Claims

[Claim 1]

A method for detecting anomalies of an infrastructure in a network comprising:

- analysing, through a network analyser (101) connected to said network, a data packet (PD) exchanged in said network;
- identifying, by analysing through said network analyser (101) only said data packet (PD), the network protocol and all the fields for said analysed data packet (PD) defining an identified protocol and identified fields of said data packet (PD);
- extracting, through computerized data processing means (102), identification fields from said identified fields to identify a device of said infrastructure in said network;
- matching, through said computerized data processing means (102), said identified device with a plurality of predefined standard devices in a predefined devices knowledge database to recognise a matching device;
- retrieving, through said computerized data processing means (102), one or more allowed fields and one or more allowed protocols of said matching device from said predefined devices knowledge database;
- comparing, through said computerized data processing means (102), said allowed fields and said allowed protocols respectively with said identified fields and said identified protocol as directly obtained by said identification through the network analyser and defining at least one critical state of said infrastructure when said identified fields differ from said allowed fields or when said identified protocol differ from said allowed protocols;
- signalling, by means of said computerized data processing means, an anomaly of said infrastructure when at least one of said critical states is identified.

[Claim 2]
The method for detecting anomalies of an infrastructure in a network according to claim 1, wherein in said extracting said identification fields comprise the vendor and product name to identify said device of said infrastructure in said network.

[Claim 3]
The method for detecting anomalies of an infrastructure in a network according to claim 1 or 2, wherein in said extracting said identified fields comprise the function codes of said identified protocol.

[Claim 4]
The method for detecting anomalies of an infrastructure in a network according to one of claims 1-3, wherein in said matching said matching device is recognized by matching the vendor and product name of said identified device.

[Claim 5]
The method for detecting anomalies of an infrastructure in a network according to one of claims 1-4, wherein in said retrieving said allowed fields comprise allowed function codes for each allowed protocol.

[Claim 6]
The method for detecting anomalies of an infrastructure in a network according to one of claims 1-5, wherein said method comprises storing, in a volatile storage (103), said identified protocol and said identified fields of said data packet (PD).

[Claim 7]
The method for detecting anomalies of an infrastructure in a network according to one of claims 1-6, wherein said method comprises storing, in a volatile storage

(103), said identification fields relating to the identity of said device of said infrastructure in said network.

[Claim 8]
The method for detecting anomalies of an infrastructure in a network according to one of claims 1-7, wherein said method comprises storing, in a volatile storage (103), said allowed fields and said allowed protocols of said matching device.

[Claim 9]
The method for detecting anomalies of an infrastructure in a network according to one of claims 1-8, wherein said method is iterated for all said data packet (PD) exchanged in said network.

[Claim 10]
The method for detecting anomalies of an infrastructure in a network according to one of claims 1-9, wherein said method comprises periodically updating, through a remote database system, said predefined devices knowledge database.

[Claim 11]
An apparatus for detecting anomalies of an infrastructure in a network comprising a network analyser (101) to be connected to a network, a computerized data processing means (102) operatively connected to said network analyser (101) and a predefined devices knowledge database operatively connected to said computerized data processing means,

wherein said network analyser (101) in use analyses a data packet (PD) exchanged in said network and identifies the network protocol and all the fields for said analysed data packet (PD) defining an identified protocol and identified fields of said data packet (PD), said network analyser (101) being configured to identify said network protocol and said fields data

packet by analysing only said data packet (PD),

wherein said computerized data processing means (102) in use extracts identification fields from said identified fields to identify a device of said infrastructure in said network,

wherein said computerized data processing means (102) in use matches said identified device with a plurality of predefined standard devices in said predefined devices knowledge database to recognise a matching device,

wherein said computerized data processing means (102) in use retrieves one or more allowed fields and one or more allowed protocols of said matching device from said predefined devices knowledge database,

wherein said computerized data processing means (102) in use compares said allowed fields and said allowed protocols respectively with said identified fields and said identified protocol as directly obtained by said identification through the network analyser defining at least one critical state of said infrastructure when said identified fields differ from said allowed fields or when said identified protocol differ from said allowed protocols, and

wherein said computerized data processing means (102) in use signals an anomaly of said infrastructure when at least one of said critical states is identified.

[Claim 12]

The apparatus for detecting anomalies of an infrastructure in a network according to claim 11, wherein said apparatus comprises a remote update system operatively connected to said predefined devices knowledge database, and

wherein in use said remote update system updates said predefined devices knowledge database.

[Claim 13]

The apparatus for detecting anomalies of an infrastructure in a network according to claim 12, wherein said remote update system is a cloud system.

[Claim 14]

The apparatus for detecting anomalies of an infrastructure in a network according to claim 12 or 13, wherein the apparatus comprises a plurality of network analysers (101) each of which to be connected to a respective network, a plurality of computerized data processing means (102) each of which operatively connected to a respective of said network analysers (101) and a plurality of predefined devices knowledge databases each of which operatively connected to a respective of said computerized data processing means,

wherein said remote update system is operatively connected to said predefined devices knowledge databases, and

wherein in use said remote update system updates said predefined devices knowledge databases.