IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF DELAWARE

SRI INTERNATIONAL, INC.,

Plaintiff,

v.

DELL INC. and SECUREWORKS, INC.,

Defendants.

Civ. No. 13-737-SLR

SRI INTERNATIONAL, INC.,

Plaintiff,

v.

CISCO SYSTEMS, INC.,

Defendant.

Civ. No. 13-1534-SLR

MEMORANDUM ORDER

At Wilmington this 14th day of May, 2015, having heard argument on, and having reviewed the papers submitted in connection with, the parties' proposed claim construction;

IT IS ORDERED that the disputed claim language of U.S. Patent Nos. 6,711,615 ("the '615 patent") and 6,484,203 ("the '203 patent") shall be construed consistent with the tenets of claim construction set forth by the United States Court of Appeals for the Federal Circuit in *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005), as follows:

1. **"[I]nvoking countermeasures:"**[1, 2] "Taking an action in response including both passive and active responses." In the absence of arguments supporting an alternative construction, the court adopts its previous construction of this term. (*See* Civ. No. 04-1199; D.I. 468 at 5)

2. **"[N]etwork traffic data:"**[3, 4] "Data obtained from direct examination of network packets." This construction is informed by the specification and the patentee's statements during reexamination, wherein the patentee argued: "According to its plain meaning, the phrase 'network traffic data' refers to data obtained from network traffic, i.e., network packets. Thus, the method of claim 1 reciting 'detecting, by the network monitors, suspicious network activity based on analysis of network traffic data' requires direct examination of network packets." (D.I. 111 at JA2835, JA3226) The patentee noted that "each enumerated category [recited in claim 1] specifically requires that the associated data be obtained by direct examination of network packets." (*Id.*) The patentee identified instances where the specification equates "traffic" and "packets," citing column 5:14-15 of the '615 patent, which recites "discarded traffic (i.e., packets)."

[1] Claims 3 and 15 of the '615 patent and claims 3 and 14 of the '203 patent.

[2] Unless otherwise specified, the court relies solely on intrinsic evidence in reaching its claim construction. *See generally Teva Pharm. USA, Inc. v. Sandoz, Inc.,* 135 S. Ct. 831, 834 (2015).

[3] Claims 1 and 13 of the '615 patent and claims 1 and 12 of the '203 patent

[4] The court declines to separately construe the partially overlapping terms "based on analysis of network traffic data" and "detecting, by the network monitors, suspicious network activity based on analysis of network traffic data / detecting suspicious network activity based on analysis of network traffic data" to avoid redundancy in the court's analysis.

(*Id.*) The patentee also distinguished "network traffic data" from the terms "network traffic measures" and "network traffic statistics," which the specification uses "when discussing information **derived** from network traffic observation, as compared to the data from which the measures and statistics are derived." (*Id.*) (emphasis in original) The patentee's careful distinction between "network traffic data" and information derived from network traffic observation (such as statistical measures) is contrary to plaintiff's proposed construction of "data derived from or describing network packets." However, defendants' proposed construction of "network packets" is lacking precision where the patentee states that network traffic data refers to data **obtained from** network traffic and then equates "traffic" with "packets." (*Id.*)

3. Regarding "direction examination," plaintiff argues that during reexamination, the patentee merely disclaimed host-based monitoring, not all methods of indirect examination of network packets. Specifically, the patentee overcame prior art disclosing a host-based audit log by arguing that the prior art method "do[es] not monitor network packets, as required by the claims." (D.I. 111 at JA1934) The patentee later clarified that "the claim language requires the suspicious network activity to follow from analysis of the network packets, not logs or other information generated therefrom or otherwise gleaned." (*Id.* at JA3489) The patentee reiterated that "the claim term 'analysis of network traffic data' refers to analysis of network packets, not some proxy thereof." (*Id.* at JA3490) The disclaimer of claim scope, therefore, is broader than excluding host-based monitoring of audit logs, and explicitly extends to proxy information or "other information generated therefrom or otherwise gleaned." The court agrees with the patentee's own statement that "by reciting 'based on analysis of

network [packets],' the claim requires direct examination of those network packets to detect suspicious network activity." (*Id.* at JA3489) (modification in original)

