US009270694B2

(12) **United States Patent**
**Loder et al.**

(10) **Patent No.: US 9,270,694 B2**
(45) **Date of Patent: Feb. 23, 2016**

(54) **SYSTEMS AND METHODS FOR ASSESSING SECURITY FOR A NETWORK OF ASSETS AND PROVIDING RECOMMENDATIONS**

(71) Applicant: **Rapid7, LLC**, Boston, MA (US)

(72) Inventors: **Chad Loder**, Los Angeles, CA (US); **Dana Elizabeth Wolf**, Boston, MA (US); **Matthew Robert Hathaway**, Boston, MA (US)

(73) Assignee: **RAPID7, LLC**, Boston, MA (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.: **13/899,117**

(22) Filed: **May 21, 2013**

(65) **Prior Publication Data**

US 2014/0351940 A1 Nov. 27, 2014

(51) **Int. Cl.**

| | |
|---|---|
| ***H04L 29/06*** | (2006.01) |
| ***G06F 9/455*** | (2006.01) |
| *G06F 21/57* | (2013.01) |
| *H04L 12/24* | (2006.01) |

(52) **U.S. Cl.**

CPC ..... ***H04L 63/1433*** (2013.01); ***G06F 9/45558*** (2013.01); *G06F 21/577* (2013.01); *H04L 41/082* (2013.01); *H04L 41/0893* (2013.01)

(58) **Field of Classification Search**

CPC .. G06F 21/554; G06F 21/557; H04L 63/1433
USPC ..... 726/25
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

| | | | | |
|---|---|---|---|---|
| 7,584,508 | B1 * | 9/2009 | Kashchenko et al. | 726/25 |
| 2002/0026591 | A1 * | 2/2002 | Hartley | H04L 63/1433 726/25 |
| 2004/0006704 | A1 * | 1/2004 | Dahlstrom | G06F 21/577 726/25 |
| 2011/0138471 | A1 * | 6/2011 | Van De Weyer et al. | 726/25 |
| 2014/0173738 | A1 * | 6/2014 | Condry et al. | 726/25 |

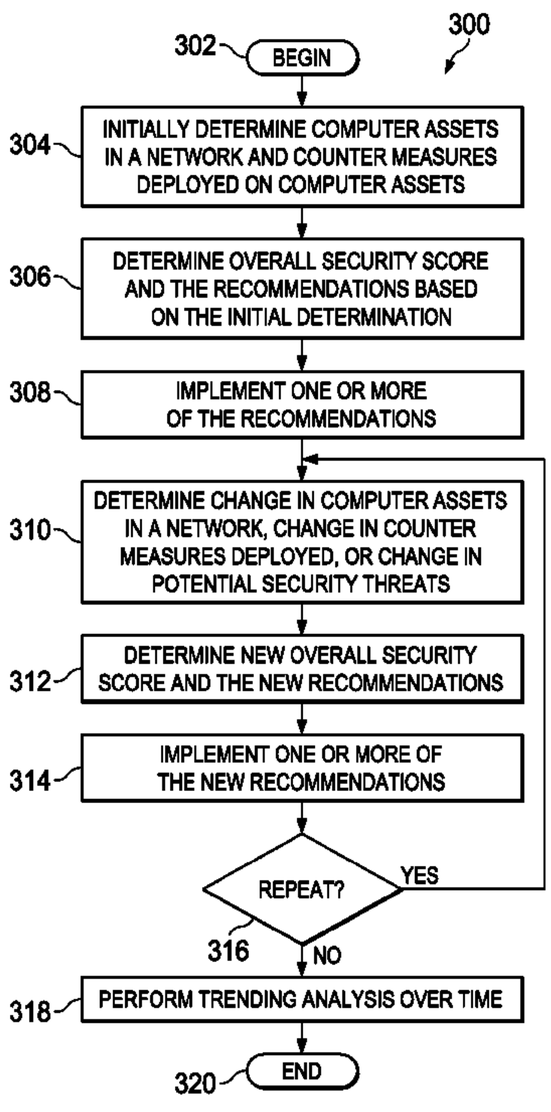
* cited by examiner

*Primary Examiner* — Dao Ho
(74) *Attorney, Agent, or Firm* — MH2 Technology Law Group, LLP

(57) **ABSTRACT**

A security assessment tool can determine computer assets in a network and provide an overall security score for the network. The overall security score can represent an objective measure of the security of the network that considers potential security threats to the computer assets, counter measures deployed in the network to address the potential security threats, and the effectiveness of the counter measures. Based on the overall security assessment, the security assessment tool can provide recommendations for improving the security of the network.

**39 Claims, 26 Drawing Sheets**



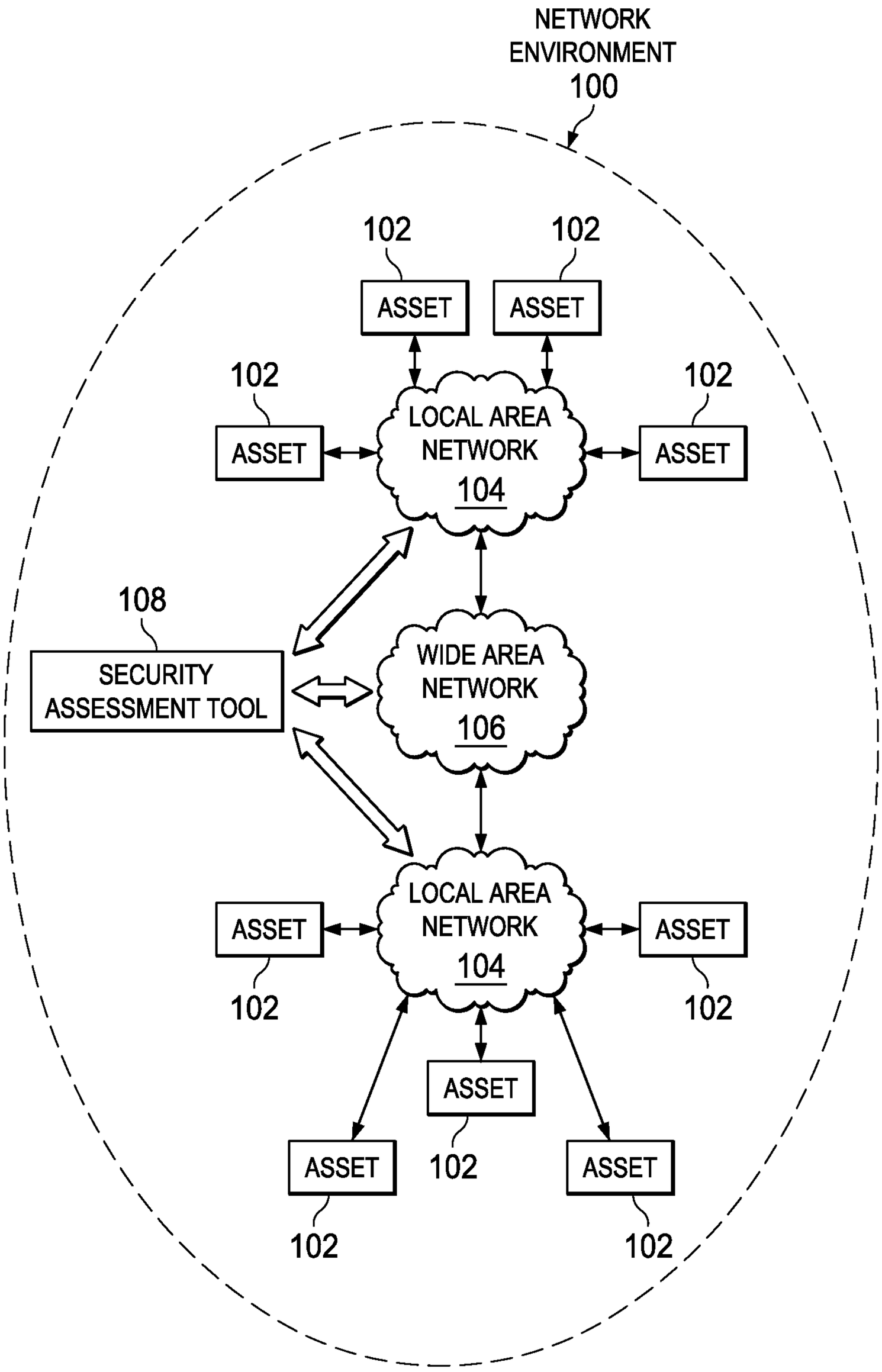

NETWORK ENVIRONMENT
100
102
ASSET
LOCAL AREA NETWORK
104
108
SECURITY ASSESSMENT TOOL
WIDE AREA NETWORK
106

FIG. 1A

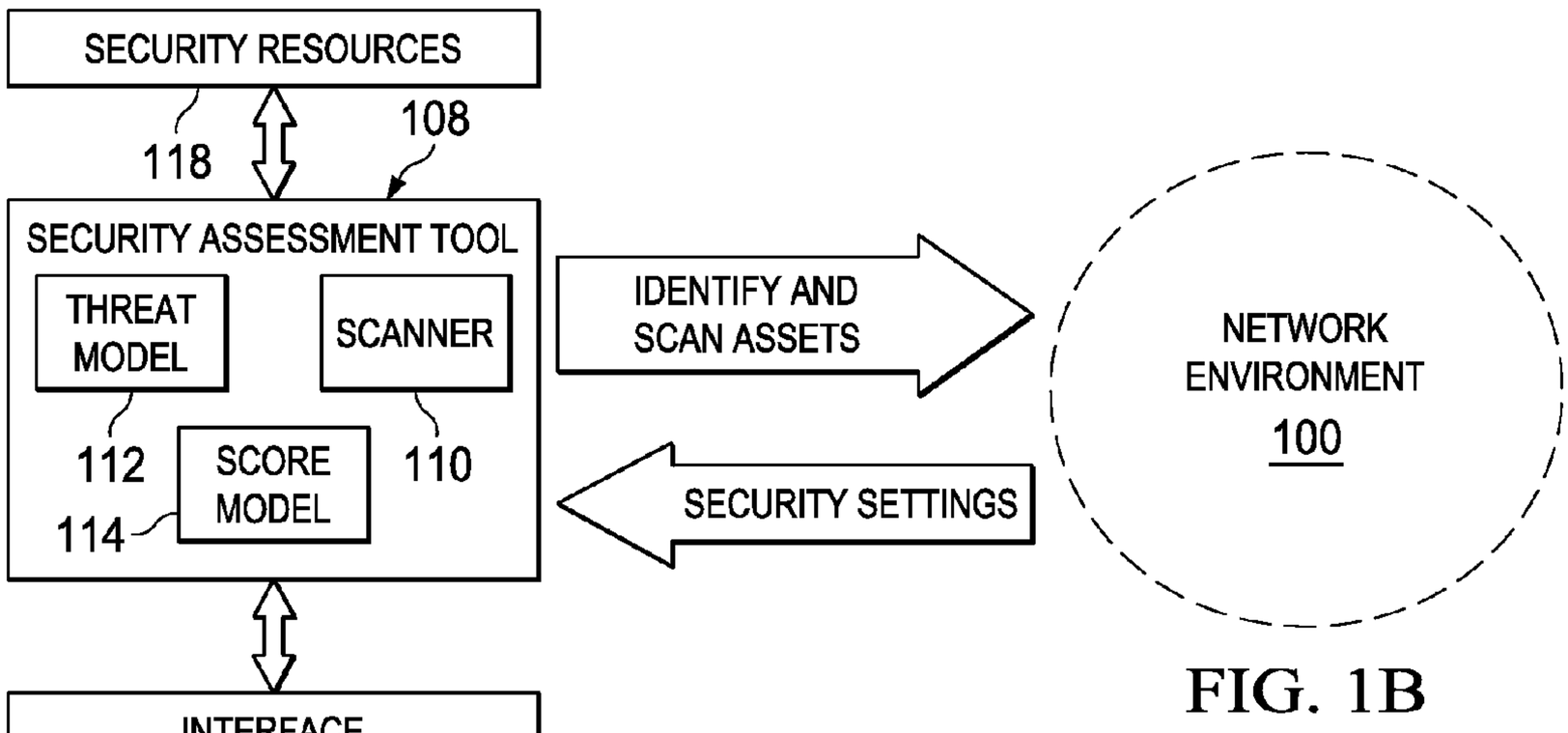

SECURITY RESOURCES
118
108
SECURITY ASSESSMENT TOOL
THREAT MODEL
SCANNER
112
SCORE MODEL
110
114
INTERFACE
116
IDENTIFY AND SCAN ASSETS
SECURITY SETTINGS
NETWORK ENVIRONMENT
100

