NOTE: This disposition is nonprecedential.

United States Court of Appeals for the Federal Circuit

_____

CENTRIPETAL NETWORKS, LLC,
Appellant

v.

PALO ALTO NETWORKS, INC.,
Appellee

_____

2023-1785

_____

Appeal from the United States Patent and Trademark Office, Patent Trial and Appeal Board in No. IPR2021-01149.

_____

Decided: October 31, 2024

_____

JAMES R. HANNAH, Kramer Levin Naftalis & Frankel LLP, Redwood Shores, CA, argued for appellant. Also represented by PAUL J. ANDRE; JEFFREY PRICE, New York, NY; JOHN R. HUTCHINS, SCOTT M. KELLY, BRADLEY CHARLES WRIGHT, Banner & Witcoff, Ltd., Washington, DC.

ANDREW T. RADSCH, Ropes & Gray LLP, East Palo Alto, CA, argued for appellee. Also represented by JAMES RICHARD BATCHELDER; ALLEN S. CROSS, DOUGLAS HALLWARD-DRIEMEIER, Washington, DC.

2   CENTRIPETAL NETWORKS, LLC v. PALO ALTO NETWORKS, INC.

———————————

Before LOURIE, TARANTO, and STARK, *Circuit Judges.*

TARANTO, *Circuit Judge.*

Centripetal Networks, LLC owns U.S. Patent No. 10,567,413, titled "Rule-Based Network-Threat Detection." Palo Alto Networks, Inc. (PAN) petitioned the Patent and Trademark Office (PTO) to institute an inter partes review of all the claims of the '413 patent, alleging that the claims were unpatentable for obviousness under 35 U.S.C. § 103. The PTO's Patent Trial and Appeal Board, acting for the PTO's Director, instituted the requested review, and after conducting the review, the Board concluded that all the challenged claims were unpatentable under § 103. J.A. 1–57; *see Palo Alto Networks, Inc. v. Centripetal Networks, Inc.*, No. IPR2021-01149, 2023 WL 2592367 (P.T.A.B. Feb. 17, 2023) (*'413 Decision*).

Centripetal timely appealed. We have jurisdiction under 28 U.S.C. § 1295(a)(4)(A). We affirm.

I

A

Centripetal's claimed invention involves the detection and prevention of "network threats" and the generation of a data "log" with information about such threats. '413 patent, col. 1, lines 16–27, 51–65. The patent discloses a "packet-filtering device" that receives data packets and determines whether each packet matches the criteria specified by one of one or more "packet-filtering rules." *Id.*, col. 1, lines 47–53. The criteria correspond to "network-threat indicators" or "threat identifiers," *id.*, col. 1, lines 53–55; *id.*, col. 3, lines 25–29; *id.*, col. 17, line 44, "e.g., network addresses, ports, fully qualified domain names (FQDNs), uniform resource locators (URLs), uniform resource identifiers (URIs), or the like." *Id.*, col. 3, lines 25–28. If a packet satisfies a packet-filtering rule, the

device may allow or prevent the packet's continued progress to its destination, create a data log entry with information about the threat that was identified and the rule that was triggered, generate a listing of some or all the "threat identifiers" that were logged, and allow the user to update the packet-filtering rule(s). *Id.*, col. 1, line 55, through col. 2, line 12; *id.*, col. 18, lines 4–8.

Claim 1 is representative for purposes of this appeal:

1. A method comprising:

receiving, by a packet-filtering device ***located at a boundary between a protected network and an unprotected network***, a plurality of threat identifiers from a plurality of network-threat-intelligence providers;

receiving, by the packet-filtering device, a plurality of packets;

responsive to a determination by the packet-filtering device that a first packet of the plurality of packets corresponds to a first packet matching criterion specified by a first packet-filtering rule of a plurality of packet-filtering rules:

> applying, by the packet-filtering device and to the first packet, a first operator specified by the first packet-filtering rule corresponding to the first packet matching criterion;

> generating, by the packet-filtering device and for the first packet, a packet log entry comprising at least one threat identifier, of the plurality of threat identifiers, corresponding to the first packet;

> determining a number of network-threat-intelligence providers, of the plurality of network-threat-intelligence providers,

> from which the at least one threat identifier corresponding to the first packet was received; and
>
> determining, by the packet-filtering device, *at least one score* associated with the at least one threat identifier by determining at least a first score based on the determined number of network-threat-intelligence providers;

generating a listing of at least a portion of the plurality of threat identifiers, comprising the at least one threat identifier, wherein a position of the at least one threat identifier in the listing is based on the determined first score; and

reconfiguring at least one packet-filtering rule based on at least the generated listing,

wherein each of the plurality of packet-filtering rules specifies at least one packet matching criterion and at least one operator.

