US009692778B1

(12) **United States Patent**
Mohanty

(10) Patent No.: **US 9,692,778 B1**
(45) **Date of Patent:** **Jun. 27, 2017**

(54) **METHOD AND SYSTEM TO PRIORITIZE VULNERABILITIES BASED ON CONTEXTUAL CORRELATION**

(71) Applicant: **Symantec Corporation**, Mountain View, CA (US)

(72) Inventor: **Shubhabrata Mohanty**, Pune (IN)

(73) Assignee: **Symantec Corporation**, Mountain View, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **14/538,599**

(22) Filed: **Nov. 11, 2014**

(51) **Int. Cl.**
H04L 29/06 (2006.01)
G06F 9/455 (2006.01)

(52) **U.S. Cl.**
CPC **H04L 63/1433** (2013.01); **G06F 9/45533** (2013.01)

(58) **Field of Classification Search**
CPC H04L 63/1433; G06F 9/45533
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

2009/0077666	A1 *	3/2009	Chen	G06F 21/577 726/25
2013/0191919	A1 *	7/2013	Basavapatna	G06F 21/577 726/25
2014/0201836	A1 *	7/2014	Amsler	H04L 63/20 726/23
2014/0223555	A1 *	8/2014	Sanz Hernando	G06F 21/55 726/22
2015/0040228	A1 *	2/2015	Lee	H04L 63/1433 726/25

OTHER PUBLICATIONS

Mell et al., (The Common Vulnerability Scoring System (CVSS) and Its Applicability to Federal Agency Systems, NIST Interagency Report 7435, Aug. 2007, 33 pages).*
Quinn et al. "Guide to Adopting and Using the Security Content Automation Protocol (SCAP) Version 1.0", NIST Special Publication 800-117, Jul. 2010, 26 pages.*

* cited by examiner
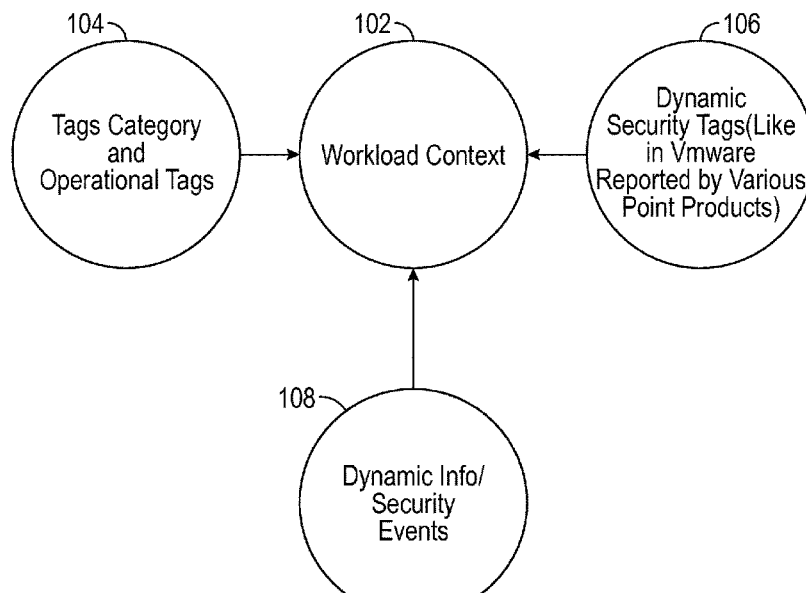
Primary Examiner — Saleh Najjar
Assistant Examiner — Oleg Korsak
(74) *Attorney, Agent, or Firm* — Maschoff Brennan

