



(86) Date de dépôt PCT/PCT Filing Date: 2015/01/29  
(87) Date publication PCT/PCT Publication Date: 2015/08/06  
(85) Entrée phase nationale/National Entry: 2016/06/30  
(86) N° demande PCT/PCT Application No.: US 2015/013522  
(87) N° publication PCT/PCT Publication No.: 2015/116819  
(30) Priorité/Priority: 2014/01/31 (US14/169,401)

(51) CI.Int./Int.Cl. G06F 21/56 (2013.01),  
G06F 17/30 (2006.01)  
(71) Demandeur/Applicant:  
CROWDSTRIKE, INC., US  
(72) Inventeurs/Inventors:  
DIEHL, DAVID, F., US;  
LAMOTHE-BRASSARD, MAXIME, CA  
(74) Agent: SMART & BIGGAR

(54) Titre : ETIQUETAGE D'OBJETS DE SYSTEME PERTINENTS POUR LA SECURITE  
(54) Title: TAGGING SECURITY-RELEVANT SYSTEM OBJECTS

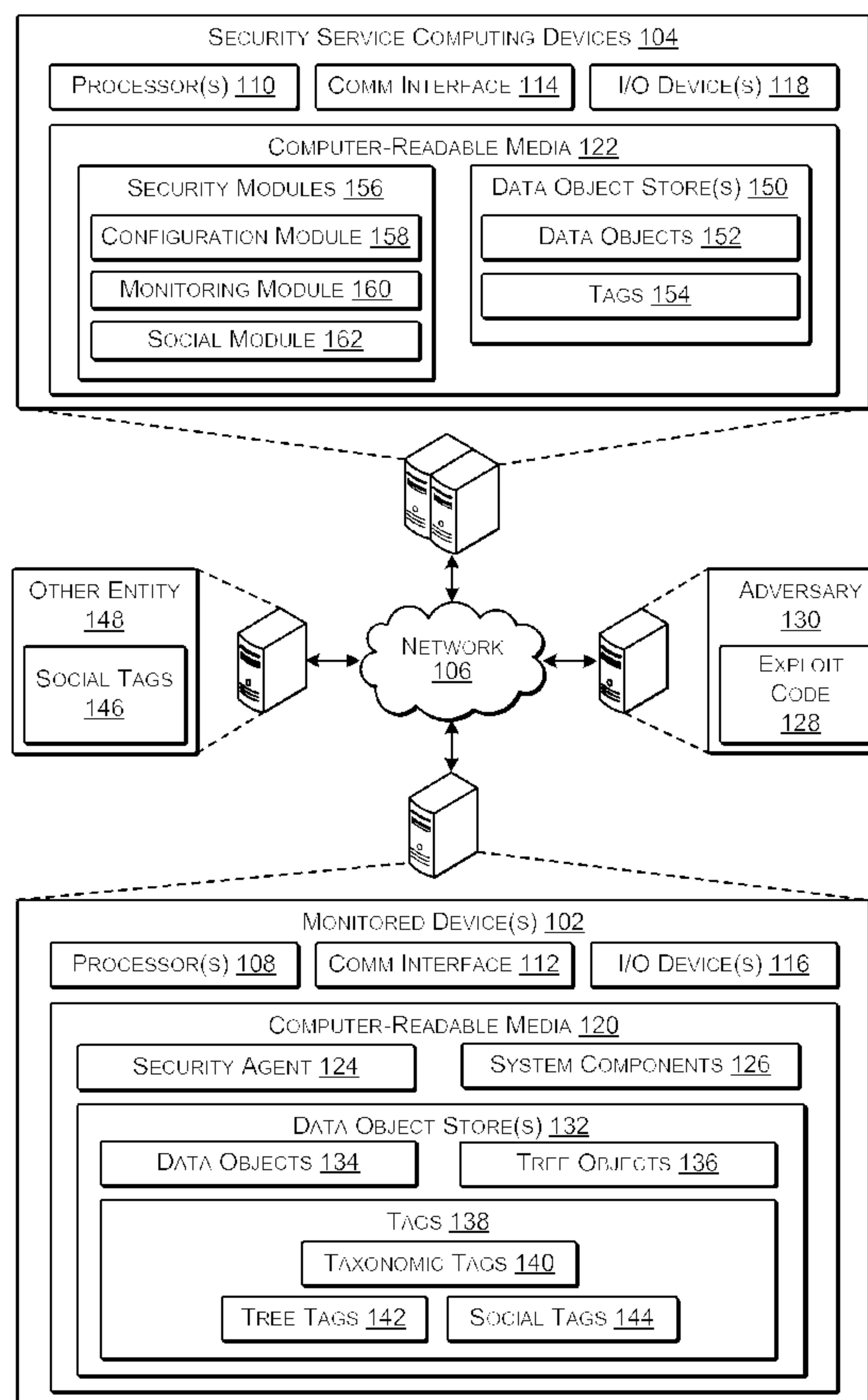


FIG. 1

(57) Abrégé/Abstract:

Devices described herein are configured to propagate tags among data objects representing system components. Such devices may detect an event associated with a plurality of system components. Based at least in part on detecting the event and on a

**(57) Abrégé(suite)/Abstract(continued):**

configurable policy, the devices may propagate a tag that is assigned to a data object representing one of the plurality of system components to another data object representing another of the plurality of system components. One example of such a tag may be associated with a tree object that represents an execution chain of instances of at least the system component represented by the data object and the other system component represented by the other data object. Another example of such a tag may be a user-specified tag of another entity that the entity associated with the devices subscribes to.

## (12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization  
International Bureau



(43) International Publication Date  
6 August 2015 (06.08.2015)

(10) International Publication Number  
**WO 2015/116819 A1**

(51) International Patent Classification:  
**G06F 21/56** (2013.01)      **G06F 17/30** (2006.01)

(74) Agents: **LEGGETT, Richard, B.** et al.; Lee & Hayes, PLLC, 601 W. Riverside Ave, Suite 1400, Spokane, WA 99201 (US).

(21) International Application Number:  
**PCT/US2015/013522**

(81) **Designated States** (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(22) International Filing Date:  
29 January 2015 (29.01.2015)

(84) **Designated States** (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK,

(25) Filing Language:  
English

(26) Publication Language:  
English

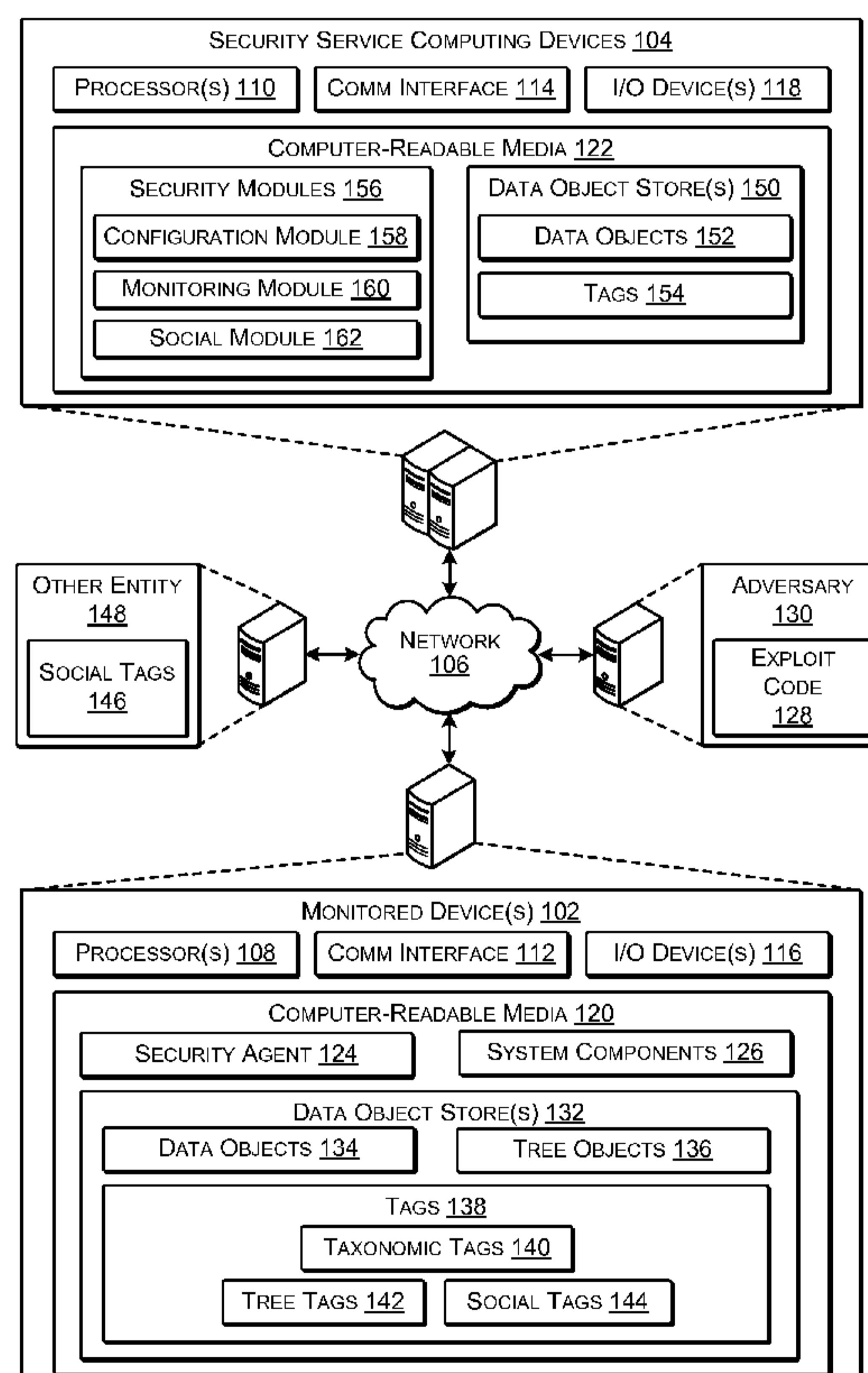
(30) Priority Data:  
14/169,401 31 January 2014 (31.01.2014) US

(71) Applicant: **CROWDSTRIKE, INC.** [US/US]; 15440 Laguna Canyon Road, Suite 250, Irvine, CA 92618 (US).

(72) Inventors: **DIEHL, David, F.**; 5324 Elliot Ave S, Minneapolis, MN 55417 (US). **LAMOTHE-BRASSARD, Maxime**; 1201-180 York Street, Ontario, Ottawa, K1N1J6 (CA).

