Claims

1. A system comprising:

one or more processors;

a memory device coupled to the one or more processors;

a databasesituational model stored in the memory device and implemented at a kernel level of the system, the databasesituational model configured to storeinclude:

security-relevant information that includes a representations of at least onea current state of the system and a past state of the system; and

corresponding metadata for the security-relevant information, the corresponding metadata either defining or used in defining a period of time in which at least a part of the security-relevant information is trustworthy; and

one or more modules implemented at the kernel-level and operated by the one or more processors to perform operations comprising:

build the situational model with storing a first portion of the security-relevant information in substantially real-time as first execution activities associated with the security-relevant information are observed, wherein the first portion of the security-relevant information relates to a first ephemeral object during a first epoch;

storing a second portion of the security-relevant information in real-time as second execution activities associated with the security-relevant information are observed, wherein the second portion of the security-relevant information relates to a second ephemeral object during a second, different epoch; and

determining a chain of execution based at least in part on the first portion of the security-relevant information and based at least in part on the second portion of the security-relevant information.

2. The system of claim 1, wherein the situational model includes a database to store the security-relevant information and corresponding metadata further definesing a period of time in which all data acquired about a collection of security-relevant information that includes the security-relevant information has consistent properties of liveness and trustworthiness.

3. The system of claim 1, the operations further comprising receiving at least the first portion or the second portionwherein the situational model includes one or more receivers to receive the security-relevant information from the one or more modules and to store the received security-relevant information in a database of the situational model.

4. The system of claim 3, the operations further comprisingwherein the one or more receivers are configured to validatinge state information associated with the execution activities of the system.

5. The system of claim 3, the operations further comprisingwherein the one or more receivers are configured to generatinge events based on at least the first portion or the second portionthe received security-relevant information and on security-relevant information stored in the database.

6. The system of claim 1, further comprisingwherein the situational model includes a query interface that enables the one or more modules to access security-relevant information stored in thea databasee of the situational model, the query interface further enabling the one or more modules to specify a level of desired trustworthiness associated with metadata that corresponds to security-relevant information stored in the database.

7. The system of claim 1, further comprisingwherein the situational model includes a pruning component to prune security-relevant information from the situational modeldatabase based on an age and a type of security-relevant information or on a prioritization of different categories of security-relevant information.

8. The system of claim 7, wherein the pruning component first prunes the security-relevant information based on age and type and then, if a size of the pruned situational model exceeds a limit, prunes the security-relevant information based on the prioritization of different categories.

9. The system of claim 1, wherein the database comprises a schema thatsituational model is dynamically configurable by a remote security service.

10. The system of claim 1, wherein the databasesituational model is further configured to cache at least one of information received from a remote security service, information that is computationally expensive to generate or fetch, or information that is high-latency to fetch.

11. The system of claim 1, wherein the one or more modules are modules of a kernel-level security agent.

12. The system of claim 1, the operations further comprisingwherein the one or more modules are operated by the one or more processors to determininge at least some of the security-relevant information based on a configuration received from a remote security service.

13. The system of claim 1, the operations further comprisingwherein the one or more modules are operated by the one or more processors to utilize the situational model to validatinge state information associated with the execution activities of the system.

14. The system of claim 1, the operations further comprising providing at least some of thewherein the one or more modules are operated by the one or more processors to provide security-relevant information to athe remote security service.

15. The system of claim 1, wherein the one or more module or a remote security service utilize the security-relevant information in determining a chain of execution.

1516. A method comprising:

receiving, by a computing device, a notification of an event associated with execution activities of the computing device;

querying, by the computing device, a situational model for security-relevant information based at least in part on the notification, the situational model being a substantially real-time representation of a state of the computing device constructed from security-relevant information representing a first state of the computing device during a first epoch; and

validating, by the computing device, state information associated with the event based at least in part on the security-relevant information, wherein the state information represents a second state of the computing device during a second, different epoch, and the validating includes a comparison of at least a part of the state information with at least a part of the security-relevant information,

wherein the receiving, the querying, and the validating are performed by a kernel-level security agent of the computing device.

1617. The method of claim 1516, further comprising, beforewherein the validating comprises conditionally performing the validating, determining that based on whether the state information is fully maintained in the situational model.

~~18. The method of claim 16, wherein the receiving, the querying, and the validating are performed by a kernel-level security agent of the computing device.~~

17~~19~~. The method of claim 15~~16~~, further comprising, in response to~~when~~ a result of the validating being~~is~~ a validation error, performing at least one security response action.

18~~20~~. The method of claim 17~~19~~, wherein the security response action comprises:~~is one of~~

reporting the validation error to a remote security service;~~,~~

monitoring further execution activities;~~,~~

taking a remediation action directed at malicious activity that is responsible for the validation error~~,~~; or

alerting a user of the computing device.

19~~21~~. One or more tangible computer-readable media having stored thereon computer-executable instructions configured to program one or more computing devices to perform operations comprising:

configuring a plurality of agents of a corresponding plurality of monitored computing devices to provide security-relevant information in substantially real-time as execution activities associated with the security-relevant information are observed, wherein the monitored computing devices are each separate and distinct computing devices from each other, the monitored computing devices include a first computing device, the plurality of agents includes a first agent corresponding to the first computing device, and the security-relevant information provided by the first agent comprises a first portion relating to a first ephemeral object during a first epoch and a second portion relating to a second ephemeral object during a second, different epoch;

receiving the security-relevant information in ~~substantially~~ real-time; and

building a situational model from the security-relevant information in ~~substantially~~ real-time as the security-relevant information is received, the situational model representing states of the monitored computing devices and the represented states including at least a first state corresponding to the first epoch and a second state corresponding to the second epoch;

configuring a device-specific situational model of the first computing device, the device-specific situation model being specific to the first computing device; and

receiving queries of the situational model from a user or from a security service.

~~22. The one or more tangible computer-readable media of claim 21, wherein the one or more computing devices implement a security service.~~

2023. The one or more tangible computer-readable media of claim 1921, wherein the one or more computing devices include one or more computing devices implementing a security service and an intermediate device, the one or more computing devices implementing a security service performing the configuring and the intermediate device performing the receiving and the building.

2124. The one or more tangible computer-readable media of claim 1921, wherein the security-relevant information is information that, when received from a plurality of agents, supports making security decisions.

2225. The one or more tangible computer-readable media of claim 1921, wherein the represented states include at least current states of at least one of the monitored computing devices.

~~26. The one or more tangible computer-readable media of claim 21, wherein the operations further comprise receiving queries of the situational model from a user or from a security service.~~

2327. The one or more tangible computer-readable media of claim 1926, wherein the operations further comprise validating state information for the monitored computing devices based at least in part on results of the queries.

2428. The one or more tangible computer-readable media of claim 1926, wherein the operations further comprise performing at least one security response action based on at least on part on results of the queries.

2529. The one or more tangible computer-readable media of claim 1926, wherein the operations further comprise updating agent configurations based at least in part on results of the queries and repeating the configuring based at least in part on the updated agent configurations.

26. The system of claim 1, wherein the operations to determine the chain of execution include retrieving the first portion of the security-relevant information from the database

when the first portion of the security-relevant information is no longer present on a host operating system of the system.

27. The method of claim 15, further comprising retrieving, by the computing device, the security-relevant information from a database when the security-relevant information is no longer present on a host operating system of the computing device.

28. The one or more non-transitory computer-readable media of claim 19, wherein the operations further comprise, in response to the receiving queries, retrieving at least the first portion of the security-relevant information from the situational model or the device-specific situational model for the first computing device when the first portion is no longer present on a host operating system of the first computing device.