result, participating entities only process and protect against a fraction of the cyber-threats published by CISCP.

Another example of an existing cyber-threat sharing network is the Research and Education Networking Information Sharing and Analysis Center (REN-ISAC), an international community of research and higher education institutions. Unfortunately, like CISCP, REN-ISAC's member colleges and universities have not automated the sharing and processing of threat information, because REN-ISAC does not share threat information in a standardized format. A member school can share threat information in whatever proprietary format it wishes, forcing other member institutions to undergo the time-consuming process of manually processing and acting on each piece of threat information.

Because of the increasing costs (both in time and financial resources) of manually processing the growing number of cyber-threats faced by organizations, what is needed is a way to automate the sharing and processing of cyber-threat information, as well as the implementation of defensive measures against identified cyber-threats. By automating the threat information sharing system, the power of these computing systems can be brought to bear against the malicious entities that threaten them. At the same time, however, because of the sensitive nature of cyber-threat attacks, it is desirable that institutions and individuals have the ability to control which detected cyber-threats they share, how they share them, and which other entities they share them with, in order to protect against sensitive and sometimes embarrassing disclosures which can damage their privacy, security, and reputation.

SUMMARY OF THE INVENTION

The present invention is directed, in certain embodiments, to computerized methods for distributing threat information, including generating threat information in a customized machine-readable language with a sensor based on an observed event, creating a first item describing the threat information by converting the machine-readable language into a common language at a first repository, distributing the first item from the first repository to a central repository for storing the first item , and distributing the first item from the central repository to a plurality of other repositories that are members of an access control group.

In certain embodiments of the invention, creating the first item includes converting an existing item that describes, in a customized language of the first repository, the observed

describing the plurality of observed events or properties, at least one piece of information selected from a group of different types of information that includes, for example: a representation of the behavior or *modus operandi* of an entity responsible for at least one of the observed events or properties; a vulnerability, weakness, or configuration issue of a victim of at least one of the observed events or properties; a particular action that could be taken to prevent, mitigate, or remediate the effects of at least one of the observed events or properties; the entity responsible for at least one of the observed events or properties; and a prediction of at least one future observed event or property. In certain further embodiments of the invention, the computerized methods further include adding the at least one piece of information to at least one of the plurality of items.

In certain embodiments of the invention, the computerized methods further include assigning a quality metric to the first item describing the observed event or property. In certain further embodiments of the invention, the reliability metric is automatically assigned and based on at least one of: an identity of an entity responsible for creating the first item describing the observed event or property; a type of the observed event or property; a set of related system or network activity associated with the observed event or property; and an entity responsible for causing the observed event or property.

The present invention is directed, in certain embodiments, to computerized systems for storing and distributing threat information, the systems including: a central repository for storing and distributing threat information, a plurality of local repositories for storing and distributing threat information, each local repository being capable of generating threat information in a customized machine-readable language based on an observed event, creating a first item describing the threat information by converting the machine-readable language into a common language, and distributing the first item to the central repository, and a network connecting the central repository with the plurality of local repositories, wherein the network allows transmission of the first item from at least one of the plurality of local repositories to the central repository, and allows transmission of the first item from the central repository to the plurality of local repositories.

In certain embodiments of the invention, the central repository for storing and distributing threat information is connected to, for example, at least one of a private feed transmitting threat information to the central repository, a public feed transmitting threat

information to the central repository, and a government feed transmitting threat information to the central repository.

In certain embodiments of the invention, at least one of the plurality of local repositories for storing and distributing threat information is connected to, for example, at least one of: a private feed transmitting threat information to the central repository, a public feed transmitting threat information to the central repository, and a government feed transmitting threat information to the central repository.

In certain embodiments of the invention, a first one of the plurality of local repositories transmits at least one item of threat information over the network via the central repository to at least a second one of the plurality of local repositories.

In certain embodiments of the invention, a first one of the plurality of local repositories transmits at least one item of threat information over the network directly to at least a second one of the plurality of local repositories.