FIG. 1B

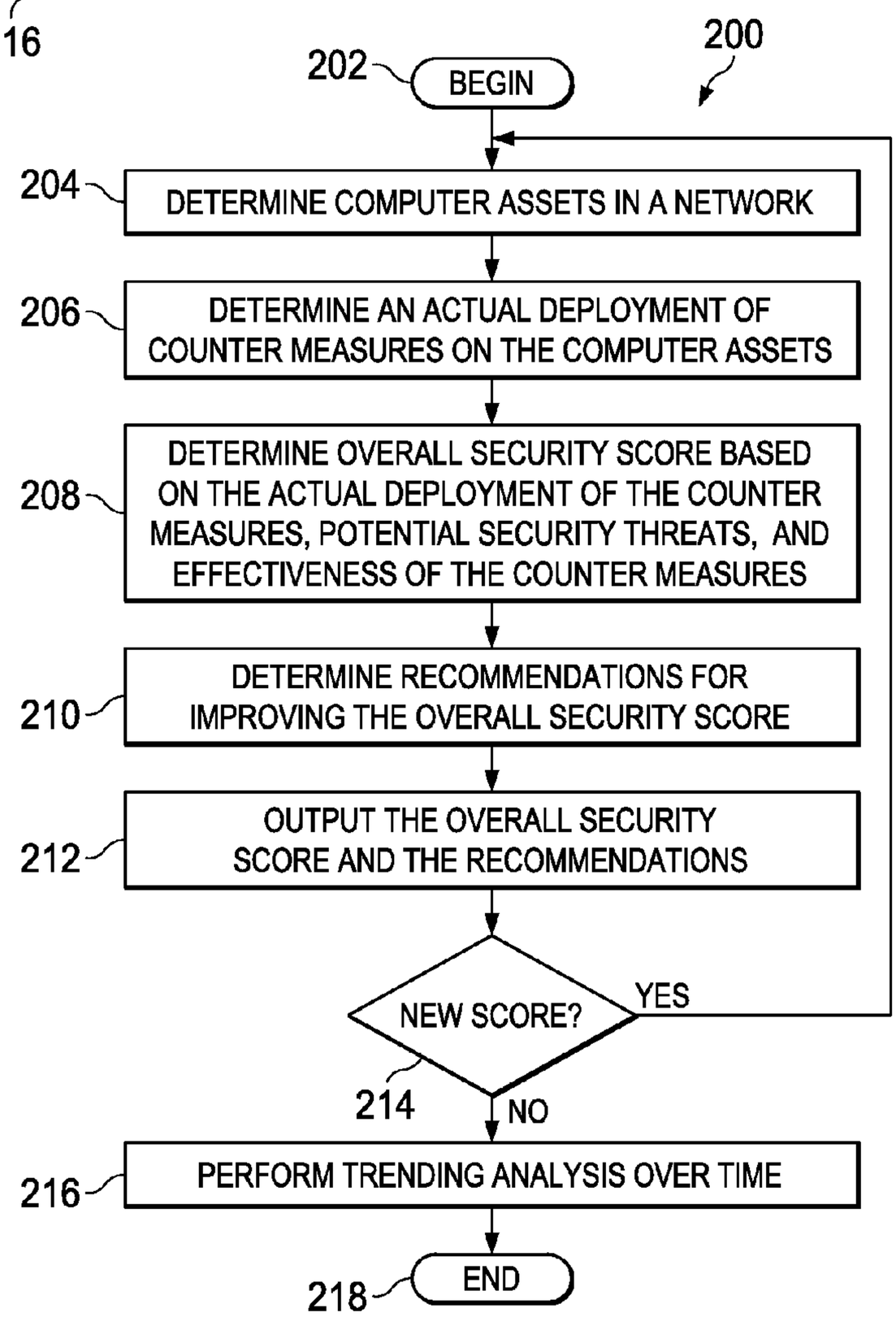

200
202
BEGIN
204
DETERMINE COMPUTER ASSETS IN A NETWORK
206
DETERMINE AN ACTUAL DEPLOYMENT OF COUNTER MEASURES ON THE COMPUTER ASSETS
208
DETERMINE OVERALL SECURITY SCORE BASED ON THE ACTUAL DEPLOYMENT OF THE COUNTER MEASURES, POTENTIAL SECURITY THREATS, AND EFFECTIVENESS OF THE COUNTER MEASURES
210
DETERMINE RECOMMENDATIONS FOR IMPROVING THE OVERALL SECURITY SCORE
212
OUTPUT THE OVERALL SECURITY SCORE AND THE RECOMMENDATIONS
NEW SCORE?
YES
214
NO
216
PERFORM TRENDING ANALYSIS OVER TIME
218
END

FIG. 2

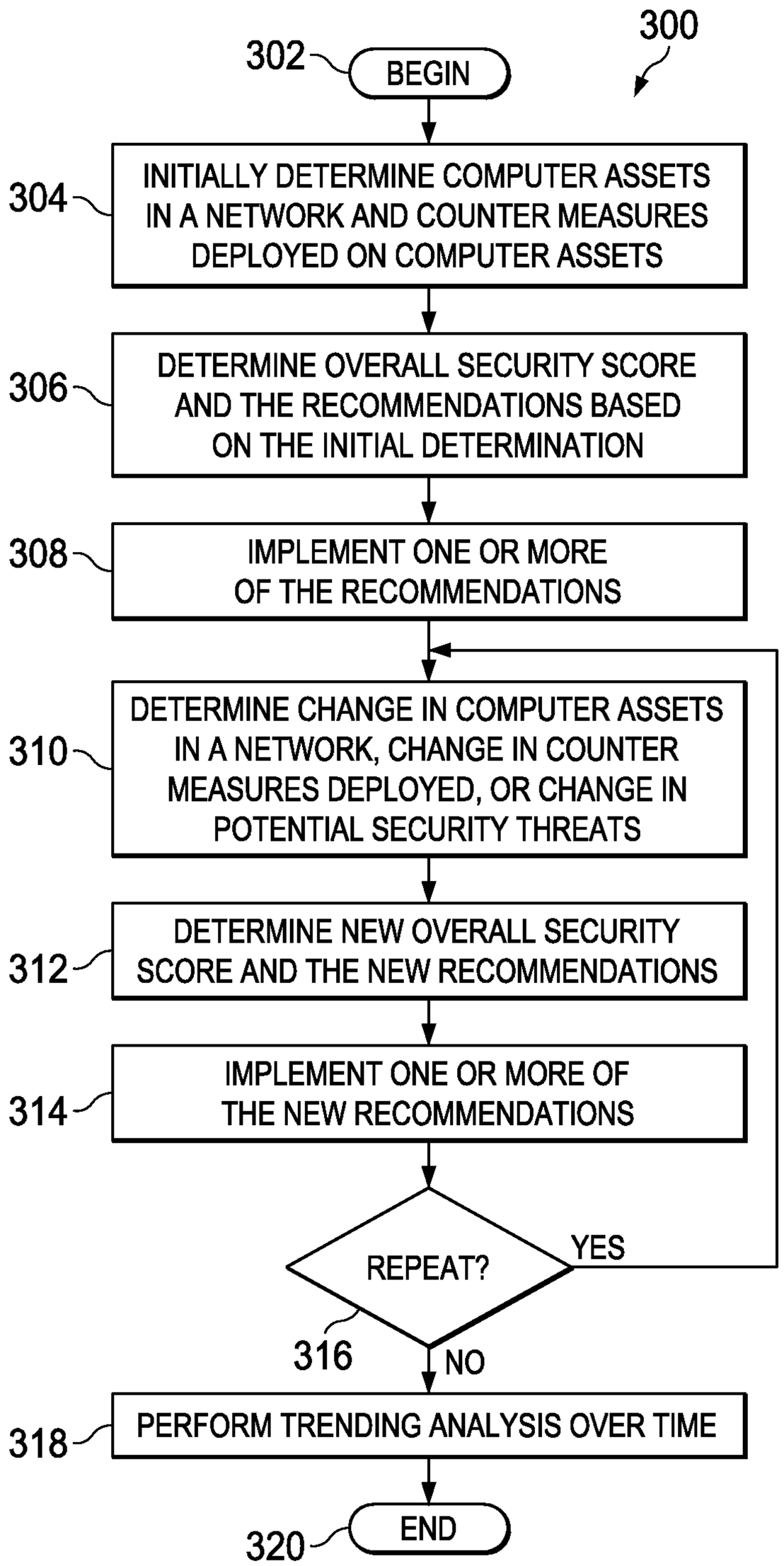

300
302
BEGIN
304
INITIALLY DETERMINE COMPUTER ASSETS IN A NETWORK AND COUNTER MEASURES DEPLOYED ON COMPUTER ASSETS
306
DETERMINE OVERALL SECURITY SCORE AND THE RECOMMENDATIONS BASED ON THE INITIAL DETERMINATION
308
IMPLEMENT ONE OR MORE OF THE RECOMMENDATIONS
310
DETERMINE CHANGE IN COMPUTER ASSETS IN A NETWORK, CHANGE IN COUNTER MEASURES DEPLOYED, OR CHANGE IN POTENTIAL SECURITY THREATS
312
DETERMINE NEW OVERALL SECURITY SCORE AND THE NEW RECOMMENDATIONS
314
IMPLEMENT ONE OR MORE OF THE NEW RECOMMENDATIONS
REPEAT?
YES
316
NO
318
PERFORM TRENDING ANALYSIS OVER TIME
320
END

