

SentinelOne Use Case

인공지능 기반 보안 공격 분석의 용이성 (워크플로우 탐색)

SentinelOne엔진에 따른 악성코드의 분류,
Overview, Story Line 등을 통해 가시화 하여
분석의 용이성을 더합니다.

SAMSUNG SDS

Analyze 화면

The Analyze screen displays detailed information about a detected file. On the left, under 'File Info', it shows the file name 'a.out', path 'C:\Users\localadm\Downloads\...', device 'win7en-VirtualBox', console visible IP '203.244.212.28', IP address '102.103.1.70.30.173.122', domain 'localdomain', username 'localadm', agent version '2.6.4.1071', site 'samsung_sds_test', and group 'Default Group'. It also lists identification and reporting times. On the right, the 'Summary' section shows risk levels as 'N/A', SHA1 hash, and signature identity. Below this, it indicates the detecting engine is 'Reputation' and provides a download link for the file. At the bottom, there are sections for 'NO NETWORK CONNECTIONS', 'ATTACK OVERVIEW', 'ATTACK STORY LINE', 'RAW DATA REPORT', and 'PROCESS (1)'.

Attack Story Line

The Attack Story Line interface visualizes the execution flow of a malware process. It shows a central node for 'cmd.exe (Modesty B...' with arrows pointing to other processes: 'cmd.exe (CLI interp...', 'instan.exe', 'conhost.exe', and 'POWERPNT.EXE (TEST...'. Each process is represented by a gear icon with a red 'X' indicating a security event. Below the diagram, the text reads: '- 악성코드의 전개방식' and '- 활동내역'.

Attack Overview

The Attack Overview screen provides a high-level summary of the attack. It features a 'CATEGORIES (Events Count)' section with a severity scale from 'LOW' to 'HIGH'. The 'EVENTS STATISTICS' section includes four circular gauges: 'FILES' (0), 'EVENTS' (1, 100%), 'PROCESSES' (1), and 'REGISTRY' (0). Below the statistics, the text reads: '- 시스템 조작도' and '- 악성 코드의 발생 이벤트통계'.