The present invention is directed, in certain embodiments, to computerized systems for automatically exchanging threat information, including: a central server comprising at least one multi-core processor, wherein the central server hosts a central repository containing a plurality of centralized threat information, the central repository comprising a MongoDB database, and the central server has SSL certification; a plurality of distributed servers, the local repository being capable of generating threat information in a customized machine-readable language based on an observed event, creating a first item describing the threat information by converting the customized machine-readable language into a common language, and distributing the first item to the central repository, wherein each of the distributed servers hosts a local repository containing a plurality of localized threat information; and wherein the central server is configured to synchronize the plurality of centralized thread information with the plurality of localized thread information contained in each of the plurality of distributed servers by exchanging, using SSL encryption, at least a portion of the plurality of centralized threat information for at least a portion of the plurality of localized threat information.

In certain embodiments, at least a first distributed server of the plurality of distributed servers also synchronizes with at least a second distributed server of the plurality of distributed servers by exchanging, using SSL encryption, at least a portion of the plurality of localized threat information from the first distributed server's local repository for at least a portion of the plurality of localized threat information from the second distributed server's local repository.

The present invention is directed, in certain embodiments, to computerized methods for securely exchanging threat information, including, at a first distributed server: creating a

CLAIMS

1. A computerized system for automatically exchanging threat information, comprising:

a central server comprising at least one multi-core processor,

wherein the central server hosts a central repository containing a plurality of centralized threat information, the central repository comprising a MongoDB database, and the central server has SSL certification;

a plurality of distributed servers,

wherein each of the distributed servers hosts a local repository containing a plurality of localized threat information, the local repository being capable of generating threat information in a customized machine-readable language based on an observed event, creating a first item describing the threat information by converting the customized machine-readable language into a common language, and distributing the first item to the central repository; and

wherein the central server is configured to synchronize the plurality of centralized threat information with the plurality of localized threat information contained in each of the plurality of distributed servers by exchanging, using SSL encryption, at least a portion of the plurality of centralized threat information for at least a portion of the plurality of localized threat information.

2. The computerized system of claim 1, wherein at least a first distributed server of the plurality of distributed servers is configured to synchronize the plurality of localized threat information contained in the first distributed server with the plurality of localized threat information contained in at least one other distributed server by exchanging, using SSL encryption, at least a portion of the plurality of localized threat information from the first distributed server's local repository for at least a portion of the plurality of localized threat information from the at least one other distributed server's local repository.

3. The computerized system of claim 1, further comprising a network connecting the central server and the plurality of distributed servers;

wherein the network is configured to transmit a plurality of localized threat information between the central server and the plurality of distributed servers in accordance with the TAXII specification.

4. A computerized method for securely exchanging threat information, comprising, at a first distributed server:

creating a first item of threat information in a machine-readable language;

converting the first item of threat information from the machine-readable language into the STIX language;

at a TAXII interface at the first distributed server, securely transmitting the converted first item of threat information to a centralized server using SSL encryption;

at the TAXII interface at the first distributed server, receiving a second item of encrypted threat information, wherein the second item is in the STIX language and has been encrypted using SSL encryption;

validating an XML schema of the second item of encrypted threat information;

analyzing the second item of encrypted threat information;

translating the second item from the STIX language into the machine-readable language; and

inserting the translated second item into a local repository, wherein the local repository is a MongoDB database.

5. A computerized method for distributing threat information, comprising:

generating threat information in a customized machine-readable language with a sensor based on an observed event;

creating a first item describing the threat information by converting the machine-readable language into a common language at a first repository;

distributing the first item from the first repository to a central repository for storing the first item; and

distributing the first item from the central repository to a plurality of other repositories that are members of an access control group.

6. The computerized method of claim 5, wherein creating the first item comprises converting an existing item that describes, in a customized language of the first repository, the observed event or property, into the first item describing the observed event or property in the common language.

7. The computerized method of claim 5, further comprising:

converting the first item, at the at least one other repository for storing and distributing threat information, into a second item describing the observed event or property in a customized language of the at least one other repository.

8. The computerized method of claim 5, wherein the common language is the STIX language, and the first item is distributed in accordance with the TAXII specification.