FIG. 3

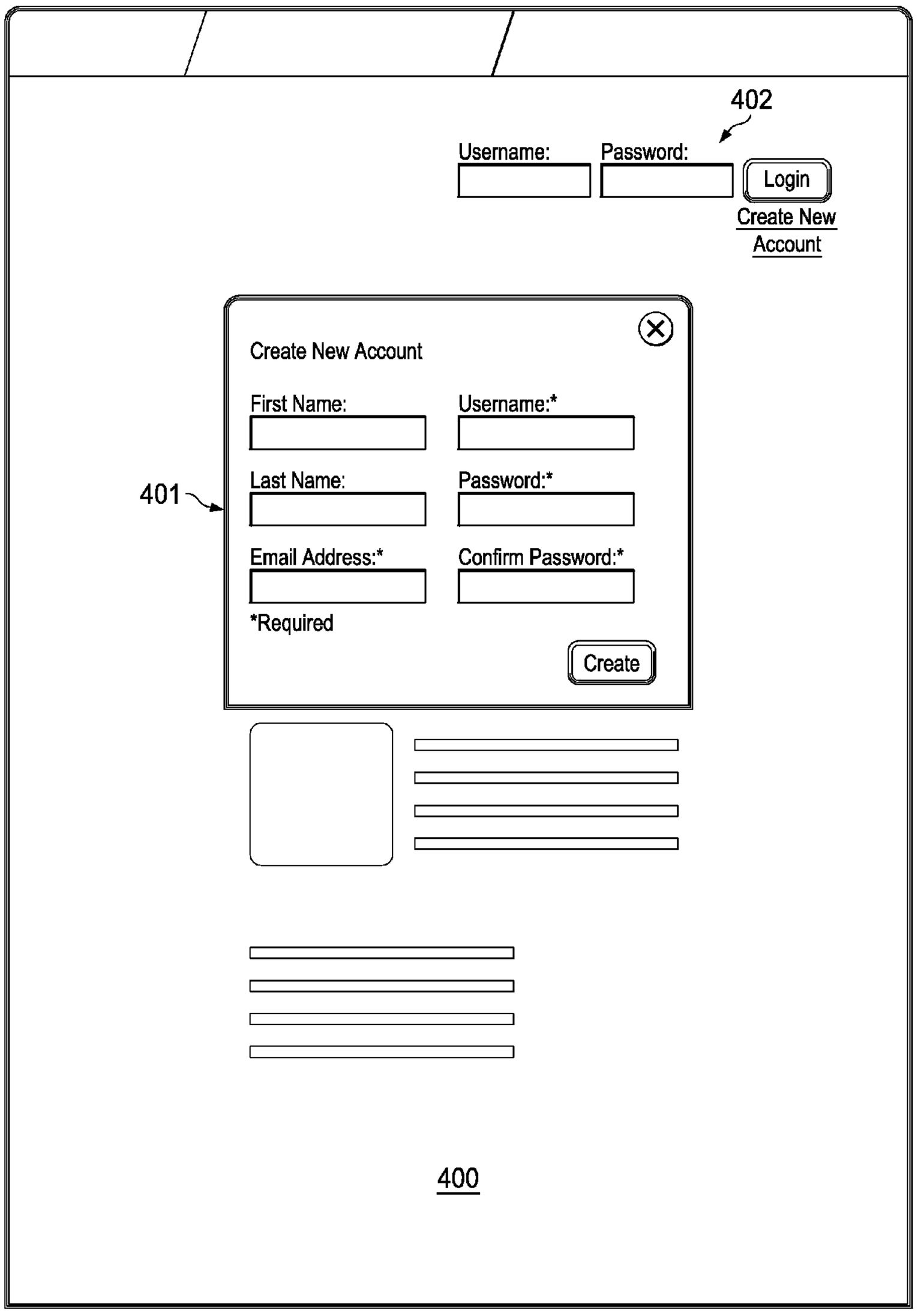

402
Username:
Password:
Login
Create New Account
401
Create New Account
First Name:
Username:*
Last Name:
Password:*
Email Address:*
Confirm Password:*
*Required
Create
400

FIG. 4A

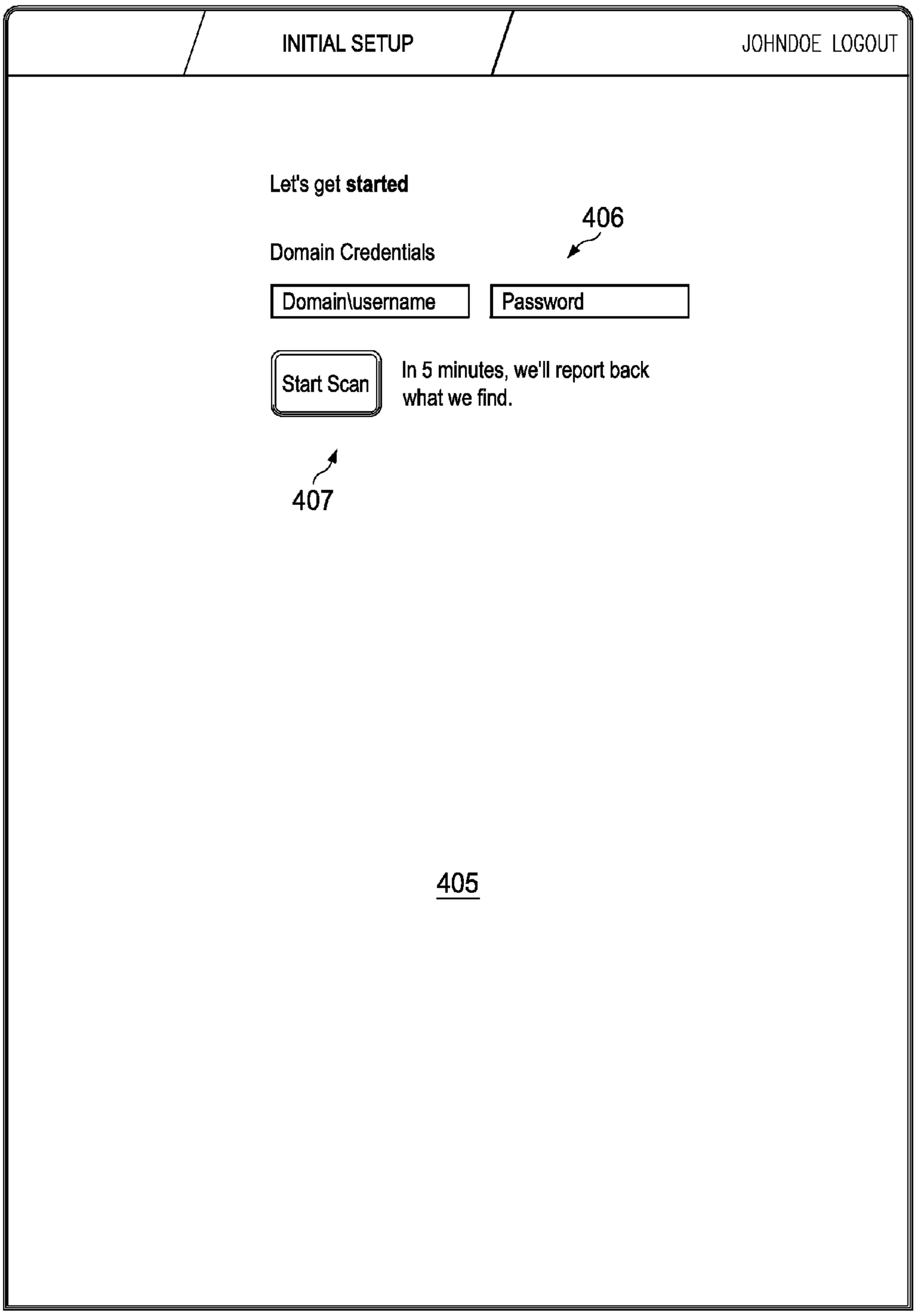

INITIAL SETUP
JOHNDOE LOGOUT
Let's get started
406
Domain Credentials
Domain\username
Password
Start Scan
In 5 minutes, we'll report back what we find.
407
405

FIG. 4B

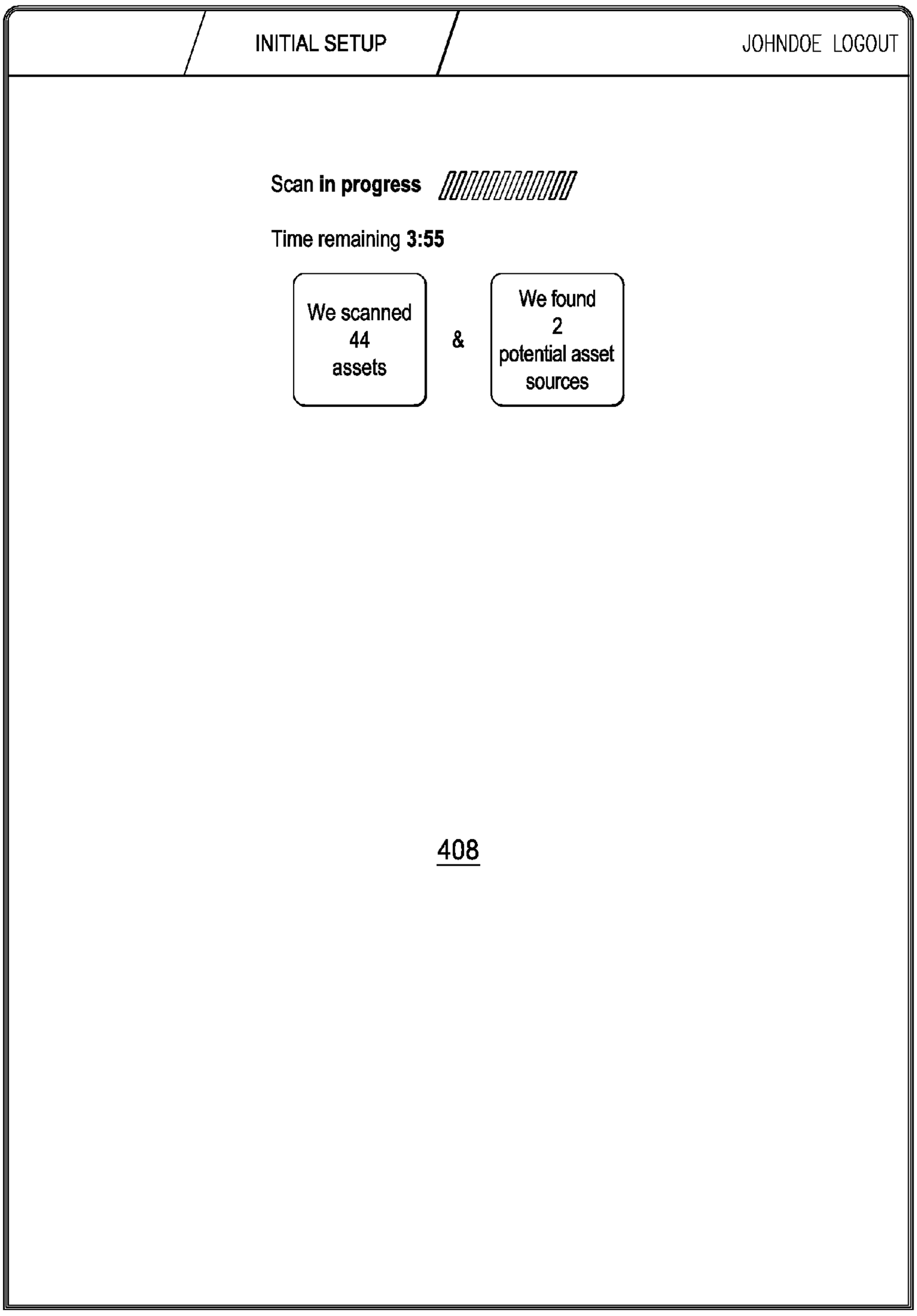

INITIAL SETUP
JOHNDOE LOGOUT
Scan in progress
Time remaining 3:55
We scanned 44 assets
&
We found 2 potential asset sources
408

