Claims

1. An endpoint agent (616) configured, when executed on an endpoint device (312), to:

access via a local traffic access function of the endpoint device (616) network traffic local to the endpoint device, the local network traffic comprising:

copies of all outgoing packets sent from a network interface of the endpoint device to a packet-switched network (630) and carrying in their payloads outbound payload data generated by one or more processes (602) executed on the endpoint device (312), and

copies of all incoming packets received at the network interface from the packet-switched network (630) and carrying in their payloads inbound payload data intended for the one or more processes (602) executed on the endpoint device (312);

extract network traffic telemetry from the headers and the payloads of the copies of the outgoing and incoming packets, the extracted network traffic telemetry including header data of the incoming and outgoing packets, and additionally summarizing the outbound and inbound payload data of the outgoing and incoming packets, wherein said extracting comprises processing each packet to determine whether the packet constitutes the start of a network flow or pertains to an existing network flow; and

transmit, to a cybersecurity service, a series of network telemetry records identifying all new network flows observed by the endpoint agent, and containing the extracted network traffic telemetry that includes the header data and summarizes the payload data for use in performing a cybersecurity threat analysis.

2. The endpoint agent of claim 1, configured to additionally monitor local activity by the processes (602) at the endpoint device (312), and associate the series of network telemetry records with endpoint data about the local activity.

3. The endpoint agent of claim 2, configured to match an incident of local activity by one of the processes (602) with at least one packet of the incoming and/or outgoing packets, and thereby obtain one or more pieces of endpoint data related to the at least one packet, wherein at least one network telemetry record of the series of summary records is associated with the pieces of endpoint data, the at least one network telemetry record pertaining to the at least one packet with which the incident of local activity has been matched, wherein the one or more pieces of endpoint data optionally comprise details of the process and/or details of a parent process.

4. The endpoint agent of claim 3, configured to perform said matching based on:

a local timing of the incident of local activity and a local timing the at least one packet, and/or

header information of the at least one packet and corresponding information obtained via said monitoring of local activity.

5. The endpoint agent of any of claim 3 or 4, wherein the incident of local activity is one of the processes establishing a flow, the at least one network telemetry record identifying the flow and containing information about the process that established the flow.

6. The endpoint agent of any of claims 3 to 5, wherein the incident of local activity is one of the processes accessing a file and the at least one network telemetry record contains information about the file.

7. The endpoint agent of any preceding claim, configured to determine a user account associated with at least one packet of the incoming and/or outgoing packets, and associate at least one network telemetry record of the series of network telemetry records with user information of the user account, the at least one network telemetry record pertaining to the at least one packet.

8. The endpoint agent of any preceding claim, wherein the local traffic access function is provided by a network activity application programming interface (API) of an operating system (604) of the endpoint device, the endpoint agent configured to access the incoming and outgoing packets via the network activity API;

wherein the endpoint agent is configured to obtain, via the operating system (604) of the endpoint device, a piece of endpoint data associated with one or more network packets of the incoming and/or outgoing packets, wherein at least one network telemetry record of the series of network telemetry records pertains to the one or more network packets with which the piece of endpoint data is associated, and the endpoint agent is configured to augment or enrich the at least one network telemetry record with the piece of endpoint data, or link at least one of the network telemetry records with at least one other record containing the piece endpoint data and transmitted from the endpoint device to the cybersecurity service.

9. The endpoint agent of claim 2 or any claim dependent thereon, wherein the associating is performed by augmenting or enriching at least one of the network telemetry records with endpoint data or by linking at least one of the network telemetry records with at least one other record containing the endpoint data.

10. The endpoint agent of claim 8, wherein the piece of endpoint data:

comprises details of a process of the one or more processes (602) that received and/or generated the one or more network packets,

comprises details of a parent process of the one or more processes (602), the parent process being a parent of another process of the one or more processes that received and/or generated the one or more network packets, or

user information of a user account associated with the one or more network packets, or information about a file associated with the one or more network packets.

11. The endpoint agent of any preceding claim, wherein the series of network telemetry records is generated independently of any local threat detection performed at the endpoint device (312).

12. An endpoint device (312) comprising:

a network interface (610) configured to send incoming packets carrying inbound payload data and/or receive outgoing packets carrying outbound payload data;

one or more processing units configured to execute:

one or more processes (602) configured to process the inbound payload data and/or generate the outbound payload data, and

the endpoint agent (616) of any preceding claim, configured to extract the network traffic telemetry from the incoming and/or outgoing packets sent from and/or received at the network interface.

13. A method of aggregating network telemetry records received from multiple endpoint agents (616) executed on multiple endpoint devices (312), the method comprising:

receiving from each of the endpoint agents (616) a series of network telemetry records, the network telemetry records containing telemetry summarising local network traffic observed at the endpoint device on which the endpoint agent is executed, the network telemetry records having been associated by the endpoint agent (616) with endpoint data

captured by monitoring local activity by one or more processes executed at the endpoint device (602), wherein the local network traffic comprises copies of all outgoing and incoming packets sent from and received a network interface of the endpoint device on which the endpoint agent is executed, and the endpoint agent (616) extracts the telemetry from the headers and the payloads of the copies of the outgoing and incoming packets, and processes each packet constitutes the start of a network flow or pertains to an existing network flow, and wherein and the network telemetry records identify all new network flows observed by the endpoint agent, and the telemetry includes header data of the incoming and outgoing packets, and additionally summarizes the outbound and inbound payload data of the outgoing and incoming packets;

detecting at least one duplicate network telemetry record received from a second of the endpoint devices, the duplicate network telemetry record duplicating network traffic information conveyed in a first network telemetry record received from a first of the endpoint devices in communication with the second endpoint device, wherein the duplicate network telemetry record is detected by matching a second deduplication key thereof with a first deduplication key of the first network telemetry record, the deduplication keys identifying a common flow to which those telemetry records pertain;

extracting from the duplicate network telemetry record a second piece of endpoint data captured at the second endpoint; and

associating the first network telemetry record received from the first endpoint device with the extracted piece of endpoint data as captured at the second endpoint device, the first network telemetry record having been additionally associated with a first piece of endpoint data at the first endpoint device.

14. The method of claim 13, wherein the first and second deduplication keys include or are based on:

TCP sequence numbers of those records, or

a payload hash of those records.

15. The method of claim 13 or 14, wherein the network telemetry records comprise a flow start record received from the first endpoint, indicating the start of a flow, the at least one duplicate telemetry record comprising a duplicate flow start record indicating the start of the flow, the duplicate flow start record received subsequently from the second endpoint, the method comprising:

determining a deduplication key (1302) for the flow start record;

determining that the deduplication key (1302) is not already associated with another endpoint identifier in a flow start cache, and associating the deduplication key (1302) with an identifier of the first endpoint in the flow start cache;

when the duplicate flow start record has been subsequently received, determining a deduplication key (1302) for the duplicate flow start record, determining that the deduplication key (1302) is already associated with the identifier of the first endpoint in the flow start cache, and extracting the second piece of endpoint data from the duplicate flow start record.

16. The method of any of claims 13 to 15, wherein the first network telemetry record is enriched or otherwise associated with the extracted piece of endpoint data, and the duplicate network telemetry record is discarded once that piece of endpoint data has been extracted.

17. The method of any of claims 13 to 16, comprising receiving at least one piece of network information about the first and/or second endpoint from a network monitoring system, and enriching or otherwise associating the first network telemetry record with the at least one piece of network information wherein the at least one piece of network information optionally comprises MPLS and/or VLAN label(s).