

CLAIMS

1. A framework for ~~efficiently and~~ automatically exploring a data network and ~~accurately~~ identifying network threats, comprising:
 - a) a plurality of ~~software and hardware based~~ agents, distributed over said data network, and being capable of:
 - a.1) continuously collecting from said data network, by said distributed sensors, data regarding the existence of forensic findings;
 - a.2) adjusting or reconfiguring, ~~on the fly,~~ the behavior of said agents ~~and their ability to~~ threats, so as to collect data in a targeted manner, ~~so as to~~ and investigate suspicious incidents and alerts and collect data that was not yet collected by the system;
 - a.23) collecting forensic data by dynamically allocating tasks to agents and deciding which agents will be active at any time and which tasks will be executed by each active agent and executing tasks defined in workflows, being distributed threat intercepting programs; which are adapted to intercept Advanced Persistent Threats (APTs) within said data network;
 - a.34) reporting about the collected forensic data, back to a Central Control Unit (C&C);
 - b) an Attack Hypotheses Generation module for generating a collection of attack hypotheses according to a combination of known attack patterns having the highest probability during an investigated incident ;
 - c) distributed threat intercepting programs (“workflows”) which are adapted to:
 - b) ~~c.1)~~ provide:
 - b.2.i) instructions to deployed agents ~~and said C&C;~~
 - b.2.ii) branches;
 - b.2.iii) instructions to said C&C;
 - c.2) determine a set of instructions for data collection that constitute an automatic forensic investigation for each hypothesis;
 - c.3) convert each investigation plan to multiple tasks that are assigned to agents;
 - e)d) a Central Control Unit (C&C) for:
 - e.d.1) orchestrating said agents to assure proper execution of said workflows;

ed.2) analyzing the collected information; and

ed.3) presenting ongoing status to an operator supervising said data network.

~~2. The framework according to claim 1, further comprising an Attack Hypotheses Generation module for generating a collection of attack hypotheses, by providing a set of known tools, malware types, and attack patterns that are used by an attacker, and having the highest probability during an investigated incident.~~

~~3.2.~~ The framework according to claim 1, further comprising a Workflow Generation module for adapting threat intercepting procedures to the latest threat intelligence obtained from external sources, or to the likeliest attack hypotheses generated by the Attack Hypotheses Generation module.

~~4.3.~~ The framework according to claim 1, in which the agents adapt their behavior to the emerging threats by executing instructions of different workflows.

~~5.4.~~ The framework according to claim 1, comprising at least one processor for adjusting workflows, based on a combination of Attack Hypotheses Generation and Workflows Generation, said adjusted workflows effectively react to emerging threats in the data network.

~~6.5.~~ The framework according to claim 1, in which the workflows are created according to the following steps:

- a) creating initial workflows are by a domain expert, based on relevant up-to-date threat information, for executing tasks ~~including such as~~ monitoring of the network, detecting anomalies, identifying required forensic data, or performing any other designated tasks;
- b) creating subsequent workflows for detecting previously unknown and undiscovered APTs, being mutations of previously known APTs, by employing the Attack Hypotheses Generation and the Workflow Generation modules; and

c) using newly found APTs to extend the pool of, from which further mutations will be created.

7.6. The framework according to claim 1, in which the agents are configured to execute multiple tasks, depending on ~~the~~ inspected threat.

8.7. The framework according to claim 1, in which the workflows include control operators such as loops and decision points, where one of a few possible steps is to be chosen.

9.8. The framework according to claim 1, in which tasks of a workflow are distributed to different agents, for optimizing one or more of the following criteria:
time efficiency;
balanced CPU consumption;
network traffic consumption.

10.9. The framework according to claim 1, in which the agents execute the various workflows in parallel, serially, or at a specific time or context as determined by an workflow execution plan.

11.10. The framework according to claim 1, in which workflows are represented using Python programming language and executed using RestrictedPython, in order to reduce the risk of exploits.

12.11. The framework according to claim 1, in which the agents are provided by a commercial of the shelf product.

13.12. The framework according to claim 1, in which the collected data is partially processed by the agents locally, and the results are transferred to a central repository for deeper analysis

~~14~~.13. The framework according to claim 1, further comprising Security Information and Event Management (SIEM) product which stores the data collected by said agents and executes a set of correlation, aggregation, and analysis rules defined in said workflows.

~~15~~.14. The framework according to claim 1, in which multi-step attacks are handled by collecting and correlating forensic information from different locations in the network.

~~16~~.15. The framework according to claim 1, in which following the detection of an anomaly, anomalous events are investigated by executing relevant workflows, so as to collect forensic data, validate the event, and track down the attack path.

~~17~~.16. The framework according to claim 1, in which the software agents are installed on PCs and servers across the organization and secured hardware agents are connected to communication switches of the organization's network.

~~18~~.17. The framework according to claim 1, in which the agents are deployed independently using a "plug-and-play" mode, or be installed on existing machines of the organization.

~~19~~.18. The framework according to claim 1, in which the software agents are installed on PCs and servers across the organization and hardened secured hardware agents are connected to network communication switches.

~~20~~.19. The framework according to claim 1, further comprising cyber security plug-ins for detecting IOCs defined in attack descriptions.

~~21~~.20. The framework according to claim 1, in which cyber security plug-ins are one or more of the following:

- anomaly detection;

- IDS rules;
- Signatures;
- Blacklists.

22.21. The framework according to claim 1, in which the switch is configured by the Trusted Monitoring Orchestration module, to mirror only specific selected traffic.