FIG. 4C

FIG. 4D

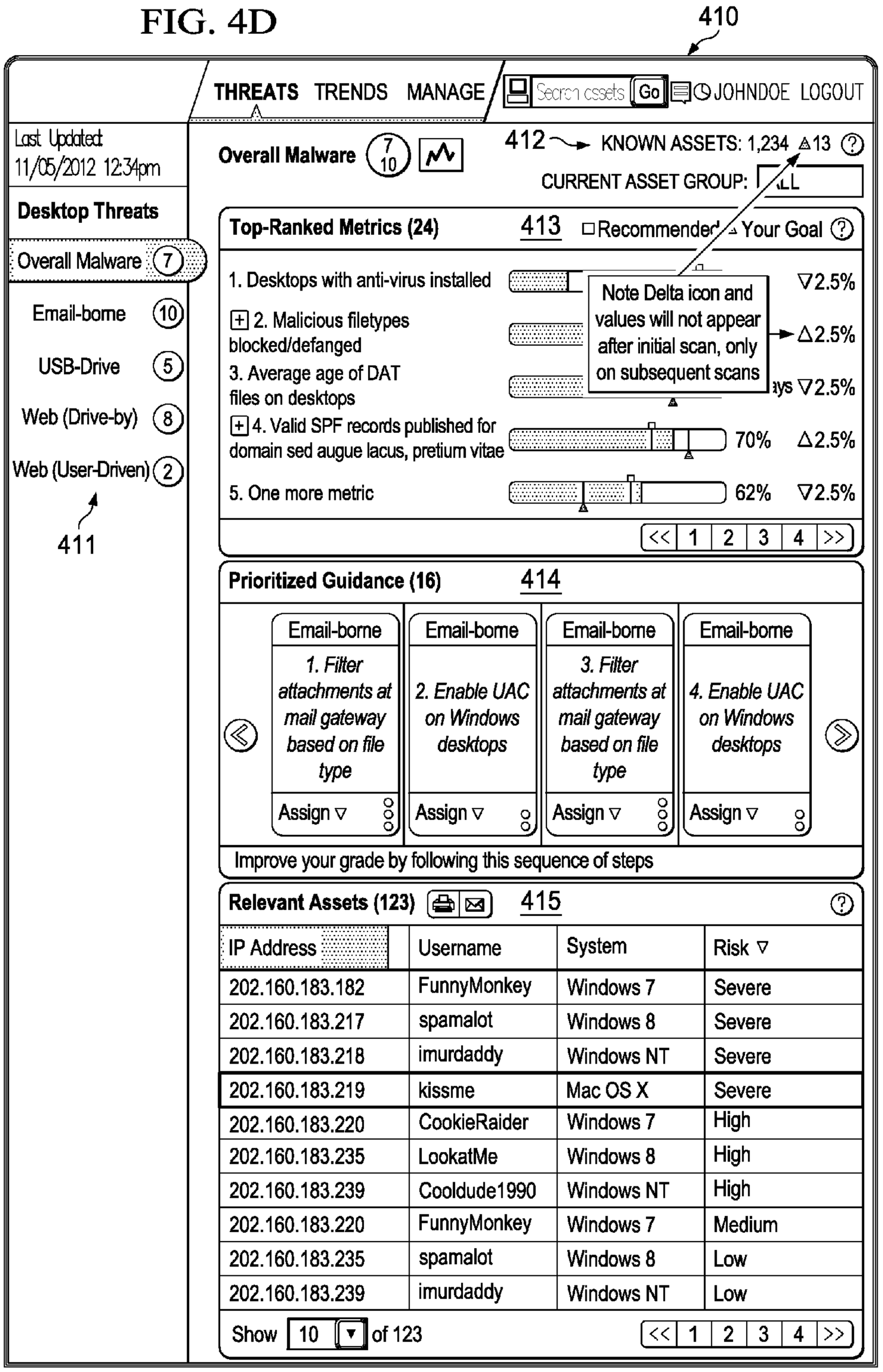

410
THREATS TRENDS MANAGE
Search assets Go
JOHNDOE LOGOUT
Last Updated: 11/05/2012 12:34pm
Overall Malware 7/10
412
KNOWN ASSETS: 1,234 13
CURRENT ASSET GROUP: ALL
Desktop Threats
Overall Malware 7
Email-borne 10
USB-Drive 5
Web (Drive-by) 8
Web (User-Driven) 2
411
Top-Ranked Metrics (24)
413
Recommended
Your Goal
1. Desktops with anti-virus installed
2. Malicious filetypes blocked/defanged
3. Average age of DAT files on desktops
4. Valid SPF records published for domain sed augue lacus, pretium vitae
5. One more metric
70%
62%
Note Delta icon and values will not appear after initial scan, only on subsequent scans
▽2.5%
△2.5%
▽2.5%
△2.5%
▽2.5%
<< 1 2 3 4 >>
Prioritized Guidance (16)
414
Email-borne
1. Filter attachments at mail gateway based on file type
2. Enable UAC on Windows desktops
3. Filter attachments at mail gateway based on file type
4. Enable UAC on Windows desktops
Assign
Improve your grade by following this sequence of steps
Relevant Assets (123)
415
IP Address
Username
System
Risk
202.160.183.182 FunnyMonkey Windows 7 Severe
202.160.183.217 spamalot Windows 8 Severe
202.160.183.218 imurdaddy Windows NT Severe
202.160.183.219 kissme Mac OS X Severe
202.160.183.220 CookieRaider Windows 7 High
202.160.183.235 LookatMe Windows 8 High
202.160.183.239 Cooldude1990 Windows NT High
202.160.183.220 FunnyMonkey Windows 7 Medium
202.160.183.235 spamalot Windows 8 Low
202.160.183.239 imurdaddy Windows NT Low
Show 10 of 123
<< 1 2 3 4 >>

FIG. 4E

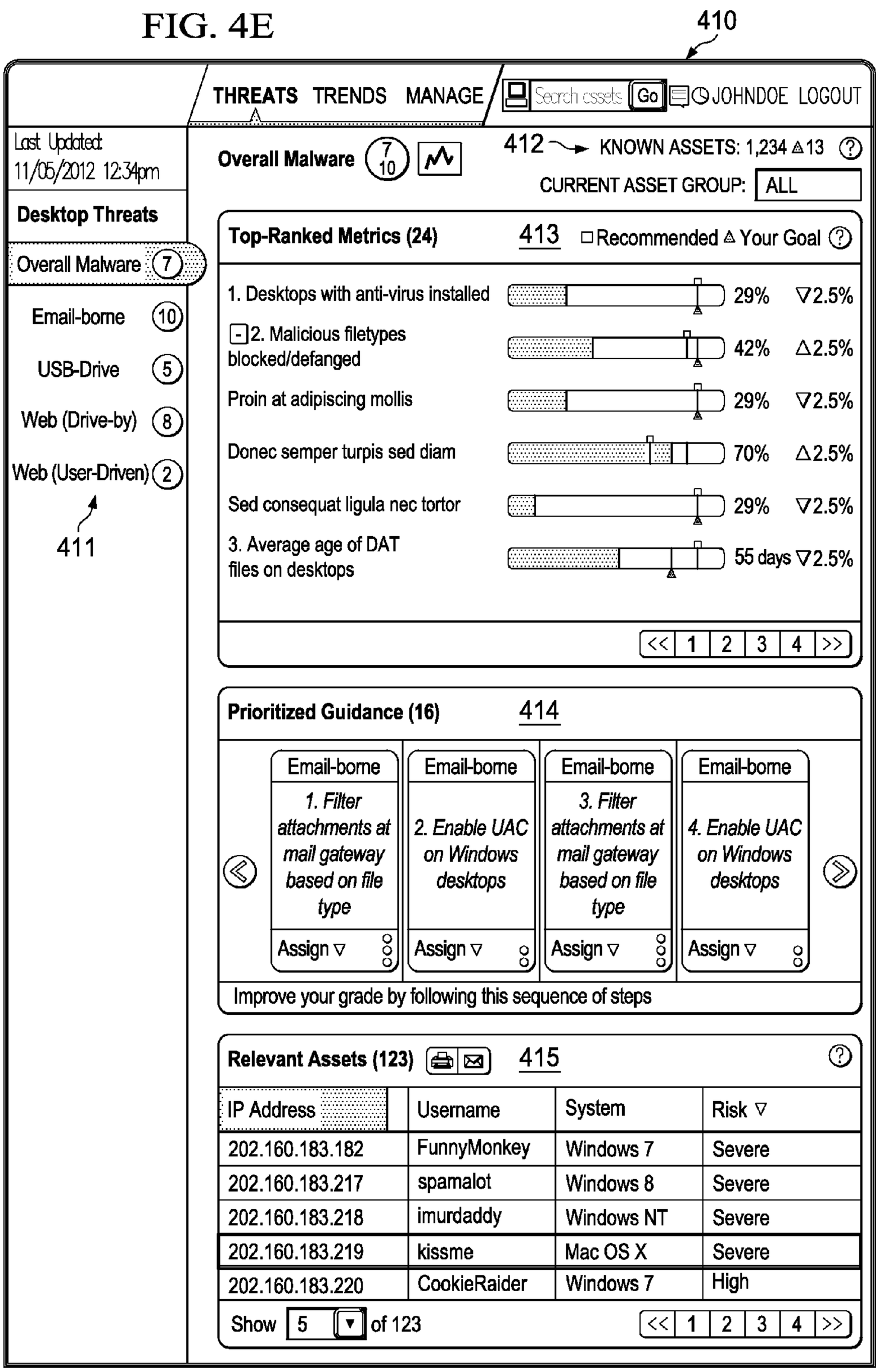

410
THREATS TRENDS MANAGE
Search assets Go JOHNDOE LOGOUT
Last Updated: 11/05/2012 12:34pm
Desktop Threats
Overall Malware 7
Email-borne 10
USB-Drive 5
Web (Drive-by) 8
Web (User-Driven) 2
411
Overall Malware 7/10
412
KNOWN ASSETS: 1,234 △13
CURRENT ASSET GROUP: ALL
Top-Ranked Metrics (24)
413
□Recommended △Your Goal
1. Desktops with anti-virus installed 29% ▽2.5%
-2. Malicious filetypes blocked/defanged 42% △2.5%
Proin at adipiscing mollis 29% ▽2.5%
Donec semper turpis sed diam 70% △2.5%
Sed consequat ligula nec tortor 29% ▽2.5%
3. Average age of DAT files on desktops 55 days ▽2.5%
<< 1 2 3 4 >>
Prioritized Guidance (16)
414
Email-borne
1. Filter attachments at mail gateway based on file type
Assign ▽
Email-borne
2. Enable UAC on Windows desktops
Assign ▽
Email-borne
3. Filter attachments at mail gateway based on file type
Assign ▽
Email-borne
4. Enable UAC on Windows desktops
Assign ▽
Improve your grade by following this sequence of steps
Relevant Assets (123)
415
IP Address | Username | System | Risk ▽
202.160.183.182 | FunnyMonkey | Windows 7 | Severe
202.160.183.217 | spamalot | Windows 8 | Severe
202.160.183.218 | imurdaddy | Windows NT | Severe
202.160.183.219 | kissme | Mac OS X | Severe
202.160.183.220 | CookieRaider | Windows 7 | High
Show 5 of 123
<< 1 2 3 4 >>