[Continued on next page]

## (54) Title: TAGGING SECURITY-RELEVANT SYSTEM OBJECTS



**FIG. 1**

**(57) Abstract:** Devices described herein are configured to propagate tags among data objects representing system components. Such devices may detect an event associated with a plurality of system components. Based at least in part on detecting the event and on a configurable policy, the devices may propagate a tag that is assigned to a data object representing one of the plurality of system components to another data object representing another of the plurality of system components. One example of such a tag may be associated with a tree object that represents an execution chain of instances of at least the system component represented by the data object and the other system component represented by the other data object. Another example of such a tag may be a user-specified tag of another entity that the entity associated with the devices subscribes to.

WO 2015/116819 A1

**WO 2015/116819 A1**



SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, **Published:**  
GW, KM, ML, MR, NE, SN, TD, TG). — *with international search report (Art. 21(3))*

## TAGGING SECURITY-RELEVANT SYSTEM OBJECTS

## RELATED APPLICATIONS

[0001] This patent application claims priority to U.S. Utility patent 5 application entitled “Tagging Security-Relevant System Objects”, with Serial No. 14/169,401, filed January 31, 2014. Application Serial No. 14/169,401 is fully incorporated herein by reference.

## BACKGROUND

10 [0002] With Internet use forming an ever-greater part of day-to-day life, malicious software (often referred to as “malware”) and other security exploits that steal or destroy system resources, data, and private information are an increasing problem. Governments, businesses and individuals may devote significant resources to preventing intrusions, damage and thefts related to 15 these security exploits. Security exploits come in many forms, such as computer viruses, worms, trojan horses, spyware, keystroke loggers, adware and rootkits. Such security exploits can be delivered in or through a variety of mechanisms, such as phishing emails, malicious clickable links, infected documents, infected executables, or infected archives.

20 [0003] Tools for addressing these threats may apply conditional logic, testing whether some aspect of a system component, such as a process or file, matches one of more criteria. Based on meeting the criteria, the tools may take some action or actions. Modifications to the criteria, which may alter the system components that are identified, may be cumbersome. For instance, such

modifications may require changes to the source code of the tools and recompiling of the tools.

## BRIEF DESCRIPTION OF THE DRAWINGS

5 [0004] The detailed description is set forth with reference to the accompanying figures. In the figures, the left-most digit(s) of a reference number identifies the figure in which the reference number first appears. The use of the same reference numbers in different figures indicates similar or identical items or features.

10 [0005] FIG. 1 illustrates an example framework and devices for enabling interaction between a monitored device and a security service cloud.

[0006] FIG. 2 illustrates an example system component associated with an event, the filtering of the event based on a configurable policy, and the assigning of a tag to a data object representing the system component based on

15 the event and the filtering.

[0007] FIG. 3 illustrates example system components associated with an event and the propagation of a tag assigned to a data object representing one of these system components to another data object representing another of the system components.

20 [0008] FIG. 4 illustrates a tree object representing an execution chain of instances of system components, the assigning of tags to the tree object, and the assigning of a tag for the tree object to data objects representing the system components.

[0009] FIG. 5 illustrates one entity subscribing to the user-specified tags of another entity and assigning those user-specified tags to ones of the data objects of monitored devices of the entity.

[0010] FIG. 6 is a flow diagram illustrating an example process for 5 detecting an event associated with system components and propagating a tag assigned to a data object representing one of these system components to another data object representing another of the system components.

## DETAILED DESCRIPTION

10 [0011] This disclosure includes techniques and arrangements for assigning tags to data objects representing system components associated with security-relevant system events (hereinafter simply “events”) and for propagating tags among the data objects based on those events and on a configurable policy. As used herein, the term “tag” refers to data object metadata that acts as a label or 15 classifier of a data object. A tag may be a string, an integer, a hash, a binary flag, or some other efficient representation. Tags enable filtering of data objects for reporting, decision-making, and event generation and allow reclassification of data objects without any need for recoding or recompiling.

[0012] In various embodiments, one or more monitored devices may each 20 be equipped with a security agent to monitor events on those respective one or more computing devices and a data store to maintain data objects representative of system components associated with those events. Those monitored computing devices may be in communication with devices of a

security service cloud. The security service cloud may be also be configured to monitor events on those monitored computing devices and to maintain data objects representative of system components associated with those events in a data object store of the security service cloud. The security agents and security 5 service cloud may monitor the same events, different events, or overlapping sets of events. Also, in some embodiments, the security agents may simply detect events and inform the security service cloud of those detected events. The data object stores of the security agents and security service cloud may include data objects representing the same system components, data objects 10 representing different system components, or an overlapping set of data objects.

[0013] A security agent or security service cloud may first assign tags to the data objects based on a configurable policy. Such tags may be considered “taxonomic tags” which classify a type, function, role, etc. of a system 15 component. For example, “document program” may be such a “taxonomic tag.” The security agent or security service cloud may also assign tags to data objects based on the observed behaviors or characteristics of the system components they represent. For instance, if a process repeatedly opens document files, the security agent or security service cloud may assign the tag 20 “document program” to the process.

[0014] The security agent or security service cloud may detect or be informed of events and the system components associated with those events. Such events could include processes spawning other processes or threads,

processes creating or opening files, etc. These events may include all events occurring on a monitored computing device or a subset of those events. If a subset, the security agent or security service cloud may be configured to filter events based on a configuration of the security agent or on a configurable 5 policy (as used herein, “configurable policy” may refer to the configuration of the security agent or to a policy utilized by the security agent or security service cloud).

[0015] Based on the detected event and on the configurable policy, the security agent or security service cloud may propagate a tag assigned to one 10 data object representing a system component associated with the event to another data object representing another of the system components associated with the event. For example, if a process creates a file, the security agent or security service cloud may propagate one or more tags of the data object for that process to the data object for that file. The security agent or security 15 service cloud may propagate all of the tags of the data object for the process or only a subset of those tags based at least in part on the configurable policy. Propagation may occur in both directions, too; tags of the data object representing the file may also be propagated to the data object representing the process. In another example, a process may spawn multiple threads, and the 20 security agent or security service cloud may propagate one or more tags of the data object for that process to all or only a subset of the data objects for those threads based at least in part on the configurable policy.

[0016] In some embodiments, the security agent or security service cloud may generate a data object that represents detected event and assign a tag to that data object, such as “suspicious event.” Such tags may be updated in response to detecting a subsequent event. For example, if a first event is 5 merely suspicious, it may later be seen as security exploit activity if a second event occurs. In such a case, the tag may be updated to reflect the additional context (e.g., the tag “suspicious event” may be updated to “exploit activity”).

[0017] In various embodiments, the security agent or security service cloud may also create a tree object to represent an execution chain of instances of the 10 system objects associated with the event. For example, if an event involves one process executing another process, that execution chain could be represented in a tree object. If the other process then creates a file, that file could also be represented in the tree object. The security agent or security service cloud can assign tags to the tree object and can assign a tree object tag 15 to data objects representing the system components with appear in the tree object. Through the tree object tag, tags assigned to the tree object may be considered as tags of the data objects assigned the tree object tag. This enables retrospective classification of system components. For instance, nothing may be suspicious about a particular process when it first executes another. But if 20 that other process then goes on to execute a further process, and the further process performs an action recognized as security exploit activity, the tag “security exploit” may be assigned to the tree object representing that execution chain. And because a tree object tag for that tree object is assigned

to the original process, that original process now, through the tree object tag and tree object, has the tag “security exploit.”

[0018] In further embodiments, the security agent or security service cloud may enable a user to assign tags to data objects representing system 5 components. These user-specified tags may be utilized by security agents of an entity associated with the user. Such tags may be utilized to classify system components that have not yet been classified in the configurable policy. For example, a particular process may be a document program, but a security agent utilizing the configurable policy may not recognize the process as such. The 10 user may assign the tag “document program” to the data object representing that process. These user-specified tags may then later be considered in updating the configurable policy and taxonomic tags. Also, an entity may subscribe to another entity’s user-specified tags, causing that other entity’s user-specified tags to be assigned to the entity’s data objects.

15 [0019] In some embodiments, the security agent or security service cloud may then utilize the tags to make decisions, generate reports, or even generate events. For example, if a tag is propagated to a data object that has been assigned a tag that conflicts with the propagated tag, the security agent or security service cloud may generate a tag conflict event.

20 [0020] Additionally, the security agent or security service cloud may update the tags assigned to the data objects based on an update to the configurable policy. Such updating may allow for reclassification without burdensome

activities like recoding or recompiling the security agent or security service cloud.

### **Example Framework and Devices**

5 [0021] FIG. 1 illustrates an example framework and systems for enabling interaction between a monitored device and a remote security service. As illustrated, one or more monitored devices 102 may be connected to security service computing devices 104 of a security service cloud via a network 106. In various embodiments, the monitored devices 102 may each be a server or 10 server farm, multiple, distributed server farms, a mainframe, a work station, a personal computer (PC), a laptop computer, a tablet computer, a personal digital assistant (PDA), a cellular phone, a media center, an embedded system, or any other sort of device or devices. When implemented on multiple computing devices, a monitored device 102 may distribute its modules and data 15 among the multiple computing devices. In some implementations, a monitored device 102 represents one or more virtual machines implemented on one or more computing devices. Also, each monitored device 102 may be associated with an entity, and the entity or entities may in turn have security service arrangements with a security service provider. The security service provider 20 may in turn operate a security service cloud, which may include the security service computing devices 104.

[0022] In some embodiments, the security service computing devices 104 may each be or include a server or server farm, multiple, distributed server

farms, a mainframe, a work station, a PC, a laptop computer, a tablet computer, a PDA, a cellular phone, a media center, an embedded system, or any other sort of device or devices. In one implementation, the security service computing devices 104 implementing the security service cloud represent a plurality of 5 computing devices working in communication, such as a cloud computing network of nodes. When implemented on multiple computing devices, a security service computing device 104 may distribute its modules and data among the multiple computing devices. In some implementations, one or more of the security service computing devices 104 represent one or more virtual 10 machines implemented on one or more computing devices.

**[0023]** The network 106 may include any one or more networks, such as wired networks, wireless networks, and combinations of wired and wireless networks. Further, the network 106 may include any one or combination of multiple different types of public or private networks (e.g., cable networks, the 15 Internet, wireless networks, etc.). For example, the network 106 may include a public network and a client network associated with one of the entities. Such a client network may each be a private network. In some instances, computing devices communicate over the network 106 using a secure protocol (e.g., Hypertext Transfer Protocol Secure (https)) and/or any other protocol or set of 20 protocols, such as the transmission control protocol/Internet protocol (TCP/IP).