4. **"[A]dapted to:"**[5] "Configured to." The Federal Circuit has held that "the phrase 'adapted to' is frequently used to mean 'made to,' 'designed to,' or 'configured to,' but it can also be used in a broader sense to mean 'capable of' or 'suitable for.'" *Aspex Eyewear, Inc. v. Marchon Eyewear, Inc.*, 672 F.3d 1335, 1348-49 (Fed. Cir. 2012). As in *Aspex*, the intrinsic evidence at bar supports a narrower interpretation of "adapted to" by describing how the hierarchical monitors "are designed or configured to accomplish the specified objective, not simply that they can be made to serve that purpose." *Id.* at 1349. For example, the specification states that the monitors 16d-f "correlate intrusion reports" ('615 patent, col. 4:8-11)[6] and a single monitor "subscribes to the analysis results produced by service monitors 16a-c, and then propagates its own analytical reports to its parent enterprise monitor 16f." (*Id.* at col. 10:8-11) Additionally, the claims recite "one or more hierarchical monitors in the enterprise network, the hierarchical monitors adapted to automatically receive and integrate the reports of suspicious activity." (*Id.* at col. 16:3-6)

5. The description of the hierarchical monitors in the intrinsic evidence suggests that monitors 16d-f are intended to actively propagate and correlate reports, not that they are merely capable of doing so. Indeed, the purpose of the invention – to "provide[] a framework for the recognition of more global threats" through an "analysis

[5] Claim 13 of the '615 patent and claim 12 of the '203 patent

[6] The '615 patent and the '203 patents share a specification, and all citations are to the '615 patent unless otherwise noted.

hierarchy" including various monitors – would be ill-served if the hierarchical monitors were not configured to perform their stated task. (*Id.* at col. 3:43-45) Moreover, the claims at issue do not use the word "for" followed by the future tense of a verb, a form of claiming that the Federal Circuit has found particularly suggestive of recitations of "capability, as opposed to actual operation." *Finjan, Inc. v. Secure Computing Corp.,* 626 F.3d 1197, 1204-05 (Fed. Cir. 2011) (claims reciting "a logical engine for preventing execution" and "a communications engine for obtaining a Downloadable); *see also Ericsson, Inc. v. D-Link Sys., Inc.*, 773 F.3d 1201, 1217 (Fed. Cir. 2014) (claim reciting "a processor for arranging information for transmission").

6. **"[W]ithin an enterprise network / in the enterprise network:"**[7] "Part of an enterprise network." The preamble is limiting. The Federal Circuit has held that if "limitations in the body of the claim rely upon and derive antecedent basis from the preamble, then the preamble may act as a necessary component of the claimed invention." *Proveris Scientific Corp. v. Innovasystems, Inc.*, 739 F.3d 1367, 1372 (Fed. Cir. 2014). Here, the term "enterprise network" derives antecedent basis from the preamble in that "**an** enterprise network" appears in the preamble and is followed by a recitation of "deploying a plurality of network monitors in **the** enterprise network" in the body of the claim. ('615 patent, col. 15:5-6) (emphasis added) Plaintiff argues that by indicating that the network monitors are in the enterprise network yet failing to indicate the location of hierarchical monitors, the drafter intentionally untethered the hierarchical monitors from the enterprise network. (*See id.* at claim 1) However, the court discerns no such intention as hierarchical monitors are a type of network monitor (D.I. 71 at 2),

[7] Claims 1 and 13 of the '615 patent and claims 1 and 12 of the '203 patent

and it would be unnecessary for the drafter to additionally specify the location of the hierarchical monitors after stating that the network monitors are within the enterprise network.

