

Claims

1. A computer-implement~~ed~~able method for executing, by an automated response system, making a decision of an automated incident response, the automated response system comprising an interface module, an analytical module, and a response module, the method comprising:

receiving, by ~~an the~~ interface module, an incident detection signal of at least one incident from an external systems, the incident detection signal being indicative of the detection of an occurrence of a computer security incident, the incident detection signal comprising incident data regarding the detected incident;

transmitting the ~~incident information~~incident data to ~~an the~~ analytical module; ~~wherein:~~

determining, by the analytical module, whether the incident has been prevented before by the automated response system, based on the incident data, and if not, then

determining, by the analytical module, the an incident threat severity for the incident, based on the incident data, and if the incident threat severity exceeds a preset threshold,

determining, by the analytical module, an automated response to the incident, based on the incident data, and

~~responding to the incident using the analytical module and executing, by a the~~ response module, the automated response.

2. The method of claim 1, wherein the ~~incident incident data~~data comprises at least one of: an incident category, the incident threat severity, a name or an address of ~~the a~~ host system where the incident occurred and a level of reliability level that the incident is not a false response.

3. The method of claim 2, wherein the incident category is additionally attributed to one of three response categories, the automated response being determined based on the attributed response category.

4. The method of claim 3, wherein, if the incident relates to ~~the a~~ first response category, the response module stops a malicious process associated with the detected incidence and isolates the host system where the incidence occurred.

5. The method of claim 3, wherein, if the incident relates to ~~the a~~ second response category, the analytical module determines ~~the an~~ account where the ~~activity incident~~ occurs, and if the account does not relate to a privileged accounts, ~~it the account~~ is blocked.

6. The method of claim 5, wherein, if the ~~activity-incident~~ occurreds from the privileged account, the reliability level is compared to ~~the a~~ further preset threshold, and if the reliability level is below the further preset threshold, the privileged account is blocked.

5

7. The method of claim 6, wherein the privileged account is blocked if ~~the a~~ a number of blocked privileged accounts for a preset time is less than N_1 accounts.

8. The method of claim 3, wherein, if the incident relates to ~~the a~~ a third response category, the analytical module determines what process has caused the incident, and whether ~~at the~~ host operating system of the host system, where the incident ~~has~~ occurred, is a server operating system.

9. The method of claim 8, wherein, if the incident is caused by a system process and the host operating system is a server operating system, the response module copies the content of the host system's random-access memory.

10. The method of claim 9, wherein the content of the host system's random-access memory is copied only if less than N_2 responses have been done for a preset time.

20

11. The method of claim 8, wherein, if the incident is caused by a non-system process and the host operating system is a server operating system, the response module copies the content of the host system's random-access memory ~~(memory dump)~~ and stops the non-system process.

12. The method of claim 11, wherein the content of the host system's random-access memory is copied only if less than N_3 responses have been done for preset time and the non-system process is stopped.

13. The method of claim 8, wherein, if the host operating system is not a server operating system, the response module isolates from the network the host system where the incident ~~has~~ occurred.

14. The method of claim 13, wherein the host system is isolated from the network only if less than N_4 host systems have been isolated for a preset time.

35

15. The method of claim 1, wherein the automated response ~~process~~ is executed by the response module at ~~the a file level of file~~, at a host system level, and at a corporate network level.

16. The method of claim 15, wherein the response at the file level comprises at least one of the following:

blocking at least one malicious file and quarantining it;

sending at least one malicious file to an isolated environment for a dynamic analysis;

searching for at least one child malicious file, ~~being child malicious file~~, on at least one host system, and deleting ~~the child malicious file~~;

stopping ~~the a~~ malicious process associated with the malicious file or the child malicious file.

17. The method of claim 15, wherein the response at the host system level comprises at least one of the following:

collecting ~~incident information~~ incident data;

copying the content of the host system's random-access memory (memory dump);

sector-based copying of nonvolatile memory of the host system;

isolating the host system from the network;

blocking a start of any applications except for original programs developed by the ~~operating system~~ a manufacturer of a host operating system run by the host system.

18. The method of claim 17, wherein the ~~incident information~~ incident data comprises at least: data on programs automatically loaded at starting the operating system, Prefetch files, running processes, system event logs, and content of temporary directories.

19. The method of claim 15, wherein the response at the corporate network level comprises at least one of the following:

blocking a user account;

running incident handling script files;

sending a report.

20. A computer-implemented method for executing an automated incident response, the method comprising:

receiving, by an automated response system, an incident detection signal from an external system, the incident detection signal comprising incident data regarding the detected incident;

determining, based on the incident data, whether the incident has been prevented before by the automated response system, and if not, then

determining, based on the incident data, an incident threat severity for the incident, and if the incident threat severity exceeds a preset threshold,

5 determining, based on the incident data, an automated response to the incident, and executing the automated response.

210. A automated response system ~~for making a decision of automated incident response, the system~~ comprising:

10 an interface module, ~~the interface module configured to receive incident detection signals from external systems;~~

an analytical module, ~~the analytical module configured to determine conditions and select methods of automated response; and~~

a response module;

15 wherein, _the automated response system module-being configured to-for executinge automated response the method according to any one of claims 1-1920 of the above method.

22. An automated response system for executing an automated incident response, the automates response system comprising:

20 an interface module configured for receiving an incident detection signal from an external system, the incident detection signal being indicative of the detection of an occurrence of a computer security incident, the incident detection signal comprising incident data regarding the detected incident;

25 an analytical module configured for determining whether the incident has been prevented before by the automated response system, based on the incident data, and if not, then determining a threat severity for the incident, and if the threat severity exceeds a preset threshold, determining an automated response to the incident, and

a response module configured for executing the automated response.