FIG. 4F

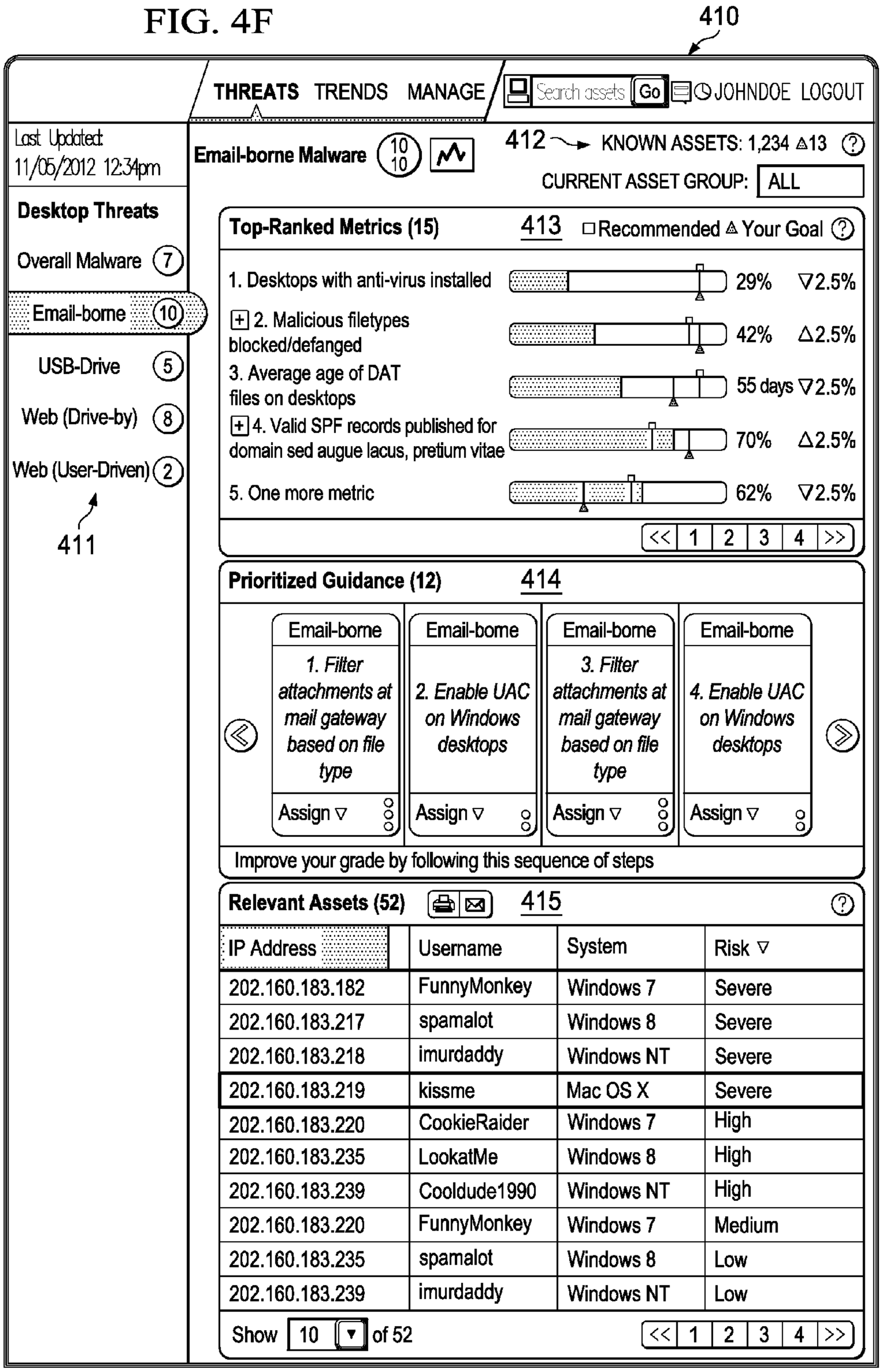

410
THREATS TRENDS MANAGE
Search assets Go JOHNDOE LOGOUT
Last Updated: 11/05/2012 12:34pm
Email-borne Malware 10 10
412
KNOWN ASSETS: 1,234 △13
CURRENT ASSET GROUP: ALL
Desktop Threats
Overall Malware 7
Email-borne 10
USB-Drive 5
Web (Drive-by) 8
Web (User-Driven) 2
411
Top-Ranked Metrics (15) 413
□Recommended △Your Goal
1. Desktops with anti-virus installed 29% ▽2.5%
2. Malicious filetypes blocked/defanged 42% △2.5%
3. Average age of DAT files on desktops 55 days ▽2.5%
4. Valid SPF records published for domain sed augue lacus, pretium vitae 70% △2.5%
5. One more metric 62% ▽2.5%
<< 1 2 3 4 >>
Prioritized Guidance (12) 414
Email-borne 1. Filter attachments at mail gateway based on file type Assign ▽
Email-borne 2. Enable UAC on Windows desktops Assign ▽
Email-borne 3. Filter attachments at mail gateway based on file type Assign ▽
Email-borne 4. Enable UAC on Windows desktops Assign ▽
Improve your grade by following this sequence of steps
Relevant Assets (52) 415
IP Address | Username | System | Risk ▽
202.160.183.182 | FunnyMonkey | Windows 7 | Severe
202.160.183.217 | spamalot | Windows 8 | Severe
202.160.183.218 | imurdaddy | Windows NT | Severe
202.160.183.219 | kissme | Mac OS X | Severe
202.160.183.220 | CookieRaider | Windows 7 | High
202.160.183.235 | LookatMe | Windows 8 | High
202.160.183.239 | Cooldude1990 | Windows NT | High
202.160.183.220 | FunnyMonkey | Windows 7 | Medium
202.160.183.235 | spamalot | Windows 8 | Low
202.160.183.239 | imurdaddy | Windows NT | Low
Show 10 of 52
<< 1 2 3 4 >>

FIG. 4G

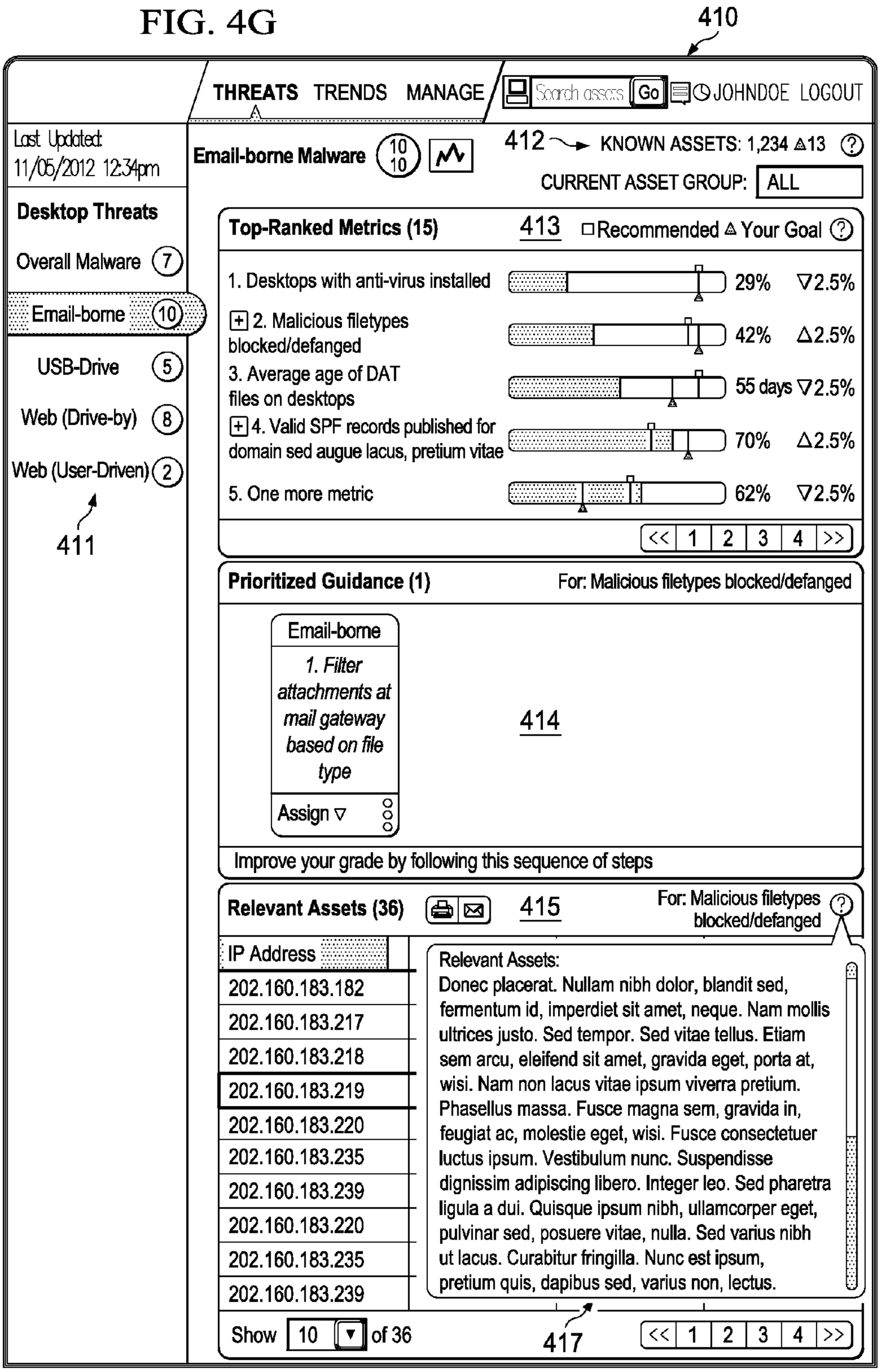

410
THREATS TRENDS MANAGE
Search assets Go
JOHNDOE LOGOUT
Last Updated: 11/05/2012 12:34pm
Email-borne Malware 10 10
412
KNOWN ASSETS: 1,234 △13
CURRENT ASSET GROUP: ALL
Desktop Threats
Overall Malware 7
Email-borne 10
USB-Drive 5
Web (Drive-by) 8
Web (User-Driven) 2
411
Top-Ranked Metrics (15)
413
□Recommended △Your Goal
1. Desktops with anti-virus installed 29% ▽2.5%
2. Malicious filetypes blocked/defanged 42% △2.5%
3. Average age of DAT files on desktops 55 days ▽2.5%
4. Valid SPF records published for domain sed augue lacus, pretium vitae 70% △2.5%
5. One more metric 62% ▽2.5%
<< 1 2 3 4 >>
Prioritized Guidance (1)
For: Malicious filetypes blocked/defanged
Email-borne
1. Filter attachments at mail gateway based on file type
Assign ▽
414
Improve your grade by following this sequence of steps
Relevant Assets (36)
415
For: Malicious filetypes blocked/defanged
IP Address
202.160.183.182
202.160.183.217
202.160.183.218
202.160.183.219
202.160.183.220
202.160.183.235
202.160.183.239
202.160.183.220
202.160.183.235
202.160.183.239
Relevant Assets:
Donec placerat. Nullam nibh dolor, blandit sed, fermentum id, imperdiet sit amet, neque. Nam mollis ultrices justo. Sed tempor. Sed vitae tellus. Etiam sem arcu, eleifend sit amet, gravida eget, porta at, wisi. Nam non lacus vitae ipsum viverra pretium. Phasellus massa. Fusce magna sem, gravida in, feugiat ac, molestie eget, wisi. Fusce consectetuer luctus ipsum. Vestibulum nunc. Suspendisse dignissim adipiscing libero. Integer leo. Sed pharetra ligula a dui. Quisque ipsum nibh, ullamcorper eget, pulvinar sed, posuere vitae, nulla. Sed varius nibh ut lacus. Curabitur fringilla. Nunc est ipsum, pretium quis, dapibus sed, varius non, lectus.
417
Show 10 of 36
<< 1 2 3 4 >>

