

CLAIMS

1. A computer-implementable method for detection of malicious activity by analysis of objects behavior in non-isolated environment, the method comprising:

collecting information into at least one event flow using a detection module;

transmitting at least one event flow to a computing device, obtaining the event flow on the computing device, and analyzing, using the computing device, the obtained event flow for a predetermined amount of time, wherein

transmitting at least one event from the event flow to input of at least one adapter, depending on an event type, wherein at least one adapter generates at least one internal event;

transmitting at least one internal event to at least one signature module, and checking at least one obtained internal event using at least one signature module according to preset rules, and in case of at least one internal event correspondence to the preset rules, creating the at least one internal state marker;

transmitting the at least one internal state marker to input of a malicious activity decision module, wherein, if a at least one internal state marker total weight or a probability of at least one internal state marker maliciousness exceeds a preset value, detecting the malicious activity using the decision module;

assembling a report on suspicious activity.

2. The method of claim 1, wherein at least one internal event enters a pipeline input, the pipeline stores the information, which further is used by the signature module.

3. The method of claim 1, wherein the at least one internal state marker has a lifetime.

4. The method of claim 1, wherein all of the at least one internal state markers have different weights.

5. The method of claim 1, wherein the at least one internal state marker consists of at least of: a set of flags, a file paths, a registry, a processes, a signatures, a mutexes, a synchronization objects, and/or a counters.

6. The method of claim 5, wherein at least one internal state has a lifetime.

7. The method of claim 1, wherein the decision module is made as at least a linear model, a trained classifier or a neural network.

8. The method of claim 1, wherein the malicious activity report comprises at least signature markers, a decision module verdict, a host information, a content of environment variables, an information about connected devices, a screenshot, a screen video during detection, a sequence of user actions, an incident graph.

9. A system for detecting malicious activity by analysis of objects behavior in non-isolated environment, the system comprises:

a detection module installed in a host and configured to collect information about at least one event flow and to transmit at least one event flow to a computing device;

the computing device configured to implement the method for detecting malicious activity by analysis of objects behavior in non-isolated environment according to claims 1-8;
a reporting module.