Id., col. 17, line 41, through col. 18, line 13 (emphases added).

The two claim limitations highlighted above are at issue here. First, the packet-filtering device must be "located at a boundary between a protected network and an unprotected network." *Id.*, col. 17, lines 42–44; *see also id.*, col. 19, lines 14–15; *id.*, col. 20, lines 37–38. Second, the packet-filtering device, to generate the listing of logged threat identifiers, must determine "at least one score associated with the at least one threat identifier" and to order each threat identifier within the listing based on that score. *Id.*, col. 17, line 66, through col. 18, line 8; *see also id.*, col. 19, lines 40–48; *id.*, col. 20, lines 59–67. Dependent claims 6–8, 15, and 20 disclose additional ways of determining or updating "the at least one score." *Id.*, col.

18, line 57, through col. 19, line 7; *id.*, col. 20, lines 28–34; *id.*, col. 22, lines 20–26.

B

In March 2021, Centripetal sued PAN in the district court, alleging infringement of the '413 patent, along with other patents not at issue in this appeal. In July 2021, PAN petitioned for institution of an inter partes review of all the claims (1–20) of the '413 patent. The Board instituted the inter partes review in February 2022 and issued a final written decision on February 17, 2023, determining that all claims were unpatentable under § 103.

In its decision, the Board stated that it would "apply the plain and ordinary meaning of the claims," as "[n]either party has disputed [the Board's] determination in the Decision to Institute that no express construction of any term is required." *'413 Decision*, at *3. The Board then determined that claims 1–20 of the '413 patent would have been obvious to a relevant artisan over a combination of two prior-art references: the Sourcefire 3D System User Guide (Sourcefire User Guide) and U.S. Patent Application Publication No. 2015/0207809 (Macaulay).[1] *Id.* at *2, *24. In making its findings, the Board considered a second document pertaining to the Sourcefire system—the Sourcefire 3D Sensor Installation Guide (Sourcefire Installation Guide)—that Centripetal had introduced in its Patent Owner's Response. *Id.* at *13 (Board decision); J.A. 462–63 (Patent Owner's Response) (citing J.A. 9243–49).

The Sourcefire User Guide is a manual for a network security system that allows a user to monitor network traffic and to analyze and respond to network threats by using a "3D Sensor" device equipped with various

---

[1]   The Board concluded that three dependent claims were also unpatentable based on a combination of those two references and a third reference not at issue on appeal.

components. J.A. 1323–26. A Sourcefire 3D Sensor uses "intrusion rules" to analyze network traffic, J.A. 1325, 1545, and to log "intrusion events" when a rule is triggered, *i.e.*, when there is a possible malicious intrusion into the user's network. J.A. 1567. The criteria for the intrusion rules correspond to information about the packet's source and destination (*e.g.*, IP addresses or ports) and may also correspond to information about the packet's contents. J.A. 2053. The Sourcefire Vulnerability Research Team provides a set of default intrusion rules, but the user can choose which rules to enable and "create custom intrusion rules tuned to [the user's] environment." J.A. 1325; *see also* 1653. Each rule is given a default "priority" level, J.A. 2063, but the user can customize the priority level (to reflect, *e.g.*, the needs of the user's organization). *See* J.A. 1600–01, 1613, 2062–63, 2831.