**[0024]** As is further shown, each monitored device 102 may have a processor 108, and each security service computing device 104 may have a processor 110. Processors 108 and 110 may each be a central processing unit

(CPU), a graphics processing unit (GPU), or both CPU and GPU, or other processing unit or component known in the art. Processors 108 and 110 may be different types of processing units or components or may be of the same type.

5 [0025] Each monitored device 102 may also have a communication interface 112, and each security service computing device 104 may have a communication interface 114. The communication interfaces 112 and 114 may be any sort of wired or wireless interfaces (or both) that enable their respective devices to communicate over the network 106 with other devices, including 10 with each other. The communication interfaces 112 and 114 may be the same or different types of communication interfaces.

[0026] The monitored device(s) 102 each have input/output (I/O) devices 116, and the security service computing devices 104 each have I/O devices 118. The I/O devices 116 and 118 may include input devices, such as a 15 keyboard, a mouse, a touch-sensitive display, voice input device, etc., and output devices such as a display, speakers, a printer, etc. The I/O devices 116 and 118 may be the same or different types of I/O devices. The I/O devices 116 of the monitored device(s) 102 may be used to enter user-specified tags, to 20 subscribe to other entities' tags, and to view reports. The I/O devices 118 of the security service computing devices 104 may be used to specify the configurable policy, specify taxonomic tags, and view reports.

[0027] In various embodiments, each monitored device has one or more computer-readable media 120, and each security service computing device 104

has one or more computer-readable media 122. Computer-readable media 120 and 122 may include any tangible, non-transitory storage media. For instance, computer-readable media 120 and 122 may include, but are not limited to, RAM, ROM, EEPROM, flash memory or other memory technology, CD-ROM, digital versatile disks (DVD) or other optical storage, magnetic cassettes, magnetic tape, magnetic disk storage or other magnetic storage devices, or any other medium which can be used to store the desired information and which can be accessed by the respective monitored device 102 or security service computing device 104. Further, computer-readable media 10 120 and 122 may be removable and/or non-removable.

[0028] As illustrated in FIG. 1, the computer-readable media 120 of each monitored device 102 stores a security agent 124. The security agent 124 may be a kernel-level agent or may reside partly on a monitored device 102 and partly on the security service cloud. The security agent 124 may include event 15 consumers that receive notifications of events associated with execution activities of system components 126, filters, an event bus that routes the events to other module(s) of the security agent 124, correlators that track types of events and/or maintain state associated with events, and actors that gather state information and act upon events. The security agent 124 may be installed by 20 and configurable by a security service cloud, such as by one or more of the security service devices 104, receiving, and applying while live, reconfigurations of module(s) of the security agent 124. The security agent 124 may also receive and apply, while live, configurable policies from the

security service cloud. Such configurable policies may be the same as or different from the configuration of the security agent 124. An example security agent is described in greater detail in U.S. patent application serial number 13/492,672, entitled “Kernel-Level Security Agent” and filed on June 8, 2012.

5 [0029] The system components 126 may be any sort of module, process, thread, file, driver, service, pipe, handle, named kernel object, memory segment, user, cryptographic signer and signature authority, registry key, Internet Protocol (IP) address and subnet, domain name service (DNS) domain, or fully-qualified domain name (FQDN) of the monitored device 102. A  
10 system component 126 that is a module may be identified by a hash of its contents. These system components 126 may include both platform and application components. As mentioned, the security agent 124 receives notifications of execution activities, such as events, associated with these system components 126, filters and dispatched the events in accordance with  
15 the configuration of the security agent 124, and acts upon the events. Such actions may simply be recording and further monitoring or may rise to the level of remediation or alerts. In monitoring these events, the security agent 124 attempts to detect indications of exploit code 128 or other malicious activity of an adversary 130.

20 [0030] The security agent 124 may further include or be associated with a data object store 132. While FIG. 1 shows the data object store 132 as separate from the security agent 124, it is to be understood that the data object store 132 may either be a part of the security agent 124 or may be separate from and

associated with the security agent 124. The data object store 132 may represent current and past states of the monitored device 102. The past states maintained include at least a subset of past states, such as states that enhance forensic and policy understanding of the current state. The data object store 132 may have

5 at least three roles. In a first role, the data object store 132 may serve as a historian, providing access to past states of the monitored device 102 that are no longer stored elsewhere on the monitored device 102. In a second role, the data object store 132 may service as a validator, maintaining an independent model of the state of the monitored device 102 that can be used to detect

10 malicious modifications of the host operating system state storage of the monitored device 102. In a third role, the data object store 132 provides a cache of configuration, information, and state that are received from a remote security service, that are computationally expensive to generate or fetch, or that are high-latency to fetch. An example of such a data object store is described

15 in greater detail in U.S. patent application serial number 13/728,746, entitled “Real-Time Representation of Security-Relevant System State” and filed on December 27, 2012.

[0031] The data object store 132 may include a plurality of data objects 134 that represent system components 126 and events. These data objects 134 may

20 form one or more graphs composed of nodes and edges, with node data objects representing system components 126 and edge data objects representing events. The security agent 124, through any of its actors or correlators, may create and update the data objects 134. In some embodiments, the data object store 132

may also be associated with functional components that are capable of creating and updating the data objects 134 based on events received from filter and dispatch components of the security agent 124.

[0032] In various embodiments, the data object store 132 may also maintain 5 one or more tree objects 136. Tree objects 136 may represent execution chains of instances of system components 126. Whether or not the security agent 124 creates a tree object 136 responsive to an event may be determined based on the configurable policy received from the security service cloud.

[0033] As is further shown in FIG. 1, the data object store 132 may maintain 10 tags 138 for some or all of the data objects 134 and tree objects 136. Each tag 138 acts as a label or classifier of a data object 134 or a tree objects 136. While the tags 138 are shown separately from the data objects 134 and tree objects 136 in FIG. 1, it is to be understood that each tag 138 may be stored as metadata of a specific data object 134 or tree object 136, although such storage 15 may be contiguous or non-contiguous.

[0034] Tags 138 may have structure. The presence of a tag 138 can require another tag 138 (e.g., "Office2010" requires "Office" requires "document program") or at least one member of a set of tags 138 (e.g., "updater" requires some other tag 138 indicating something which can be updated). Alternatively, 20 such structure may be avoided with a hierarchy or via tag duplication. Such alternatives may be considered to avoid the computational expense of the tag structure. Tags 138 can also be mutually exclusive with each other (e.g., "document program" and "system program" may be mutually exclusive).

[0035] Further, tags 138 may be of any of a number of varieties, such as taxonomic tags 140, tree tags 142, and social tags 144. Tags 138 may also be of any of any number of different types, depending on implementation. Taxonomic tags 140 may be centrally declared and standardized (e.g., by the 5 security agent 124 or by the security service cloud), and may be used to pass defined indications that may enable decision-making and direct actions. In some embodiments, taxonomic tags 140 may only be assigned by security service cloud code or authorized employees of the security service provider through controlled interfaces. Examples of taxonomic tags 140 may be 10 classifications, such as a "CS\_ShowInUI" tag for use in detections. Taxonomic tags 140 may be flagged to never display to a customer.

[0036] Tree tags 142 are dynamically created on a monitored device 102 along with tree objects 136 and serve to identify those tree objects 136. Each tree tag 142 may be assigned to data objects 134 which represent system 15 components 126 that are included the tree object 142 identified by that tree tag 142. Tree tags 142 serve to associate data objects 134 with the taxonomic tags 140, social tags 144, or other tags 138 that are assigned to their respective tree objects 136.

[0037] Social tags 144 may be created and assigned by users of the 20 monitored devices 102. Social tags 144 may be controlled by an entity associated with a monitored device 102 rather than centrally controlled by the security service cloud. The social tags 144 may, however, be provided to the security service cloud and have indirect effects on the security service cloud

based on data analytics or manual propagation rules using the social tags 144 to assign taxonomic tags 140. Social tags 144 may include the identifier of the entities whose users created those social tags 144. Also, many taxonomic tags 140 may appear as social tags 144. For example, with a user associated with an 5 entity may assign a "document program" tag 144 to an executable that the security service cloud has not classified with a taxonomic tag 140.

[0038] Also, in some embodiments, the tags 138 may include a tag 138 for a "system" data object 134 that can be tagged to adjust overall posture of the monitored device 102, as a lightweight alternative to full multi-modal 10 configurations. This may cause the event filtering of the security agent 124 to start with a posture check.

[0039] In various embodiments, the security agent 124 may, in accordance with the configurable policy received from the security service cloud, assign tags 138 to data objects 134. For example, the security agent 124 may assign 15 taxonomic tags 140 to at least some of the data objects 134 based on the types, observed behaviors, or characteristics of the system components 126 or events that those data objects 134 represent. The security agent 124 may also assign tags 138 to tree objects 136 based at least in part on the configurable policy. The security agent 124 may assign or remove tags 138 from data objects 134 or 20 tree objects 136 directly with standard events, allowing dynamic control of tags 138, both programmatically and manually. Also, or instead, tag assignment may be triggered by any detected event. In such circumstances, tags 138 may be assigned to the data objects 134 representing the system components 126

associated with the event, to a data object 134 that represents the detected event, or to both.

[0040] Further, as illustrated in FIG. 2, the security agent 124 may assign tags 138 to data objects 134 based on events and on the configurable policy. At 5 202, the security agent 124 may detect the occurrence of an event associated with a system component 126, such as a file 204. The security agent 124 may then, at 206, filter the event based on the configurable policy. Based on the detection of the event and the filtering, the security agent 124 then, at 208, assigns a tag 138, such as tag X 210, to the data object 134 representing the 10 system component 126 (e.g., file data object 212 representing file 204).

[0041] In some embodiments, tags 138 may be propagated between data objects 134 by the security agent 124 based at least in part on the configurable policy and on detecting an event. When the security agent 124 detects an event, the security agent 124 consults the configurable policy and determines 15 which tags 138 should be propagated among the data objects 134 representing the system components 126 associated with the event. For example, if a parent process creates a child process, some or all of the tags 138 of the data object 134 representing the parent process may be propagated by the security agent 124 to the data object 134 representing the child process. Which tags 138 are 20 propagated may be determined based on propagation rules associated with the tags 138 and included in the configurable policy. The configurable policy may include a propagation mask for each tag 138 that indicates the events that will cause the propagation of that tag 138. Such propagation masks may be

compiler-generated bitmasks for each propagating event, allowing for a small, fixed number of operations for even a very large number of tags 138.

