UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CROWDSTRIKE, INC.

Petitioner

v.

OPEN TEXT INC.

Patent Owner

Case IPR2023-00289

Patent No. 8,418,250

PATENT OWNER'S RESPONSE

Mail Stop PATENT BOARD
Patent Trial and Appeal Board
U.S. Patent & Trademark Office
P.O. Box 1450
Alexandria, VA 22313–1450

TABLE OF CONTENTS

I. INTRODUCTION 1

II. THE '250 PATENT 4

A. Inadequacy of the Prior Art and The Need for Improved Malware Detection 4

B. Innovations of the '250 Patent 5

C. Claim Construction 8

1. "automatically" (claims 1, 13, 25) 8

2. "a mask for the computer object that defines acceptable behavior for the computer object" (claims 1, 13, 25) 12

3. Additional Terms At Issue In The District Court 14

D. Level of Ordinary Skill in the Art 15

III. OVERVIEW OF THE RELEVANT PRIOR ART 16

A. Overview of Kester 16

B. Overview of Honig 19

IV. THE CHALLENGED CLAIMS ARE PATENTABLE 20

A. Both of Petitioner's Grounds Fail Because Kester Is Non-Analogous Art 22

1. Kester and the '250 patent are non-analogous. 22

2. Kester and Honig are non-analogous. 30

B. Ground 1: The Combination of Kester and Honig Does Not Render The Challenged Independent Claims Obvious 31

1. Petitioner's combination does not disclose or suggest a mask that defines acceptable behavior for the object (Claims 1, 13, 25).....31

2. Petitioner's combination does not disclose or suggest automatically generating a mask. (Claims 1, 13, 25.) 41

C. Ground 1: The Combination of Kester and Honig Does Not Render The Challenged Dependent Claims Obvious 59

1. Petitioner fails to show the cited combination renders dependent claims 7 and 19 obvious. 59

2. The cited combination does not render dependent claims 12 and 24 obvious. 59

3. The cited combination does not render obvious dependent claims 2, 9-11, 14, 19, 21-23, 27-30. 61

D. Ground 2: The Combination of Kester, Honig, and Kennedy Does Not Render The Challenged Claims Obvious.....62

V. THERE ARE OBJECTIVE INDICIA OF NON-OBVIOUSNESS 62

VI. CONCLUSION.....63

TABLE OF AUTHORITIES

Page(s)

Cases

ActiveVideo Networks, Inc. v. Verizon Comms., Inc.,
694 F.3d 1312 (Fed. Cir. 2012) 46

AO Kaspersky Lab v. Open Text Inc.,
IPR2023-01334 (PTAB Aug. 18, 2023) 2

ADT LLC v. Vivint, Inc.,
IPR2022-00642, Paper 7 (PTAB Oct. 4, 2022) 47

In re Clay,
966 F.2d 656 (Fed. Cir. 1992) 26, 29

Dynamic Drinkware, LLC v. Nat'l Graphics, Inc.,
800 F.3d 1375 (Fed. Cir. 2015) 21

Eli Lilly & Co. v. Teva Pharms. Int'l GmbH,
8 F.4th 1331(Fed. Cir. 2021) 46

Graham v. John Deere Co.,
383 U.S. 1 (1966).....62

Harmonic Inc. v. Avid Tech., Inc.,
815 F.3d 1356 (Fed. Cir. 2016) 43

In re Huang,
100 F.3d 135 (Fed. Cir. 1996) 62

In re Klein,
647 F.3d 1343 (Fed. Cir. 2011) 22, 27, 29

Leo Pharm. Prods., Ltd. v. Rea,
726 F.3d 1346 (Fed. Cir. 2013) 62

Liberty Mutual Ins. Co. v. Progressive Cas. Ins. Co.,
CBM2012-00003 Paper 8 (PTAB Oct. 25, 2012) 47

Lyft, Inc. v. Quartz Auto Techs., LLC,
IPR2020-01450, Paper 7 at 18 (PTAB Mar. 4, 2021) 46

In re Magnum Oil Tools Int'l, Ltd.,
829 F.3d 1364 (Fed. Cir. 2016) 47

N. Telecom Ltd. v. Samsung Elec. Co.,
215 F.3d 1281 (Fed. Cir. 2000) 10

Pers. Web Techs., LLC v. Apple, Inc.,
848 F.3d 987 (Fed. Cir. 2017) 43, 46

Smith & Nephew, Inc. v. Hologic, Inc.,
721 F. App'x 943 (Fed. Cir. 2018).....29

Ex Parte Sokoly,
No. 2019-006703, 2020 WL 5587537 (PTAB Sept. 15, 2020).....22

T-Mobile US, Inc. v. TracBeam LLC,
IPR2015-01687, Paper 10 (PTAB Feb. 12, 2016).....47

TikTok Inc. v. Advanced Coding Techs. LLC,
IPR2022-01546, Paper 9 (PTAB June 15, 2023) 43

Vizio, Inc. v. Nichia Corp.
IPR2017-00552, Paper 9 (PTAB July 7, 2017) 25

Statutes

37 C.F.R. § 42.100(b) 8

EXHIBIT LIST

Exhibit	Description
2001	Declaration of Professor Nenad Medvidovic, Ph.D.
2002	*Curriculum Vitae* of Professor Nenad Medvidovic, Ph.D.
2003	*Webroot, Inc. and Open Text Inc., v. CrowdStrike, Inc. and CrowdStrike Holdings, Inc.,* Case No. 6:22-cv-00241-ADA-DTG, First Amended Complaint for Patent Infringement, Dkt. 60 (W.D. Tex., Sept. 8, 2022) (excerpted)
2004	*Sonrai Memory Ltd. v. Kingston Tech. Co. and Kingston Tech. Corp.,* Case No. 6:21-cv-1284-ADA, Order Denying Kingston Tech. Co. and Kingston Tech. Corp.'s Opposed Motion to Stay Pending Resolution of *Inter Partes* Review, Dkt. 94 (W.D. Tex., Oct. 18, 2022)
2005	*mCom IP, LLC v. Cisco Systems, Inc.,* Case No. 6:22-cv-00261-ADA, Order Denying Defendant's Motion to Stay Pending *Inter Partes* Review, Dkt. 42 (W.D. Tex., Oct. 20, 2022)
2006	*Intellectual Ventures I LLC et al. v. Hewlett Packard Enterprise Co.*, No. 6:21-cv-00596-ADA, Order Denying Hewlett Packard Enterprise Company's Opposed Motion to Stay Pending Resolution of *Inter Partes* Review, Dkt. 104 (W.D. Tex., Dec. 22, 2022)
2007	*Webroot, Inc. and Open Text Inc., v. AO Kaspersky Lab. et al.,* Case No. 6:22-cv-243-ADA-DTG, March 9, 2022 Transcript of Motions Hearing, Dkt. 133 (W.D. Tex. Dec. 15, 2022) (excerpted)
2008	Dani Kass, "Catching Up On Patent Litigation With Judge Albright" (Law360 Mar. 14, 2023); https://www.law360.com/pulse/articles/1582438/print?section=pulse/courts
2009	*Webroot, Inc. and Open Text Inc., v. AO Kaspersky Lab. et al.,* Case No. 6:22-cv-243-ADA-DTG, Order Granting Fourth Amended Scheduling Order, Dkt. 160 (W.D. Tex. Jan. 22, 2023)
2010	*Webroot, Inc. and Open Text Inc., v. Sophos Ltd.,* Case No. 6:22-cv-00240-ADA-DTG, Minute Entry for proceedings held before Judge Derek T. Gilliland, Notice of Electronic Filing, Dkt. 102 (W.D. Tex., Mar. 7, 2023)

Exhibit	Description
2011	*Webroot, Inc. and Open Text Inc., v. AO Kaspersky Lab. et al.,* Case No. 6:22-cv-243-ADA-DTG, Scheduling Order, Dkt. 39 (W.D. Tex. Aug. 8, 2022)
2012	*Webroot, Inc. and Open Text Inc., v. AO Kaspersky Lab. et al.,* Case No. 6:22-cv-243-ADA-DTG, Claim Construction Order, Dkt. 236 (W.D. Tex. Mar. 16, 2023)
2013	*Webroot, Inc. and Open Text Inc., v. Sophos Ltd.,* Case No. 6:22-cv-00240-ADA-DTG, Defendant Sophos Ltd.'s Preliminary Invalidity Contentions (W.D. Tex., Sept. 13, 2022) (excerpted)
2014	*Webroot, Inc. and Open Text Inc., v. Trend Micro, Inc..,* Case No. 6:22-cv-00239-ADA-DTG, Defendant's Preliminary Invalidity Contentions (W.D. Tex., Sept. 13, 2022) (excerpted)
2015	*Ex Parte* James M. Brennan, et al., Appeal 2021-003606, Application 15/285,875, Decision On Appeal Statement of the Case (PTAB Jul. 26, 2022)
2016	*Webroot, Inc. and Open Text Inc., v. CrowdStrike, Inc. and CrowdStrike Holdings, Inc..,* Case No. 6:22-cv-00241-ADA, Complaint for Patent Infringement, Dkt. 1 (W.D. Tex., Mar. 4, 2022)
2017	*Webroot, Inc. and Open Text Inc., v. AO Kaspersky Lab. et al.,* Case No. 6:22-cv-243-ADA-DTG, Plaintiffs' SurReply Claim Construction Brief, Dkt. 147 (W.D. Tex. Jan. 6, 2023) (excerpted)
2018	Transcript of Deposition of Wenke Lee dated September 29, 2023
2019	Declaration of Nenad Medvidovic, Ph.D. in Support of Patent Owner's Response
2020	*Webroot, Inc. and Open Text, Inc. v. AO Kaspersky Lab, et al.,* Case No. 22-cv-00243-AdA-DTG, Opening Claim Construction Brief From: AO Kaspersky Lab et al., Dkt. 86 (W.D. Tex. Oct. 28, 2022) (excerpted)

Open Text Inc. ("Patent Owner") submits this Response to the Petition of CrowdStrike, Inc. ("Petitioner") seeking *inter partes* review ("IPR") of the U.S. Patent No. 8,418,250 ("the '250 patent").

I. INTRODUCTION

The '250 patent introduced a revolutionary malware classification technology that eliminated many of the inefficiencies and risks associated with prior art methods. Before its development, malware solutions were limited in their ability to run unknown computer objects (*e.g.*, files or processes) safely without considerable delay—due to waiting either for a human to review the object and determine whether it should be permitted or for the industry to determine through trial and error whether the object was safe. The advancements claimed in the '250 patent implemented the automatic generation of a mask that defines acceptable behavior for an object, enabling the system to monitor object behavior and efficiently determine whether objects needed to be reclassified as malware. Patent Owner's subsidiary, Webroot, Inc., has implemented this technology in its security products.

