tramite elementi grafici e widget intuitivi.

Report

Offre riepiloghi dettagliati degli alert nel tempo, fornendo approfondimenti in linea con la classificazione dei TTP (Tattiche, tecniche e procedure dei cyber criminali) stabiliti dal MITRE.

Rule Builder e regole

Permette di creare regole di sistema e personalizzate, utilizzando l'apposito strumento di creazione di regole (Rule Builder): definisci così regole e procedure personalizzate per individuare attività afferenti al framework MITRE e qualsiasi altre attività insolite sugli endpoint.

Gestione della policy di risposta e risposta basata sul rischio

Implementa policy di risposta alle minacce in tempo reale e offline con scopi predefiniti per attivare l'auto risposta in base al rischio.
Utilizza policy generiche o personalizzate.

Strumento di investigazione degli incidenti

Aiuta le indagini sugli incidenti fornendo analisi approfondite, informazioni utili rispetto al contesto in cui l'incidente è occorso, interrogando i sistemi per avere dati in tempo reale e elencando gli alert: facilita così risposte centralizzate in base agli alert.

Gestione degli incidenti

Consente di gestire gli incidenti attraverso l'elenco degli incidenti, informando gli utenti e elencando gli endpoint colpiti mentre stabilisce le azioni di recupero.

SEQRITE

Vantaggi di Seqrite EDR Cloud

Contrasta gli attacchi avanzati

Il nostro sistema di rilevamento degli endpoint analizza ogni evento di telemetria generato dai sensori attraverso più fasi di analisi per eseguire una verifica contestuale approfondita. Se viene rilevata un'attività sospetta, il nostro sistema EDR può bloccarla immediatamente.

Blocca i malware prima che possano colpire

Attraverso azioni automatizzate in tempo reale, come l'isolamento del sistema o l'interruzione dell'esecuzione dei file, vengono notevolmente ridotte le possibilità che un attaccante riesca ad eseguire un attacco con successo.

Tutti i vantaggi dell'analisi approfondita

Seqrite EDR raccoglie informazioni estremamente utili riguardo all'esecuzione di file, script, comandi e catene di processi: grazie a questi importantissimi dati viene ridotto drasticamente il tempo necessario agli analisti per l'analisi e la risposta. Questa funzionalità permette di soddisfare più facilmente i requisiti di conformità e gli standard.

Riduce la necessità di rivolgersi a terze parti per la risposta agli incidenti e l'analisi forense

Il nostro sistema Endpoint Detection & Response consente al team di sicurezza IT di condurre analisi dettagliate sugli attacchi ma in maniera del tutto indipendente: non serviranno consulenti o aziende terze per svolgere queste attività.

Analisi dei dati storici in cerca di minacce nascoste

Gli attacchi avanzati utilizzano tecnologie elusive e silenziose per rimanere nascosti nell'ambiente aziendale per molti mesi. Sfruttando il nostro archivio di dati degli eventi e la Threat Hunting, combinati con le più recenti informazioni di Threat Intelligence, è possibile individuare comunque le minacce nascoste e intraprendere azioni di risposta immediate.

Rafforza la protezione degli endpoint della tua azienda con il rilevamento e il blocco di malware complessi. Ottieni tutti i vantaggi dell'analisi degli endpoint tramite un vero sistema EDR.

SEQRITE | Quick Heal Technologies Limited
Seqrite Italia www.seqrite.it | cs@s-mart.biz | +39 055 43 03 52 | Distribuito da s-mart.biz