

Claims

1. An n-tiering security threat inference and correlation apparatus for monitoring and anticipating cyber attacks, the apparatus comprising:
 - 5 a plurality of groups of inference-correlation systems, each group arranged with at least one inference system and at least one associated correlation system configured to monitor at least one network; and
 - an input/output (I/O) system configured to receive security events, and broadcast the received security events to the plurality of groups of inference-
 - 10 correlation systems;
 - wherein the respective groups of inference-correlation systems are configured to process only the broadcasted security events relevant to the respective networks to identify the cyber attacks.
- 15 2. The apparatus of claim 1, wherein the at least one inference system includes being arranged to perform the processing based on defined inference rules to identify high value and low value events, and the inference rules are obtained from stochastic parameters that are user-customisable according to severity attributes.
- 20 3. The apparatus of any preceding claims, wherein the at least one correlation system includes being arranged to perform the processing based on defined deterministic rules, which are derived from historical data for anticipating cyber attacks.
- 25 4. The apparatus of any preceding claims, wherein the at least one inference system includes a plurality of inference systems, which are dynamically generated when required.
- 30 5. The apparatus of any preceding claims, wherein the at least one correlation system includes a plurality of correlation systems, which are dynamically generated when required.

6. The apparatus of any preceding claims, wherein the at least one inference system includes being communicatively coupled to the at least one associated correlation system.
- 5 7. The apparatus of any preceding claims, wherein the at least one inference system and the at least one associated correlation system include being configured to be logically executed in a virtual machine environment.
8. The apparatus of any preceding claims, wherein the broadcasted security
10 events include being broadcasted as data packets respectively configured with a first identifier and a payload which includes information relating to the security events, the first identifier arranged with a unique value associated with the network to enable the respective groups of inference-correlation systems to determine whether the broadcasted security events are relevant for processing
15 the payload.
9. The apparatus of claim 8, wherein the data packets are further configured with a second identifier to enable the at least one inference system and the at least one associated correlation system of a same group to determine whether to
20 process the payload, subsequent to determining that the broadcasted security events are relevant.
10. The apparatus of claim 8 or 9, wherein the data packets are broadcasted via the User Datagram Protocol.
- 25 11. The apparatus of any preceding claims, wherein at least one of the at least one inference system and the at least one associated correlation system of a same group is configured to process the broadcasted security events.
- 30 12. A method of operating an n-tiering security threat inference and correlation apparatus for monitoring and anticipating cyber attacks, the apparatus includes an input/output (I/O) system, and a plurality of groups of inference-correlation systems, each group being arranged with at least one inference system and at least one associated correlation system configured to
35 monitor at least one network, the method comprises:

- receiving security events by the I/O system;
 - broadcasting the received security events by the I/O system to the plurality of groups of inference-correlation systems; and
 - processing only the broadcasted security events relevant to the
- 5 respective networks by the respective groups of inference-correlation systems to identify the cyber attacks.