Petitioner[1] is a direct competitor of Webroot and began providing endpoint

[1] CrowdStrike, Inc. filed the petition in this proceeding. After a settlement between the parties, CrowdStrike and Patent Owner filed a joint motion to terminate this

security software and systems that, without authorization, implemented Patent Owner's patented technology, including the '250 patent. In March 2022, Patent Owner filed suit against Petitioner in the Western District of Texas, asserting infringement of the '250 patent and other patents in Patent Owner's endpoint security portfolio.

Petitioner's challenge to the '250 patent should be rejected. Petitioner's grounds rely primarily on non-analogous art and mischaracterizations of the primary prior art's disclosure. Kester, Petitioner's primary reference, suffers from the very same prior art problems that the '250 patent sought to resolve. Kester uses a human reviewer to perform in-depth review of each application and/or network access request to determine expected network activity and associate each reviewed activity with a workstation-specific policy that allows or disallows the activity. That is, Kester's expected network activity encompasses both acceptable and unacceptable

---

proceeding on November 20, 2023. AO Kaspersky Lab, who is also a direct competitor of Webroot and petitioner in another *inter partes* review proceeding (IPR2023-01334), filed a motion to join this proceeding, and that motion was granted on December 21, 2023. *See* AO Kaspersky Lab v. Open Text Inc., IPR2023-01334, Paper 9.

activity—depending on the workstation. Like the prior art, where Kester's system encounters new activity, the activity must again be reviewed by a human reviewer to determine whether it should be permitted or not. Thus, Kester fails to disclose automatically generating a mask or a mask that defines acceptable behavior.

Honig's teachings do not resolve this key deficiency. Honig discloses an adaptive learning model that is limited to a binary decision, *e.g.*, yes/no, true/false, etc. In addition to Petitioner's failing to explain how such a model could be used to automate Kester's determination of expected network behavior, no POSITA would be motivated to do so because it would require either costly, ongoing modifications and the continued need for human review, or it would sacrifice Kester's ability to achieve its intended purpose by defining permissible and non-permissible application activity on a workstation-specific basis. Furthermore, even if a POSITA were to combine Kester's and Honig's teachings, the resulting combination still does not render obvious a mask that defines acceptable behavior.

Petitioner fails to articulate a combination of the prior art that renders obvious key limitations of the '250 patented technology. The challenged claims should be confirmed patentable.

II. THE '250 PATENT

A. Inadequacy of the Prior Art and The Need for Improved Malware Detection

"Malware" generally refers to an executable computer file or an "object" that is or contains malicious code, e.g., viruses, trojans, worms, etc. (EX-2019 ¶27.) The term "object" may include a computer file, partial file, sub-program, web page, piece of code, etc. (*Id.* 7:63-66.)

Much of the prior art anti-malware or anti-virus software focused on scanning and stopping ***known*** malware. (EX-1001 1:18-2:18.) For example, some prior art anti-virus software analyzed objects for "signatures"—something within the object that was known to be indicative of malware. (EX-1001 1:18-28.) Whenever new malware was detected by the industry, service providers would craft new signatures and release them as updates to their anti-malware programs. (*Id.*) Other prior art systems checked databases of known files to determine whether a file had been known for long enough that it could be deemed safe. (EX-1001 1:43-47.)

These prior art methods for detecting known malware suffered from inevitable extensive delays—either waiting for malware to be detected and a signature generated or waiting long enough with no adverse events that a program could be deemed safe. (EX-1001 1:30-37, 1:48-54; EX-2019 ¶28.)

Other anti-malware systems sought to protect against malware that previously was undetected or unknown. For example, prior art community-based anti-malware systems—*e.g.*, systems having a central computer and local computers on a network—relied on analysis at the central computer to determine whether a file was known or unknown. (EX-1001 1:60-2:4.) But when a file was unknown, the system had to provide the entire file to the central computer, where a manual or semi-manual detailed analysis of the file would be performed. (EX-1001 2:4-11.) This analysis "can still take days given the human involvement that is typically required." (*Id.*) Other prior art systems similarly relied on a human administrator to "make a better informed though still 'manual' decision as to whether or not the file is safe to run." (*E.g.*, EX-1001 2:18-27.)

Thus, such prior art systems still resulted in considerable delay before a new file could be classified as safe or malware. (EX-1001 2:12-13; EX-2019 ¶¶29-31.) Accordingly, there was a long-felt need for an improved technique to efficiently determine whether files were safe or malware. (EX-2019 ¶32.)

B. Innovations of the '250 Patent

One way the '250 patent improved upon the prior art is by introducing an automated masking technique that allows objects to be run within the confines of a mask, rather than delaying some amount of time to allow for independent review by

an administrator or general detection by the industry. Use of such a mask increases efficiency and streamlines the object classification process by automatically monitoring the object and offering "a rapid determination of the nature of the object…without requiring detailed analysis of the object itself…to determine whether it [is] malware." (EX-1001 3:8-18.)

The invention achieves this ability by collecting object data and automatically generating a mask that defines acceptable behavior for objects. (EX-1001 cls. 1, 13, 25.) Object data may include behavior information, such as executable instructions contained within the object, the size of the object, the current name of the object, the creation and modification dates of the object, or events initiated by or involving the object. (EX-1001, cl. 25.) Remote computers provide this data to a base computer, and the invention generates a mask that defines permissible behavior. (EX-1001 cl. 1, cl. 25, 14:58-61, Fig. 3 (steps 38-39).) That is, instead of waiting to run an object until the industry decides if an object is malware and instead of relying on an administrator to explicitly allow or disallow specific behaviors, the invention uses object data to automatically generate a mask that will monitor an object's behavior. (*Id.*)

Claim 1 recites a computer-implemented method corresponding to this continuous monitoring and classification using a mask, and claim 13 recites a system for implementing this method.

The claimed method starts with a centralized base computer receiving data about a computer object from multiple remote computers on which the object or similar objects are stored, including behavior data. (EX-1001, cl. 1, EX-1001 8:17-18, 8:44-47.) When the data does not indicate that the object is malware, *e.g.*, no industry signature designates it as known malware, the object is initially classified as "not malware." (EX-1001 8:47-9:7, Fig. 2 (steps 25-27).)

However, as explained above, an object not yet known by the industry to be malware may still be malicious. In order to allow the object to run without delay while still providing protection from malware, the invention automatically generates a mask based on object data, which defines acceptable behavior for the object and which may automatically monitor the object's behavior moving forward. (*See e.g.*, EX-1001 cl. 1, 14:58-61, Fig. 3 (steps 38-39).) If the behavior of the object is within the parameters set by the mask, the object is allowed to continue running. (EX-1001 15:45-47, cl. 1.) However, if the object's behavior extends beyond the mask, the object is not permitted to continue running. (EX-1001 15:47-52, cl. 1.) By continuously monitoring an object using the mask, it is possible to quickly recognize

when an object has attempted to extend beyond the mask and should be reclassified as malware. (EX-1001 15:64-16:3.)

Claim 25 recites a similar computer-implemented method that also uses an automatically-generated mask to monitor an object; however, it recites more specific details as to what data is transmitted from the remote computers to the base computer and how that data is transmitted to further support a rapid determination of whether an object should be classified as malware.

C. Claim Construction

1. "automatically" (claims 1, 13, 25)

a) Petitioner's construction is incorrect.

Petitioner's proposed construction of "automatically" is inconsistent with the district court's final construction of "automatically" in the parallel litigation, which the Board's regulations require that the Board consider. (*Compare* Petition 8-9 *with* EX-2012 4; 37 C.F.R. § 42.100(b).)

The district court correctly construed "automatically" as having its "[p]lain-and-ordinary meaning," which the court clarified as "includ[ing], ***but is not limited to***, 'without human involvement.'" (EX-2012 4.) This is consistent with the '250 patent's claims and specification, which use the term "automatically" to describe actions that necessarily and inevitably occur as a result of a particular circumstance—though a human may have been involved somewhere along the way.

(EX-2019 ¶51; EX-1001 3:31-35.) For example, the specification explains that by identifying relationships between an object and other objects, this information "can be used immediately and automatically to mark a child object as bad (or good) if the [ ] parent or other related object is bad (or good)." (EX-1001 3:31-35.)

The petition duplicates the same argument the district court already rejected—*i.e.*, that "the file history is [allegedly] unequivocal that the term 'automatically' excludes human involvement." (Petition 8.) Because Petitioner's district court arguments were unsupported by the applicant's statements during prosecution (just as Petitioner's arguments are here), the district court rejected Petitioner's narrowing construction.

During prosecution, the examiner issued a rejection based on reading U.S. Patent Publication No. 2005/0210035 ("Kester"), the same reference cited in the petition, as disclosing "automatically generating a mask…wherein the mask is generated in accordance with normal behaviour of the object determined from said received data." (EX-1002 611.) However, the applicant successfully traversed Kester, explaining that Kester required that a human reviewer determine the expected network activity and decide what behavior is allowable, whereas in the '250 patent, "human decision is not ***necessary*** to generate the mask or monitor the operation" of the object. (EX-1002 632-33.) The applicant made similar statements

regarding U.S. Patent Publication No. 2003/0177394 to Lambert. (EX-1002 585-586.)

The applicant's statements that human decision is not ***necessary*** to the step of generating a mask and monitoring an object do not rise to a clear and unambiguous exclusion of ***all*** human involvement. EX-2019 ¶¶56-59; *N. Telecom Ltd. v. Samsung Elecs. Co.*, 215 F.3d 1281, 1293–95 (Fed. Cir. 2000); EX-2017 5-6. Even Petitioner's own expert testified that, based on his review of the file history, he understood that "automatically" in the context of the '250 patent "means a human decision is not necessary to generate the mask." (EX-1003 ¶121.)

The district court agreed with Patent Owner's reading of the claims and prosecution history, rejecting a construction of "automatically" that is limited to "without human involvement." (EX-2012 4.) In its claim construction order,[2] the Court construed "automatically" as having its plain and ordinary meaning, which "includes, ***but is not limited to***, 'without human involvement.'" (*Id.* (emphasis added))

[2] While the district court indicated that it would later provide a more detailed claim construction order, it has not yet done so.

Patent Owner and its expert apply the plain and ordinary meaning of this term as construed by the district court. (EX-2019 ¶¶48-60.)

b) Petitioner's grounds fail under either Petitioner's construction or Patent Owner's construction.

