

CLAIMS:

1. A method of heuristically analysing Binary Large Objects (BLOBs) of information security events as the BLOBs are received for content of potential interest, the method comprising:

buffering a first BLOB of the information security events and a successive second BLOB of the information security events;

forming a first dataset from the first BLOB, the first dataset comprising data indicative of a characteristic of the first BLOB;

forming a second dataset from the second BLOB, the second dataset being formed using a similar characteristic as the first BLOB;

determining statistical parameters of the first dataset and the second dataset;

generating a first behavioural pattern using the statistical parameters of the first and second datasets;

analysing the first behavioural pattern for a variation from a past or an expected behaviour or a predefined behavioural pattern consistent with the content of potential interest; and

issuing a command to a downstream post-processing processor upon detection of the variation or the predefined behavioural pattern.

2. The method according to claim 1, wherein the analysing the first behavioural pattern includes accessing historic data indicative of the past, or the expected behaviour, or of the predefined pattern, and comparing the generated first behavioural pattern with the historic data.

3. The method according to claim 1, wherein the first and second datasets conform to the Central Limit Theorem.

4. The method according to claim 1, wherein the statistical parameters comprise a mean, a variance, a median, a skew or a kurtosis.

5. The method according to claim 1, wherein the generating the first behavioural pattern using the statistical parameters of the first and second datasets comprises:

using the statistical parameters of the first dataset as a start point of the first behavioural pattern generation; and

using the statistical parameters of the second dataset as a second subsequent sequential point of the first behavioural pattern generation,

wherein portions of the generated first behavioural pattern exhibits Brownian motions.

6. The method according to claim 1, wherein the first dataset comprises event log data associated with the first BLOB of the information security events.

7. The method according to claim 6, wherein the second dataset comprises event log data associated with the second BLOB of the information security events.

8. The method according to claim 1, wherein the content of potential interest comprises:

- i) content of potential security concern;
- ii) anomalies in or predefined features of the information security events;
- iii) content contrary to rules of use of a computing system, or impermissible content or illegal content;
- iv) image, audio or video data;
- v) biometric data; or
- vi) bad traffic in an implicit norm policy computer network.

9. The method according to claim 1, wherein the characteristic of the first BLOB comprises a number of hits per data port or ports of receipt of the first BLOB.

10. The method according to claim 1, wherein the command to the downstream post-processing processor comprises a signal configured to initiate a further analysis wherein the further analysis comprises:

buffering a third successive BLOB of the information security events;

forming a third dataset from the third BLOB, the third dataset being formed using a similar characteristic as the first BLOB;

determining statistical parameters of the third dataset;

generating a second behavioural pattern using the statistical parameters of the first, second and third datasets;

analysing the second behavioural pattern for a variation from a past or an expected behaviour or a predefined behavioural pattern consistent with the content of potential interest; and

issuing a further alert upon detection of the variation or the predefined behavioural

pattern.

11. The method according to claim 10, wherein the analysing the second behavioural pattern comprises:

accessing historic data indicative of the past, or the expected behaviour, or of the predefined pattern, and comparing the generated behavioural pattern with the historic data.

12. The method according to claim 10, wherein the first, second and third datasets conform to the Central Limit Theorem.

13. The method according to claim 10, wherein the generating the behavioural pattern using the statistical parameters of the first, second and third datasets comprises:

using the statistical parameters of the first dataset as a start point of the second behavioural pattern generation;

using the statistical parameters of the second dataset as a second subsequent sequential point of the second behavioural pattern generation; and

using the statistical parameters of the third dataset as a third subsequent sequential point of the second behavioural pattern generation,

wherein portions of the generated second behavioural pattern exhibits Brownian motions.