[0042] For example, in accordance with the configurable policy, a process may acquire some tags 138 by propagation from a file it loads, and we might 5 define different propagation behavior based on whether or not the file was loaded as a primary module.

[0043] FIG. 3 illustrates one example of such a tag propagation. As illustrated in FIG. 3, a security agent 124 may detect 302 an event that is associated with a process 304 and a file 306. For example, the process 304 10 might create, read, write to, or delete the file 306. In response, and in accordance with the configurable policy, the security agent 124 may propagate 308 a tag 310 (shown as “tag X 310”) from data object 312 representing the process 304 to a data object 314 representing the file 306. The process data object 312 may also have additional tags, such as tag Y 316, which are not 15 propagated to the file data object 314, in accordance with the configurable policy.

[0044] As described above, the security agent 124 may create tree objects 136 and tree tags 142 in accordance with the configurable policy. FIG. 4 illustrates an example of such tree object creation and tree tag assignment. As 20 shown in FIG. 4, a security agent 124 detects 402 an event associated with a process 404 and a file 406, such as the execution of the file 406 by the process 404. In response, and in accordance with the configurable policy, the security agent 124 constructs 408 a tree object 410 for the execution chain 412 of the

process 404 executing the file 406. Subsequent to creating the tree object 410, the security agent 124 may expand the representation of the execution chain 412 to represent additional events and instances of system components. For example, if the file 406 is an executable that then reads another file, the 5 security agent 124 may update the representation of the execution chain 412 in the tree object 410 to reflect the extension of the execution chain 412. The security agent 124 may also assign tags 138 to the tree object 410, such as tag A 414 and tag B 416. These tags 414 and 416 may be taxonomic tags 140 or social tags 144. The security agent 124 may assign the tags 414 and 416 in 10 accordance with the configurable policy. For example, if a system component 126 or event included in the execution chain 412 is determined to be suspicious, the tag “suspicious” could be assigned to the tree object 410. When creating the tree object 410, the security agent 124 also creates a tree tag 142 for the tree object 410 and assigns 418 the tree tag 142 (shown as “Tag T 420”) 15 to data objects 422 and 424 representing the process 404 and file 406, respectively. While data objects 422 and 424 are each shown as being assigned only a single tree tag 142, it is to be understood that any data object 134, such as data objects 422 and 424, may have multiple tree tags 142 assigned to it if the system component 126 or event represented by that data object 134 appears 20 in multiple tree objects 136. The data objects 422 and 424 may also have other tags 138 assigned to them. For example, the process data object 422 may have a tag C 426 assigned to it. When the security agent 124 subsequently filters the data objects 422 and 424 based on tags 138, the security agent 124 will

consider, for instance, the process data object 422 to have tag C 426, tag T 420, and by virtue of tag T 420, both tag A 414 and tag B 416 as well. Process data object 422 will be considered to have tag A 414 and tag B 416 transitively – there is no need for these tags 414 and 416 to be explicitly assigned as their 5 association with tree tag T 420 is sufficient to ensure their application to the process data object 422.

[0045] Returning to FIG. 1, the security agent 124 or a user interface received from the security service provider (e.g., a web page) may also enable a user of the monitored device 102 to subscribe to social tags 146 of another 10 entity 148 on behalf of the entity associated with the monitored device 102. The monitored device 102 may then receive the social tags 146, either directly from monitored devices of the other entity 148 or through a security service computing device 104 of the security service cloud. The monitored device 102 may also continue to receive the subscribed-to social tags 146 on an ongoing 15 basis, as the social tags 146 are created. Upon receiving the social tags 146, the security agent 124 may assign the social tags 146 to data objects 134. The social tags 146 are assigned to data objects 134 that are equivalents of the data objects of the other entity. “Equivalent” data objects may be those representing a same or similar type of system component 126 or event. Upon receiving and 20 assigning the social tags 146, those social tags 146 may be considered part of social tags 144.

[0046] Social tags 144 can be used to provide a number of capabilities; for instance, social tags 144 may be used arbitrarily for annotation, allowing

coordination between multiple analysts and across entities. Social tags 144 on patterns and files can allow for expression of entity preferences about policy and priority of different patterns, and to allow entities to rapidly whitelist local programs and files overall or with respect to specific patterns.

5 [0047] FIG. 5 illustrates an example of subscription to another entity's social tags. As illustrated in FIG. 5, a first entity 502 may subscribe 504 to social tags 506 of a second entity 508. The social tags 506 may be assigned to data objects, such as data object 510, which represent system components 126 or events of monitored devices 102 of the second entity 508. Responsive to the 10 subscription, the first entity 502 may receive 512 the social tags 506. Security agents 124 of the monitored devices 102 of the first entity 502 may then assign the social tags 506 to data objects 514. Data objects 514 may then have both any tags of their own, such as tag D 516, and the subscribed-to social tags 506.

[0048] In various embodiments, referring again to FIG. 1, the security agent 15 124 may utilize the tags 138 for reporting, decision-making, or event-generating. The security agent 124 may utilize the configurable policy and tags 138 to filter the data objects 134. The result of that filtering may then be utilized to generate a report, which may be provided to a user of the monitored device 102 through the security agent 124 or through a user interface provided 20 by the security service cloud (e.g., a web page). The security agent 124 may also or instead make a decision based on the filtered data objects 134. For example, if the filtered data objects 134 include any data objects 134 with the tag 138 "suspicious", the security agent 134 may decide to perform additional

monitoring or take remedial action. Further, the security agent 124 may generate events. For example, if the security agent 124 propagates a tag 138 to a data object 134, and that data object 134 has another tag 138 that conflicts with the propagated tag 138, the security agent 124 may generate an event 5 indicative of a tag conflict.

[0049] Tags 138 can also be used by the security agent 124 to trigger runtime policy. For example, a tag 138 could indicate that a process should not be allowed to make outbound network connections. Such tags 138 take their effect from the configurable policy that is used by the security agent 124 to 10 filter on the presence of the tag 138.

[0050] In various embodiments, the security service computing devices 104 of the security service cloud may each maintain in its computer-readable media 122, a data object store 150, which may include data objects 152 and tags 154. The data object store 150 may represent current and past states of one or more 15 of the monitored devices 102. The past states maintained include at least a subset of past states, such as states that enhance forensic and policy understanding of the current state(s). The data object store 150 may include a plurality of data objects 152 that represent system components 126 and events of the one or more monitored computing devices. These data objects 152 may 20 form one or more graphs composed of nodes and edges, with node data objects representing system components 126 and edge data objects representing events. The data object store 150 may maintain separate graphs for each of the monitored devices 102, a graph for multiple ones of the monitored devices, or

both. A graph representing multiple ones of the monitored devices 102 may include representation of events associated with system components 126 from multiple monitored devices 102, such as a process on one monitored device 102 accessing a file on another monitored device 102. While not shown, the 5 data object store 150 may include copies of the tree objects 136 created on the monitored devices 102.

[0051] In some embodiments, the tags 154 may be represent a superset of the tags 138 of the one or more monitored devices 102. Because the taxonomic tags 140 may be centrally created by the security service computing devices 10 104, the taxonomic tags 140 included in the tags 154 may be the same as, or at least include all of, the taxonomic tags 140 included in the tags 138. The taxonomic tags 140 included in the tags 154 may also include additional taxonomic tags 140 that have not yet been assigned to any data objects 134 or tree objects 136 of the monitored devices. The tree tags 142 of the tags 154, in 15 addition to identifying tree objects 136 of monitored devices 102, also include identifiers of the monitored devices 102 to which the tree objects 136 belong. The social tags 144 of the tags 154 include identifications of the entities that created those social tags 144. As mentioned above, the security service cloud may utilize these social tags 144 in defining additional taxonomic tags 140.

20 [0052] The communications model for tags 138 and 154 implemented by the security agents 124 and the security service cloud may define under what circumstances tags 138 flow between monitored devices 102 and security service computing devices 104. This flow may be implemented as another

propagation operation, or possibly as two operations: one to passively forward tag 138 and another to push changes to the tag assignment proactively.

[0053] In further embodiments, the security modules 156 of the security service computing devices may be configured to provide information security services to individual users and client entities through their monitored devices 102, such as maintenance and configuration of the security agent 124 and data object store 134, threat modeling, and/or remediation. The security modules 156 may include a configuration module 158 to configure the security agents 124 and to provide the configurable policy to the security agents 124, a monitoring module 160 to detect events on the monitored devices 102 or to receive indications of the occurrences of those events, and a social module 162 to enable social aspects of the security services, such as the sharing of social tags 144.

[0054] In further embodiments, the security modules 156 may build and maintain the data object store 150. The monitoring module 160 of the security modules 156 may detect events or receive indications of the occurrence of events and use that information to build the data object store 150. Such information may be received in substantially real time as the events are observed. The configuration module 158 may configure the monitored devices 102, specifying the events that the monitored devices 102 are to notify the monitoring module 160 of and the tags 138 which the monitored devices 102 are to share. Further, the configuration module 158 may update the configurable policy and disseminate the updated configurable policy to the

monitored devices 102. Such an updated configurable policy may result in the updating of assignments of tags 138, removing some tags 138 and adding others. The updated configurable policy may also update propagation masks for tags 138, resulting in different propagation behaviors.

5 [0055] In some embodiments, the social module 162 may also provide social aspects to the security services, forming groups of users and/or client entities and automatically sharing security information among the users and/or client entities constituting a group. Alternatively or additionally, the social module 162 may enable the users or entities to subscribe to the social tags 144  
10 of other users or other entities and enable the exchange of the subscribed-to tags 144, either retrieving and providing them or enabling users/entities to provide the social tags 144 to each other directly.

[0056] While not shown, the security modules 156 may also include one or more modules to act filter the tags 154 and act upon the filtering. Such actions  
15 may include decision-making, report-generating, or event-generating, in the manner described above with respect to the security agent 124. The actions may further include causing the configuration module 158 to update the configurable policy.

## 20 Example Processes

[0057] FIG. 6 illustrates an example processes. This process is illustrated as a logical flow graph, each operation of which represents a sequence of operations that can be implemented in hardware, software, or a combination

thereof. In the context of software, the operations represent computer-executable instructions stored on one or more computer-readable storage media that, when executed by one or more processors, perform the recited operations. Generally, computer-executable instructions include routines, programs, 5 objects, components, data structures, and the like that perform particular functions or implement particular abstract data types. The order in which the operations are described is not intended to be construed as a limitation, and any number of the described operations can be combined in any order and/or in parallel to implement the processes.