While Petitioner's proposed construction is incorrect, as discussed above, Petitioner's grounds fail under both Patent Owner's and Petitioner's constructions. Whether applying Petitioner's proposed construction or the plain and ordinary meaning as understood by the District Court and Patent Owner, both constructions require some degree of automation. (EX-2019 ¶¶51, 60.) Specifically, under the plain and ordinary meaning, those limitations which must be performed "automatically" must necessarily and inevitably occur as a result of a particular circumstance. *See* Section II(C)(1)(a), *supra*. Petitioner's proposed construction is even more stringent, such that those limitations must be performed without human involvement. (Petition 8.) Thus, under either construction, the parties and experts agree that at least some degree of automation is required, where human intervention is, at the very least, not necessary to generate the mask or monitor an object's behavior.

2. "a mask for the computer object that defines acceptable behavior for the computer object" (claims 1, 13, 25)

Petitioner "asks the Board [to] apply PO's interpretation of the plain meaning of this limitation for the purposes of this proceeding," citing a sentence from Patent Owner's claim construction briefing at the district court, which states that a mask should "encompass[ ] any suitable way to define acceptable behavior" for the object. (Petition 27-28.) However, the district court did not agree and specifically rejected the argument that acceptable behavior could be defined by unacceptable behavior.

In the district court proceeding, Petitioner proposed that this term should be construed as "a list of acceptable actions for the object to perform," while Patent Owner found no construction necessary and proposed the limitation's plain and ordinary meaning. (EX-2012 4.) Citing the plain language of the claims, Petitioner identified as "[c]entral to the disclosure of the '250 patent [] the concept of an automatically generated 'mask' that lists the *acceptable* behaviors that a computer object may take, such that if the computer object does something *other* than those behaviors, it can be classified as malware." (EX-2020 9 (citing EX-1001 15:52-58, cl. 1).) Petitioner asserted that "if the mask includes unacceptable behavior, the claim's requirement of monitoring the behavior of the object would be superfluous, because there is no need to monitor the behavior of an object that is already known

to be malware." (EX-2020 10 ("[T]he mask does not list forbidden behavior but instead lists the behaviors that are acceptable.").)

Petitioner further noted that "[t]he specification *never* describes the mask as including 'unacceptable,' 'abnormal,' unexpected,' or 'non-allowable' behaviors." (EX-2020 10.) Petitioner also explained that "[t]he specification [] states that 'the behaviour of the object is continually monitored…to determine whether the object is running *within* its expected mask,' and '[a]ny behaviour that extends *beyond* the mask is identified and can be used to continually assess whether the object continues to be safe or not.'" (EX-2020 10 (citing EX-1001 15:5-12).)

The district court accepted Petitioner's arguments and construed the term to have its plain and ordinary meaning, while specifically explaining that "the plain-and-ordinary meaning of this term is ***not the inverse of a mask of unacceptable behavior***." (EX-2012 4 (emphasis added).) Thus, the district court limited the scope of the claimed mask by holding that acceptable behavior cannot be defined by the inverse of unacceptable behavior.

Consistent with the district court's final claim construction order, Patent Owner adopts a construction consistent with Petitioner's and the court's understanding of the term—*i.e.*, that a "mask…that defines acceptable behavior for

the computer object" must define only acceptable object behavior and cannot define acceptable object behavior by defining unacceptable behavior.

3. Additional Terms At Issue In The District Court

The district court construed all other disputed terms to have their plain and ordinary meaning:

- **"similar objects":** The court held that this term has its plain and ordinary meaning. (EX-2012 3.) The court rejected the defendants' argument that this term was indefinite. (*Id.*)
- **"behaviour of the object":** The court held that this term has its plain and ordinary meaning, wherein the plain and ordinary meaning does not include the static attributes of the object. (*Id.*) The court rejected a proposal that this term be construed as "actions performed by the object." (*Id.*)
- **"running said object":** The court held that this term has its plain and ordinary meaning, while noting that this term includes but is not limited to "carrying out the object's computer code." (*Id.* 5.)
- **"events initiated by or involving the computer object":** The court held that this term has its plain and ordinary meaning, while noting that

this term includes but is not limited to "actions or behaviours of an object acting upon another object or some other entity." (*Id.*)

- **"first remote computer" / "second remote computer":** The court held that this term has its plain and ordinary meaning. (*Id.* 5, 8.)

Patent Owner and its expert apply the plain and ordinary meaning of these claim terms, consistent with the district court's constructions. (EX-2019 ¶60.)

D. Level of Ordinary Skill in the Art

The '250 patent claims priority to an earlier application (GB 0513375.6) filed in Great Britain on June 30, 2005. A POSITA at the time of the invention of the '250 patent would have had a bachelor's degree in an accredited program of electrical engineering, computer engineering, computer science, or a similar discipline and 2-3 years of practical work or research experience in the general fields of electrical engineering, computer science, networking, communications, and device and network security. (EX-2019 ¶63.) More advanced degrees and/or training in a related discipline can compensate for shorter work experience. (*Id.* ¶¶ 63-65(noting that minor distinctions in Petitioner's and Patent Owner's definitions would not alter the analysis).)

III. OVERVIEW OF THE RELEVANT PRIOR ART

A. Overview of Kester

Kester observes that the rise in internet connectivity meant an increase in employee communications and with that, an increased risk of employees installing applications or transmitting programs or files their employers may disapprove of. (EX-1004 [0005].) For example, instant messaging, while improving productivity, could pose a risk to sensitive data. (*Id.*) Media streaming, while useful, could drain network bandwidth. (*Id.*) Although traditional filter systems existed to manage how employees' access the Internet in the workplace, the need to control a broad range of issues across a large number of users and wide variety of applications meant "employers need[ed] new solutions to manage the broader intersection of employees with their computing environments." (EX-1004 [0006]-[0007], [0040]; EX-2019 ¶68.)

The solution Kester proposes for "controlling application files" is having a human administrator review each application or network access request individually and associate it with an access privilege, *i.e.*, policy, unique to each workstation and/or user. (EX-1004 [0003], [0042], [0057] [0059]; EX-2019 ¶¶69, 72-73, 78, 86.) Specifically, hash values are generated for each application, including the predetermined network access data, and a workstation management module (WMM)

"stores the expected network activity in the hash/policy table." (EX-1004 [0011], [0183].) Kester records the reviewer's predetermined category and/or policy associations in the workstation- or user-specific hash/policy table, which the WMM may consult to determine the appropriate policy for *previously reviewed* applications or network access attributes. (EX-1004 [0011], [0050]-[0054], [0042]; EX-2019 ¶¶72-77.) That is, Kester first uses "expected" or "predetermined" to refer to whether the application or activity has previously been reviewed and exists within the hash/policy table. (EX-2019 ¶¶80-85.)

The hash/policy table includes a list of hashes, application names, publishers, suites, ports, protocols, I.P. addresses, and/or categories, as well as the policies that a reviewer has associated therewith that either permit or not permit the activity. (EX-1004 [0054].) Kester teaches that the "hash" may represent an application or a particular combination of one or more network attributes, *e.g.*, protocol, IP address, or access port, associated with a network access request. (EX-1004 [0050]-[0051]).)

Applications may be directly associated with an access privilege, *i.e.*, policy, or associated with a category, which then has its own access privilege/policy. (EX-1004 [0040].) Kester relies on a human reviewer to conduct an in-depth analysis of each application and combination of network attributes, related information, internet research, and/or related documentation to determine the appropriate categories.

(EX-1004 [0134]-[0135], Fig. 13; EX-2019 ¶¶77-86.) Kester discloses more than forty different exemplary categories, including those related to productivity (*e.g.*, project managers, word processing), communication (*e.g.*, email, instant messaging), audio/video (*e.g.* media players), and entertainment (*e.g.* games), as well as "expected" or "unexpected network access." (EX-1004 [0178]-[0182], Fig. 20 (steps 2004, 2006).). (EX-1004 Fig. 4A, [0082]; EX-2019 ¶69.) Because network attributes may vary for each network access request, "[e]ach combination of the one or more attributes can be associated with one or more categories." (EX-1004 [0184]-[0186].)

Periodically, or at set intervals, an upload/download module creates a hash/policy table with the designated policies for a particular workstation and downloads the hash/policy table to the corresponding workstation. (EX-1004 [0116].) "[T]he same application may be allowed to run on a workstation but not allowed to run on a different workstation." (EX-1004 [0116]; EX-2019 ¶¶72-74.)

When the WMM detects a request to launch an application or access a network, a hash is created from properties unique to that request and compared to the hash/policy table. (EX-1004 [0051], [0053], [0140]-[0142], Fig. 14 (steps 1402, 1404, 1406).) If the hash and/or data correspond to an entry in the hash/policy table—*i.e.*, the application or behavior has been previously reviewed by an

administrator—then the policy predetermined by a human reviewer is applied. (EX-1004 [0143], Fig. 14 (step 1410).) Policies might include allowing or not allowing the request, alerting the user, allowing the user a limited amount of time to continue the action, etc. (EX-1004 [0055].)

If the hash and/or data do not correspond to a predetermined entry in the hash/policy table—*i.e.*, the application or behavior has not been previously reviewed by an administrator and is unexpected—a default "not classified" policy is applied to the request and the application/behavior is logged to a database for future review. (EX-1004 [0059], [0145].) That is, Kester is limited to running the application without any kind of monitoring or halting the application altogether until the application/behavior can be reviewed. (EX-2019 ¶¶128-129, 138.)

B. Overview of Honig

Honig discloses a computer system architecture that supports the automation of certain steps in deploying "data-mining" intrusion detection systems (IDSs). (EX-1005 4:53-56; EX-2019 ¶87.) Data-mining IDSs collect data from sensors monitoring a system and use machine learning algorithms on a large set of "training data" to build detection models. (EX-1005 2:5-16.)

The type of training data needed is dependent on the type of detection model (and, therefore, the type of machine learning algorithm) that will be used to detect

intrusions. (EX-2019 ¶88.) Honig discloses at least three general types of model generation algorithms that its architecture may support: (1) "misuse detection," which models known attack behavior and trains on labeled normal and attack data; (2) "supervised (traditional) anomaly detection," which detect activity that diverges from a model of normal activity and trains on normal data; and (3) "unsupervised anomaly detection," which also detects activity that diverges from a model of normal activity but which trains on unlabeled data. (EX-1005 2:29-49, 20:33-38; EX-2019 ¶¶88-89, 93-94.)

Honig's architecture consists of: sensors and detectors for collecting information from the monitored system; a data warehouse which stores the collected data; model generators which access the data and train data mining-based detection models; model distributors which transfer the models to detectors; and analysis engines to provide data analysis capabilities. (EX-1005 6:64-7:7, 1:44-47, 4:53-56, 3:24-30.)

