SentinelOne

SCHEDA TECNICA

Nexus Embedded AI SDK

Sfruttate la potenza del machine learning basato sull'AI per individuare le minacce nelle superfici di attacco esterne agli endpoint

Nexus Embedded AI è un kit di sviluppo software (SDK) che include il potente motore AI statico di SentinelOne.

Permette alle organizzazioni di analizzare i file e di individuare quelli malevoli. La tecnologia Nexus SDK è rapida, flessibile e portatile ed è progettata per diverse applicazioni di controllo tecnico della sicurezza. Nexus SDK è ideale per gli scenari d'uso in cui un dispositivo non supporta l'installazione di un agente SentinelOne tradizionale.

Consente di analizzare e identificare i malware all'interno di servizi cloud come gateway e-mail e web, CASB, servizi di sincronizzazione e condivisione di file, file server tradizionali, chioschi di scansione USB, dispositivi medicali, istanze SCADA/ICS, container e numerose applicazioni personalizzate.

Nexus SDK classifica ogni file analizzato come benigno, malevolo o sospetto e include uno o più indicatori per spiegare la classificazione. Questo permette agli operatori di capire meglio perché la piattaforma SentinelOne ha considerato un file come una minaccia.

Scenari d'uso

GATEWAY FIREWALL/WEB/E-MAIL

Rilevazione di attacchi basati su file mediante analisi statica nei punti di ingresso della rete

APPLICAZIONI SAAS

Analisi e messa in quarantena delle minacce introdotte dai prodotti per la sincronizzazione e la condivisione dei file aziendali, oltre all'analisi integrata dei dispositivi di archiviazione cloud (ad esempio, Bucket S3 AWS)

SANDBOXING/RAPPORTI FORENSI

Pre-scansione dei file prima dell'analisi della sandbox per l'assegnazione delle priorità delle code, l'inserimento dinamico negli elenchi consentiti e gli indicatori statici per il malware

DISPOSITIVI DI ARCHIVIAZIONE PORTATILI

Protezione delle immagini del sistema operativo, come Windows to Go, che vengono caricate su unità USB consegnate ai dipendenti o ai consulenti esterni

SISTEMI DI INTRATTENIMENTO PER VEICOLI

Prevenzione del download accidentale di minacce che potrebbero avere un impatto negativo sui sistemi di intrattenimento per veicoli

PANORAMICA DI NEXUS SDK

+ Non è richiesto l'uso di Internet
  Supporto Air gap e SCIF
+ Classificazione dei tipi di file supportati in benigni, malevoli e sospetti
+ Indicatori per spiegare le classificazioni
+ Classificazione fornita in millisecondi
+ Campioni di codice SDK inclusi

REQUISITI DI SISTEMA

Windows 7, 8, 8.1, 10 (32/64 bit) Ubuntu 14.04 e versioni successive (64 bit). Attualmente l'SDK supporta linguaggi C, C# e Python. Predisposizione per ICAP.

FORMATI FILE DI SUPPORTATI

Windows PE, PDF, Linux ELF, Microsoft Office (.doc, .ppt, .xls, .docx, .pptx, .xlsx) e file di archivio (RAR, 7zip, tar, tar.bz2, Zip), Mach-O, LNK con mappatura CVE.

Nexus SDK offre la rilevazione di malware basata su modelli AI/ML, non su firme.

Maggiori informazioni su sentinelone.com