10 [0058] FIG. 6 is a flow diagram illustrating an example process for detecting an event associated with system components and propagating a tag assigned to a data object representing one of these system components to another data object representing another of the system components. The process includes, at 602, a security agent or security service cloud assigning 15 tags to data objects representing system components of a computing device. Such assignment may be based on a configurable policy. The tags may each be one of a string, an integer, a hash, or a binary flag, and the system components may include at least one of modules, processes, threads, files, drivers, services, pipes, handles, named kernel objects, memory segments, users, cryptographic 20 signers and signature authorities, registry keys, Internet Protocol (IP) addresses and subnets, domain name service (DNS) domains, or fully-qualified domain names (FQDNs). Also, the tags may have structure; a tag can imply another tag or be mutually exclusive with another tag. Further, a tag may be associated

with logic which, when executed, classifies the system component represented by the data object and assigns a new tag (either in addition to the previous tag or replacing the previous tag) that is associated with the classification of the system component. At 604, the assigning may include enabling a user to 5 associate the tag with a system component represented by a data object and assigning that user-associated tag to the data object. At 606, the assigning may include assigning a tag based at least in part on observed behavior or characteristics of a system component represented by a data object. Additionally or instead, the assigning may include assigning a tag to a data 10 object representing a system component based at least in part on detecting an event associated with that system component and on filtering of that event using the configurable policy.

[0059] At 608, a security agent of a first entity may subscribe to user-specified tags of a second entity. The security agent may then assign the 15 second entity's user-specified tags to data objects representing system components of computing devices of the first entity.

[0060] At 610, the security agent or security service cloud may detect an event occurring on a computing device that is associated with multiple system components of the computing device.

20 [0061] At 612, based on the configurable policy, the security agent or security service cloud may assign another tag to a data object representing the detection of the event. At 614, the security agent or security service cloud may

detect a subsequent event and, based at least in part on detecting the subsequent event, update the other tag.

[0062] At 616, the security agent or security service cloud may construct a tree object representing an execution chain of instances of at least a subset of 5 the system components. The security agent or security service cloud may construct the tree object in response to detecting execution of one system component of the subset of the system components by another system component of the subset of system components. The subset of system components may include both processes and non-process system components.

10 At 618, the security agent or security service cloud may assign a tag for the tree object to the data objects representing the subset of the system components.

[0063] At 30620, based at least in part on detecting the event and on the configurable policy, the security agent or security service cloud propagates a tag that is assigned to a data object representing one system component of the 15 plurality of system components to another data object representing another of the plurality of system components. In some embodiments, the propagating comprises propagating, based at least in part on the configurable policy, less than all of a plurality of tags assigned to the data object. Also or instead, the propagating may comprise propagating, based at least in part on the configurable policy, the tag to data objects representing a subset of the plurality 20 of system components. Further, the system components may be system components of a computing device and the propagating may be performed by one or more other computing devices. In such embodiments, the data object

and other data object may be stored on the one or more other computing devices. In addition, in some embodiments, the system component represented by the data object may be a system component of a first computing device, the other system component represented by the other data object may be a system component of a second computing device, and the propagating may be performed by any of the first computing device, the second computing device, or third one or more computing devices.

[0064] At 622, the security agent or security service cloud may generate an event based on the tag propagation. For example, the propagated tag may be mutually exclusive with another tag associated with the other data object, and the security agent or security service cloud may generate an event indicative of a tag conflict. Also or instead, at 624624, based at least in part on tags associated with data objects representing the plurality of system components, the security agent or security service cloud may perform at least one of making a decision or generating a report.

## CONCLUSION

[0065] Although the subject matter has been described in language specific to structural features and/or methodological acts, it is to be understood that the subject matter defined in the appended claims is not necessarily limited to the specific features or acts described. Rather, the specific features and acts are disclosed as example forms of implementing the claims.

## CLAIMS

## WHAT IS CLAIMED IS:

1. A computer-implemented method comprising:
  - 5 detecting an event associated with a system component;
  - filtering the event based on a configurable policy; and
  - based at least in part on the detecting and the filtering, assigning a tag to a data object representing the system component.
- 10 2. The method of claim 1, wherein the detecting, the filtering, and the assigning are performed by a kernel-level security agent.
- 15 3. The method of claim 1, wherein the tag is one of a string, an integer, a hash, or a binary flag.
4. The method of claim 1, further comprising assigning, based at least in part on the configurable policy, another tag to a data object representing the detection of the event.
- 20 5. The method of claim 1, wherein the tag can imply another tag or be mutually exclusive with another tag.

6. The method of claim 1, wherein the assigning is based at least in part on observed behavior or characteristics of the system component represented by the data object.

5 7. The method of claim 1, wherein the tag is associated with logic which, when executed, classifies the system component represented by the data object and assigns a new tag that is associated with the classification of the system component.

10 8. The method of claim 1, further comprising, based at least in part on the tag associated with the data object representing the system component, performing at least one of making a decision or generating a report.

15 9. The method of claim 1, further comprising:  
enabling a user to associate the tag with the system component represented by the data object, and  
performing the assigning of the tag to the data object based at least in part on the user associating the tag with the system component.

20 10. The method of claim 9, wherein the tag is shareable with one or more other users of one entity that subscribes to tags associated by the user or another user of another entity with the system component.

11. A computer-implemented method comprising:  
detecting an event associated with a plurality of system components; and  
based at least in part on a configurable policy and on detecting the event,  
propagating a tag that is assigned to a data object representing one of the  
5 plurality of system components to another data object representing another of  
the plurality of system components.

12. The method of claim 11, wherein the tag is one of a string, an  
integer, a hash, or a binary flag.

10

13. The method of claim 11, wherein the propagating comprises  
propagating, based at least in part on the configurable policy, less than all of a  
plurality of tags assigned to the data object.

15 14. The method of claim 11, wherein the propagating comprises  
propagating, based at least in part on the configurable policy, the tag to data  
objects representing a subset of the plurality of system components.

15. The method of claim 11, wherein the tag is mutually exclusive with  
20 another tag associated with the other data object, and the method further  
comprises generating an event indicative of a tag conflict.

16. The method of claim 11, wherein the system components include at least one of modules, processes, threads, files, drivers, services, pipes, handles, named kernel objects, memory segments, users, cryptographic signers and signature authorities, registry keys, Internet Protocol (IP) addresses and 5 subnets, domain name service (DNS) domains, or fully-qualified domain names (FQDNs).

17. The method of claim 11, wherein the tag is associated with a tree object that represents instances of at least a subset of the plurality of system 10 components.

18. The method of claim 11, wherein the system components are system components of a computing device and the propagating is performed by one or more other computing devices, the data object and other data object being 15 stored on the one or more other computing devices.

19. The method of claim 11, wherein the system component represented by the data object is a system component of a first computing device, the other system component represented by the other data object is a system component 20 of a second computing device, and the propagating is performed by any of the first computing device, the second computing device, or a third one or more computing devices.

20. A system comprising:

a processor;

a memory coupled to the processor, the memory storing:

data objects representing a plurality of system components,

5 a tree object representing an execution chain of instances of at

least a subset of the system components, and

executable instructions, which, when operated by the processor,

perform operations including:

assigning a tag for the tree object to the data objects

10 representing the subset of the system components,

assigning one or more tags to the tree object, those tags

applying to the data objects having the tag for the tree object, and

making a decision based at least in part on tags assigned to

the data objects representing the subset of the system components

15 and the tags assigned to tree object.

21. The system of claim 20, wherein the operations further include

constructing the tree object in response to detecting execution of one system

component of the subset of the system components by another system

20 component of the subset of system components.

22. The system of claim 20, wherein the subset of system component

includes both processes and non-process system components.

23. The system of claim 20, wherein the memory stores multiple tree objects, and tags for the multiple tree objects are assigned to a data object representing a system component which appears in execution chains 5 represented by the multiple tree objects.

24. One or more non-transitory computer-readable media having stored thereon a plurality of programming instructions that, when executed by a computing device, cause the computing device to perform operations 10 comprising:

subscribing, by an entity, to user-specified tags of another entity, the user-specified tags being associated with data objects representing system components of computing devices of the other entity,

15 assigning the other entity's user-specified tags to data objects representing system components of computing devices of the entity; and

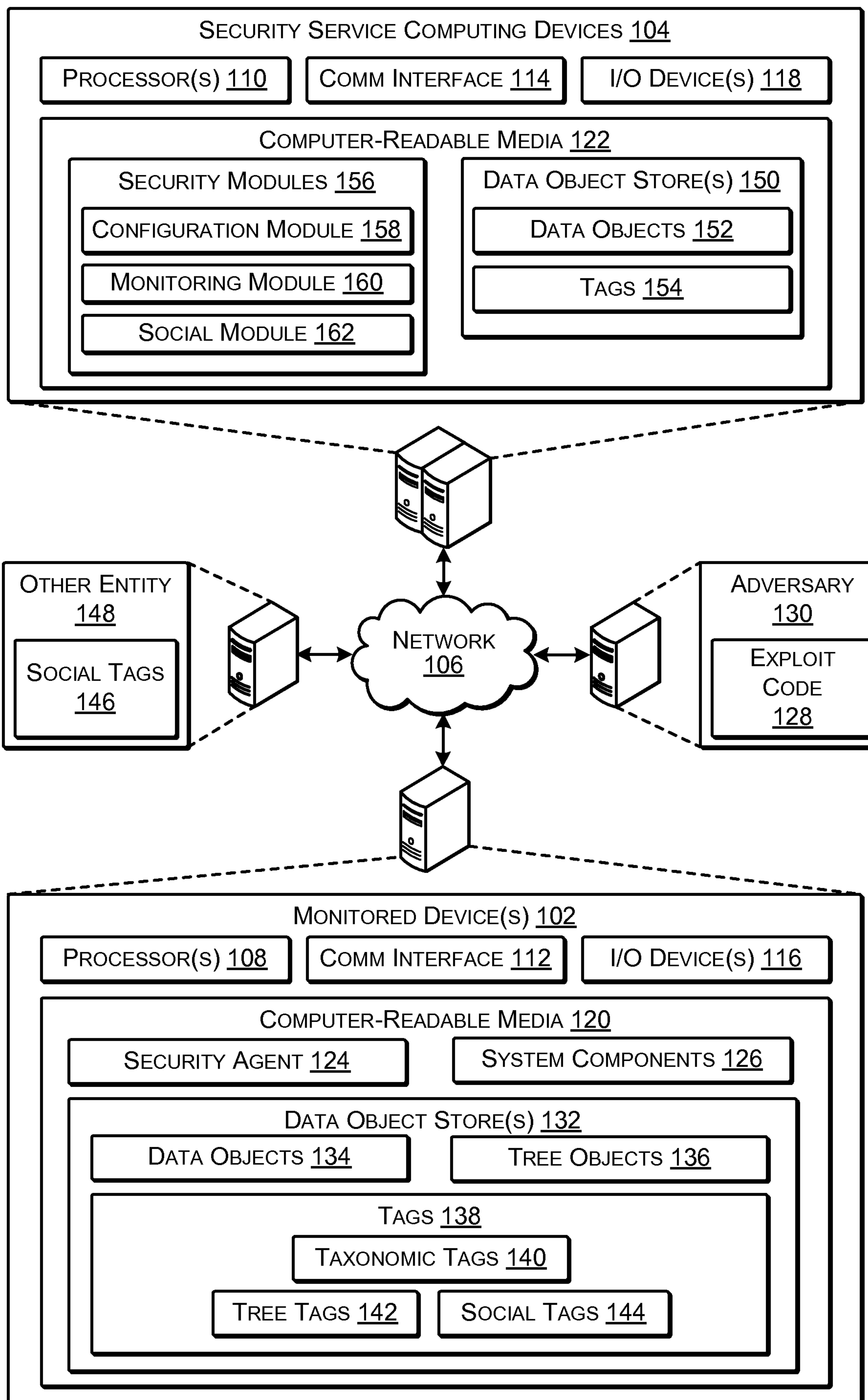
making a decision based at least in part on the other entity's user-specified tags.