IV. THE CHALLENGED CLAIMS ARE PATENTABLE

The petition presents two grounds challenging the claims of the '250 patent, both of which rely on the combination of Kester and Honig as allegedly rendering the independent claims obvious:

Ground 1	Section 103(a)	Obvious over Kester in view of Honig	Claims 1-2, 7-14, 19-30
Ground 2	Section 103(a)	Obvious over Kester in view of Honig and Kennedy	Claims 3-6, 15-18

Petitioner fails to establish that the combination of Kester and Honig renders obvious every limitation of the challenged independent claims; therefore the claims should be found patentable over both grounds. "In an *inter partes* review, the burden of persuasion is on the petitioner . . . . Failure to prove the matter as required by the applicable standard means that the party with the burden of persuasion loses on that point—thus, if the fact trier of the issue is left uncertain, the party with the burden loses." *Dynamic Drinkware, LLC v. Nat'l Graphics, Inc.*, 800 F.3d 1375, 1378-79 (Fed. Cir. 2015).

A. Both of Petitioner's Grounds Fail Because Kester Is Non-Analogous Art

1. Kester and the '250 patent are non-analogous.

Kester is non-analogous art to the '250 patent, as it is neither in the same field of endeavor nor reasonably pertinent to the problems considered by the inventors of the '250 patent.

> "A reference qualifies as prior art for an obviousness determination under § 103 only when it is analogous to the claimed invention. Two separate tests define the scope of analogous prior art: (1) whether the art is from the same field of endeavor, regardless of the problem addressed, and (2) if the reference is not within the field of the inventor's endeavor, whether the reference still is reasonably pertinent to the particular problem with which the inventor is involved.'"

In re Klein, 647 F.3d 1343, 1348 (Fed. Cir. 2011) (internal citations omitted); *Ex Parte Sokoly*, No. 2019-006703, 2020 WL 5587537 (PTAB Sept. 15, 2020) (the fact that the prior art was used to "hang the roof tiles on the roof" did not mean that it was analogous to the claimed "utility hanger").

The '250 patent was classified as "information security." (EX-1001 p.1.) And while the patent states that it "relates ***generally*** to methods and apparatus for dealing with malware," the '250 patent explains that its particular field of endeavor is the

rapid determination of whether an object is safe or malware. (EX-1001 1:4-5, 3:8-18, 4:65-5:2, 8:4-7, 11:42-57, cls. 1, 13, 25; EX-2019 ¶¶103-105.)

Petitioner misstates the problems the '250 patent sought to solve, merely parroting select limitations of the claims. (Petition 10-11.) But the '250 patent explicitly identifies the relevant prior art problems, explaining that prior art methods for determining whether a file was safe or malware involved "considerable delay" "given the human involvement that is typically required." (EX-1001 2:4-13.) The '250 patent sought to improve upon these prior art methods that relied on manual or semi-manual detailed analysis of an object and a human administrator to decide whether or not the file is safe or malware. (EX-1001 2:4-27.) The '250 patent thus claims a method and system which "allows a rapid determination of the nature of the object to be made, without requiring detailed analysis of the object itself as such to determine whether it [is] malware." (EX-1001 3:8-18; EX-2019 ¶¶103-104.)

a) Kester is not in the same field of endeavor.

Kester is not in the same field of endeavor as the '250 patent. Petitioner wrongly asserts that Kester is directed to classifying a computer object as malware. (Petition 10-11.) Kester was classified as "data processing" during prosecution and explicitly defines its "[f]ield of [i]nvention" as "related to computing devices and, more particularly to monitoring and controlling application files operating thereon."

(EX-1004 [0002]-[0003], Title, cls. 1, 23, 37, 39; EX-2019 ¶106.) Kester explains that while prior art software was available for "preserving employee productivity, conserving network bandwidth and storage costs, limiting legal liability and improving network security," Kester sought to provide a "new solution[] to manage the broader intersection of employees with their computing environments" through monitoring and control of application files. (EX-1004 [0006], Title, [0003].) Thus, Kester's field of endeavor (monitoring and controlling application files) is not the same field of endeavor as the '250 patent (rapid determination of whether an object is safe or malware). (EX-2019 ¶¶105-112.)

Petitioner's assertion that Kester is in the general field of classifying an object as malware is based on a single exemplary category Kester discloses. (Petition 10-11.) As discussed above, Kester discloses forty-four exemplary categories in Figure 4A, one of which is "malicious applets and scripts." (EX-1004 Fig. 4A, [0082].) But aside from this single reference, Kester contains no disclosure regarding when or why an application should be categorized as "malicious applets or scripts," no disclosure regarding what might distinguish an application as safe as opposed to a malicious applet, and no disclosure as to what policy should be applied to applications categorized as a malicious applet or script. A single reference to

"malicious applets and scripts" does not place Kester in the same field of endeavor as the '250 patent. (EX-2019 ¶¶71, 108.).

In *Vizio, Inc. v. Nichia Corp.*, the Board found that prior art reference "Pinnow," which was cited in an IDS during prosecution of the challenged patent, was non-analogous. IPR2017-00552, Paper 9 at 11, 20-21 (PTAB July 7, 2017). The Board characterized the challenged patent's field of invention as relating to "a light emitting diode used in LED display, back light source, traffic signal, trailway signal, illuminating switch, indicator, etc." *Id.* at 21. In contrast, the Board defined Pinnow's field of invention as "concerned with projection display systems and is primarily concerned with those producing black and white images." *Id.* Thus, despite the fact that both the challenged patent and Pinnow "discuss" converting light from a monochromatic light source, the Board found Pinnow was not in the same field of endeavor. *Id.*

Similarly, in *Ex Parte Brennan*, the Board overturned an examiner's obviousness rejection because the prior art was non-analogous. EX-2015, Application No. 15/285,875, Appeal No. 2021-003606, Decision on Appeal at 7-8 (PTAB July 26, 2022). While acknowledging that both references shared a common classification and both disclosed two-stage produce washing systems, the Board found that the challenged patent's field of endeavor was better defined as "the field

of washing and sanitizing harvested produce," whereas the prior art's field was "more reasonably stated as the field of preserving produce freshness, especially for use in retail transport, storage and displays." *Id.* at 6-7.

If one were to accept Petitioner's assertion that a single one of 44 exemplary categories places Kester in the field of malware classification, it would mean that Kester is also in the field of "instant messaging" classification, "media player" classification, "gambling" classification, and more than forty other fields of endeavor despite Kester's lack of disclosure as to when or why each of these categories should be applied. (*See* EX-1004 Fig. 4A.) A POSITA would not have looked to Kester for a determination of whether an object is safe or malware. (EX-2019 ¶108.)

As Kester is not directed to a determination of whether an object is safe or malware, and certainly not a "rapid determination," Kester is in a different field of endeavor than that of the '250 patent. *See In re Clay*, 966 F.2d 656, 659 (Fed. Cir. 1992) (overruling a determination that patent and prior art were analogous finding that one's field of endeavor was ***storage*** of refined liquid hydrocarbons, while the other's field was ***extraction*** of crude petroleum).

b) Kester is not reasonably pertinent to the '250 patent.

Kester is also not reasonably pertinent to the problem faced by the '250 patent inventors. (EX-2019 ¶¶111-112.) A reference is reasonably pertinent if "it is one which, because of the matter with which it deals, logically would have commended itself to an inventor's attention in considering his problem." *In re Klein*, 647 F.3d at 1348 (internal citations omitted). As discussed above, the '250 patent sought to improve upon time-consuming prior art methods for determining whether an object is malware or safe, including those that relied on manual or semi-manual detailed analysis of an object and a human administrator to make the determination. (EX-1001 2:4-27.)

A POSITA would not have looked to Kester in considering these problems because Kester itself embodies the same problems the '250 patent sought to solve. (EX-2019 ¶110.) Kester's ability to control application files requires that a human reviewer conduct a detailed analysis of each application such as Internet research, determine expected network activity, decide how applications should be categorized, and make policy decisions based on a specific user or workstation. (EX-1004 [0089], [0178]-[0179].) And Kester contains no disclosure regarding why an application would be determined to be malicious versus safe. Thus, a POSITA

would not have looked to Kester as reasonably pertinent to avoiding time-consuming analysis and the need for human decision-making. (EX-2019 ¶110.)

Although the Board found in its institution decision that Petitioner "relies on Kester's teachings related to malware-classification of objects and related mask generation" (Paper 7 at 37), Kester does not include such teachings. (EX-2019 ¶108) As noted above, Kester includes only one reference to "malicious applets and scripts" and one reference to "malware," both as exemplary categories for an application among a laundry list of forty-four possible categories. (*Id.*; EX-1004 Fig. 4A, [0082].) Kester does not disclose how an application would be categorized, let alone how it would be categorized as malware. In fact, in response to a rejection based on Kester during prosecution, the applicant provided at least three reasons that "Kester is impractical for identifying malware." (EX-1002 633; EX-2019 ¶109.) The examiner subsequently allowed the '250 patent to issue. *Id.*

Similarly, Kester does not disclose or suggest mask generation. Kester, being directed to controlling employee activity, simply allows a human to record guidelines for permissible or impermissible activity on employee workstations. (EX-1004 [0089], [0178]-[0179].) Those guidelines are based on what the human expects an employee to attempt while using a workstation or otherwise accessing a network. (*Id.*) While Petitioner attempts to shoehorn Kester's identification of

"expected" activity as being a mask that defines "acceptable behaviour" as claimed in the '250 patent, Kester does not teach a mask the defines acceptable behavior. (EX-1004 [0089], [0178]-[0179].) Rather, Kester discloses a table of "expected" behaviors previously anticipated by a human reviewer, which may include both permissible activity and impermissible activity. (EX-2019 ¶111). As such, a POSITA would not have looked to Kester in considering how to generate a mask that defines acceptable activity for a computer object. (*Id.*) Further, because Kester does not describe systems and methods for malware detection or classification, a POSITA also would not have looked to Kester in considering how to generate such a mask for the purposes of malware detection or classification. (EX-2019 ¶¶111-112.)

Accordingly, Kester is not reasonably pertinent to the particular problem with which the inventors of the '250 patent were involved. *See In re Klein*, 647 F.3d at 1348, 1351-52 (despite both patent and prior art disclosing a partitioned container intended to facilitate mixing of two separated substances, they were non-analogous because neither prior art reference would fulfill the patent's purpose); *In re Clay*, 966 F.2d at 659; *Smith & Nephew, Inc. v. Hologic, Inc.*, 721 F. App'x 943, 949 (Fed. Cir. 2018) ("Even though both [the patent and the reference] ended up with similar mechanical solutions, it is beyond a stretch to say that [the reference] 'logically

would have commended itself to an inventor's attention in considering his problem.'").

During prosecution of the '250 patent, after the examiner opined in an office action that "Dozortsev and Kester are from the same field of endeavor, monitoring for malware," the applicant corrected the examiner, explaining that Kester was in a different field and concerned with different problems. (EX-1002 633-634; EX-2019 ¶111.) While not commenting on this correction, the examiner subsequently allowed the '250 patent to issue.