Macaulay, a published patent application, identifies the challenge of "[p]ersistently changing and evolving [network] threats and threat agents," calling for "a real-time system for information and intelligence sharing" about "threat agents and threatened assets on the Internet." J.A. 3461 ¶¶ 3, 6. Macaulay discloses a method of "refining cyber threat intelligence data" by sending a threat list to two "cyber threat intelligence sources" (*e.g.*, a telecommunications company or a security-product vendor such as McAfee), receiving threat data back from the two sources, updating the threat list based on such data, and then repeating the above steps with the updated threat list. J.A. 3461 ¶ 7, 3462 ¶ 20, 3467 ¶ 69. A threat may be assigned "reputation score[s]" for various attributes, *e.g.*, one score for its IP address and another for its domain. J.A. 3467 ¶¶ 69–71; *see also* J.A. 3458, fig. 3. Such a reputation score reflects the extent to which traffic having a particular attribute is considered "compromised," J.A. 3467 ¶¶ 70–71—a determination that can be based on multiple factors, including "the number of cyber threat intelligence sources

that have revealed the particular instance of the particular traffic attribute as a potential threat." J.A. 3468 ¶¶ 76–77.

The Board found that the Sourcefire User and Installation Guides teach a packet-filtering device that is "located at the boundary between the protected and unprotected network." *'413 Decision*, at *13; *see also id.* at *12–13. The Board then found that the other limitations were taught by a combination of the Sourcefire User Guide and Macaulay. *Id.* at *12–24. The Board noted the parties' agreement that the Sourcefire User Guide does not explain what factors are used to set priority levels, *id.* at *7, *10, and found that a relevant artisan would have been motivated to combine the Sourcefire User Guide's network protection system with Macaulay's reputation scores "to more accurately identify and categorize potential threats." *Id.* at *11; *see also id.* at *7–11.

II

We decide the correctness of the Board's legal determinations *de novo*, and we review the Board's factual findings for substantial-evidence support. *See*, *e.g.*, *Nobel Biocare Services AG v. Instradent USA, Inc.*, 903 F.3d 1365, 1374 (Fed. Cir. 2018) (citation omitted). "A finding is supported by substantial evidence if a reasonable mind might accept the evidence to support the finding." *Id.* (citing *Consolidated Edison Co. v. National Labor Relations Board*, 305 U.S. 197, 229 (1938)). We review "the Board's ultimate claim constructions and any supporting determinations based on intrinsic evidence" without deference, whereas "[w]e review any subsidiary factual findings involving extrinsic evidence for substantial evidence." *Personalized Media Communications, LLC v. Apple Inc.*, 952 F.3d 1336, 1339 (Fed. Cir. 2020). We review the Board's ultimate determination of obviousness without deference, and we review the underlying factual determinations for substantial evidence. *Personal Web*

Technologies, LLC v. Apple, Inc., 848 F.3d 987, 991 (Fed. Cir. 2017).

On appeal, Centripetal makes three sets of arguments. First, Centripetal challenges the Board's interpretation of, and findings about, the "boundary" limitation. Second, Centripetal argues that PAN did not sufficiently articulate its obviousness challenge to dependent claims 6–8, 15, and 20. Third, Centripetal challenges the Board's finding that there was a motivation for, and no teaching away from, combining the Sourcefire User Guide and Macaulay to use a "score" required by the claim limitation at issue. We examine each set of arguments in turn.

A

1

Regarding the "boundary" limitation, Centripetal argues that the Board prejudicially changed the claim construction—departing from the "well-understood plain and ordinary meaning," Centripetal Opening Br. at 39; *id.* at 40–41, in such a way as to deny it fair notice and an opportunity to address how the adopted construction read on the prior art at issue, in violation of recognized procedural rights. *See Axonics, Inc. v. Medtronic, Inc.*, 75 F.4th 1374, 1383 (Fed. Cir. 2023); *M & K Holdings, Inc. v. Samsung Electronics Co.*, 985 F.3d 1376, 1385–86 (Fed. Cir. 2021). We disagree.

In the Board discussion relied on by Centripetal, *'413 Decision*, at *13, the Board did not purport to depart from any ordinary meaning. Rather, in that discussion, the Board explained why features of Sourcefire User Guide's disclosures *sufficed* to meet the boundary limitation. *See id.* (determining that "the disclosure in Sourcefire that '[p]lacement [of the 3D Sensor] outside the firewall gives you a clear picture of all the traffic traversing your network via this gateway' indicates that the 3D Sensor is located at the boundary between the unprotected and protected

network, as recited in this claim limitation." (alteration in original) (citation omitted) (quoting J.A. 9243)). And that discussion is not on its face a departure from an otherwise-clear "ordinary" understanding, but an application of what is within the concept of a boundary between the protected and unprotected networks.

