family: The classification of the malware family (or category) to which the sample belongs.

proc\_pid: Process ID associated with the analyzed sample's execution.

file, urls, type, name, ext\_urls, path: Various details about the analyzed file.

program: Program or executable associated with the analyzed sample.

info, positives, families, description: Different pieces of information about the sample.

sign\_name, sign\_stacktrace, arguments, api, category, imported\_dll\_count, dll: Information about dynamic link libraries (DLLs) and APIs used by the sample.

pe\_res\_name, filetype, pe\_sec\_name, entropy: PE (Portable Executable) resource information, file type, section names, and entropy.

hosts, requests, mitm, domains, dns\_servers, tcp, udp, dead\_hosts: Network-related information, such as hosts, requests, domains, and protocol usage.

proc, beh\_command\_line, process\_path, tree\_command\_line, children, tree\_process\_name, command\_line: Information about executed processes and their command lines.

regkey\_read, directory\_enumerated, regkey\_opened, file\_created, wmi\_query, dll\_loaded, regkey\_written, file\_read: Activities related to reading, writing, and interacting with the Windows Registry, files, and other resources.

apistats, errors, action, log: Miscellaneous statistics, errors, actions, and log information.