As Kester is neither in the same field of endeavor nor reasonably pertinent to the particular problem with which the inventors of the '250 patent were involved, Kester is non-analogous to the '250 patent and cannot serve as a primary reference for Petitioner's Section 103(a) grounds. (EX-2019 ¶¶99-112.) Since both of Petitioner relies on Section 103(a) for both of its grounds, the Board should reject Petitioner's invalidity challenges on this basis alone.

2. Kester and Honig are non-analogous.

Kester and Honig are neither in the same field of endeavor nor pertinent to the same problems, and a POSITA would not have looked to the teachings of one to modify the other. (EX-2019 ¶¶113-115.)

Kester's method relates "to monitoring and controlling application files" on computing devices. (EX-1004 [0002]-[0003]; Sections IV(A)(1), *supra*.) Honig's disclosure relates to "detecting anomalies in a computer system, and more particularly to an architecture and data format for using a central data warehouse and heterogeneous data sources." (EX-1005 1:42-47.) Whereas Kester addresses difficulties in controlling employee access to a network across a wide variety of application categories (EX-1004 [0006]-[0007], [0040]-[0042], Fig. 4A), Honig addresses the cost and inefficiencies associated with model generation. (EX-1005 2:65-3:12, 4:48-57.) Kester and Honig are non-analogous, such that no POSITA would have combined their teachings.

B. Ground 1: The Combination of Kester and Honig Does Not Render The Challenged Independent Claims Obvious

Both of Petitioner's grounds rely on its argument that a combination of Kester and Honig renders independent claims 1, 13, and 25 obvious. However, the combination of Kester and Honig does not render obvious: (1) a mask that defines acceptable behavior; or (2) automatically generating a mask.

1. Petitioner's combination does not disclose or suggest a mask that defines acceptable behavior for the object (Claims 1, 13, 25).

Petitioner's combination of Kester and Honig does not disclose or suggest a mask that defines acceptable behavior for the object. (EX-1001 cls. 1, 13, 25.)

With respect to the claimed "mask," Petitioner asserts that Kester's determination of expected network activity—*i.e.*, network attributes for inclusion in the hash/policy table—discloses a mask. (Petition 28.) This assertion forms the foundation of its combination and its arguments for other limitations. For example, for limitations [1.7]-[1.9], Petitioner relies on Kester's use of the hash/policy table "to ensure that the applications continue to operate in the predetermined manner." (Petition 33-36.) Petitioner asserts that Kester will allow access where activity matches the "expected network activity (as listed in the hash/policy table 204 of each remote workstation)," but will disallow access where "the application requests access to the network using a different protocol than the expected protocol listed in the hash/policy table 204." (Petition 36.) And for limitation [1.10], Petitioner asserts that Kester teaches categorization of applications that are not operating in a predetermined manner—i.e., where the activity has not been previously reviewed as part of the hash/policy table. (Petition 38.) That is, Petitioner contends that the human reviewer's determination of expected network activity for the hash/policy table allegedly constitutes the claimed mask.

However, Kester's expected network activity—contained within its hash/policy table—is not a mask that "defines acceptable behavior" because the hash/policy table and the expected network activity identified within that table

includes unacceptable behavior. (*See* EX-1004 [0070], [0185]; EX-2019 ¶¶125-126.)

For example, Kester teaches that when an application is not operating in a "predetermined manner," it is placed in the uncategorized applications database for future review, such that those attributes might be added to the hash/policy table. (EX-1004 [0070]; EX-2019 ¶126.) That is, whether an application is operating in a "predetermined" or "expected" manner is dependent on whether that activity is contained within the hash/policy table and not whether that activity is acceptable or unacceptable. (EX-2019 ¶126.) Petitioner's discussion of the combination does not address this deficiency in any way, let alone provide any explanation for why a skilled artisan would have found this limitation obvious in light of both references. Thus, Petitioner has failed to show that the combination of Kester and Honig would have rendered the independent claims obvious. (EX-1001 cls. 1, 13, 25.)

As the summaries above make plain, the invention claimed in the '250 patent is starkly different from Kester's approach. *See* Sections II(B), III(A), *supra*. The invention of the '250 patent automatically generates a mask that defines only acceptable object behavior, thereby enabling the system to safely run and monitor an object based on whether it is operating within the boundaries of the mask. *See* Section II(C)(2), *supra*. Kester does not teach or suggest this approach. Rather,

Kester embodies the same problem that the '250 patent sought to overcome—*i.e.*, the need for a human administrator to review applications or network access requests to determine whether each request or application launch should be permitted or not. (EX-1004, Fig. 20 ("Human reviewer uses hints and web information to research network access by application. Using evidence from hints and other research, determine allowed behavior for each application."), [0089]-[0090], [0187].)

The independent claims—claim 1 for example—rely on a mask that defines the boundaries of an object's behavior by defining acceptable behavior:

> [1.5] automatically generating ***a mask for the computer object that defines acceptable behaviour*** for the computer object…
>
> …
>
> [1.7] automatically monitoring operation of the object on the at least one of the remote computers;
>
> [1.8] allowing the computer object to continue to run when behaviour of the computer object is permitted by the mask;
>
> [1.9] disallowing the computer object to run when the actual monitored behaviour of the computer object extends beyond that permitted by the mask; and
>
> [1.10] reclassifying the computer object as malware when the actual monitored behaviour extends beyond that permitted by the mask.

(*See also* EX-1001 cls. 13, 25.) The invention limits the mask to acceptable behavior, such that future object behavior can be allowed or disallowed based on

whether it falls within or outside of the mask. (Section II(C)(2), *supra*; EX-2019 ¶127.) The benefits of using an automatically-generated mask that defines acceptable behavior are that: (1) the invention avoids the delay associated with waiting for a human to review each object and designate whether specific behaviors should be permitted or not; and (2) when an object's behavior extends beyond the mask, the invention knows that the object should be reclassified from "not malware" to "malware." (EX-2019 ¶¶127-130.)

Kester fails to disclose automatically generating a mask and fails to disclose a mask that defines only acceptable behavior. As discussed above, the challenged claims recite automatically generating a mask and using a mask that defines acceptable behavior to allow or disallow an object to run. In contrast, Kester relies on a human to pre-review each application and/or behavior and designate whether each application/behavior should be permitted or not before the hash/policy table may be used to monitor it. (*Id.*; EX-2018 at 8:3-20.) When Kester's system encounters a new behavior that has not yet been reviewed, that behavior is logged to a database to eventually be reviewed by a human reviewer. (EX-1004 [0059], [0144]-[0145].)

To argue that Kester discloses a mask that defines acceptable object behavior, Petitioner asserts that Kester discloses "expected or allowed network activity (also

referred to as expected or predetermined behavior)." (Petition 28.) But Petitioner wrongly equates "expected" network activity with "allowed network activity." Kester teaches that expected network activity may be allowed or disallowed ***based on the human reviewer's determination***.[3] (*E.g.*, EX-1004 [0185].) Specifically, Kester teaches that because "network attributes associated with the application may be different for each attempted access," its system "may allow a first combination of one or more network attributes while disallowing a second combination of the one or more network attributes." (EX-1004 [0185], [0083].) Kester describes network activity as "expected" or "predetermined" to indicate that a human reviewer has previously reviewed the specific combination of network attributes and that a

[3] Although Kester does use the quoted phrase "expected or allowed network activity;" "expected" and "allowed" are two distinct types of activity. (*See, e.g.*, EX-1004 [0179], [0181], [0185].) Kester discloses that a human reviewer not only determines the "expected" network activity of an application (*id.* [0182]-[0183]) but also determines the "allowed" network activity by associating a policy with each activity that either allows or disallows the activity (*id.* [0057], [0185]). While "expected" behavior may be allowed or acceptable, it may also be disallowed or unacceptable. (*E.g.*, *id.* [0185]; EX-1003 ¶¶124-126.)

predetermined association with a policy (to allow or not allow) has been stored in the hash/policy table. (EX-1004 [0057]-[0059] ("If the execution launch detection module…does not find the application hash in the hash/policy table [] (for example, the application is uncategorized ***or the application is behaving unexpectedly***)….").)

That is, an application operating in an expected or predetermined manner—*i.e.*, within the boundaries of Petitioner's alleged "mask"—might still be disallowed from continuing to run, based on the associated policy. (EX-2019 ¶¶124-126.) This result is intuitive based on Kester's distinct goal—*i.e.*, "to manage the broader intersection of employees with their computing environments" on a workstation-by-workstation basis. (EX-1004 [0006], [0115]-[0116].) Within this context, Kester's system seeks to provide a different type of protection that is distinct from that of the '250 patent.

For example, an employer might wish to limit particular activity to management only. (EX-2019 ¶¶73, 129-130, 133.) Following Kester's approach, a human administrator reviews the application and associated network access data. (*Id.*) The human administrator then determines that, where the network access attributes indicate that a manager's workstation has made the request, the request should be associated with a policy that allows the request. (*Id.*) But if a non-manager's workstation makes the request, the human administrator determines that

such attributes should be associated with a policy that does not allow the request. (*Id.*) Kester teaches that a hash/policy table will be generated specific to the requesting workstation and download it to the workstation. (*Id.* [0116].) Thus, while the particular activity, *e.g.*, the network access request, may be expected or predetermined such that it is included in the hash/policy table, it may be unacceptable and will not be allowed. (*Id.*, EX-2019 ¶¶131-132, 135-136)

Accordingly, Kester relies on a hash/policy table containing "expected" activity reviewed by a human administrator that may include acceptable activity but that also includes unacceptable activity. Under the district court's claim construction—which Petitioner urged in the parallel litigation—the claimed mask must define only acceptable behavior, and acceptable behavior cannot be defined by the inverse of unacceptable behavior. *See* Section II(C)(2), *supra*. Thus, Kester does not disclose a mask that defines acceptable behavior of the object.

