SecneurX

Solution Brief

SecneurX Advanced Malware Analysis platform (Sandbox alternative)

Product Overview

SecneurX Advanced Malware Analysis platform helps users make an intelligent decision based on a file's or URLs behavior. The platform detonates and analyses sophisticated, targeted and evasive threats and collects IOCs based on behavioral and network analysis to detect malicious objects.

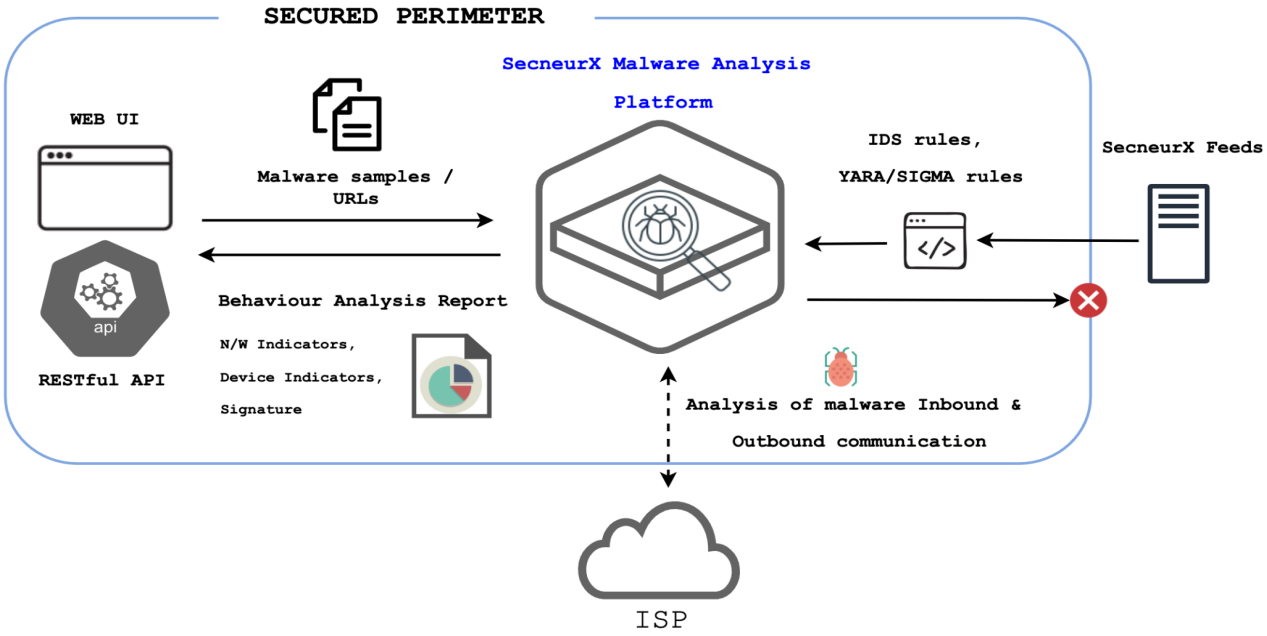
Technology

Threat landscape is changing and newer malware is adopting a variety of methods to avoid executing its malicious code in a sandbox environment. For the malicious code to execute, the analysis environment must therefore be capable of accurately mimicking normal end-user behavior. Our platform is based on a unique architecture that emulates an enterprise environment for analyzing the most evasive and concealed malware. It offers a hybrid approach, combining behavioral analysis, and anti-sandbox detection techniques. an AI-based module interacts with the user interface to expose its possible malicious actions and identifies 'dormant code' for deep analysis. This increases the accuracy of threat detection and the speed of investigation. It can be deployed as a cloud or on-premises solution.

Product highlights / Capabilities

- Supports the analysis of a variety of file types including Windows executables, Office documents, and Android APKs.
- Advanced anti-sandbox detection techniques
- Detect suspicious activities with associated network connections
- Detailed analysis reports, including all process activities, files dropped, network activities (PCAP)
- UI based file/URL submission and RESTful API for seamless integration and automation of security operations
- Supports custom images to analyze threats across a variety of operating systems and applications

The diagram below describes the high-level architecture of SecneurX Advanced Malware Platform



Once the analysis is complete it provides a detailed report on the behavior and functionality of the analyzed sample, allowing user to define the appropriate response procedures:

- Summary — general information about a file's execution/URL browsing results.
- Process Tree – Showing the relations between different processes and their sub-processes (second stage attack).
- Process Created — a list of processes created and their command line
- Screenshots — a set of screenshots can be taken during the file execution/URL browsing.
- File operations — a list of file operations that were registered during the file execution/URL browsing.
- Registry operations — a list of operations performed on the OS registry that were detected during the file execution/URL browsing.
- Downloaded files — a list of files that were extracted from network traffic during the file execution/URL browsing.
- Dropped files — a list of files that were saved (created or modified) by the executed file.
- HTTPS/HTTP/DNS/IP/TCP/UDP and etc. — network sessions/requests details that were registered during the file execution/URL browsing.
- Network traffic dump (PCAP) — network activity can be exported in PCAP format.