For Centripetal to argue otherwise, it does and must insist that the "boundary" claimed must be "where an internal network device *first* interfaces with an unprotected network like the Internet," so that the packet-filtering device must be the *first* device on the user's network to contact the unprotected network. Centripetal Opening Br. at 4 (emphasis added); *id.* at 34 (similar). We reject that contention. We generally give the words of a patent claim their ordinary and customary meaning as understood by a relevant artisan at the time of the invention and in the context of all the intrinsic evidence. *Phillips v. AWH Corp.*, 415 F.3d 1303, 1313–14 (Fed. Cir. 2005) (en banc). The specification of the '413 patent makes it clear that the packet-filtering device does not have to be the first device on the user's network to contact the unprotected network: Figure 2A of the patent shows a packet-filtering device interfacing with two "Tap" devices and "Network Device(s)," which *then* interface with the unprotected network (labeled Network D) across the "boundary" (shown by a dashed line). '413 patent, fig. 2A; *id.*, col. 3, line 47, through col. 4, line 7 (describing Figure 2A); *id.*, col. 2, line 66, through col. 3, line 9 (labeling the different networks). Centripetal attempts to differentiate a tap from other devices (*e.g.*, a router). But even a tap undermines Centripetal's bright-line interpretation of "boundary." In addition, the specification indicates that the two taps in Figure 2A are optional, *id.*, col. 3, lines 52–53, thus contemplating a configuration in which the packet-filtering device connects with an unprotected network solely through "Network Device(s)," which include

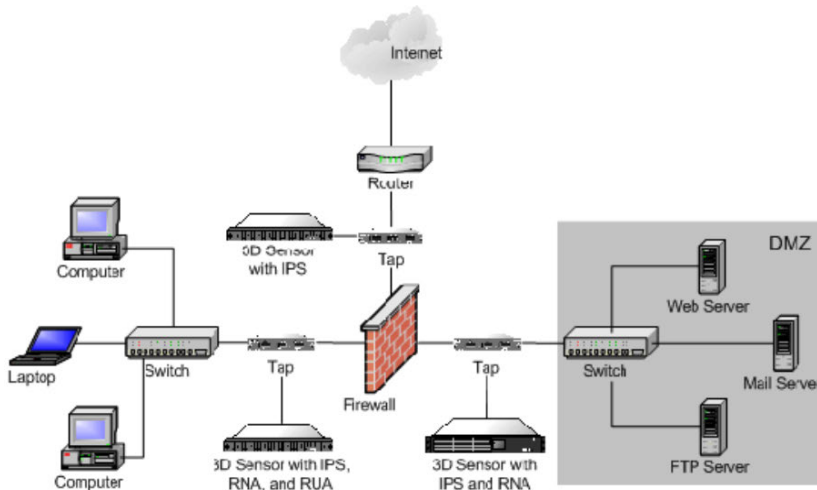10   CENTRIPETAL NETWORKS, LLC v. PALO ALTO NETWORKS, INC.

"e.g., servers, routers, gateways, switches, access points, or the like." *Id.*, col. 3, lines 49–52.

We therefore see no reversible error regarding claim construction, even apart from the Board's finding (noted *infra*) of satisfaction of the claim limitation at issue under Centripetal's construction.

2

The Board's findings that Sourcefire taught the "boundary" limitation are supported by substantial evidence, and those findings make it clear that Sourcefire teaches the "boundary" limitation—under both the Board's construction and even under Centripetal's proposed alternative.

Under the Board's understanding of the "boundary" limitation, the Board found that Sourcefire discloses this limitation based on the Sourcefire Installation Guide, *'413 Decision*, at *13, which Centripetal had cited in its Patent Owner's Response, J.A. 462–63 (citing J.A. 9243–49). *See Rovalma, S.A. v. Bohler-Edelstahl GmbH & Co. KG*, 856 F.3d 1019, 1026–28 (Fed. Cir. 2017) (concluding that the Board properly relied on a patent owner's own submissions in determining unpatentability where the patent owner

had adequate notice and an adequate opportunity to be heard). In the Sourcefire Installation Guide, the Board relied on the following diagram depicting three potential placements of the Sourcefire 3D Sensor (*i.e.*, the claimed "packet-filtering device"):

'413 Decision, at *13; J.A. 9243. The Board, quoting from the Installation Guide, found that this diagram taught the placement of a Sourcefire 3D Sensor "outside the firewall" where it has "a clear picture of all the traffic traversing [the] network via this gateway." *'413 Decision*, at *13 (quoting J.A. 9243).