25. The one or more non-transitory computer-readable media of claim 20 24, wherein one of the user-specified tags is a taxonomic tag applied to an unclassified system component.

26. The one or more non-transitory computer-readable media of claim 24, wherein user-specified tags are shared with a service cloud and utilized by the service cloud in determining global changes in tag assignments.

5

1/6

**FIG. 1**

2/6

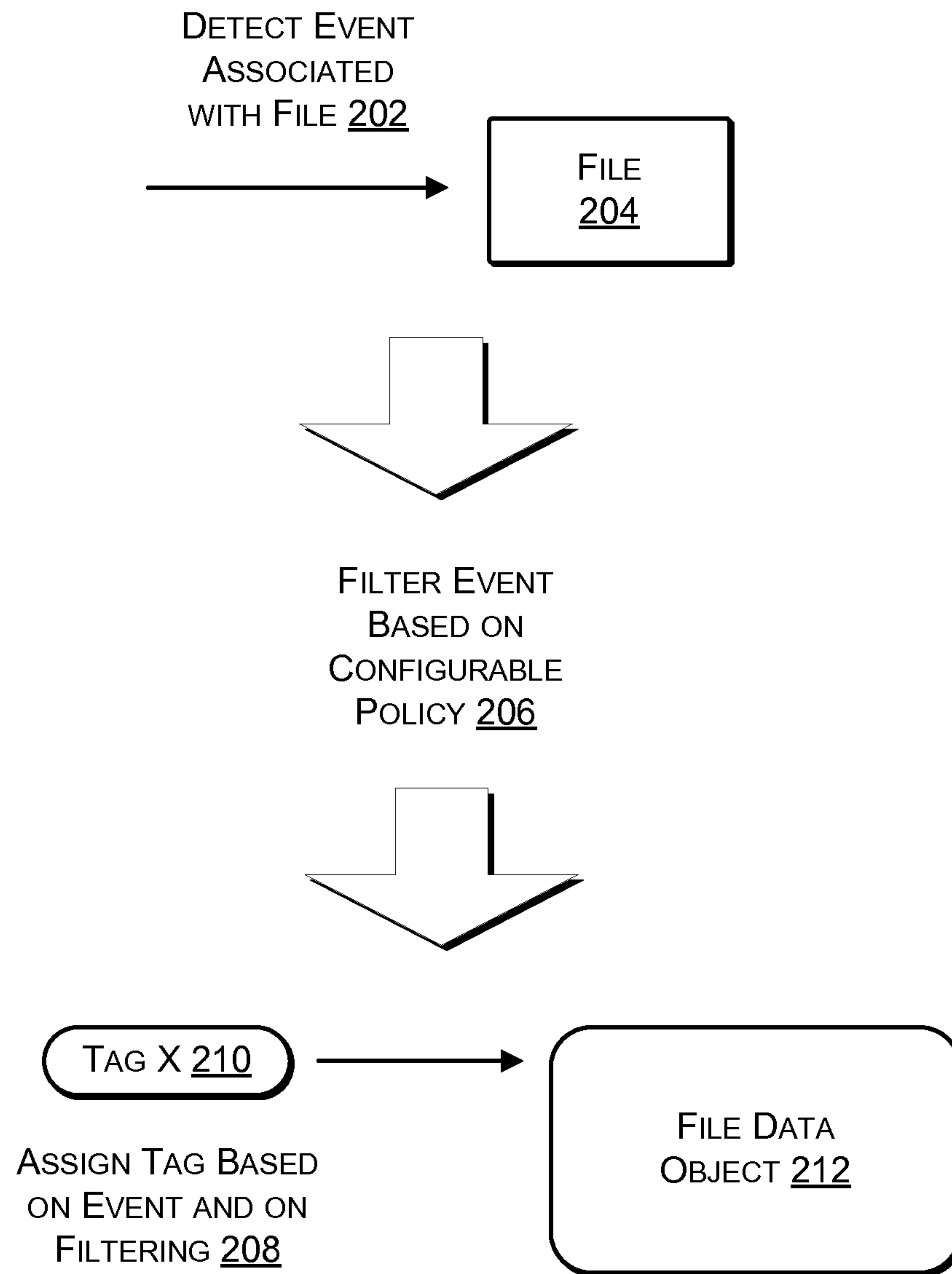


FIG. 2

3/6

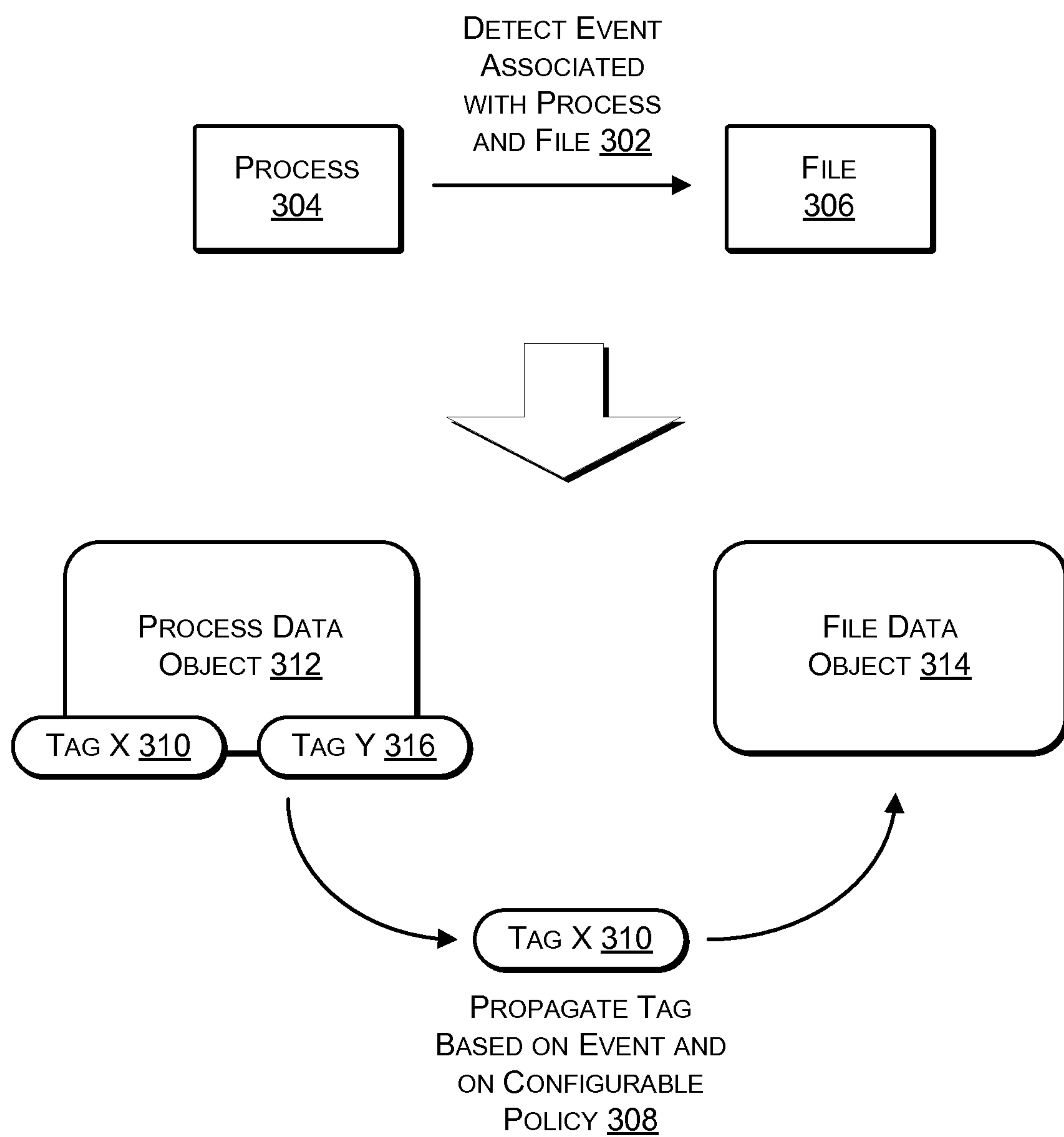
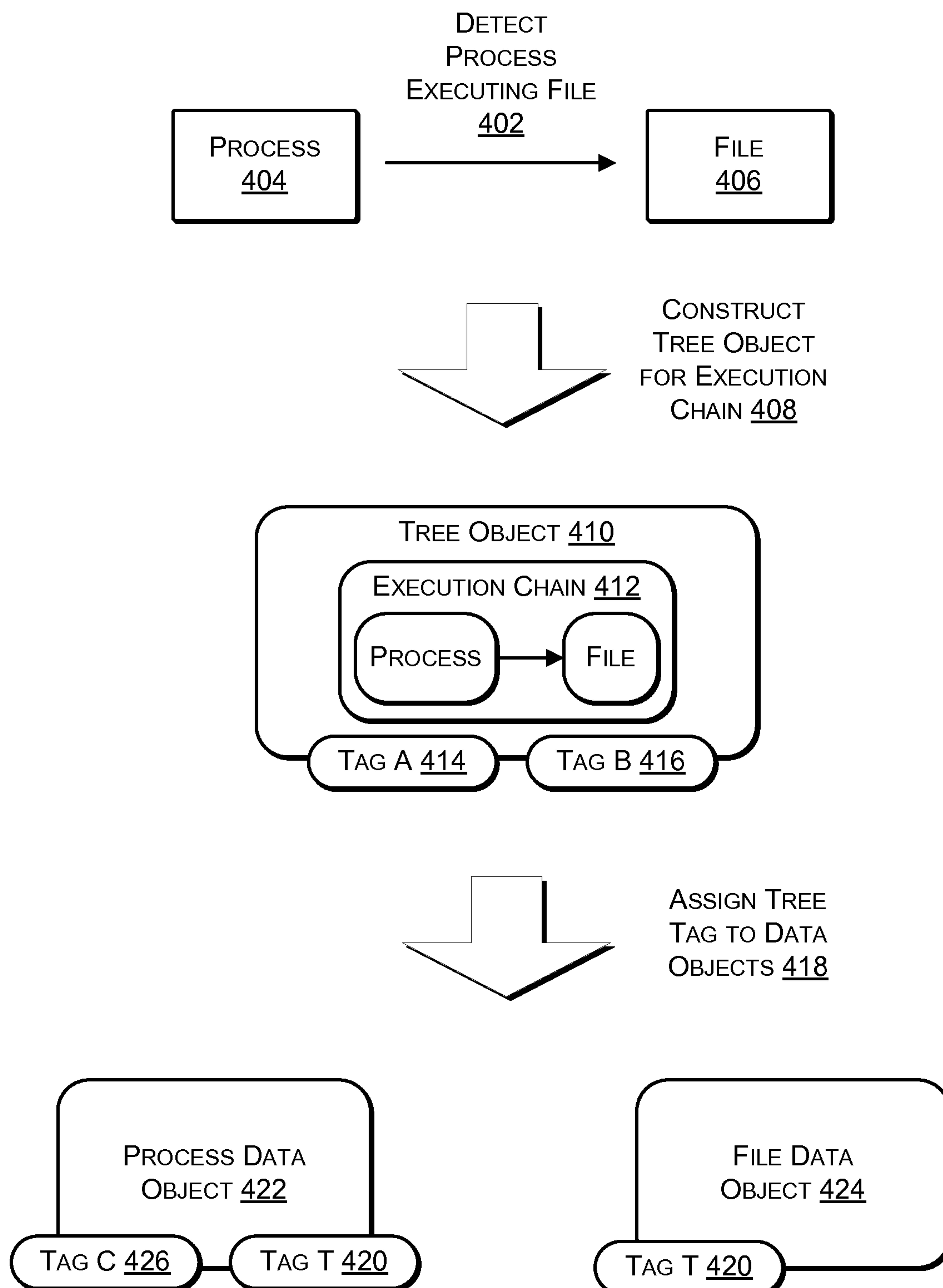
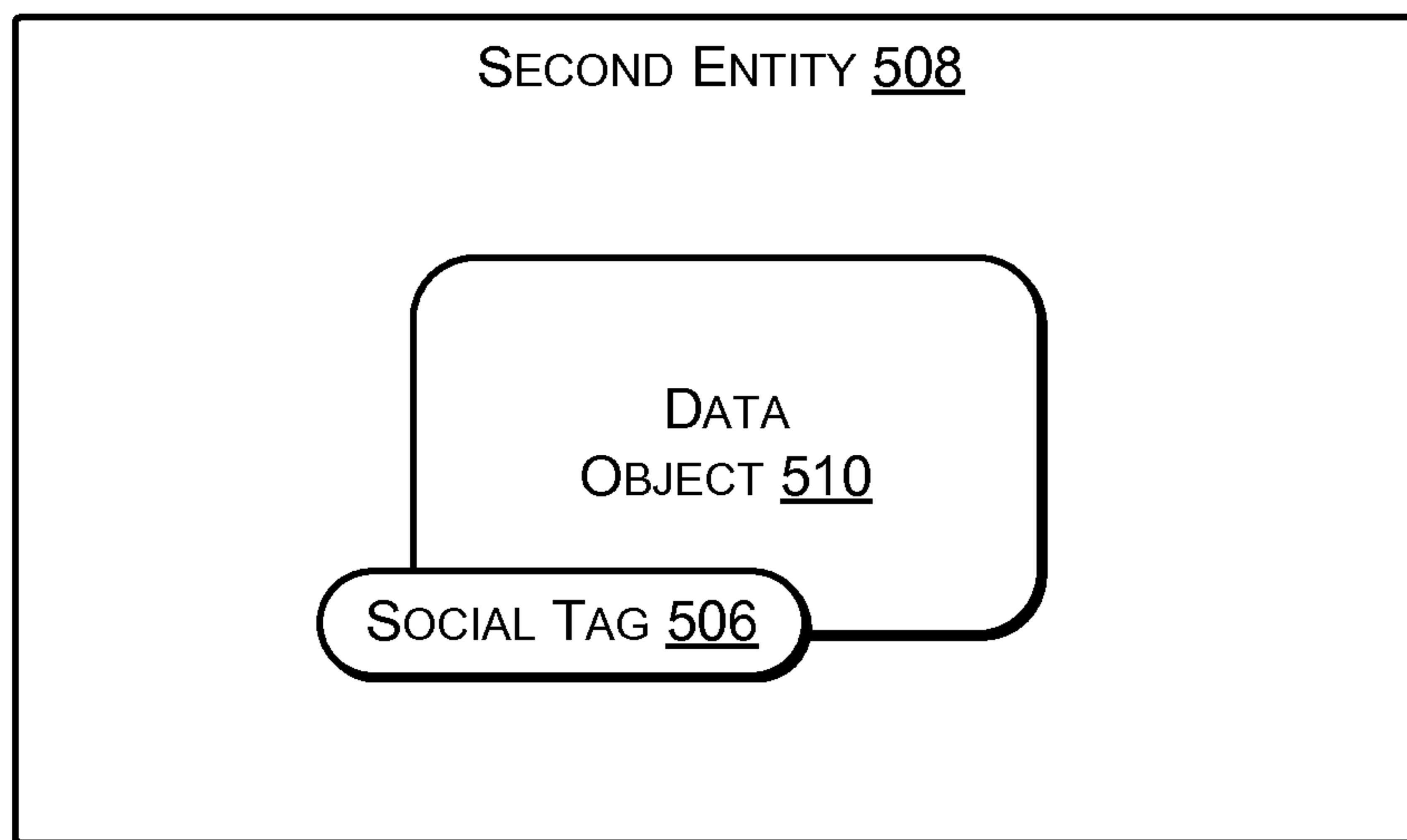
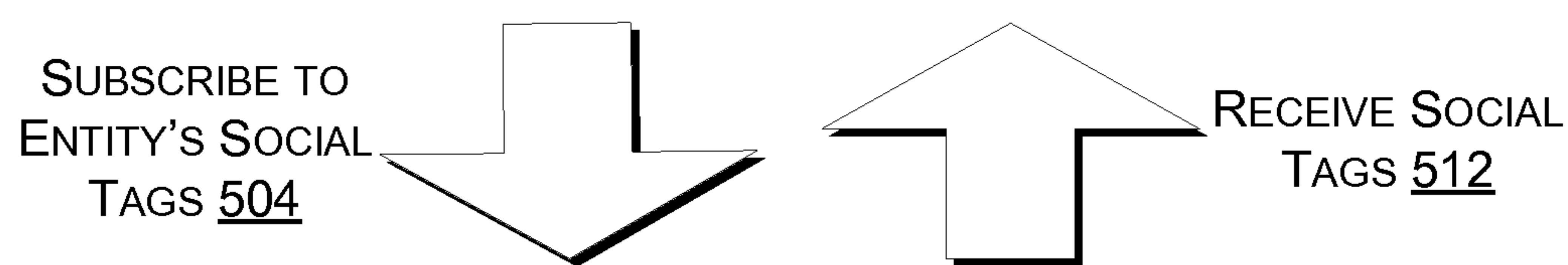
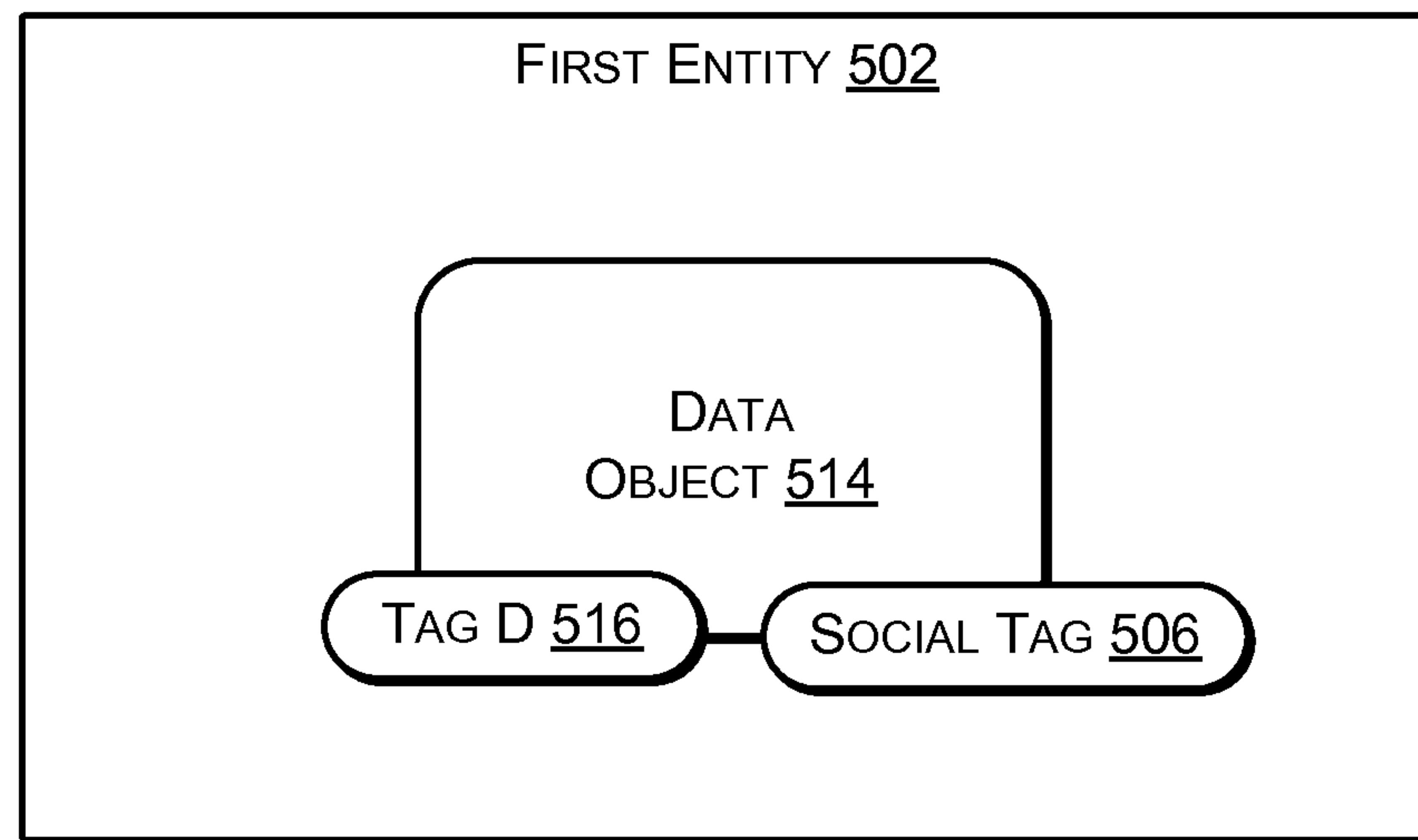