As a result of this critical distinction, Kester's "expected network activity" cannot provide the same benefits as the '250 patent's claimed mask. (EX-2019 ¶¶128-131.) For example, the '250 patent allows an object to run when its monitored behavior falls within the object's mask:

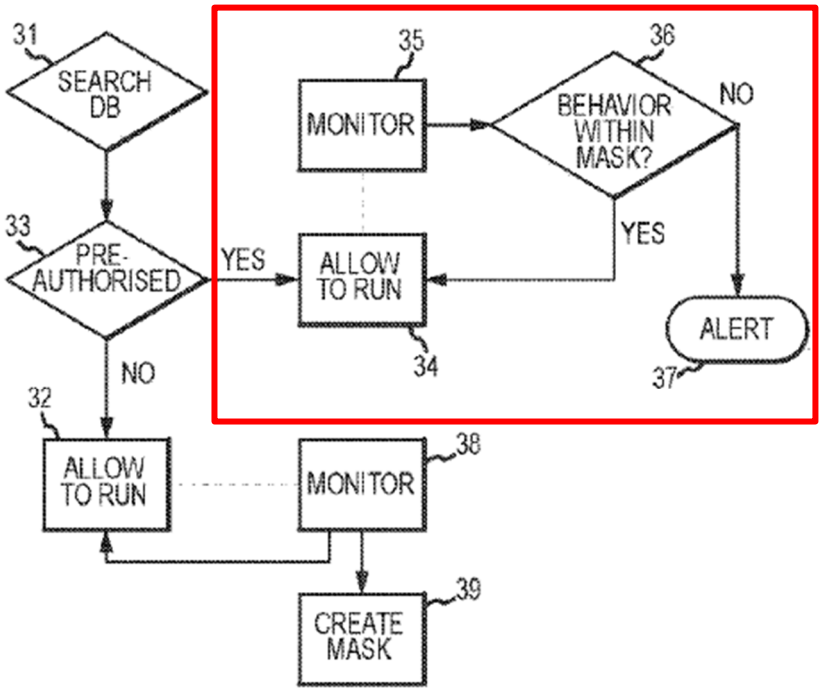

FIG.3

(EX-1001 Fig. 3; *id.i* cls. 1, 13, 25 (annotated).) And when that behavior extends beyond the mask, the object is not allowed to run and is reclassified as malware. (EX-1001, cls. 1, 13, 25.) Petitioner expressly acknowledged this in its district court briefing. (EX-2020 10-11.) But because Kester's expected network activity contains both acceptable and unacceptable activity, an application whose behavior is within this alleged mask cannot categorically be allowed to run. (EX-1004 [0042]-[0043], [0185]-[0186].) To do so would contradict Kester's purpose, which is to apply predetermined policies on a workstation-by-workstation basis across all expected activity, thereby controlling employees' interaction with the internet. (EX-1004 [0006], [0042]-[0043].)

As another example, because Kester's expected network activity defines unacceptable behavior, it cannot be used as a tool for informing when an application must be reclassified as malware. (EX-2019 ¶131.) Within the context of Kester's disclosure, when an application is operating unexpectedly—*i.e.*, its hash does not match an existing hash in the hash/policy table—that merely means that the application or the application's particular activity has not yet been reviewed, categorized, or associated with a policy by an administrator. (EX-1004 [0059].) Thus, the application—whether previously categorized or uncategorized—is added to the "uncategorized applications database" and subsequently reviewed by an administrator. (EX-1004 [0070]-[0071].) However, the fact that the activity-in-question was unexpected, *i.e.*, previously unreviewed, does not mean that it is necessarily malicious or that the application should be categorized as malicious. (EX-2019 ¶131.) Again, a human administrator will be required to review the application and the network attributes associated with its activity to determine whether such activity should be permitted or not, as well as whether the application should be categorized and/or recategorized. (EX-1004 [0070]-[0071].)

Because Kester's hash/policy table includes unacceptable expected network activity and because a human must determine expected network activity, Kester's teachings do not practice or suggest the challenged claim limitations and a POSITA

could not achieve the same benefits of the claimed invention. (EX-2019 ¶¶128-135.) Accordingly, Petitioner has not shown (and cannot show) that Kester discloses or suggests automatically generating a mask that defines acceptable behavior as recited in the independent claims of the '250 patent.

While Petitioner asserts that a POSITA would have been motivated to automate the human reviewer's determination of expected network activity in Kester's system based on Honig's teachings, this does not address the deficiency already present in Kester. Even if a POSITA were motivated to attempt to automate Kester's determination of expected network activity (which he would not be, as discussed further below), the discussion above shows that Kester's expected network activity is not a mask that defines acceptable behavior as claimed. *See* Section III.A, *supra*. Thus, automatically generating Kester's expected network activity still would not practice the method or achieve the same benefits of the challenged '250 patent claims. Petitioner does not address this deficiency or argue that the prior art would have rendered such a mask obvious. Accordingly, Kester and Honig do not render any of the challenged claims obvious.

2. Petitioner's combination does not disclose or suggest automatically generating a mask. (Claims 1, 13, 25.)

The combination of Kester and Honig also fails to render the independent claims obvious for a second, independent reason—the combination does not disclose

or render obvious *automatically* generating a mask. (EX-1001 cls. 1, 13, 25.) First, Petitioner fails to explain how Kester could be modified in view of Honig's teachings. Second, a POSITA would not have been motivated to automate Kester's determination of expected network activity.

a) Petitioner does not adequately articulate a combination of Kester's and Honig's teachings that automatically generates a mask.

First, it should be noted that Petitioner and its expert concede that Kester's method requires a human to review applications/behavior, at which point the human generates / adds to a hash/policy table that reflects the human's review; therefore, under either party's construction, Kester does not "automatically" generate a mask because a human is actively involved throughout Kester's entire process. (Petition 28, 30; EX-2019 ¶137; EX-2018 6:14-20 ("Q: Do you agree that Kester teaches that it's a human analyst who performs Kester's categorization steps? A: . . . so to answer your question, I would say that human reviewer is involved in the categorization and recategorization.").) As the applicant explained during prosecution, Kester's method is distinct from and does not teach the claimed method of the '250 patent, in which "human decision ***is not necessary***" to the step of generating the mask. (*See* EX-1002 632-33.)

While Petitioner asserts that it would have been obvious to modify Kester to automatically determine expected network activity using Honig's teachings, Petitioner fails to adequately articulate a combination of Kester's and Honig's teachings that would satisfy this claim limitation. Petitioner does not identify any one of Honig's embodiments with any particularity, explain whether any of Honig's models were capable of automating Kester's determination, or articulate how Kester would be modified to implement an automated determination. (Petition 30-32.)

"It [i]s Petitioner's 'burden to explain to the Board how' the combination of references 'rendered the challenged claims unpatentable.'" *TikTok Inc. v. Advanced Coding Techs. LLC*, IPR2022-01546, Paper 9 at 7 (PTAB June 15, 2023) (citing *Harmonic Inc. v. Avid Tech., Inc.*, 815 F.3d 1356, 1363 (Fed. Cir. 2016). While the features of a secondary reference need not be bodily incorporated into the structure of the primary reference, "[a] clear, evidence-supported account ***of the contemplated workings of the combination is a prerequisite*** to adequately explaining and supporting a conclusion that a relevant skilled artisan would have been motivated to make the combination and reasonably expect success in doing so." *Pers. Web Techs., LLC v. Apple, Inc.*, 848 F.3d 987, 994 (Fed. Cir. 2017) (emphasis added) (overturning a panel's decision where "the Board nowhere clearly explained, or cited

evidence showing, *how* the combination of the two references was supposed to work").

Even though Honig discloses several, distinct adaptive learning models, *e.g.*, misuses detection algorithms, supervised anomaly detection algorithms, and unsupervised anomaly detection algorithms (EX-1005 2:29-49, 20:33-63), Petitioner does not identify a single algorithm that would suggest to a POSITA that Kester's determination could be automated. (Petition 30-32.) Petitioner states only generally that "*Honig* provides a detailed discussion of adaptive learning model generators that were known in the field." (Petition 31.) And Petitioner describes Honig's system as "scalable" with components that can be "plugged" into the system architecture. (Petition 31.) But Petitioner does not even identify a particular adaptive learning model or the associated component(s) necessary to automatically generate the model that a POSITA allegedly would be motivated to implement within Kester. (EX-2019 ¶142.)

Honig teaches a POSITA that the degree of possible automation in the overall process of generating and deploying an adaptive learning model is dependent upon the specific algorithm/model being used, the type of data on which the model is trained, and which components of Honig's architecture have been "plugged" into the system. (EX-1005 20:33-38.) Petitioner mischaracterizes Honig's algorithms as

"fully automated" (Petition 30), when that phrase is used by Honig to describe only the process for converting data into the appropriate format for training a model. (EX-1005 7:19-20.)

In fact, neither Honig nor Kester suggest "fully" automating their methods. Honig discloses that "[s]ome of the processes still require ***some manual intervention***," for example, labeling data used to train and generate the adaptive learning model. (EX-1005 3:24-30 (emphasis added).) Kester teaches that, while categorization may be "based on" adaptive learning systems, such systems will still merely "enable the human reviewer" or provide hints "to enhance productivity of the human reviewer." (EX-1004 [0092], [0090].) Petitioner concedes that its proposed combination's generation of a mask may not be fully automated, acknowledging that automation may merely make a method "more efficient ***for a human reviewer to use***." (Petition 32 (emphasis added).) Because the specific model and context within which a model might be implemented determines the degree of possible automation, a clear articulation of the combination of Kester's and Honig's teachings is critical to Petitioner's argument.

By failing to identify a particular adaptive learning model or explain how such a model might have supposedly suggested automating Kester's determination step, Petitioner has failed to provide an "evidence-supported account ***of the contemplated***

workings of the combination," failed to explain whether the resulting combination would actually read on the challenged claims under its own definition, and failed to show that the combination would yield a predictable result for which a POSITA would have had a reasonable expectation of success. *Pers. Web Techs.*, 848 F.3d at 994; *ActiveVideo Networks, Inc. v. Verizon Comms., Inc.*, 694 F.3d 1312, 1327 (Fed. Cir. 2012) (affirming summary judgment of no invalidity where the defendant's expert "failed to explain how specific references could be combined, which combination(s) of elements in specific references would yield a predictable result, or how any specific combination would operate or read on the asserted claims"); *Lyft, Inc. v. Quartz Auto Techs., LLC*, IPR2020-01450, Paper 7 at 18 (PTAB Mar. 4, 2021) (denying institution where petitioner "[did] not articulate adequately how it propose[d] to modify one of the references or to combine the two references' teachings"); *Eli Lilly & Co. v. Teva Pharms. Int'l GmbH*, 8 F.4th 1331, 1344 (Fed. Cir. 2021) ("A finding by the Board that a patent challenger has demonstrated a motivation to combine references does not necessarily imply that the challenger has also met its burden of showing a reasonable expectation of success.").