9. The computerized method of claim 8, wherein the first item contains descriptions of one or more of:

(a) an observed event or property;

(b) a pattern of relevant observed activity;

(c) a set of related system or network activity associated with the observed event or property;

(d) an entity responsible for causing the observed event or property;

(e) a representation of the behavior or modus operandi of the entity responsible for the observed event or property;

(f) a vulnerability, weakness, or configuration issue of a potential victim of the observed event or property;

(g) a particular action that can be taken to prevent, mitigate, or remediate the effects of the observed event or property; and

(h) related activities executed by the entity responsible for the observed event or property.

10. The computerized method of claim 5, wherein distributing the first item comprises transmitting the first item to a plurality of other repositories, and the first repository and the plurality of other repositories are members of an access control group.

11. The computerized method of claim 5, further comprising manually analyzing or automatically analyzing the first item at the at least one other repository.

12. The computerized method of claim 11, wherein automatically analyzing the first item comprises automatically determining whether to implement a response to the observed event or property.

13. The computerized method of claim 12, further comprising automatically implementing a response to the observed event or property.

14. The computerized method of claim 5, further comprising analyzing, at the first repository for storing and distributing the threat information, a plurality of items describing a plurality of observed events or properties.

15. The computerized method of claim 14, further comprising determining, from the analysis of the plurality of items describing the plurality of observed events or properties, at least one piece of information selected from the group comprising:

(a) a representation of the behavior or modus operandi of an entity responsible for at least one of the plurality of observed events or properties;

(b) a vulnerability, weakness, or configuration issue of a victim of at least one of the plurality of observed events or properties;

(c) a particular action that could be taken to prevent, mitigate, or remediate the effects of at least one of the plurality of observed events or properties;

(d) the entity responsible for at least one of the plurality of observed events or properties; and

(e) a prediction of at least one future observed event or property.

16. The computerized method of claim 15, further comprising adding the at least one piece of information to at least one of the plurality of items.

17. The computerized method of claim 5, further comprising assigning a quality metric to the first item describing the observed event or property.

18. The computerized method of claim 17, wherein the quality metric is automatically assigned or manually assigned to the first item, and the quality metric is based on at least one confidence metric previously assigned to the first item.

19. The computerized method of claim 18, wherein the at least one confidence metric was automatically assigned or manually assigned to the first item, and the confidence metric is based on at least one of:

(a) an identity of an entity responsible for creating the first item describing the observed event or property;

(b) a type of the observed event or property;

(c) a set of related system or network activity associated with the observed event or property; and

(d) an entity responsible for causing the observed event or property.

20. A computerized system for storing and distributing threat information, comprising:

a central repository for storing and distributing threat information;

a plurality of local repositories for storing and distributing threat information, each local repository being capable of generating threat information in a customized machine-readable language based on an observed event, creating a first item describing the threat information by converting the machine-readable language into a common language, and distributing the first item to the central repository; and

a network connecting the central repository with the plurality of local repositories, wherein the network allows transmission of the first item from at least one of the plurality of local repositories to the central repository, and allows transmission of the first item from the central repository to the plurality of local repositories.

21. The computerized system of claim 20, wherein the central repository for storing and distributing threat information is connected to at least one of:

(a) a private feed configured to transmit threat information to the central repository;

(b) a public feed configured to transmit threat information to the central repository; and

(c) a government feed configured to transmit threat information to the central repository.

22. The computerized system of claim 20, wherein at least one of the plurality of local repositories for storing and distributing threat information is connected to at least one of:

(a) a private feed configured to transmit threat information to the central repository;

(b) a public feed configured to transmit threat information to the central repository; and

(c) a government feed configured to transmit threat information to the central repository.

23. The computerized system of claim 20, wherein a first one of the plurality of local repositories is configured to transmit at least one item of threat information over the network via the central repository to at least a second one of the plurality of local repositories.

24. The computerized system of claim 20, wherein a first one of the plurality of local repositories is configured to transmit at least one item of threat information over the network directly to at least a second one of the plurality of local repositories.