(57) **ABSTRACT**

A method for prioritizing vulnerabilities of an asset in a virtual computing environment is provided. The method includes determining a vulnerability score for the asset, based on at least one of a base vulnerability score or a temporal vulnerability score and receiving information about a threat. The method includes correlating the information about the threat with information about the open vulnerabilities on the asset and also about the asset to determine a threat score for the asset and determining a contextual score for the asset based on at least one tag of the asset. The method includes deriving a prioritization score for the asset, the prioritization score a combination of the vulnerability score, the threat score and the contextual score, wherein at least one method action is performed by a processor.
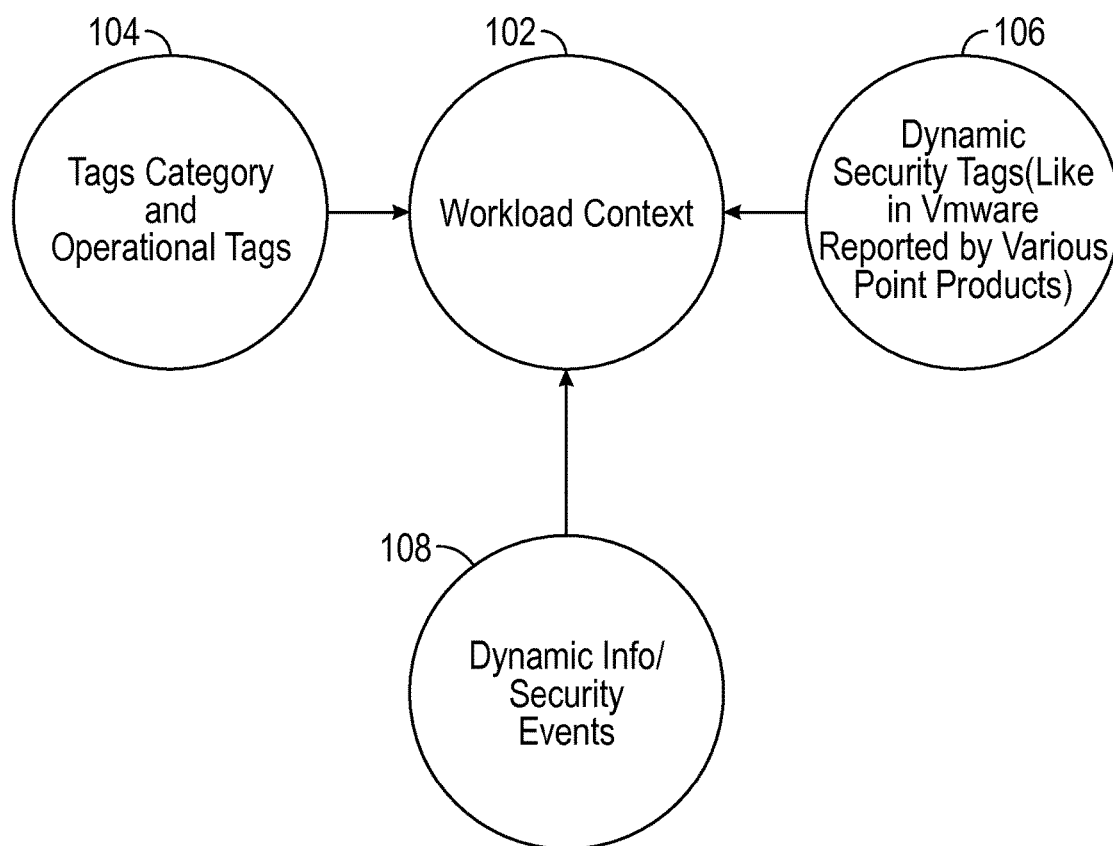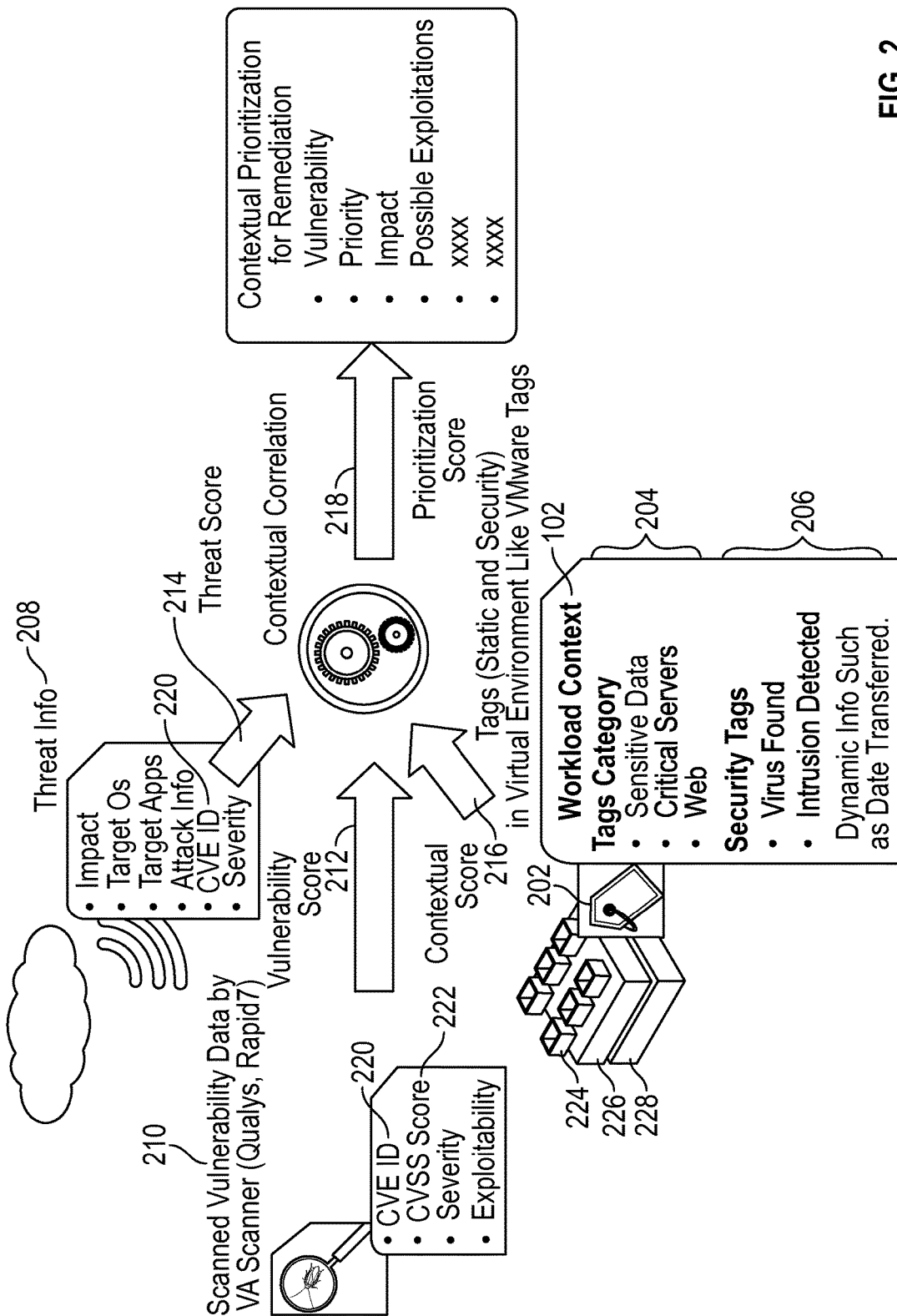
20 Claims, 5 Drawing Sheets