FIG. 3

4/6

**FIG. 4**

5/6

**FIG. 5**

6/6

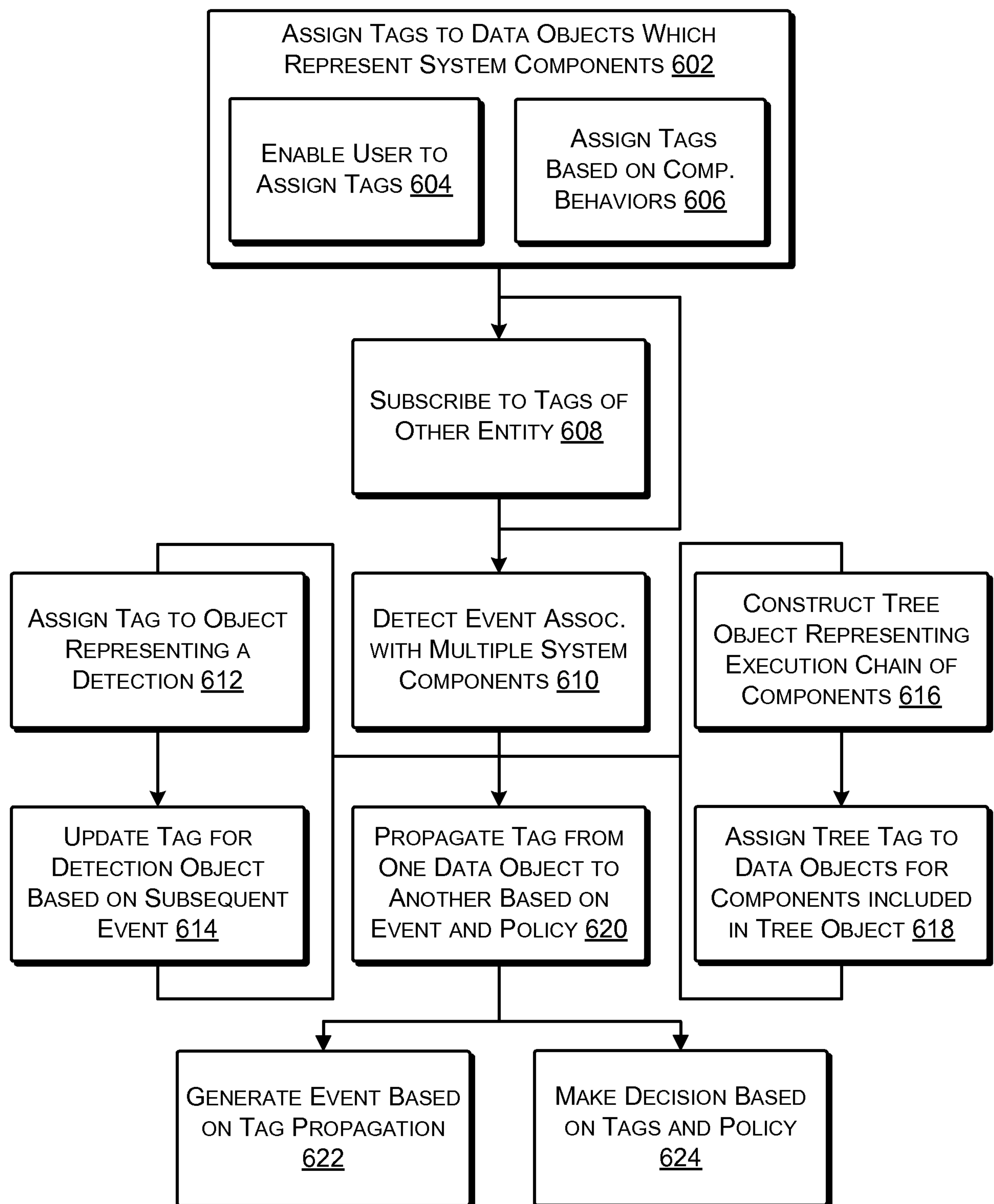


FIG. 6

# SECURITY SERVICE COMPUTING DEVICES 104

PROCESSOR(s) 110

COMM INTERFACE 114

I/O DEVICE(s) 118

## COMPUTER-READABLE MEDIA 122

SECURITY MODULES 156

CONFIGURATION MODULE 158

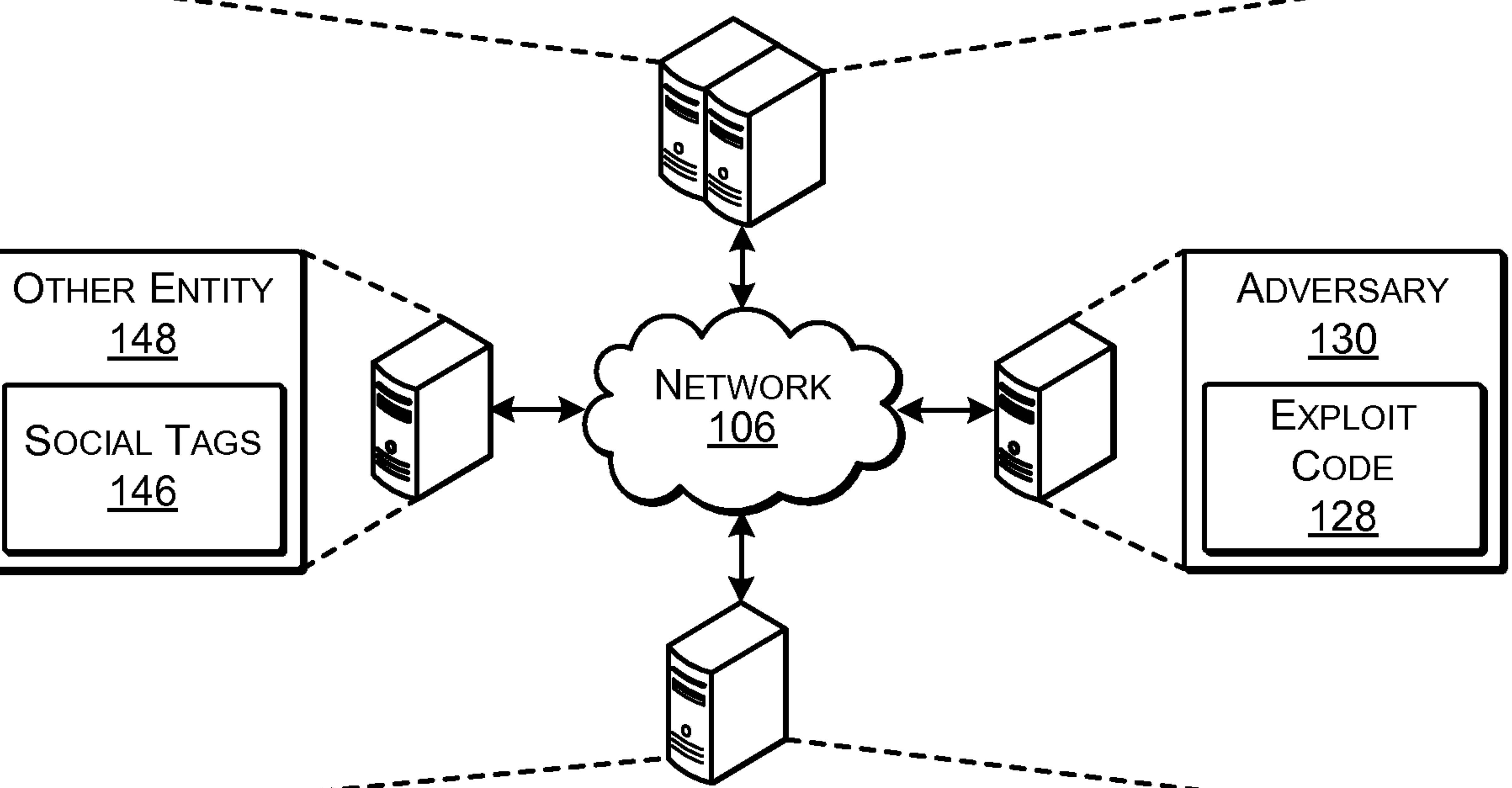
MONITORING MODULE 160

SOCIAL MODULE 162

DATA OBJECT STORE(s) 150

DATA OBJECTS 152

TAGS 154



## MONITORED DEVICE(s) 102

PROCESSOR(s) 108

COMM INTERFACE 112

I/O DEVICE(s) 116

## COMPUTER-READABLE MEDIA 120

SECURITY AGENT 124

SYSTEM COMPONENTS 126

## DATA OBJECT STORE(s) 132

DATA OBJECTS 134

TREE OBJECTS 136

## TAGS 138

TAXONOMIC TAGS 140

TREE TAGS 142

SOCIAL TAGS 144

**FIG. 1**