

CLAIMS

WHAT IS CLAIMED IS:

1. A computer-implemented method comprising:
- 5 providing, by a security service, one or more secure mechanisms for forming a group among client entities, each client entity being associated with a different security organization; and
- automatically sharing, by the security service, security information of a client entity in the group with one or more other client entities in the group.
- 10
2. The method of claim 1, wherein providing the one or more secure mechanisms comprises enabling a client entity to invite another client entity to join the group by providing a unique identifier of the other client entity to the security service.
- 15
3. The method of claim 1, wherein providing the one or more secure mechanisms comprises:
- providing a blind search mechanism that enables a client entity to provide identifying information for an entity to the security service;
- 20 determining based at least in part on the identifying information whether the entity is a client entity; and
- in response to determining that the entity is a client entity, inviting the entity to join the group.

4. The method of claim 3, wherein the inviting is performed conditionally based on whether the entity has performed a blind search for the searching client entity.

5

5. The method of claim 1, wherein providing the one or more secure mechanisms comprises:

providing a search mechanism that enables a client entity to search for other client entities and to receive, in return, a list of client entities matching a

10 search query; and

enabling the searching client entity to invite one or more of the client entities included in the list of client entities to join or form a group with the searching client entity.

15

6. The method of claim 1, wherein providing the one or more secure mechanisms comprises inviting client entities associated with a security threat to join the group.

7. The method of claim 1, wherein providing the one or more secure mechanisms comprises creating the group and inviting the client entities to join the group based at least in part on preferences specified by the client entities.

20

8. The method of claim 1, wherein providing the one or more secure mechanisms comprises creating the group and associating the group with at least one of an industry sector of the client entities, a geographic location of the client entities, a size range of the client entities, or interests of the client entities.

9. The method of claim 8, further comprising inviting the client entities to join the group or opening the group to the public.

10. The method of claim 8, further comprising assigning the client entities to the group and providing the client entities with an option to opt out of the group.

11. The method of claim 1, wherein providing the one or more secure mechanisms comprises creating the group based at least in part on complementary behaviors of the client entities.

12. The method of claim 1, wherein providing the one or more secure mechanisms comprises creating the group based at least in part on one or more social network groups.

13. The method of claim 1, wherein the group is associated with a setting that allows the client entities to be anonymous with respect to each other.

5 14. The method of claim 1, wherein the group is associated with a trusted moderator or group of moderators who controls admission to the group.

15 15. The method of claim 1, wherein providing the one or more secure mechanisms comprises enabling one or more of the client entities of the group to specify sharing parameters and policy parameters for the group.

16. The method of claim 1, wherein the providing and automatic sharing utilize one or more of keys, hashing, certificates from a certificate authority, an identity verification mechanism, or other security features to prevent identity spoofing and secure the shared security information.

17. The method of claim 1, wherein the shared security information is viewable by the client entity sharing the security information and the client entities receiving the security information and is not viewable by the security service or other parties.

18. The method of claim 1, further comprising enabling a client entity to set system-wide or group-based sharing parameters for the client entity.

19. The method of claim 1, further comprising enabling a client entity to advertise security information for sharing in exchange for security information from another client entity.

5

20. The method of claim 1, wherein the automatic sharing includes sharing security information from third party sources with the client entities of the group.

10

21. The method of claim 1, further comprising sharing the security information with a third party security product or service.

22. The method of claim 1, further comprising performing at least one of:

15

enabling at least one client entity in the group of client entities to affect a rating of another client entity; or

adjusting the rating based on actions of the other client entity either taken or refrained from with respect to sharing threat information, remediation information, or policies with one or more client entities in the group of client entities.

20

23. The method of claim 1, further comprising associating one or more of the client entities with merit indicia based at least in part on contributions of

the one or more client entities to a security ecosystem of the security service or to the group.

24. The method of claim 1, further comprising providing the client
5 entities with client entity profiles and enabling the client entities to modify their corresponding client entity profiles and to set access restrictions to their corresponding client entity profiles.

25. The method of claim 1, wherein the security information includes at
10 least one of threat information, remediation information, policies, attack data, vulnerability information, reverse engineering information, packet data, network flow data, protocol descriptions, victim information, threat attribution information, incident information, proliferation data, user feedback, or information on software or systems.