FIG. 4H

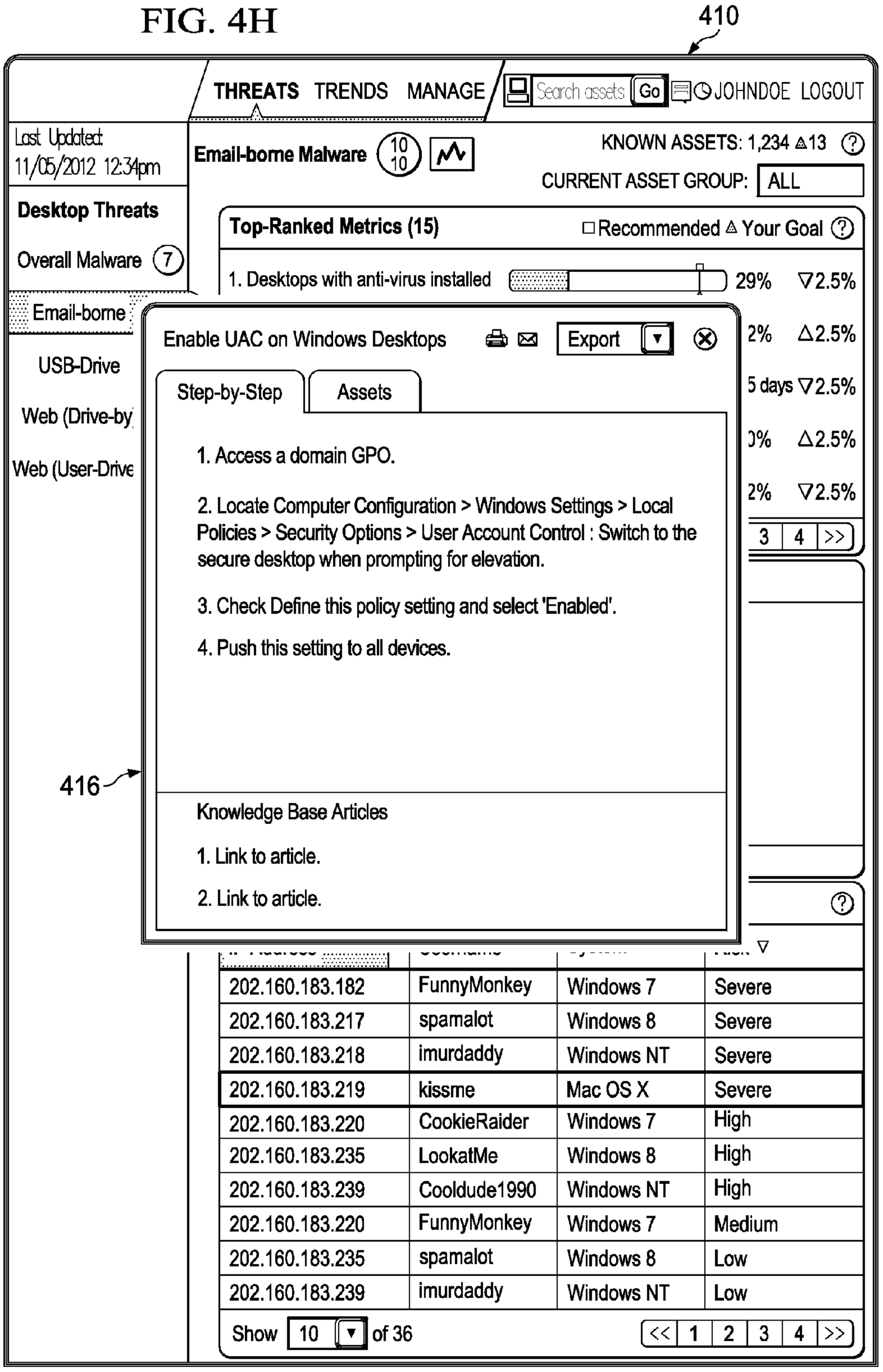

410
THREATS TRENDS MANAGE
Search assets Go
JOHNDOE LOGOUT
Last Updated: 11/05/2012 12:34pm
Email-borne Malware 10 10
KNOWN ASSETS: 1,234 △13
CURRENT ASSET GROUP: ALL
Desktop Threats
Overall Malware 7
Top-Ranked Metrics (15)
□ Recommended △ Your Goal
1. Desktops with anti-virus installed 29% ▽2.5%
Email-borne
USB-Drive
Web (Drive-by
Web (User-Drive
Enable UAC on Windows Desktops
Export
Step-by-Step
Assets
1. Access a domain GPO.
2. Locate Computer Configuration > Windows Settings > Local Policies > Security Options > User Account Control : Switch to the secure desktop when prompting for elevation.
3. Check Define this policy setting and select 'Enabled'.
4. Push this setting to all devices.
416
Knowledge Base Articles
1. Link to article.
2. Link to article.
2% △2.5%
5 days ▽2.5%
0% △2.5%
2% ▽2.5%
3 4 >>
202.160.183.182 FunnyMonkey Windows 7 Severe
202.160.183.217 spamalot Windows 8 Severe
202.160.183.218 imurdaddy Windows NT Severe
202.160.183.219 kissme Mac OS X Severe
202.160.183.220 CookieRaider Windows 7 High
202.160.183.235 LookatMe Windows 8 High
202.160.183.239 Cooldude1990 Windows NT High
202.160.183.220 FunnyMonkey Windows 7 Medium
202.160.183.235 spamalot Windows 8 Low
202.160.183.239 imurdaddy Windows NT Low
Show 10 of 36
<< 1 2 3 4 >>

FIG. 4I

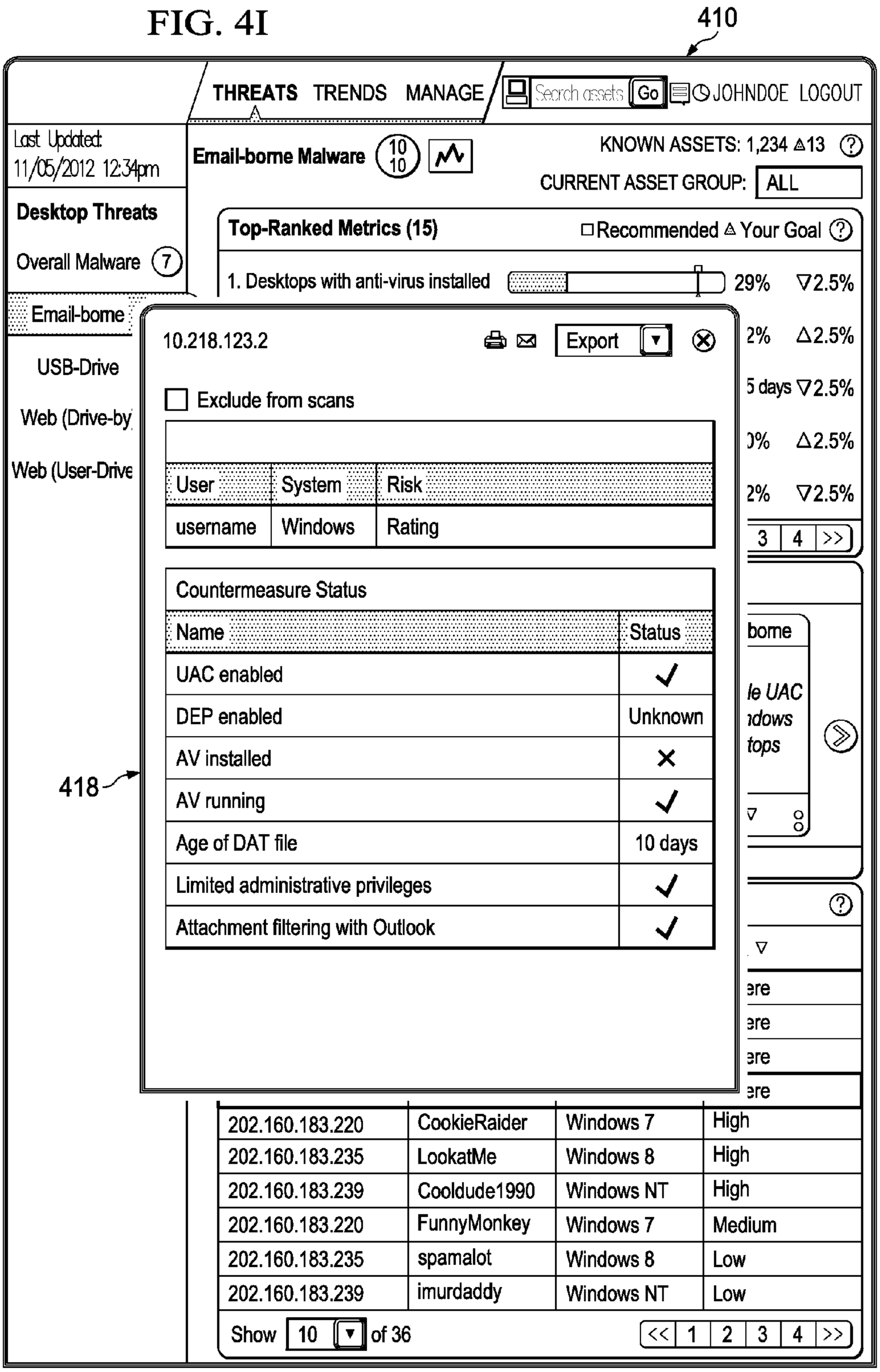

410
THREATS TRENDS MANAGE
Search assets Go JOHNDOE LOGOUT
Last Updated: 11/05/2012 12:34pm
Email-borne Malware 10 10
KNOWN ASSETS: 1,234 △13
CURRENT ASSET GROUP: ALL
Desktop Threats
Overall Malware 7
Top-Ranked Metrics (15)
□Recommended △Your Goal
1. Desktops with anti-virus installed 29% ▽2.5%
Email-borne
USB-Drive
Web (Drive-by
Web (User-Drive
10.218.123.2
Export
Exclude from scans
User System Risk
username Windows Rating
Countermeasure Status
Name Status
UAC enabled ✓
DEP enabled Unknown
AV installed ✗
AV running ✓
Age of DAT file 10 days
Limited administrative privileges ✓
Attachment filtering with Outlook ✓
418
2% △2.5%
5 days ▽2.5%
0% △2.5%
2% ▽2.5%
3 4 >>
202.160.183.220 CookieRaider Windows 7 High
202.160.183.235 LookatMe Windows 8 High
202.160.183.239 Cooldude1990 Windows NT High
202.160.183.220 FunnyMonkey Windows 7 Medium
202.160.183.235 spamalot Windows 8 Low
202.160.183.239 imurdaddy Windows NT Low
Show 10 of 36
<< 1 2 3 4 >>