The Board's finding that Sourcefire discloses the "boundary" limitation is supported by substantial evidence. The page on which the diagram appears in the Sourcefire Installation Guide states that there are "three areas with three different security policies": (1) "between the border router and the firewall," (2) "in the demilitarized zone, or DMZ," and (3) "in the internal, protected network." J.A. 9243. The installation guide notes that "[d]eploying your 3D Sensors in each of these locations serves different purposes"; the installation guide then lists three purposes, seemingly in the same order as it lists the three areas. J.A. 9243. In particular, the installation guide states the following purpose of placing the 3D Sensor in the first area: "Placement outside the firewall gives you a clear picture of all the traffic traversing your network via this gateway." J.A. 9243. The combination of the diagram and the relevant description adequately supports the Board's finding.

Under Centripetal's proposed construction of the "boundary" limitation—as meaning "[at] the boundary where an internal network device *first* interfaces with an unprotected network like the Internet," Centripetal Opening Br. at 4 (emphasis added); *see also id.* at 34 (similar)—the Board also should be understood to have

found that Sourcefire taught this element. In the Petition, PAN included the following annotated figure:
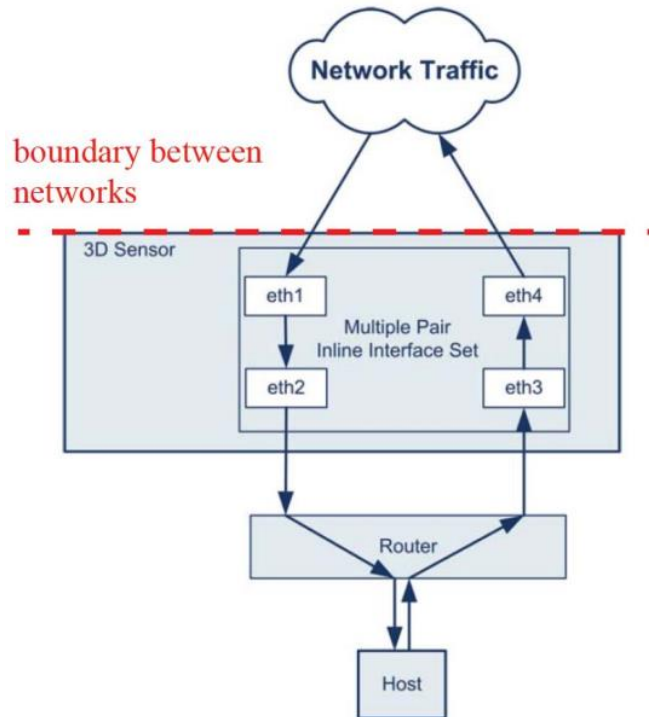
J.A. 156; *see also* J.A. 1188 (showing the same annotated figure in the declaration of PAN's expert, Dr. Lee). In the Patent Owner's Response, Centripetal argued that PAN had misread the figure and that the cloud at the top represents the protected network while the "host" rectangle at the bottom represents the unprotected network.   J.A. 424, 460–61.   The Board summarized Centripetal's arguments and—in the immediately following sentence—rejected them as "unavailing," thus finding that PAN had correctly interpreted this figure. *'413 Decision*, at *12.

The page of Sourcefire where this figure originally appears provides substantial-evidence support for the Board's finding. The figure contains the following caption:

> Your network may be set up to route traffic between *a host* on your network and external *hosts* through different interface pairs depending on whether the traffic is inbound or outbound.

