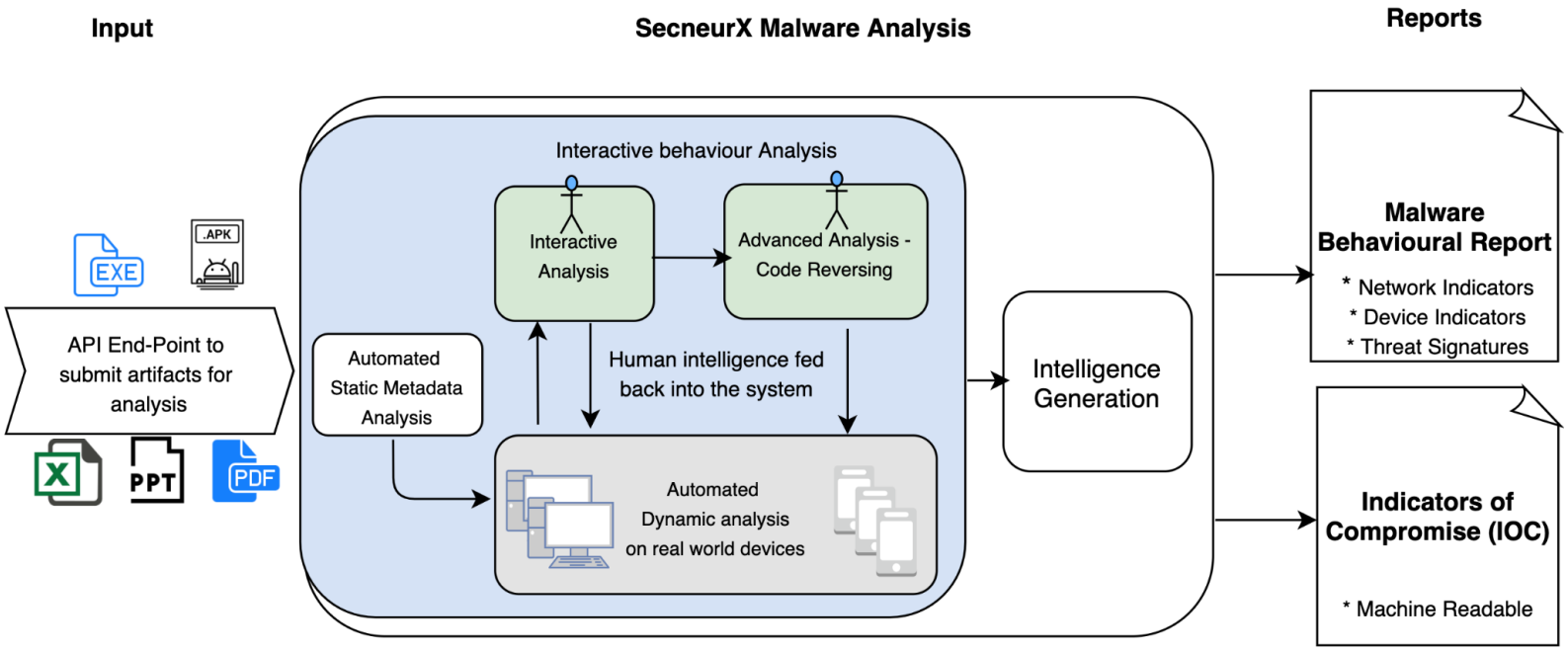
SecneurX

Advanced Malware Analysis as a Service

COMPLETE VISIBILITY INTO UNKNOWN THREATS

SecneurX Advanced Malware Analysis gives security analysts ability to understand sophisticated malware attacks and strengthen their defenses. SecneurX Malware Analysis performs deep analysis of evasive and unknown threats, and enriches the results with threat intelligence. Analysts can safely execute and inspect advanced malware, zero-day and advanced persistent threat (APT) attacks embedded in web pages, email attachments and files.



Stages of Malware Analysis

Static Metadata Analysis

Static properties include strings embedded in the malware code, header details, hashes, metadata, embedded resources, etc. This type of data can be acquired very quickly because there is no need to execute the program in order to see them.

Dynamic Analysis on Real world devices

Dynamic malware analysis executes suspected malicious artifacts in real world devices. This helps detect unknown threats, even those from the most sophisticated malware and provides threat hunters and incident responders with deeper visibility, allowing them to uncover the true nature of a threat.

Interactive Behaviour Analysis

If the automated dynamic analysis fails to collect information on the Malware then the creative analyst at SecneurX steps in for deep analysis. Data generated by the interactive Behaviour Analysis is rich & unique in the industry.

FEATURES:

- Analyzed using real-world devices with human in the loop to defeat even the most evasive malware.
- Saves time with easy-to-understand reports, actionable IOCs and seamless integration.
- Supports Windows and Android operating systems.
- Analyzes all major file types that include a wide variety of executables, document, image formats, and script and archive files.
- Comprehensive visibility on network activity with decrypted SSL communication.

BENEFITS

- Eliminate the cost and overhead of creating and maintaining multiple test configurations.
- Generates intuitive reports with In-depth insight into all files, Registry network and malware process activity.
- Automated Analysis to improve efficiency.
- Identify signature less malware.

EMPOWER SECURITY TEAM

Deep analysis of evasive and unknown threats and enriching the results with threat intelligence delivers actionable indicators of compromise (IOCs). Analysis reports provide visibility into real-world threats, enabling security teams to make faster, better decisions, enhancing the capability of all members.

Analyse Unknown Threats

Unique hybrid analysis technology detects unknown and zero-day exploits.

Complete Visibility

Gain insight into cyber attacks to lower business risks.

Easy to Understand Reports

Improve the effectiveness of the security team with easy to understand reports, actionable IOCs.

---

contact@secneurx.com | www.secneurx.com
Copyright © 2021 SecneurX Technologies Private Limited