FIG. 4J

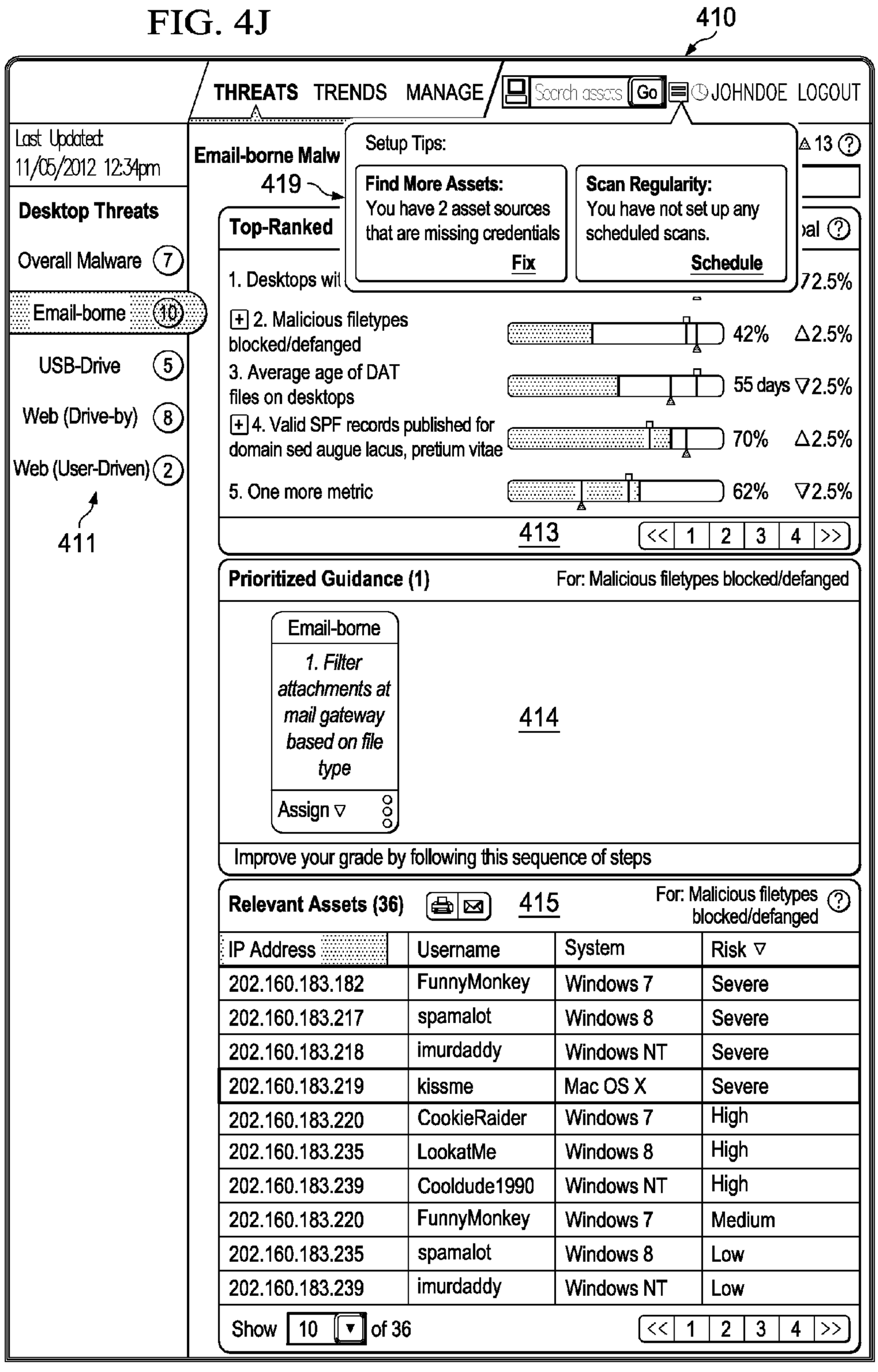

410
THREATS TRENDS MANAGE
Search assets Go
JOHNDOE LOGOUT
Last Updated: 11/05/2012 12:34pm
Desktop Threats
Overall Malware 7
Email-borne 10
USB-Drive 5
Web (Drive-by) 8
Web (User-Driven) 2
411
Email-borne Malw
419
Setup Tips:
Find More Assets: You have 2 asset sources that are missing credentials Fix
Scan Regularity: You have not set up any scheduled scans. Schedule
13
Top-Ranked
1. Desktops wit
72.5%
2. Malicious filetypes blocked/defanged 42% Δ2.5%
3. Average age of DAT files on desktops 55 days ∇2.5%
4. Valid SPF records published for domain sed augue lacus, pretium vitae 70% Δ2.5%
5. One more metric 62% ∇2.5%
413
<< 1 2 3 4 >>
Prioritized Guidance (1)
For: Malicious filetypes blocked/defanged
Email-borne
1. Filter attachments at mail gateway based on file type
Assign ∇
414
Improve your grade by following this sequence of steps
Relevant Assets (36)
415
For: Malicious filetypes blocked/defanged
IP Address | Username | System | Risk ∇
202.160.183.182 | FunnyMonkey | Windows 7 | Severe
202.160.183.217 | spamalot | Windows 8 | Severe
202.160.183.218 | imurdaddy | Windows NT | Severe
202.160.183.219 | kissme | Mac OS X | Severe
202.160.183.220 | CookieRaider | Windows 7 | High
202.160.183.235 | LookatMe | Windows 8 | High
202.160.183.239 | Cooldude1990 | Windows NT | High
202.160.183.220 | FunnyMonkey | Windows 7 | Medium
202.160.183.235 | spamalot | Windows 8 | Low
202.160.183.239 | imurdaddy | Windows NT | Low
Show 10 of 36
<< 1 2 3 4 >>

FIG. 4K

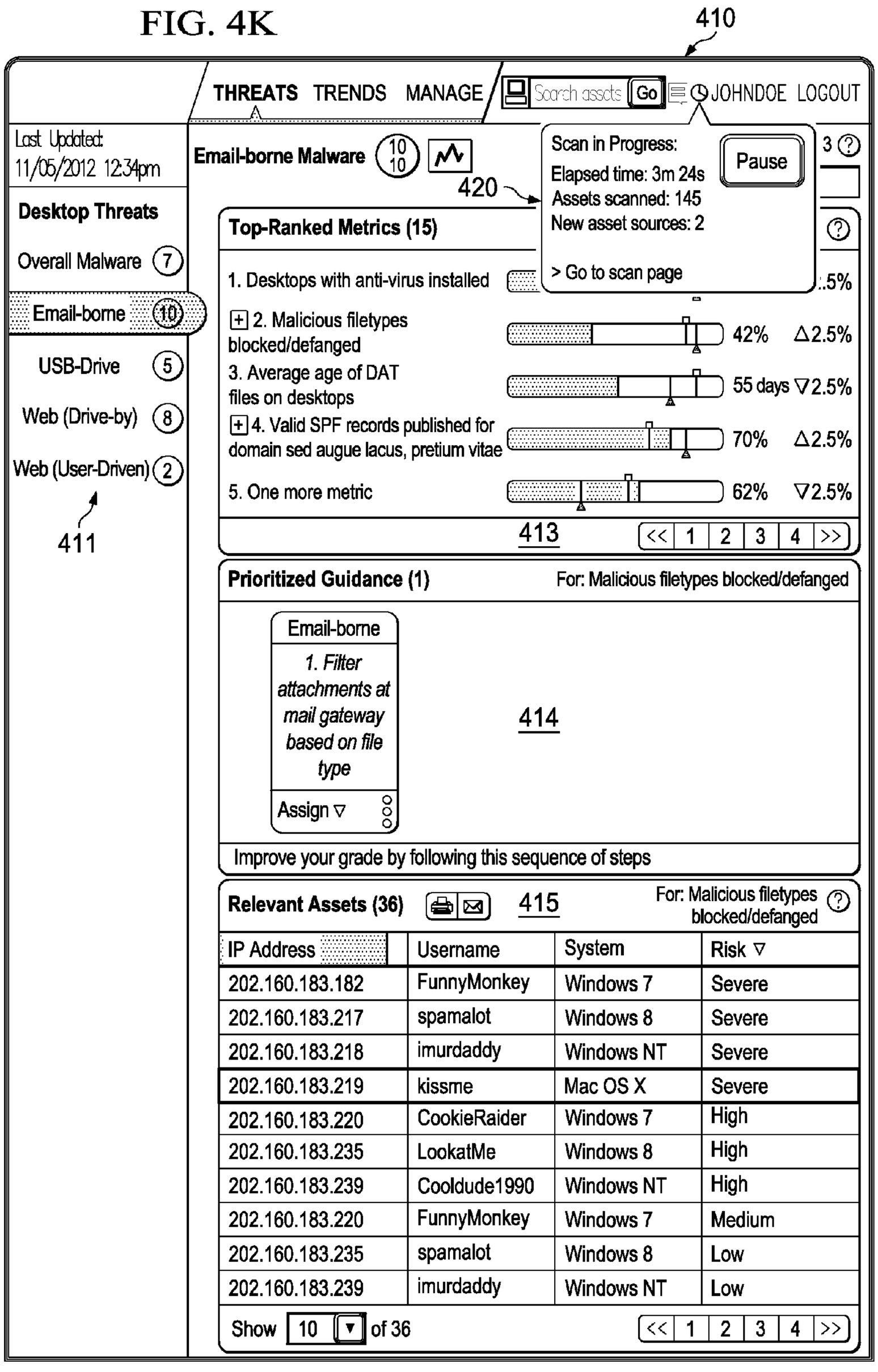
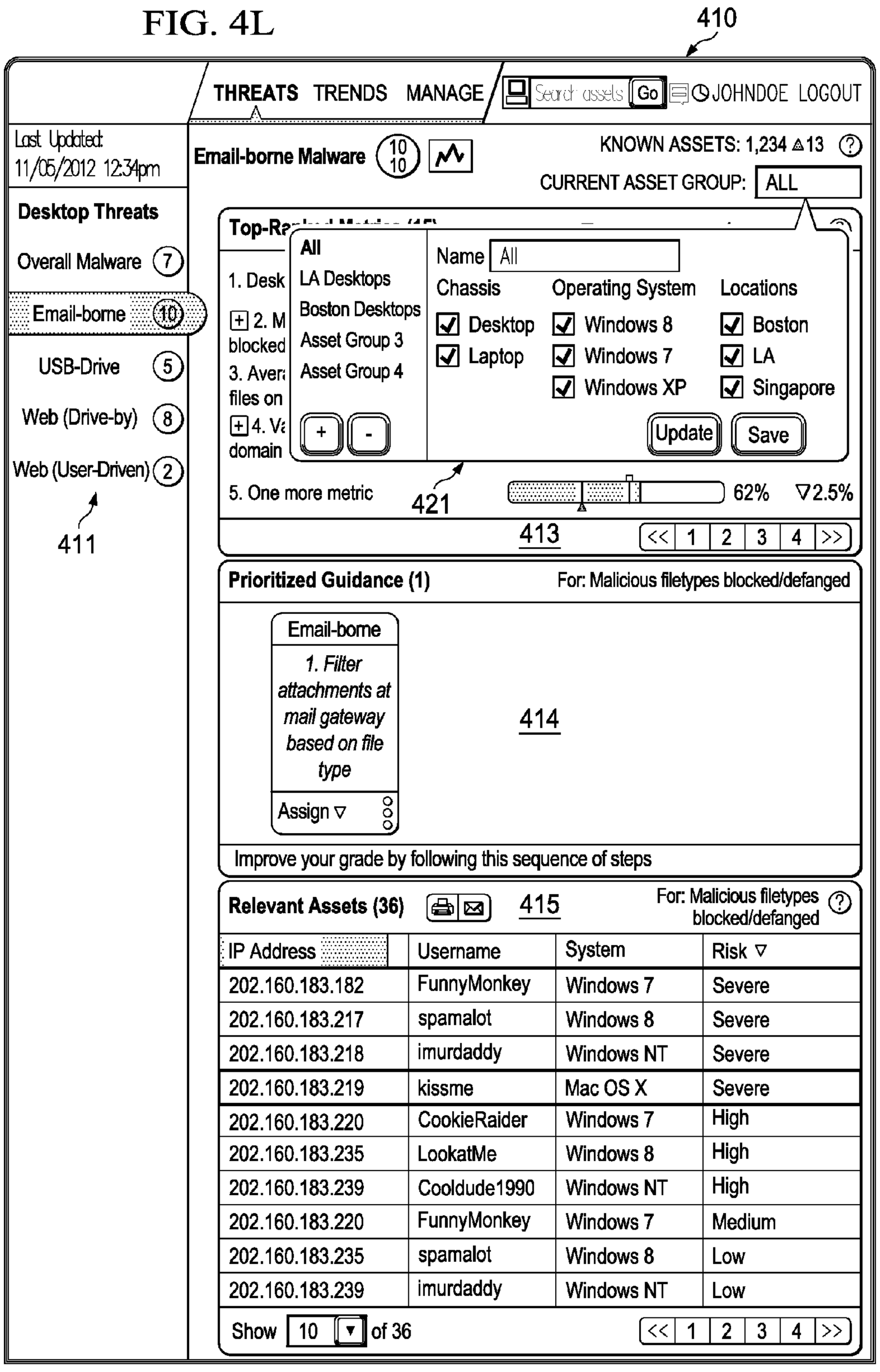

