





Introduzione

Seqrite Malware Analysis Platform (SMAP) è una soluzione avanzata di cybersecurity progettata per analizzare, rilevare e rispondere alle minacce malware in evoluzione. La piattaforma sfrutta l'elaborazione multi-stadio, il rilevamento basato sul comportamento e un'analisi forense profonda per fornire una miniera di intelligence sulle minacce completa. Si integra perfettamente con le piattaforme SIEM, SOAR e EDR/XDR, garantendo un rilevamento e una mitigazione delle minacce migliorati.



Funzionalità chiave



Analisi multi-fase

Combina analisi statica, basata sul comportamento e manuale per una valutazione completa delle minacce.



Rilevamento basato su firma

Identifica rapidamente malware noti utilizzando database di pattern esistenti.



Rilevamento basato sul comportamento

Rileva comportamenti sospetti o dannosi monitorando le attività di runtime e Indicators of Compromise (IOC).



Analisi del traffico di rete

Analizza il comportamento di rete per rilevare comunicazioni C2 (Command-and-Control), traffico di botnet e tentativi di esfiltrazione dei dati.



Estrazione IOC

Estrae automaticamente e presenta tutti gli Indicatori di Compromissione osservati per il threat hunting e la correlazione.



Ricerca di reputazione

Sfrutta oltre un miliardo di record classificati (Clean/Malicious) per una rapida arricchimento delle minacce intelligenti.



Supporto al ricercatore delle minacce

Consente agli analisti di contribuire con riscontri manuali e migliorare l'accuratezza del rilevamento e la base di conoscenze.



Analisi del codice QR

Estrae e analizza URL incorporati e payload dai codici QR per rilevare collegamenti dannosi e minacce nascoste.



Supporto esteso ai tipi di file

Supporta l'analisi di eseguibili, documenti, PDF, script, archivi e altro.



Integrazione con controlli di sicurezza

Consente l'invio automatico di campioni e integrazione senza soluzione di continuità con controlli di sicurezza minaccia esterni es. SOAR, SIEM, XDR, ecc.



Distribuzione on-premise e cloud

La soluzione è funzionale sia nel cloud sia in ambienti isolati.



Ricerca avanzata

Consente una ricerca granulare tra hash SHA-256, tipi di file, livelli di gravità, verdetti e altro.



Reporting dettagliato

Genera report JSON e PDF mappati a MITRE ATT&CK. Include alberi di processo grafici, relazioni tra processo padre-figlio e prove visive di esecuzione.



Integrazione con Seqrite Threat Intel (STI)

Arricchisce l'intelligence identificata con attributi aggiuntivi e contesto con supporto alla condivisione di riscontri a livello di comunità.



Controllo degli accessi basato sui ruoli (RBAC)

Fornisce accesso sicuro multi-utente con permessi personalizzabili in base ai ruoli e alle responsabilità.



Vantaggi della Piattaforma di Analisi Malware Seqrite



Protezione Completa

Analizza i file in più fasi per rilevare e mitigare una vasta gamma di minacce.



Accesso Esteso al Repository

Sfrutta le informazioni provenienti da oltre cinquecentomila campioni analizzati quotidianamente nel database completo di Seqrite.



Risposta agli Incidenti più Rapida

Riduci i tempi di risposta agli incidenti eseguendo una verifica della reputazione o un'analisi dettagliata del comportamento del campione sospetto utilizzando la nostra Piattaforma di Analisi Malware Seqrite.



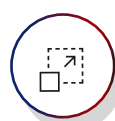
Conformità Migliorata

Aiuta a soddisfare gli standard di settore identificando e mitigando proattivamente i rischi.



Informazioni Utili

I rapporti di analisi dettagliati forniscono azioni immediate per affrontare le vulnerabilità.



Architettura Scalabile

Adatto per aziende di tutte le dimensioni.



Informazioni su Seqrite

Seqrite è un fornitore leader di soluzioni di cybersecurity per aziende. Con focus sulla semplificazione della cybersecurity, Seqrite offre soluzioni e servizi completi attraverso il nostro stack tecnologico brevettato basato su AI/ML per proteggere le aziende dalle minacce più recenti, mettendo in sicurezza dispositivi, applicazioni, reti, cloud, dati e identità. Seqrite è la branca Enterprise del marchio globale di cybersecurity, Quick Heal Technologies Limited, l'unica azienda quotata di prodotti e soluzioni di cybersecurity in India.

Oggi, oltre 30.000 aziende in più di 70 paesi si affidano a Seqrite per le loro esigenze di cybersecurity.

SEQRITE

Distribuito da s-mart.biz

Telefono: +39 055 43 03 52 | cs@s-mart.biz | www.seqrite.it |

 /Seqrite Italia