J.A. 1526 (emphases added). In other words, the prior-art reference appears to use the singular ("a host") when it refers to part of the user's network and the plural ("hosts") when it refers to part of the external network. The Board reasonably agreed with PAN's interpretation of the cloud as the unprotected network, the labeled "host" as the protected network, and (accordingly) the 3D Sensor as a device at the boundary where a protected network device *first* interfaces with an unprotected network.

On appeal, Centripetal argues that PAN failed to rebut the evidence supporting the interpretation of the Sourcefire User Guide offered by Centripetal's expert, Dr. Orso. Centripetal Opening Br. at 18 (citing J.A. 9166–69 ¶¶ 80–81). In the pertinent portions of Dr. Orso's declaration, however, Dr. Orso cites to different sections of the Sourcefire User Guide and the Sourcefire Installation Guide, none of which describe the figure in question. J.A. 9166–69 ¶¶ 80–81. And Centripetal does not identify any other evidence the Board failed to consider or weigh.

We cannot say that the Board erred in rejecting Centripetal's arguments. *See Quanergy Systems, Inc. v. Velodyne Lidar USA, Inc.*, 24 F.4th 1406, 1417 (Fed. Cir. 2022) ("Under our standard of review, we sustain a finding of the Board that may reasonably be drawn from the evidence in record, even if the Board reasonably could have drawn other inconsistent findings from the same record."); *see also Elbit Systems of America, LLC v. Thales Visionix, Inc.*, 881 F.3d 1354, 1356 (Fed. Cir. 2018). We conclude that the Board's findings that Sourcefire taught the "boundary" limitation—under both the Board's interpretation and Centripetal's—are supported by substantial evidence.

B

Centripetal argues that the Board erred in its obviousness determination regarding claims 6–8, 15, and 20 by relying on an analysis insufficiently set out in PAN's Petition. Centripetal argues that PAN's Petition relied crucially on Macaulay (as opposed to a combination of Macaulay and the Sourcefire User Guide) for PAN's challenge to the patentability of those claims. For each of those claims, the Petition discusses how Macaulay discloses the unique limitations of these dependent claims and includes a signal, "*see* [1.g]." J.A. 186–90. Earlier, the Petition uses "[1.g]" as a label for a related limitation that exists in each of the *independent* claims. J.A. 167. According to Centripetal, the Petition's uses of "*see* [1.g]" to refer to "a discussion of an entirely different claim limitation" are insufficient to cross-reference the obviousness arguments set forth for the independent claims. Centripetal Opening Br. at 57–58; *see also id.* at 59; J.A. 186–90 (Petition).

We conclude that Centripetal's arguments lack merit, whether we consider the adequacy of the Petition de novo or with deference to the Board's decision. Claims 6–8, 15, and 20 are dependent claims. *See* '413 patent, col. 18, line 57, through col. 19, line 7; *id.*, col. 20, lines 28–34; *id.*, col. 22, lines 20–26. PAN's Petition sufficiently indicates that PAN was cross-referencing any relevant arguments (based on both Sourcefire *and* Macaulay) that it had made for the obviousness of the independent claims. First, the header of PAN's claim chart for claims 6–8, 15, and 20 is "Sourcefire in View of Macaulay." J.A. 186–90. Second, the Petition states that "Ground 1" of unpatentability is that "Claims 1–20 Are Rendered Obvious Over Sourcefire in View of Macaulay." J.A. 142. Third, the "*see* [1.g]" signals regarding the dependent claims refer back to discussion of a [1.g] limitation—"[determining/determine] at least one score associated with the at least one threat identifier," J.A. 167—that is obviously tied to what the dependent claims

focus on: ways to determine or update "*the* at least one score." '413 patent, col. 18, line 57, through col. 19, line 7; *id.*, col. 20, lines 28–34; *id.*, col. 22, lines 20–26 (emphasis added). We conclude that PAN sufficiently stated its arguments for the obviousness of claims 6–8, 15, and 20 in view of the combination of Sourcefire and Macaulay.

C

Centripetal challenges the Board's finding of a relevant artisan's motivation to combine the Sourcefire User Guide and Macaulay to arrive at the subject matter of the score-determination limitation. We reject this challenge.