FIG. 1

FIG. 2

FIG. 3

402 — Determine vulnerability score for asset

404 — Obtain threat information

406 — Correlate open vulnerability information with threat

408 — Determine threat score for asset

410 — Correlate vulnerability data and tag information

412 — Determine contextual score for asset

414 — Determine prioritization score for asset based on vulnerability score, threat score, contextual score

416 — Prioritization score meets threshold ?   **No**

Yes

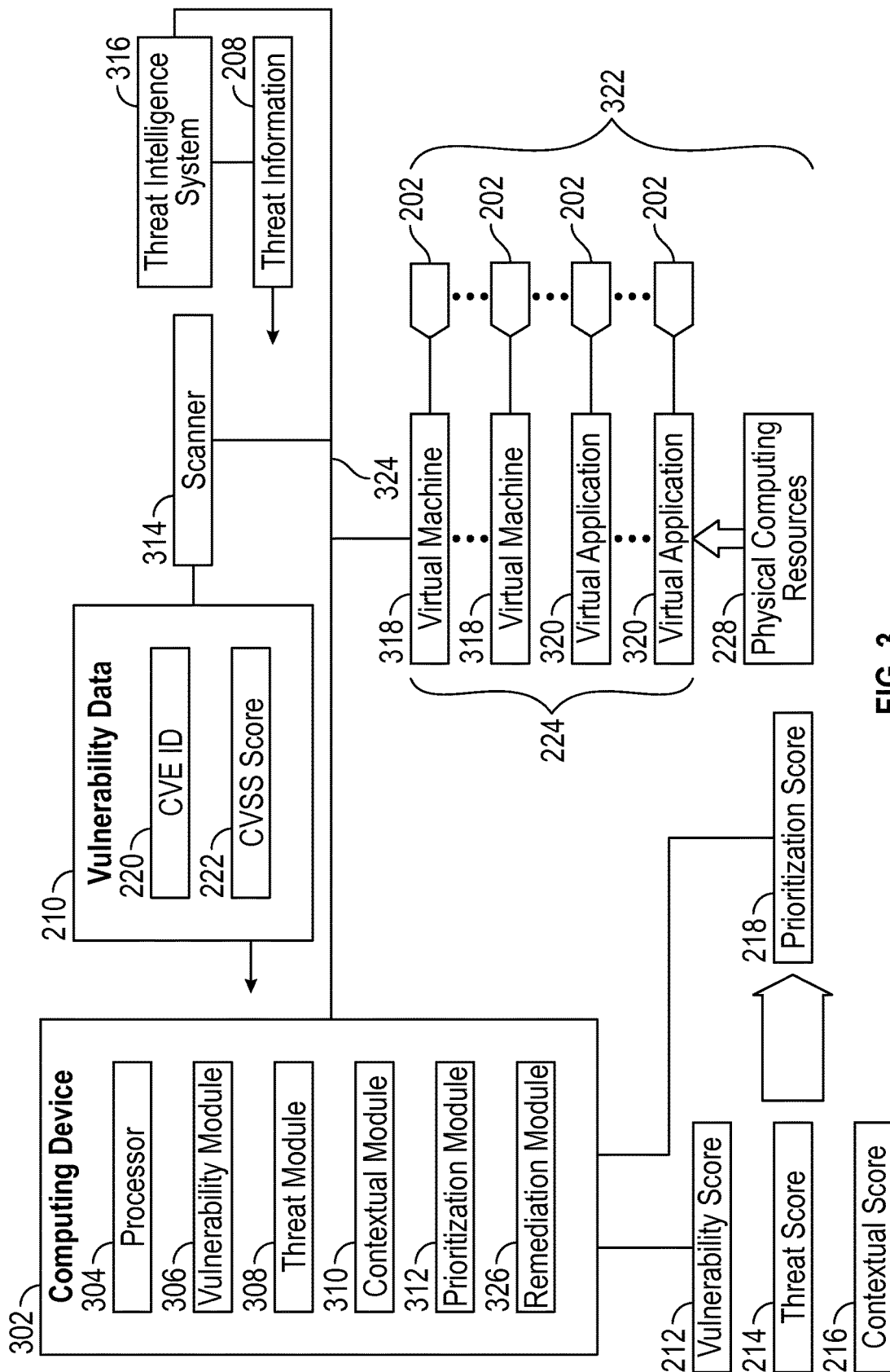418 — Determine remediation for asset
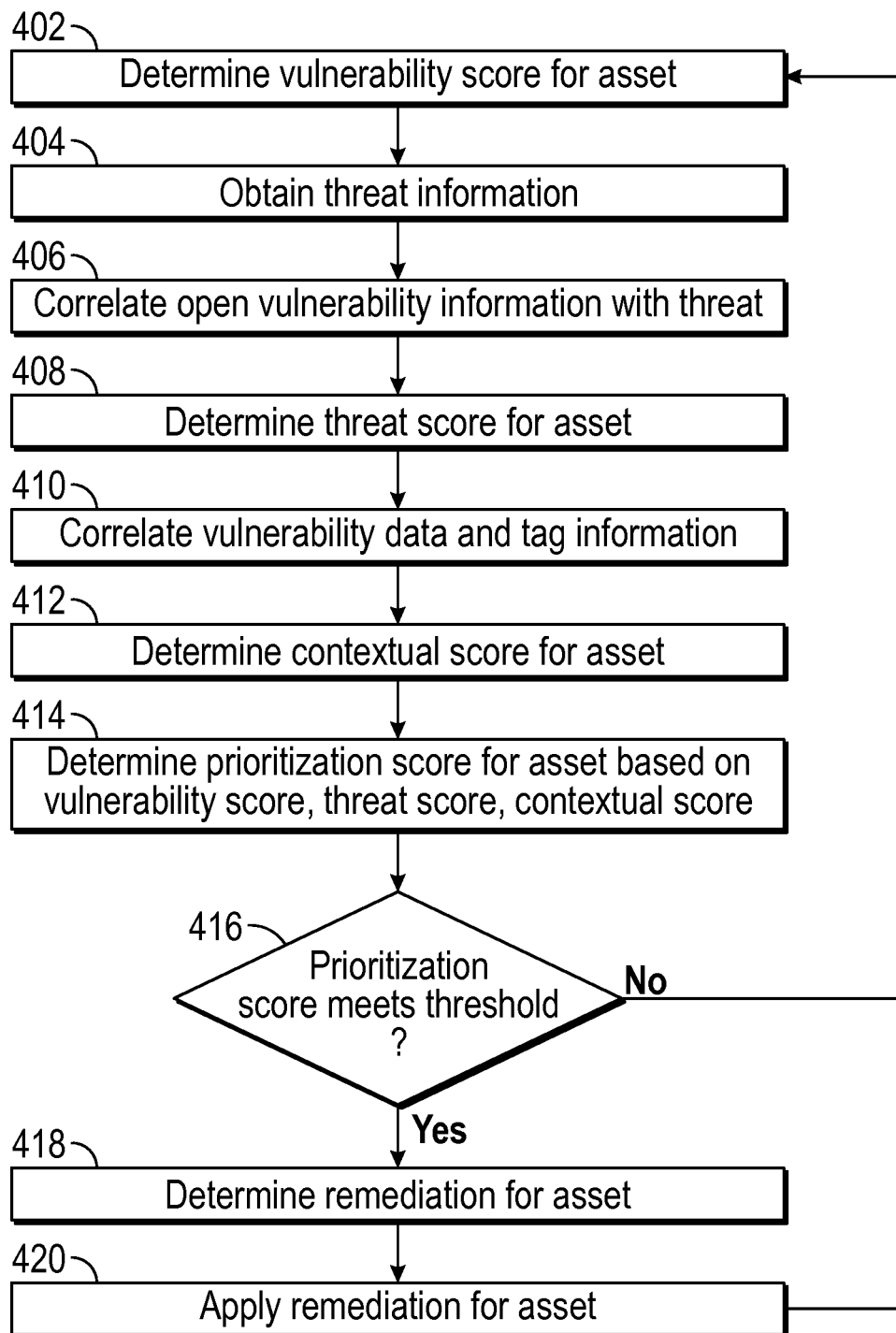
420 — Apply remediation for asset

FIG. 4

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.

fastcase®
Smarter legal research.