7. **"[S]uspicious network activity:"**[8] "Activity that indicates an unknown, but suspected, intrusion." Plaintiff proposes that suspicious activity is an umbrella term that encompasses malicious activity, while defendants argue that suspicious and malicious activity are distinct categories. The specification describes how the signature engine 24 "maps an event stream against abstract representation of event sequences that are known to indicate undesirable activity." ('615 patent, col. 7:33-35) Next, "[t]he signature engine scans the event stream for events that represent attempted exploitations of **known attacks** against the service, or other activity that stands alone as warranting a response from the monitor." (*Id.* at col. 7:40-43) (emphasis added) Examples of known attacks include "address spoofing, tunneling, source routing, SATAN attacks, and abuse of ICMP messages ('Redirect' and 'Destination Unreachable' messages in particular)." (*Id.* at col. 7:51-55) In addition to detecting known attacks, the "signature engine 24 can also examine the data portion of packets in search of a variety of transactions that indicate **suspicious, if not malicious**, intentions by an external client." (*Id.* at col. 7:64-66) (emphasis added) The specification describes how "analysis engines 22, 24 receive large volumes of events and produce smaller volumes of intrusion or suspicion reports." (*Id.* at col. 8:23-25) The court agrees with defendants that the specification draws a distinction between suspicious and malicious activity, a distinction that is consistent with the specification and the plain and ordinary meaning of the words.

[8] Claims 1 and 13 of the '615 patent and claims 1 and 12 of the '203 patent

However, defendants' proposed addition of "unconfirmed" is likely to introduce unnecessary ambiguity in that the patent uses the word "known" rather than "confirmed" to characterize malicious attacks. (*See id.* at col. 7:34-36; 7:40-43)

8. **"[S]elected from the following categories: {. . .}:"**[9] "Chosen from at least one of the specified categories: {. . .}." The parties dispute whether the term should be characterized as a Markush group. The Federal Circuit has held that "[a] Markush group is a listing of specified alternatives of a group in a patent claim, typically expressed in the form: a member selected from the group consisting of A, B and C." *Abbott Labs. V. Baxter Pharm. Prods., Inc.*, 334 F.3d 1274, 1280 (Fed. Cir. 2003); *see also Gillette Co. v. Energizer Holdings, Inc.*, 405 F.3d 1367, 1372 (Fed. Cir. 2005) ("If an applicant tries to claim a Markush group without the word 'consisting,' the PTO will insist upon the addition of this word to ensure a closed meaning."). The MPEP defines a Markush group as "any claim that recites a list of alternatively useable species regardless of format." MPEP § 2173.05(h). For example, the MPEP states that "[a]lternative expressions using 'or' are acceptable, such as 'wherein R is A, B, C, or D." *Id.*

9. Claims 1 and 12 of the '203 patent do not use the language "consisting of" and do not recite the enumerated categories in the alternative, thereby failing to satisfy either of the most fundamental hallmarks of Markush claiming. Defendants argue that plaintiff should be held to its repeated representation in previous litigation (D.I. 127, ex. 4 at 5, ex. 5 at 3-4, ex. 6 at ¶ 26, ex. 7 at 90:10-23; D.I. 143 ex. 17 at 1, ex. 18 at 3, ex. 19 at 7, ex. 23 at ¶ 33) and reexamination (D.I. 111 at JA2614) that the claims involve a

[9] Claims 1 and 12 of the '203 patent

Markush group. However, it is the court's opinion that these representations were ill-founded, and that merely stating (albeit repeatedly) that a phrase is a Markush group does not make it so.

10. **"[E]nterprise network:"**[10] "A network having a plurality of network monitors used in connection with a project or undertaking, for example, a large, privately owned wide area network." The specification states that "enterprise 10 surveillance **may be used** where domains 12a-12c are interconnected under the control of a single organization, such as a large privately owned WAN (Wide Area Network)." ('615 patent, col. 4:27-31) (emphasis added) The specification also states that "enterprise 10, however, need not be ...centrally administered." (*Id.* at col. 4:33-34) Under the most straightforward reading of this disclosure, the conditional language "may be used" demonstrates the patentee's unwillingness to make control by a single organization a necessary feature of the invention. The additional disclosure that an enterprise need not be centrally administered does not add clarity, as the parties' experts' dispute whether a person of ordinary skill in the art would expect an enterprise lacking central administration to be under the control of a single organization. (D.I. 110, ex. 3 at ¶¶ 6-11; D.I. 128 at ¶ 19) The court discerns no other disclosure in the specification or claims that compels a different conclusion.

Sue L Robinson

United States District Judge

[10] Claims 1, 6, 13 and 18 of the '615 patent and claims 1, 6, 12 and 17 of the '203 patent