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, 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

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.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a diagram of a "hub & spoke" computerized system for sharing threat information.

FIG. 2 is a diagram of a "hub & spoke" computerized system for sharing threat information that includes an access control group.

FIG. 3 is a diagram of a "hub & spoke" and "peer-to-peer" computerized system for sharing threat information.

FIG. 4 is a diagram of a computerized system for sharing threat information.

DETAILED DESCRIPTION OF THE INVENTION

As discussed above, an exemplary existing association for sharing threat information, such as REN-ISAC or CISCP, shares threat information by first manually processing a piece of threat information, and then distributing the processed threat information, (usually in a language or format that is customized and proprietary to that member) to other members of the sharing association. These other members must then translate the received piece of threat information from the customized language into one or more languages that those other members' systems can understand.