15

26. The method of claim 1, wherein the security service is a public service open to interested client entities or a private service open to specific client entities.

20 27. The method of claim 1, further comprising enabling manual sharing of security information between the client entities in the group.

28. The method of claim 1, further comprising providing, to a client entity, an indication of available security information through a user interface and providing the available security information to the client entity responsive to that client entity electing to share security information of the client entity with another client entity that is associated with the available security information.

29. The method of claim 28, wherein the available security information indicated through the user interface is selected for the client entity based on security information possessed or provided by the client entity.

30. The method of claim 1, wherein the group belongs to one or more hierarchies of groups, each hierarchy of groups being associated with access controls to security information or with policies pushed to member client entities.

31. One or more tangible computer-readable media storing computer-executable instructions configured to program one or more computing devices of a security service to perform operations comprising:

associating a rating with a client entity, the rating indicative of the client entity's participation in a group of client entities that share security information with one another; and

performing at least one of:

enabling at least one other client entity in the group of client entities to affect the rating of the client entity; or
adjusting the rating based on actions of the client entity either taken or refrained from with respect to sharing security information with one or more other client entities in the group of client entities.

32. The one or more tangible computer-readable media of claim 31, wherein the operations further comprise associating one or more of the client entities with merit indicia based at least in part on contributions of the one or more client entities to a security ecosystem of the security service or to the group.

33. The one or more tangible computer-readable media of claim 31, wherein the operations further comprise associating a point currency with a client entity and adjusting that point currency based at least in part on contributing or consuming security information.

34. The one or more tangible computer-readable media of claim 31, wherein the client entities have different ratings for a security ecosystem comprised of multiple groups and for the group.

35. The one or more tangible computer-readable media of claim 31, wherein the operations further comprising increasing the rating of one of the

client entities in response to the client entity adding to or completing a client entity profile of the client entity.

36. A system comprising:

5 a plurality of computing devices associated with a plurality of entities, the entities belonging to a group of entities that share security information with each other; and

a plurality of agents respectively implemented on the plurality of computing devices, the agents sharing the security information with one
10 another and utilizing the security information in observing or reacting to execution activities of the computing devices on which they are implemented.

37. The system of claim 36, further comprising a security service to provide one or more secure mechanisms for forming the group of entities and
15 to automatically share the security information received from one of the plurality of agents with the other agents of the plurality of agents.

38. The system of claim 36, wherein the agents observe and react to the execution activities of their respective computing devices in parallel with
20 respect to each other.

CLAIMS

1. A computer-implemented method comprising:

forming, by a group formation module of security service computing device(s), a
5 group including multiple client entities, each client entity being associated with a different
security organization and each client entity having one or more computing devices, each
computing device configured with an executable security agent; and

automatically sharing, by a sharing module of the security service computing
device(s), security information generated by the executable security agent(s) of a client entity
10 in the group with the executable security agent(s) of computing device(s) of one or more
other client entities in the group,

wherein the security information is generated by the executable security agent(s) of
the client entity based on monitoring of execution activities of the computing device(s) of the
client entity,

15 wherein the security information is indicative of whether the client entity is
experiencing a security threat, and wherein each client entity is able to impose a security
scheme or policy on its computing device(s) but is unable to impose the security scheme or
policy on computing device(s) of other client entities.

20 2. The method of claim 1, further comprising enabling a client entity of the multiple
client entities to invite another client entity to join the group by providing a unique identifier
of the other client entity to the security service.

3. The method of claim 1, further comprising:

providing a blind search mechanism that enables a client entity of the multiple client entities to provide identifying information for an entity to the security service;

5 determining based at least in part on the identifying information whether the entity is a client entity; and

in response to determining that the entity is a client entity, inviting the entity to join the group.

10 4. The method of claim 3, wherein the inviting is performed conditionally based on whether the entity has performed a blind search for the searching client entity.

5. The method of claim 1, further comprising:

enabling a client entity of the multiple client entities to search for other client entities

15 and to receive, in return, a list of client entities matching a search query; and

enabling the searching client entity to invite one or more of the client entities included in the list of client entities to join or form a group with the searching client entity.

