Claims

1. A method of detecting security threats, the method comprising the following steps, implemented in a cyber defence system:

in an enrichment stage, receiving events pertaining to a monitored private network; enriching the events by augmenting them with enrichment data; and

receiving, at an analysis engine, the enriched events and analysing the enriched events to detect security threat conditions indicated by the enriched events;

wherein at least one of the events is enriched based on external reconnaissance by:

determining a related public network address on a network interface between the private network and a public network, and

augmenting the event with external reconnaissance data, as determined by transmitting at least one reconnaissance message from an external reconnaissance device on the public network to the related public network address on the network interface between the public and the private networks.

2. The method of claim 1, wherein the events comprise at least one of:

network events generated by monitoring network traffic within the private network; and

endpoint events generated using endpoint agents executed on endpoints of the monitored private network to monitor local activity at those endpoints.

3. The method of claim 2, wherein the events comprise network events and endpoint events and the method comprises linking network events and endpoint events together based on at least one of: respective timestamps and respective entity identifiers in those events, wherein the security threat conditions are detected from the enriched and linked events.

4. The method of claim 2 or any claim dependent thereon, wherein the event that is enriched based on external reconnaissance is a network event and wherein that event is linked with one or more related endpoint events.

5. The method of claim 3, wherein the event that is enriched based on external reconnaissance is an endpoint event and wherein that event is linked with one or more related events.

6. The method of claim 5, wherein the one or more related events comprise one or more related network events.

7. The method of claim 2 or 4, wherein the event that is enriched is a joined network event created by joining two or more events together, the two or more events comprising a network event and an endpoint event.

8. The method of any preceding claim, wherein the external reconnaissance message is transmitted to a port associated with the public network address.

9. The method of any preceding claim, wherein the enriched event is associated with an internal port, and wherein the external reconnaissance data is obtained by matching activity at the internal port to the external reconnaissance message.

10. The method of any preceding claim, comprising a step of attempting to obtain the external reconnaissance data in response to determining that the event is associated with an internal port in a listening state.

11. The method of any preceding claim, wherein the external reconnaissance data indicates whether or not an internal port with which the event is associated has been determined to correspond to an external port in a listening state, wherein if the internal port has been determined to correspond to an external port in a listening state, the external reconnaissance data comprises an identifier of the external port.

12. The method of any preceding claim, wherein the external reconnaissance data comprises content obtained by the external reconnaissance device from an entity in the private network that is listening on the external port, or information about such content.

13. The method of any preceding claim, wherein the external reconnaissance message is transmitted as part of a port scan operation, to determine information about a state of

an external port associated with the public network address on the network interface, the external reconnaissance data comprising results of the port scan operation.

14. The method of claim 13, wherein information about the state of the port indicates the port is in one of the following states:

a listening state, implying an internal service is listening on the port,

a closed state, based on a received reply indicating that incoming connections to the port are not accepted, and

a blocked state, implying that a traffic regulation component associated with the network interface is blocking access to that port for external clients.

15. The method of any preceding claim, wherein the enrichment based on external reconnaissance comprises: extracting from the event a private network address within the private network, and determining the related public address from the private network address, the related public address being a public address corresponding to the private network address.

16. The method of claim 5, wherein that determination is made based on a mapping between the public and private network addresses that is stored at the network interface.

17. The method of any of claims 1 to 16, comprising:

analysing the received events to identify at least one event that meets a case creation condition and, in response, creating a case in an experience database, the case being populated with data of the identified at least one event;

assigning a threat score to the created case based on the event data;

matching at least one further event to the created case and populating the case with data of the at least one further event, the threat score assigned to that case being updated in response; and

in response to the threat score for one of the cases meeting a significance condition, rendering that case accessible via a case interface.

18. The method of claim 17, wherein one of the event and the further event is the event enriched or associated with the external reconnaissance data is, wherein the threat

score for that case meeting the significance condition constitutes a security threat condition.

19. A system for detecting security threats comprising an input configured to receive events and one or more processors configured to execute instructions, which cause the one or more processors to implement the method of any preceding claim.

20. A computer program or set of computer programs comprising instructions stored on a computer-readable storage medium and configured, when executed on one or more processors, to implement the method of any of claims 1 to 18.