14. A system for heuristically analysing Binary Large Objects (BLOBs) of information security events as the BLOBS are received by the system for content of potential interest, the system comprising:

a processing unit; and

a non-transitory media readable by the processing unit, the media storing instructions that when executed by the processing unit, cause the processing unit to:

buffer a first BLOB of the information security events and a successive second BLOB of the information security events;

form a first dataset from the first BLOB, the first dataset comprising data indicative of a characteristic of the first BLOB;

form a second dataset from the second BLOB, the second dataset being formed using a similar characteristic as the first BLOB;

determine statistical parameters of the first dataset and the second dataset;

generate a first behavioural pattern using the statistical parameters of the first and second datasets;

analyse the first behavioural pattern for a variation from a past or an expected behaviour or a predefined behavioural pattern consistent with the content of potential interest; and

issue a command to a downstream post-processing processor upon detection of the variation or the predefined behavioural pattern.

15. The system according to claim 14, wherein the instructions to analyse the first behavioural pattern comprises:

instructions for directing the processing unit to:

access historic data indicative of the past, or the expected behaviour, or of the predefined pattern, and comparing the generated first behavioural pattern with the historic data.

16. The system according to claim 14, wherein the first and second datasets conform to the Central Limit Theorem.

17. The system according to claim 14, wherein the statistical parameters comprise a mean, a variance, a median, a skew or a kurtosis.

18. The system according to claim 14, wherein the instructions to generate the first behavioural pattern using the statistical parameters of the first and second datasets comprise:

instructions for directing the processing unit to:

use the statistical parameters of the first dataset as a start point of the first behavioural pattern generation; and

use the statistical parameters of the second dataset as a second subsequent sequential point of the first behavioural pattern generation,

wherein portions of the generated first behavioural pattern exhibits Brownian motions.

19. The system according to claim 14, wherein the first dataset comprises event log data associated with the first BLOB of the information security events.

20. The system according to claim 19, wherein the second dataset comprises event log data associated with the second BLOB of the information security events.

21. The system according to claim 14, wherein the content of potential interest comprises:

- i) content of potential security concern;
- ii) anomalies in or predefined features of the information security events;
- iii) content contrary to rules of use of a computing system, or impermissible content or illegal content;
- iv) image, audio or video data;
- v) biometric data; or
- vi) bad traffic in an implicit norm policy computer network.

22. The system according to claim 14, wherein the characteristic of the first BLOB comprises a number of hits per data port or ports of receipt of the first BLOB.

23. The system according to claim 14, wherein the command to the downstream post-processing processor comprises a signal configured to initiate a further analysis wherein the further analysis comprises:

instructions for directing the processing unit to:

- buffer a third successive BLOB of the information security events;
- form a third dataset from the third BLOB, the third dataset being formed using a similar characteristic as the first BLOB;
- determine statistical parameters of the third dataset;
- generate a second behavioural pattern using the statistical parameters of the first, second and third datasets;
- analyse the second behavioural pattern for a variation from a past or an expected behaviour or a predefined behavioural pattern consistent with the content of potential interest; and
- issue a further alert upon detection of the variation or the predefined behavioural pattern.

24. The system according to claim 23, wherein the instructions to analyse the second behavioural pattern comprises:

instructions for directing the processing unit to:

- access historic data indicative of the past, or the expected behaviour, or of the predefined pattern, and comparing the generated behavioural pattern with the historic data.

25. The system according to claim 23, wherein the first, second and third datasets conform to the Central Limit Theorem.

26. The system according to claim 23, wherein the instructions to generate the behavioural pattern using the statistical parameters of the first, second and third datasets comprises:

- instructions for directing the processing unit to:

- use the statistical parameters of the first dataset as a start point of the second behavioural pattern generation;

- use the statistical parameters of the second dataset as a second subsequent sequential point of the second behavioural pattern generation; and

- use the statistical parameters of the third dataset as a third subsequent sequential point of the second behavioural pattern generation,

- wherein portions of the generated second behavioural pattern exhibits Brownian motions.