20 6. The method of claim 1, further comprising inviting client entities associated with a security threat to join the group.

7. The method of claim 1, wherein the forming further comprises creating the group and inviting the client entities to join the group based at least in part on preferences specified by the client entities.

8. The method of claim 1, wherein the forming further comprises creating the group and associating the group with at least one of an industry sector of the client entities, a geographic location of the client entities, a size range of the client entities, or interests of the client
5 entities.

9. The method of claim 8, further comprising inviting the client entities to join the group or opening the group to the public.

10 10. The method of claim 8, further comprising assigning the client entities to the group and providing the client entities with an option to opt out of the group.

11. The method of claim 1, wherein the forming further comprises creating the group based at least in part on complementary behaviors of the client entities.

15

12. The method of claim 1, wherein the forming further comprises creating the group based at least in part on one or more social network groups.

13. The method of claim 1, wherein the group is associated with a setting that allows the
20 client entities to be anonymous with respect to each other.

14. The method of claim 1, wherein the group is associated with a trusted moderator or group of moderators who controls admission to the group.

15. The method of claim 1, further comprising enabling one or more of the client entities of the group to specify sharing parameters and policy parameters for the group.

5 16. The method of claim 1, wherein the automatic sharing involves utilizing one or more of keys, hashing, certificates from a certificate authority, an identity verification mechanism, or other security features to prevent identity spoofing and secure the shared security information.

10 17. The method of claim 1, wherein the shared security information is viewable by the client entity sharing the security information and the client entities receiving the security information and is not viewable by the security service or other parties.

18. The method of claim 1, further comprising enabling a client entity to set system-wide
15 or group-based sharing parameters for the client entity.

19. The method of claim 1, further comprising enabling a client entity to advertise security information for sharing in exchange for security information from another client entity.

20

20. The method of claim 1, wherein the automatic sharing includes sharing security information from third party sources with the client entities of the group.

21. The method of claim 1, further comprising sharing the security information with a
25 third party security product or service.

22. The method of claim 1, further comprising associating one or more of the client entities with merit indicia based at least in part on contributions of the one or more client entities to a security ecosystem of the security service or to the group.

5

23. The method of claim 1, further comprising providing the client entities with client entity profiles and enabling the client entities to modify their corresponding client entity profiles and to set access restrictions to their corresponding client entity profiles.

10 24. The method of claim 1, wherein the security information includes at least one of threat information, remediation information, policies, attack data, vulnerability information, reverse engineering information, packet data, network flow data, protocol descriptions, victim information, threat attribution information, incident information, proliferation data, user feedback, or information on software or systems.

15

25. The method of claim 1, wherein the security service is a public service open to interested client entities or a private service open to specific client entities.

26. The method of claim 1, further comprising enabling manual sharing of security
20 information between the client entities in the group.

27. The method of claim 1, further comprising providing, to a client entity, an indication of available security information through a user interface and providing the available security information to the client entity responsive to that client entity electing to share security

information of the client entity with another client entity that is associated with the available security information.

28. The method of claim 27, wherein the available security information indicated through the user interface is selected for the client entity based on security information possessed or provided by the client entity.

29. The method of claim 1, wherein the group belongs to one or more hierarchies of groups, each hierarchy of groups being associated with access controls to security information or with policies pushed to member client entities.

30. A system comprising:

a plurality of computing devices associated with a plurality of entities, wherein the entities belong to a group of entities that share security information with each other and each entity is associated with a different security organization; and

a plurality of security agents respectively implemented on the plurality of computing devices, the security agents observing execution activities of their respective computing devices, generating the security information based on the observed execution activities, sharing the security information with one another, and utilizing the security information in observing or reacting to further execution activities of the computing devices on which they are implemented,

wherein the security information is indicative of whether the security agents are experiencing a security threat, and

wherein each entity is able to impose a security scheme or policy on its computing device(s) but is unable to impose the security scheme or policy on computing device(s) of other entities.

5 31. The system of claim 30, further comprising a security service to form the group of entities and to automatically share the security information received from one of the plurality of security agents with the other security agents of the plurality of security agents.

10 32. The system of claim 30, wherein the security agents observe and react to the execution activities of their respective computing devices in parallel with respect to each other.