A vague petition based on an unspecified combination of prior art disclosures hamstrings Patent Owner's ability to respond. Thus, the Board, too, should "address only the basis, rationale, and reasoning put forth by the Petitioner and resolve all

vagueness and ambiguity in Petitioner's arguments against the Petitioner." *Liberty Mutual Ins. Co. v. Progressive Cas. Ins. Co.*, CBM2012-00003 Paper 8 at 14 (PTAB Oct. 25, 2012); *T-Mobile US, Inc. v. TracBeam LLC*, IPR2015-01687, Paper 10 at 20 (PTAB Feb. 12, 2016) ("[W]e will not…improperly shift the burden of deciphering the arguments onto the Patent Owner"). Because Petitioner fails to articulate a combination that renders obvious "automatically" generating a mask that defines acceptable behavior, its grounds fail to render obvious any challenged claim. *See ADT LLC v. Vivint, Inc.*, IPR2022-00642, Paper 7 at 13-14 (PTAB Oct. 4, 2022); *In re Magnum Oil Tools Int'l, Ltd.*, 829 F.3d 1364, 1381 (Fed. Cir. 2016) ("[T]he Board must base its decision on arguments that were advanced by a party, and to which the opposing party was given a chance to respond.").

b) A POSITA would not be motivated to automate Kester's determination of expected network activity.

Honig does not resolve Kester's shortcomings with respect to automatically generating a mask that defines acceptable behavior. Petitioner argues that "[i]t would have been obvious to 'automatically' generate…Kester's mask in view of the teachings of Honig"—specifically, that a POSITA would have generated Kester's expected network activity using an adaptive learning model as disclosed in Honig. (Petition 30.)

In addition to the fact that Petitioner has failed to adequately articulate a specific combination, Petitioner fails to address: (1) the costly and time-consuming modifications (including ongoing modifications) that would have to be made to any of Honig's models to make them of limited use in Kester's system/method; (2) the capabilities in Kester's system that would be lost and the detrimental impact on Kester's intended purpose; and (3) the lack of expected success in the proposed combination, due to Petitioner's blending of two different steps in Kester.

(i) A binary model—such as Honig's—could not be used to automate Kester's determination of expected network activity without extensive, ongoing modifications.

Honig's adaptive learning model seeks to answer a binary question: malicious or not? (EX-1005 8:15-24; EX-2019 ¶168.) While Honig discloses several distinct types of models, each of these models is considered a "binary classifier" because it is only capable of making a binary determination. (*See* EX-1005 2:29-50, 2:67-3:2; EX-2019 ¶168.) For example, Honig specifically describes a support vector machine (SVM)—which can be used for both traditional and unsupervised anomaly detection—as a binary classifier. (EX-1005 21:39-47; EX-2018 48:3-50:9.) Honig explains that for an SVM, data is mapped to a feature space, in which a set of labeled training data is used to determine "a linear decision surface (hyperplane)." (EX-1005 21:47-51.) "This surface is then used to classify future instances of

data…based upon which side of the decision surface it falls." (EX-1005 21:51-53.) Because there are only two sides to that linear decision surface, the models contemplated by Honig are limited to two results—*i.e.*, a binary outcome. (EX-2019 ¶168.)

Unlike Honig, Kester sought to offer a "broader" solution to managing employees' interactions with the internet and, as such, Kester's method and system are capable of handling multiple questions with "n" (or unlimited) possible outcomes. (EX-1004 [0006], [0081]-[0082], Fig. 4A; EX-2019 ¶¶141, 171, 175-176; *see also* EX-2018 53:7-54:7.) For example, Kester discloses workstation-specific hash/policy tables because rules and policies may vary workstation-to-workstation or user-to-user for each application. (*See, e.g.*, EX-1004 [0116].) That is, while certain expected network activity may be permitted for a first workstation, that same expected network activity may not be permitted for a second workstation. (*Id.*; EX-2019 ¶¶141, 171.)

Petitioner does not explain how a single binary model could be used to automate Kester's determination of expected network activity on a workstation-by-workstation basis and, therefore, fails to explain how Honig's disclosure of a binary model would have motivated a POSITA to automate this step. (EX-2019 ¶¶141, 171-173.) Petitioner's proposed combination therefore begs the question: why

would a POSITA automate Kester's case-by-case, user-by-user, and workstation-by-workstation determination using teachings from Honig that were incapable of efficiently automating Kester's determination, especially given that Honig provides no guidance as to how such automation would be implemented? They would not. (EX-2019 ¶¶141-142, 171-172.)

Indeed, a POSITA would have limited options in trying to shoehorn any of Honig's teachings into Kester's system/method. If a POSITA were to apply a binary model that decides between expected network activity and unexpected network activity, such a model would still need to be able to implement Kester's user-specific policies or surrender that capability of Kester's system, making it less useful for its intended purpose. (*Id.*) The cost of training numerous models—each being trained on a particular user's set of training data—to apply workstation-specific determinations would be excessive. (*Id.* ¶174.) This is particularly true when one considers that training data for each workstation would need to include data across all applications intended to be included in the model. (*Id.* ¶¶171-174.) The addition of a new user or a new application on any workstation would require the expensive training or retraining of a binary model. (*Id.* ¶174.)

Alternatively, if a POSITA were to try and apply one massive binary model that accounts for all employees and all applications, this would still require a massive

amount of training data that covers all employees and all applications. (*Id.* ¶¶170-174.) And it would still require costly retraining every time a new user or new application was added to the environment. (*Id.* ¶174.)

Furthermore, these attempts to apply a binary model assume that all expected network activity will be permitted and that all unexpected network activity will not be permitted. (EX-2019 ¶¶131, 142.) But, as explained above, that is not how Kester's system functions. Kester specifically teaches that expected network activity merely indicates that the activity is known and has been reviewed (and therefore, exists in the hash/policy table); but expected network activity in Kester's method may still be considered unacceptable—*i.e.*, not permitted. (*See* EX-1004 [0011], [0183], [0185]; EX-2019 ¶¶131-132.) Again, one would have to fundamentally alter the operation of Kester's system and sacrifice the capabilities that enable Kester's intended goal—providing a means for controlling employee interactions with the Internet across all applications in a way that applies policies specific to each workstation or user.

Within the context of Kester's system, method, and stated goal, no POSITA would have been motivated to implement any of Honig's binary models due to the cost, effort, and inability of Honig's models to efficiently automate Kester's determination of expected network activity. (EX-2019 ¶¶125-134, 141, 166-176.)

To be clear, Patent Owner's argument is distinct from the argument that one could not bodily incorporate Honig's model into Kester's system. (*See* Paper 7 at 39-40.) Regardless of whether one of the models (and the necessary supporting architecture) could be bodily incorporated into Kester's system, those models would not be capable of automating the relevant determinations made by a human reviewer in Kester. And where Honig's models are not capable of efficiently automating the determinations, Honig's teachings would not suggest to or motivate a POSITA to modify Kester in the suggested manner.

(ii) Applying Honig's teachings to automate Kester's determination of expected network activity would undermine Kester's stated goal and reduce system capabilities.

As noted above, Kester discloses a "broader" solution to managing employees' interactions with the internet and, as such, Kester's method and system are capable of handling multiple questions with "n" (or unlimited) possible outcomes. (EX-1004 [0006], [0081]-[0082]; EX-2019 ¶¶141, 171, 175-176; *see also* EX-2018 53:7-54:7.) Specifically, Kester's method provides the ability to control usage and network access across all potential applications, including those related to productivity, privacy, communication, entertainment, and any of the more than forty categories Kester discloses. (EX-1004 [0081]-[0082], Fig. 4A.)

Kester's entire system relies on the ability to apply a hash/policy table containing human-specified activity, categories, and policies to an application launch or network access request to determine whether such action is expected and whether it should be permitted. (EX-1004 [0042]-[0043].) The system therefore relies on a human administrator to review applications, associate the applications with any applicable categories, investigate and determine the expected network activity, ***and*** associate each expected activity with a policy "unique…for the workstation 101 and/or user" that might permit or not permit the activity. (EX-1004 [0042], [0180]-[0186]; EX-2019 ¶142.)

Petitioner's assertion that a POSITA would be motivated to implement Honig's teachings in order to eliminate the need for time-consuming human review fails for two reasons. First, even if a POSITA were able to train and implement a binary model to determine expected network activity (which they would not be), such a model merely identifies expected activity that should be included in the hash/policy table. (EX-2019 ¶170.) That is, a human would still need to review the application and activity, categorize the application, and associate each expected activity with workstation-specific policies. (*Id.*) A binary model implemented in the combination Petitioner proposes is unable to do that because it merely answers the question: expected or unexpected? (*Id.* ¶172.) Thus, the human reviewer will

still be required to perform the same amount of work. No POSITA would have been motivated to add a costly binary model that would require constant updating with no discernable benefit. (*Id.* ¶¶170-172.)

Second, even if one assumes that Kester's human reviewer is eliminated after implementing a binary model, then Kester's capabilities would be so drastically reduced and the system so fundamentally altered that it could no longer achieve its intended purpose of controlling users' application activity. (EX-2019 ¶¶166-171.) If a binary model is implemented and no administrator reviews the application, then the application is never categorized and no policies can be applied based on the application's category. (*Id.*) If no administrator associates the categories and expected network activity with workstation-specific policies, then the resulting hash/policy table is limited to identifying whether activity is expected or not and is unable to determine whether activity should be permitted or not. (*Id.*) And the table cannot apply workstation-specific hash/policy tables when no reviewer ever made those associations. (*Id.*)

During prosecution, the applicant explained that no POSITA would have been motivated to automate Kester's method, "as to do so would mean that the system of Kester would no longer be able to perform its function of allowing a company to implement appropriate policies governing what their employees can do on their

computers." (EX-1002 634.) Again, because Kester does not disclose a mask that defines acceptable behavior as claimed, automating the determination of expected network activity does not practice the '250 invention.

Because applying Honig's teachings would *either* (i) result in costly model development, zero benefits, and an ongoing need for modifications (the implementation of which is not described anywhere in Honig or Kester), *or* (ii) eliminate critical capabilities of Kester's system, a POSITA would not be motivated to automate Kester's determination of expected network activity.

(iii) Petitioner fails to articulate sufficient motivation to combine Kester's and Honig's teachings.

Petitioner's asserted motivation to modify Kester attempts to blend two distinct steps within Kester and, as a result, leads to the incorrect conclusion that such a modification would have been obvious.

As discussed above, Kester discloses many different "predetermined associations" that a human reviewer must make. (Section III(A), *supra*.) In particular, after reviewing the application, related data, research, and or related documentation, Kester's human reviewer determines: (1) the "expected network activity," including network attributes, for the hash/policy table and the associated policies; and (2) which categories should be applied to an application/request, such

as "expected network access" and associated policies. (EX-1004 [0178]-[0187]; EX-2019 ¶¶166-171, 176-177.)