27. A system for heuristically analysing Binary Large Objects (BLOBs) of information security events as the BLOBs are received by the system for content of potential interest, the system comprising:

- circuitry configured to buffer a first BLOB of the information security events and a successive second BLOB of the information security events;

- circuitry configured to form a first dataset from the first BLOB, the first dataset comprising data indicative of a characteristic of the first BLOB;

- circuitry configured to form a second dataset from the second BLOB, the second dataset being formed using a similar characteristic as the first BLOB;

- circuitry configured to determine statistical parameters of the first dataset and the second dataset;

- circuitry configured to generate a first behavioural pattern using the statistical parameters of the first and second datasets;

- circuitry configured to analyse the first behavioural pattern for a variation from a past or an expected behaviour or a predefined behavioural pattern consistent with the content of potential interest; and

- circuitry configured to issue a command to a downstream post-processing processor upon detection of the variation or the predefined behavioural pattern.

28. The system according to claim 27, wherein the circuitry configured to analyse the first behavioural pattern comprises:

circuitry configured to access historic data indicative of the past, or the expected behaviour, or of the predefined pattern, and comparing the generated first behavioural pattern with the historic data.

29. The system according to claim 27, wherein the first and second datasets conform to the Central Limit Theorem.

30. The system according to claim 27, wherein the statistical parameters comprise a mean, a variance, a median, a skew or a kurtosis.

31. The system according to claim 27, wherein the circuitry configured to generate the first behavioural pattern using the statistical parameters of the first and second datasets comprise:

circuitry configured to use the statistical parameters of the first dataset as a start point of the first behavioural pattern generation; and

circuitry configured to use the statistical parameters of the second dataset as a second subsequent sequential point of the first behavioural pattern generation,

wherein portions of the generated first behavioural pattern exhibits Brownian motions.

32. The system according to claim 27, wherein the first dataset comprises event log data associated with the first BLOB of the information security events.

33. The system according to claim 32, wherein the second dataset comprises event log data associated with the second BLOB of the information security events.

34. The system according to claim 27, wherein the content of potential interest comprises:

- i) content of potential security concern;
- ii) anomalies in or predefined features of the information security events;
- iii) content contrary to rules of use of a computing system, or impermissible content or illegal content;
- iv) image, audio or video data;
- v) biometric data; or

vi) bad traffic in an implicit norm policy computer network.

35. The system according to claim 27, wherein the characteristic of the first BLOB comprises a number of hits per data port or ports of receipt of the first BLOB.

36. The system according to claim 27, wherein the command to the downstream post-processing processor comprises a signal configured to initiate a further analysis wherein the further analysis comprises:

circuitry configured to buffer a third successive BLOB of the information security events;

circuitry configured to form a third dataset from the third BLOB, the third dataset being formed using a similar characteristic as the first BLOB;

circuitry configured to determine statistical parameters of the third dataset;

circuitry configured to generate a second behavioural pattern using the statistical parameters of the first, second and third datasets;

circuitry configured to analyse the second behavioural pattern for a variation from a past or an expected behaviour or a predefined behavioural pattern consistent with the content of potential interest; and

circuitry configured to issue a further alert upon detection of the variation or the predefined behavioural pattern.

37. The system according to claim 36, wherein the circuitry configured to analyse the second behavioural pattern comprises:

circuitry configured to access historic data indicative of the past, or the expected behaviour, or of the predefined pattern, and comparing the generated behavioural pattern with the historic data.

38. The system according to claim 36, wherein the first, second and third datasets conform to the Central Limit Theorem.

39. The system according to claim 36, wherein the circuitry configured to generate the behavioural pattern using the statistical parameters of the first, second and third datasets comprises:

circuitry configured to use the statistical parameters of the first dataset as a start point of the second behavioural pattern generation;

circuitry configured to use the statistical parameters of the second dataset as a

second subsequent sequential point of the second behavioural pattern generation; and  
circuitry configured to use the statistical parameters of the third dataset as a third  
subsequent sequential point of the second behavioural pattern generation,  
wherein portions of the generated second behavioural pattern exhibits Brownian  
motions.