CLAIMS

What is claimed is:

1. A cyber breach diagnostics system (100) for diagnosing whether a target network system (102) is breached by hackers, the cyber breach diagnostics system (100) comprising:

an activity records collection device (130), coupled with the target network system (102), and arranged to operably collect multiple suspicious activities records related to multiple computing devices (111~115) in the target network system (102), corresponding multiple time stamps, and corresponding multiple attribute tags, and further arranged to operably process the multiple suspicious activities records, the multiple time stamps, and the multiple attribute tags to generate a return data; and

a suspicious event analysis device (140), arranged to operably receive the return data generated by the activity records collection device (130), and conduct a suspicious event sequence diagram generating operation according to the return data, so as to identify multiple suspicious events with respect to the target network system (102), identify multiple time records respectively corresponding to the multiple suspicious events, and generate and display a suspicious event sequence diagram (550) corresponding to the multiple suspicious events according to the multiple suspicious events and the multiple time records;

wherein the suspicious event sequence diagram (550) comprises: a first main visual object (903) corresponding to a first participating device (111), a second main visual object (905) corresponding to a second participating device (112), a first vertical pattern (933) corresponding to the first main visual object (903), and a second vertical pattern (935) corresponding to the second main visual object (905);

wherein when the suspicious event analysis device (140) identifies that a first device internal event took place in the first participating device (111), and a second device internal event took place in the second participating device (112), but whether a device interaction event of a predetermined type took place between the first participating device (111) and the second participating device (112) cannot be confirmed, the suspicious event sequence diagram generating operation further comprises:

calculating a time difference between a first time record corresponding to the first device internal event and a second time record corresponding to the second device internal event;

comparing the time difference with a predetermined threshold value; and

establishing a speculated relation line (1157) corresponding to a device interaction event of the predetermined type if the time difference is less than the predetermined threshold value.

2. The cyber breach diagnostics system (100) of claim 1, wherein the multiple suspicious events comprise multiple device internal events and multiple device interaction events, while the suspicious event sequence diagram generating operation further comprises:

establishing multiple main visual objects (701~705; 901~909) respectively corresponding to multiple participating devices involving in the multiple suspicious events, wherein at least a part of the multiple main visual objects (701~705; 901~909) corresponds to computing devices of the target network system (102);

horizontally arranging the multiple main visual objects (701~705; 901~909) in an upper area (710) of the suspicious event sequence diagram (550);

establishing multiple vertical patterns (731~735; 931~939) respectively corresponding to the multiple main visual objects (701~705; 901~909);

respectively arranging the multiple vertical patterns (731~735; 931~939) below the multiple main visual objects (701~705; 901~909);

establishing multiple auxiliary visual objects (741~746; 941~946) respectively corresponding to the multiple device internal events;

arranging one or more auxiliary visual objects corresponding to respective participating devices on a vertical pattern below a corresponding main visual object from top to bottom according to a chronological order of corresponding device internal events;

establishing multiple relation lines (751~756; 951~956) respectively corresponding to the multiple device interaction events;

arranging the multiple relation lines (751~756; 951~956) from top to bottom according to their chronological order, and rendering two ends of each relation line to respectively touch two vertical patterns corresponding to two involving participating devices;

configuring a corresponding orientation symbol (761~766, 961~966) on each relation line according to a content of a device interaction event corresponding to the relation line to indicate an orientation of the device interaction event; and

displaying a concise description of a device interaction event corresponding to each relation line.

3. The cyber breach diagnostics system (100) of claim 2, wherein the suspicious event sequence diagram generating operation further comprises:

displaying a concise description of a participating device corresponding to each main visual object; and

displaying a concise description of a device internal event corresponding to each auxiliary visual object.

4. The cyber breach diagnostics system (100) of claim 3, wherein the suspicious event sequence diagram generating operation further comprises:

displaying a corresponding time record of a device internal event corresponding to each auxiliary visual object; and

displaying a corresponding time record of a device interaction event corresponding to each relation line.

5. The cyber breach diagnostics system (100) of claim 2, wherein the suspicious event sequence diagram generating operation further comprises:

repeatedly displaying the multiple main visual objects (701~705; 901~909) in a lower area (720) of the suspicious event sequence diagram (550) according to an identical sequence of the multiple main visual objects (701~705; 901~909) in the upper area (710).

6. The cyber breach diagnostics system (100) of claim 2, further comprising:

multiple device activities reporting programs (120), respectively stored in the multiple computing devices (111~115), and arranged to operably generate the multiple suspicious activities records related to the multiple computing devices (111~115) as well as the multiple time stamps, and to operably establish the multiple attribute tags respectively corresponding to the multiple suspicious activities records.

7. The cyber breach diagnostics system (100) of claim 2, further comprising:

multiple device activities reporting program (120), respectively stored in the multiple computing devices (111~115), and arranged to operably generate the multiple suspicious activities records related to the multiple computing devices (111~115) as well as the multiple time stamps;

wherein the activity records collection device (130) is further arranged to operably establish the multiple attribute tags respectively corresponding to the multiple suspicious activities records.

8. The cyber breach diagnostics system (100) of claim 2, wherein the suspicious event sequence diagram generating operation further comprises:

rendering two ends of the speculated relation line (1157) to respectively touch the first vertical pattern (933) and the second vertical pattern (935);

configuring a corresponding orientation symbol (1167) on the speculated relation line (1157) according to a relative magnitude of the first time record and the second time record, so as to indicate an orientation of the device interaction event of the predetermined type; and

displaying a concise description of the device interaction event of the predetermined type.

9. The cyber breach diagnostics system (100) of claim 8, wherein both the first device internal event and the second device internal event are file generating events with respect to a same file.

10. The cyber breach diagnostics system (100) of claim 2, wherein when the multiple participating devices comprise one or more malicious file providing devices (160) located outside the target network system (102), at least a part of the multiple main visual objects (701~705; 901~909) corresponds to the one or more malicious file providing devices (160).