As previously explained, Petitioner's grounds rely on Kester's determination of expected network activity—*i.e.*, expected network attributes for inclusion in the hash/policy table—discloses a mask. (Petition 28; Section IV(B)(1), *supra*.) However, in arguing that a POSITA would be motivated to automate Kester in view of Honig's teachings, Petitioner repeatedly references the administrator's ***categorization*** of activity. (*See e.g.*, Petition 29-30.) For example, Petitioner argues that it would have been obvious to implement an adaptive learning model like Honig's because Kester "explains the process ***for classifying or categorizing*** applications 'can be based upon [] adaptive learning systems.'" (Petition 29-30 (emphasis added).) And thus, Petitioner concludes it would have been obvious "to look to known adaptive learning systems ***to perform Kester's classification and/or categorization*** processes." (Petition 30 (emphasis added); *see also id.* 21 (asserting similarly for Limitation 1.2 that a POSITA would automate "Kester's application ***categorization*** process"); EX-2018 10:16-12:18.) However, aside from the conclusory argument that a POSITA would have used Honig's teachings to automate virtually anything computer-related, (EX-2018 11:12-12:13), Petitioner and its expert have failed to articulate how a POSITA would have modified Kester's

teachings with Honig to automate a human's determination of expected network activity/attributes.

Kester merely states that ***categorization***—not the human's ***determination*** of expected network activity/attributes—"can be based upon…adaptive learning systems." (EX-1004 [0092]; EX-2019 ¶¶162-163.) That is, Petitioner attempts to rely on a suggestion or motivation to automate the categorization of applications as motivation to automate the determination of expected network activity.

While the Board's institution decision notes Dr. Lee's purported assertion that a POSITA would apply the automation identified in one portion of Kester's human-reviewer activities to other portions of those activities, Dr. Lee's declaration contains no such explanation. (Paper 38; EX-1003 ¶¶121-132.) At his deposition, Dr. Lee again failed to provide such an explanation, merely reiterating without any evidentiary support that because one machine learning process ***could*** be automated, other portions of Kester's human-reviewer activities ***could*** be automated as well. (EX-2018 12:19-13:20.) In fact, Dr. Lee essentially ignores the fact that Kester suggests the use of an adaptive learning system only for ***categorization***, and not for the determination of expected network activity. (*Id.* ("Q. . . And in Kester, you agree that Kester teaches using adaptive learning systems only for the categorization step and not for the determining step; is that fair? A. . . What I'm trying to say is that,

yes, that's what Kester is saying, but Kester did not exclude say, Oh, you should only use machine learning for classification.")).

While Dr. Lee highlights several benefits that Honig's system, as a whole, purports to achieve, neither Petitioner nor Dr. Lee provides an explanation of what the combination of Kester's and Honig's teachings would suggest, how the proposed combination of teachings would function, or whether the same benefits would be achieved. (*See id.*)

Indeed, such benefits would not be achieved. As explained above, if Kester's suggestion of an adaptive learning system or Honig's disclosure of a binary model were applied to Kester's determination of expected network activity, the result would ***not*** achieve the same benefits. *See* Section IV(B)(2)(b)(i), *supra*. Specifically, due to the limitations of a binary model, any resulting implementation would either require costly, ongoing modifications ***and*** the continued need for human input, or it would sacrifice all of Kester's key capabilities and the system's ability to achieve its intended purpose. *See* Sections IV(B)(2)(b)(i)-(ii), *supra*. Accordingly, Petitioner's proffered motivation is unsupported, and a POSITA would not have been motivated to automate the human reviewer's determination of expected network activity.

C. Ground 1: The Combination of Kester and Honig Does Not Render The Challenged Dependent Claims Obvious

1. Petitioner fails to show the cited combination renders dependent claims 7 and 19 obvious.

Dependent claims 7 and 19 recite a method according to the independent claims, "*wherein the data is sent in the form of key that is obtained by a hashing process carried out in respect of the objects on the respective remote computers*." (EX-1001 cls. 7, 19.)

The evidence Petitioner cites in support of its argument against these claims merely establishes that Kester discloses generating a hash for the application launch or network access request that is to be evaluated by comparing it to the local hash/policy table. (EX-1004 [0011], [0051]-[0052].) None of the cited evidence, nor the declaration of Dr. Lee, shows that Kester's remote computers carry out a hashing process on the collection data before sending the collection data to the base computer in the form of a key/hash. (*See id.*; EX-1003 ¶¶152-154.) Accordingly, Petitioner fails to show that the combination of Kester and Honig renders claims 7 and 19 obvious.

2. The cited combination does not render dependent claims 12 and 24 obvious.

Where the behavior extends beyond the boundaries of the mask, claims 12 and 24 recite comparing the behavior with the behavior of other objects and, if the

behavior is known to be not malicious for other objects, allowing the behavior for the object-in-question and modifying the mask to allow that behavior for that object in the future. (EX-1001, cl. 12.)

Petitioner first asserts that Kester discloses this limitation, pointing to the exact same disclosure that it does for limitation [1.10], which recites reclassifying the object as malware when behavior extends beyond that permitted by the mask. (Petition 38-39, 43-45.) But when Kester encounters an application or network access request that does not match a hash in the hash/policy table, Kester (a) applies a default "not-classified application policy" that may include allowing or denying access; and (b) logs the application and the associated attributes to the uncategorized application database for future review. (EX-1004 [0145], Fig. 14; EX-2018 52:17-54:7 (admitting the Kester is incompatible with binary systems and methods; "Q. What do you mean when you say 'cases where it does not match'? . . A. . . Yeah, so my point is that it's not a simple allow/not allow. When it does not match, there is further action to be taking [sic] by posing this query into the database of the application server module, for example, and then also application inventory database to essentially do some further analysis down the road.").) That is, instead of comparing the activity-in-question with known activity of other objects to determine whether the activity-in-question should be allowed, Kester will immediately permit

or not permit access based on the default "not classified" policy. (*Id.*; EX-2019 ¶¶128-129.) Accordingly, Kester does not disclose *allowing said behavior for the object if said behavior is known to be not malicious for other objects*.

Petitioner alternatively asserts that Kester in view of Honig would render claim 12 obvious but relies on Honig only for its teaching of updating or altering an existing model. (Petition 45-46.) That is, Petitioner does not address the deficiency in Kester or explain why a POSITA would have modified Kester to delay applying its "not classified" policy until a human reviewer has the opportunity to review the activity, compare it with the activity of other objects, and determine whether that activity is malicious for other objects. Indeed, a POSITA would not be motivated to do so, because the delay would unreasonably interrupt the user's computer activity. (EX-2019 ¶¶128-129.) Thus, neither Kester nor the combination of Kester and Honig discloses or renders obvious *allowing behavior for the object if said behavior is known to be not malicious for other objects*.

3. The cited combination does not render obvious dependent claims 2, 9-11, 14, 19, 21-23, 27-30.

Because Petitioner's obviousness challenges against all dependent claims depend on Petitioner's deficient analysis of the independent claims, the remaining dependent claims fail for the same reasons as the independent claims.

D. Ground 2: The Combination of Kester, Honig, and Kennedy Does Not Render The Challenged Claims Obvious

Ground 2 fails for the same reasons as Ground 1. In Ground 2, Petitioner adds Kennedy only to purportedly teach the limitations *added* by dependent claims 3-6 and 15-18. (Petition at 54.) Because Ground 2 includes no argument that Kennedy remedies any of Ground 1's shortcomings regarding the independent claims, and the claims it challenges all depend on those independent claims, Ground 2 cannot render any of the challenged claims obvious.

V. THERE ARE OBJECTIVE INDICIA OF NON-OBVIOUSNESS

In determining obviousness of the claimed invention, objective evidence of secondary considerations pertaining to nonobviousness must be considered, including long-felt but unsolved needs, failure of others, and commercial success. *In re Huang*, 100 F.3d 135, 139 (Fed. Cir. 1996) (citing *Graham v. John Deere Co.*, 383 U.S. 1, 17-18 (1966)); *Leo Pharm. Prods., Ltd. v. Rea*, 726 F.3d 1346, 1358 (Fed. Cir. 2013).

As discussed above, a long-felt and persistent need existed for an improved technique to efficiently determine whether files were safe or malware. (*See* Section II(A), *supra*.) Prior attempts to monitor unknown objects and/or determine whether objects were safe or malware were plagued by considerable delay and increased risk.

(*Id.*; EX-1001 2:12-13.) Where others failed, the innovative approach claimed in the '250 patent succeeded. (*See* Section II(B), *supra*.)

Patent Owner currently accuses at least four industry participants, including Petitioner, of infringing the innovative technology claimed in the '250 patent, demonstrating the critical need and widespread industry reliance on these novel methods. Petitioner, for example, markets and provides the CrowdStrike Falcon Platform, the components of which practice the systems and methods claimed in the '250 patent.

Accordingly, secondary objective indicia of nonobviousness exist, such that Petitioner's grounds fail. (EX-2019 ¶¶180-182.)

VI. CONCLUSION

For the foregoing reasons, the Board should deny institution.

Date: December 21, 2023

Respectfully submitted,

KING & SPALDING LLP

/Brian Eutermoser/

Brian Eutermoser
Registration No. 64,058

Attorney for Patent Owner
Open Text Inc.

CERTIFICATION OF WORD COUNT

The undersigned hereby certifies that the portions of the above-captioned **PATENT OWNER RESPONSE** specified in 37 C.F.R. § 42.24 have 12,793 words, in compliance with the 14,000 word limit set forth in 37 C.F.R. § 42.24. This word count was prepared using Microsoft Word 365 v.2022.

Date: December 21, 2023

Respectfully submitted,

KING & SPALDING LLP

/*Brian Eutermoser*/

Brian Eutermoser
Registration No. 64,058

Attorney for Patent Owner
Open Text Inc.

CERTIFICATE OF SERVICE

The undersigned hereby certifies that the foregoing **PATENT OWNER RESPONSE** and all supporting **EXHIBITS 2018-2020** were served by filing the documents through the Patent Trial and Appeal Case Tracking System (P-TACTS) on December 21, 2023 and courtesy copies were also served via electronic mail, in their entireties on the following:

Adam P. Seitz (Reg. No. 52,206)
Adam.Seitz@eriseip.com
Hunter A. Horton (*pro hac vice to be submitted*)
Hunter.horton@eriseip.com
ERISE IP, P.A.
7015 College Blvd., Suite 700
Overland Park, Kansas 66211
Telephone: (913) 777-5600
Fax: (913) 777-5601

Paul R. Hart, (Reg. No. 59,646)
Paul.Hart@eriseip.com
ERISE IP, P.A.
5299 DTC Blvd., Suite 1340
Greenwood Village, CO 80111
Telephone: (913) 777-5600
Fax: (913) 777-5601

Counsel for Petitioner
CrowdStrike, Inc.

Date: December 21, 2023

KING & SPALDING LLP

/Brian Eutermoser/

Brian Eutermoser
Registration No. 64,058

Attorney for Patent Owner
Open Text Inc.