List of covered sigma rules

Antivirus Password Dumper Detection
- **description**: Detects a highly relevant Antivirus alert that reports a password dumper
- **category**: data/test
- **level**: critical
- **id**: 78cc2dd2-7d20-4d32-93ff-057084c38b93

Antivirus Hacktool Detection
- **description**: Detects a highly relevant Antivirus alert that reports a hack tool or other attack tool
- **category**: data/test
- **level**: high
- **id**: fa0c05b6-8ad3-468d-8231-c1cbccb64fba

Antivirus Ransomware Detection
- **description**: Detects a highly relevant Antivirus alert that reports ransomware
- **category**: data/test
- **level**: critical
- **id**: 4c6ca276-d4d0-4a8c-9e4c-d69832f8671f

Antivirus Exploitation Framework Detection
- **description**: Detects a highly relevant Antivirus alert that reports an exploitation framework
- **category**: data/test
- **level**: critical
- **id**: 238527ad-3c2c-4e4f-a1f6-92fd63adb864

Antivirus Web Shell Detection
- **description**: Detects a highly relevant Antivirus alert that reports a web shell. It's highly recommended to tune this rule to the specific strings used by your anti virus solution by downloading a big webshell repo from e.g. github and checking the matches.
- **category**: data/test
- **level**: critical
- **id**: fdf135a2-9241-4f96-a114-bb404948f736

Antivirus PrinterNightmare CVE-2021-34527 Exploit Detection
- **description**: Detects the suspicious file that is created from PoC code against Windows Print Spooler Remote Code Execution Vulnerability CVE-2021-34527 (PrinterNightmare), CVE-2021-1675 .
- **category**: data/test
- **level**: critical
- **id**: 6fe1719e-ecdf-4caf-bffe-4f501cb0a561

Antivirus Relevant File Paths Alerts
- **description**: Detects an Antivirus alert in a highly relevant file path or with a relevant file name
- **category**: data/test
- **level**: high
- **id**: c9a88268-0047-4824-ba6e-4d81ce0b907c