Substantial evidence supports the Board's finding that a relevant artisan would have been motivated to make the combination at issue. The Board reviewed in a detailed manner the evidence and arguments presented by both parties, summarizing the materials presented to it and citing to the testimony of Centripetal's expert (Dr. Orso) and PAN's expert (Dr. Lee). *'413 Decision*, at *7–11. On each point, we see ample support in the cited evidence for the Board's findings: Sourcefire taught the setting of organization-specific rules and priorities, *id.* at *11, but (as the parties agreed, *id.* at *7) "Sourcefire does not teach *how* to set threat priorities," *id.* at *10 (emphasis added), and a relevant artisan starting with Sourcefire would have had reason to consider "industry consensus of concerning traffic characteristics of potential threats" "in the form of Macaulay's reputation scores" in setting threat priorities for a particular network, "especially given [that] Sourcefire's [Vulnerability Research Team] . . . assigns [default] event priorities that are not network specific." *Id.* at *11; *see also* J.A. 2063 (discussing default priority levels). The evidence on these points and their logical connection support the Board's motivation finding.

Centripetal argues that the finding must be set aside because it relies on the rejection of evidence that prior art taught away from the combination and that rejection relies

on a misstatement of the legal standard for teaching away. We agree with Centripetal only to this extent: One sentence in the Board's opinion mistakenly transforms a sentence in *Syntex (U.S.A.) LLC v. Apotex, Inc.* that states a *sufficient* condition for teaching away, 407 F.3d 1371, 1380 (Fed. Cir. 2005) ("[A] reference will teach away when it suggests that the developments flowing from its disclosures are unlikely to produce the objective of the applicant's invention."), into a *necessary* condition, *'413 Decision*, at *9 ("[I]t is *not* a 'teaching away' *unless* one with ordinary skill in the art would have understood that teaching as conveying that the method or structural configuration at issue reasonably cannot be expected to achieve what it is required to achieve according to the claimed invention.") (emphases added). We disagree, however, with Centripetal's contention that this misstatement warrants setting aside the Board's decision: In context, it is harmless error. *See Elbit Systems*, 881 F.3d at 1359 ("[W]e will not find legal error based upon an isolated statement stripped from its context."); *Bot M8 LLC v. Sony Interactive Entertainment LLC*, 66 F.4th 1380, 1385 (Fed. Cir. 2023) (noting applicability of harmless-error analysis).

First, the Board applied the correct legal rule when it found that there is no teaching away, stating: "The evidence of record does not support a conclusion that an ordinarily skilled artisan setting priorities of threat events in Sourcefire for a particular network would have been discouraged from considering the reputation of traffic characteristics in setting such priorities." *'413 Decision*, at *9. That statement accurately reflects the legal standard set out in *In re Gurley*: "A reference may be said to teach away when a person of ordinary skill, upon reading the reference, would be discouraged from following the path set out in the reference, or would be led in a direction divergent from the path that was taken by the applicant." 27 F.3d 551, 553 (Fed. Cir. 1994).

Second, the Board's finding that there was no teaching away is supported by substantial evidence under the proper teaching-away standard. The Board acknowledged Centripetal's argument that Sourcefire's encouragement of the organization-specific customization of priority levels and incident response plans would have discouraged a relevant artisan from looking to Macaulay and "Dr. Orso's testimony that Macaulay's reputation scores are created for a different purpose and that Macaulay operates differently," as cited by PAN. *'413 Decision*, at *9. But the Board observed, correctly, that the fact that the "bodily incorporation of Macaulay[] . . . into Sourcefire" was not possible does not mean that the Sourcefire User Guide taught away from this combination. *Id.*, at *8–9; *see In re Keller*, 642 F.2d 413, 425 (CCPA 1981) ("The test for obviousness is not whether the features of a secondary reference may be bodily incorporated into the structure of the primary reference . . . . Rather, the test is what the combined teachings of the references would have suggested to those of ordinary skill in the art."). Given the reasons supporting a motivation to make the combination at issue, the Board reasonably found Centripetal's limited argument and evidence unconvincing as a basis to determine "that an ordinarily skilled artisan setting priorities of threat events in Sourcefire for a particular network would have been discouraged from considering the reputation of traffic characteristics in setting such priorities." *'413 Decision*, at *9.

III

We have considered Centripetal's remaining arguments and find them unpersuasive. We affirm the decisions of the Board.

AFFIRMED