410
THREATS TRENDS MANAGE
Search assets Go
JOHNDOE LOGOUT
Last Updated: 11/05/2012 12:34pm
Email-borne Malware 10 10
420
Scan in Progress:
Elapsed time: 3m 24s
Assets scanned: 145
New asset sources: 2
> Go to scan page
Pause
3
Desktop Threats
Overall Malware 7
Email-borne 10
USB-Drive 5
Web (Drive-by) 8
Web (User-Driven) 2
411
Top-Ranked Metrics (15)
1. Desktops with anti-virus installed
2. Malicious filetypes blocked/defanged 42% Δ2.5%
3. Average age of DAT files on desktops 55 days ∇2.5%
4. Valid SPF records published for domain sed augue lacus, pretium vitae 70% Δ2.5%
5. One more metric 62% ∇2.5%
413
<< 1 2 3 4 >>
Prioritized Guidance (1)
For: Malicious filetypes blocked/defanged
Email-borne
1. Filter attachments at mail gateway based on file type
Assign ∇
414
Improve your grade by following this sequence of steps
Relevant Assets (36)
415
For: Malicious filetypes blocked/defanged
IP Address | Username | System | Risk ∇
202.160.183.182 | FunnyMonkey | Windows 7 | Severe
202.160.183.217 | spamalot | Windows 8 | Severe
202.160.183.218 | imurdaddy | Windows NT | Severe
202.160.183.219 | kissme | Mac OS X | Severe
202.160.183.220 | CookieRaider | Windows 7 | High
202.160.183.235 | LookatMe | Windows 8 | High
202.160.183.239 | Cooldude1990 | Windows NT | High
202.160.183.220 | FunnyMonkey | Windows 7 | Medium
202.160.183.235 | spamalot | Windows 8 | Low
202.160.183.239 | imurdaddy | Windows NT | Low
Show 10 of 36
<< 1 2 3 4 >>

FIG. 4L


410
THREATS TRENDS MANAGE
Search assets Go
JOHNDOE LOGOUT
Last Updated: 11/05/2012 12:34pm
Email-borne Malware 10 10
KNOWN ASSETS: 1,234 ⚠13
CURRENT ASSET GROUP: ALL
Desktop Threats
Overall Malware 7
Email-borne 10
USB-Drive 5
Web (Drive-by) 8
Web (User-Driven) 2
411
All
LA Desktops
Boston Desktops
Asset Group 3
Asset Group 4
Name All
Chassis
Desktop
Laptop
Operating System
Windows 8
Windows 7
Windows XP
Locations
Boston
LA
Singapore
Update
Save
421
62%
▽2.5%
413
<< 1 2 3 4 >>
Prioritized Guidance (1)
For: Malicious filetypes blocked/defanged
Email-borne
1. Filter attachments at mail gateway based on file type
Assign ▽
414
Improve your grade by following this sequence of steps
Relevant Assets (36)
415
For: Malicious filetypes blocked/defanged
IP Address
Username
System
Risk ▽
202.160.183.182 FunnyMonkey Windows 7 Severe
202.160.183.217 spamalot Windows 8 Severe
202.160.183.218 imurdaddy Windows NT Severe
202.160.183.219 kissme Mac OS X Severe
202.160.183.220 CookieRaider Windows 7 High
202.160.183.235 LookatMe Windows 8 High
202.160.183.239 Cooldude1990 Windows NT High
202.160.183.220 FunnyMonkey Windows 7 Medium
202.160.183.235 spamalot Windows 8 Low
202.160.183.239 imurdaddy Windows NT Low
Show 10 of 36
<< 1 2 3 4 >>

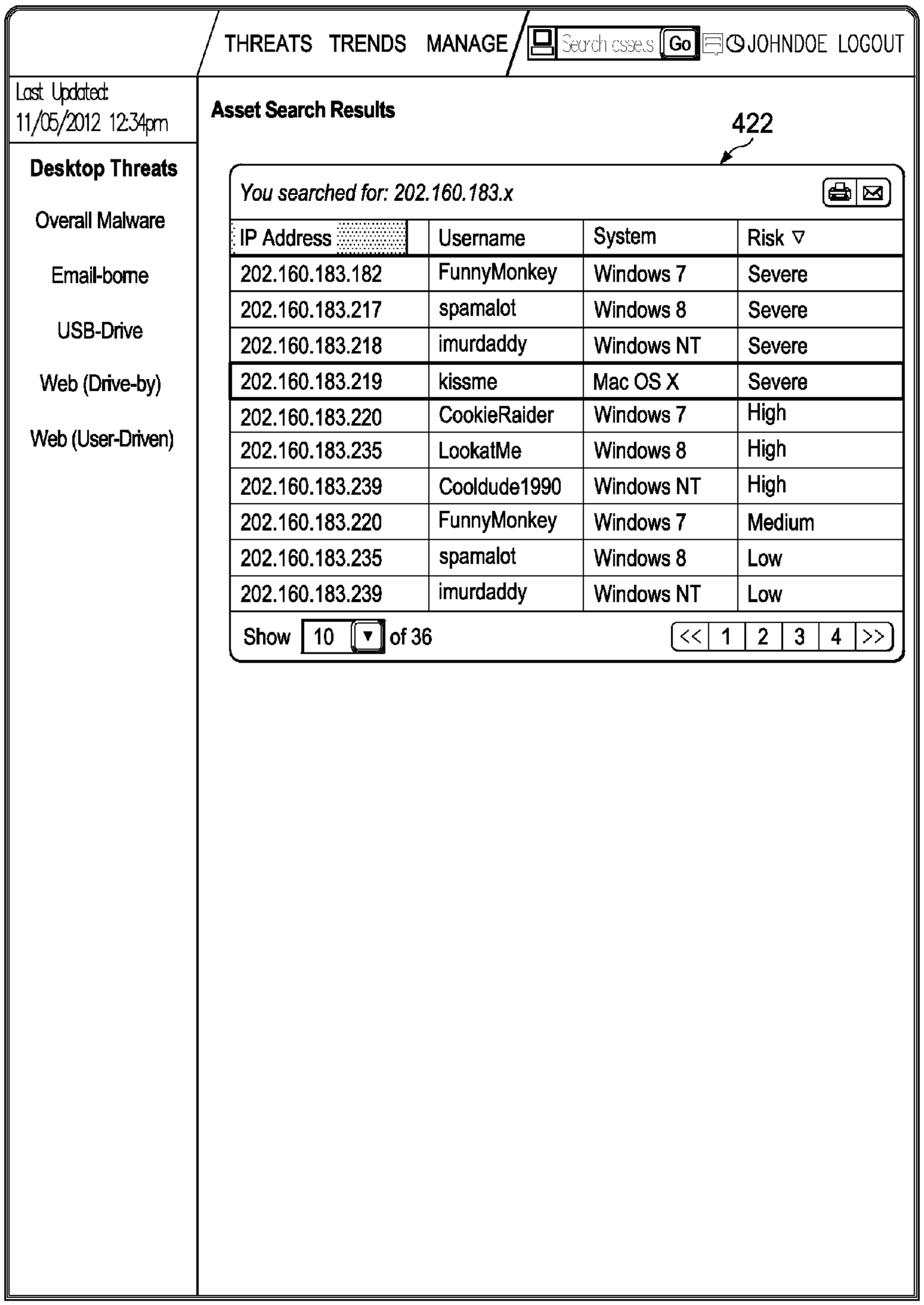

THREATS TRENDS MANAGE
Search cases
Go
JOHNDOE LOGOUT
Last Updated:
11/05/2012 12:34pm
Desktop Threats
Overall Malware
Email-borne
USB-Drive
Web (Drive-by)
Web (User-Driven)
Asset Search Results
422
You searched for: 202.160.183.x
IP Address
Username
System
Risk
202.160.183.182 FunnyMonkey Windows 7 Severe
202.160.183.217 spamalot Windows 8 Severe
202.160.183.218 imurdaddy Windows NT Severe
202.160.183.219 kissme Mac OS X Severe
202.160.183.220 CookieRaider Windows 7 High
202.160.183.235 LookatMe Windows 8 High
202.160.183.239 Cooldude1990 Windows NT High
202.160.183.220 FunnyMonkey Windows 7 Medium
202.160.183.235 spamalot Windows 8 Low
202.160.183.239 imurdaddy Windows NT Low
Show 10 of 36
<< 1 2 3 4 >>

FIG. 4M

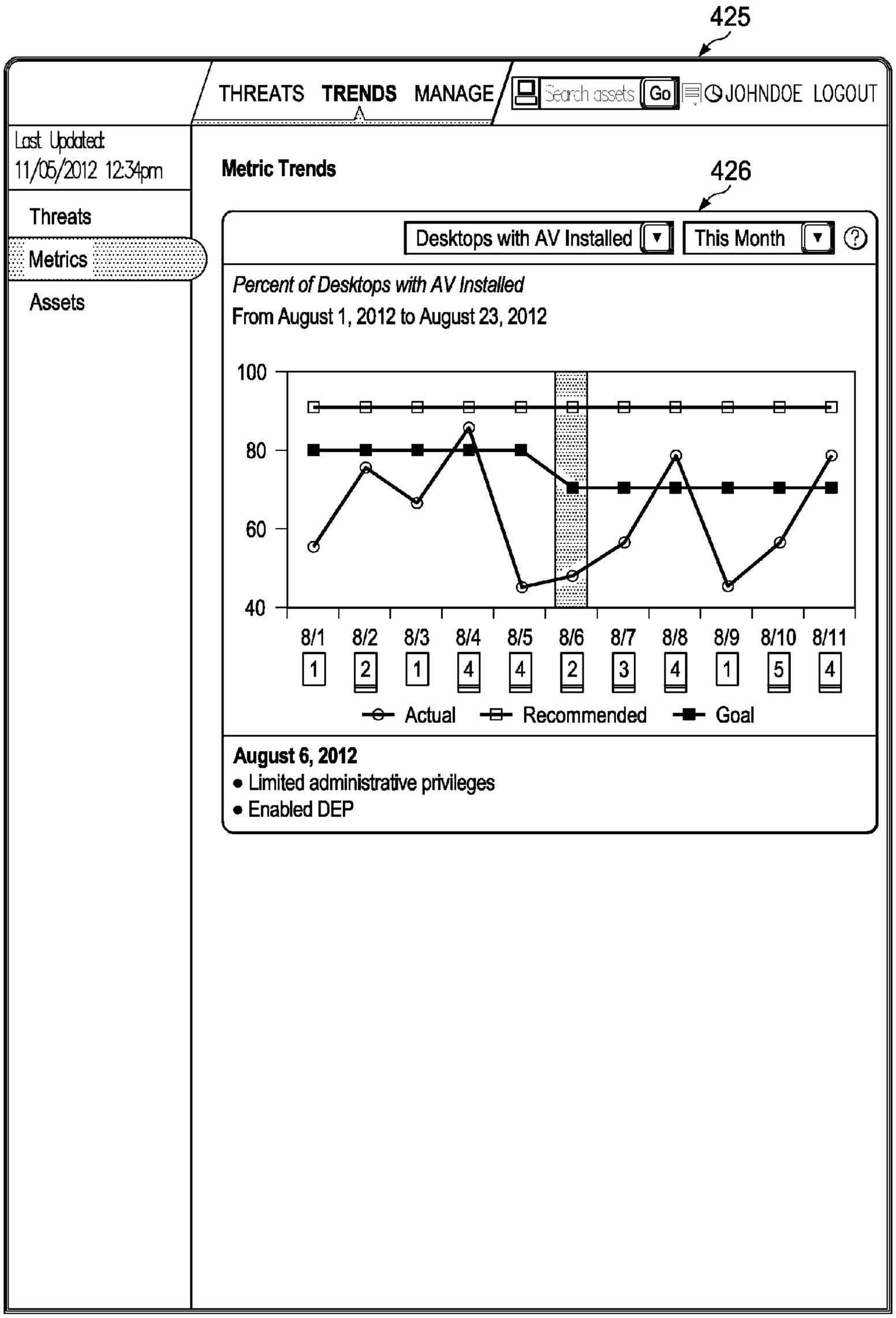

425
THREATS TRENDS MANAGE
Search assets Go
JOHNDOE LOGOUT
Last Updated:
11/05/2012 12:34pm
Threats
Metrics
Assets
Metric Trends
426
Desktops with AV Installed
This Month
Percent of Desktops with AV Installed
From August 1, 2012 to August 23, 2012
100
80
60
40
8/1 8/2 8/3 8/4 8/5 8/6 8/7 8/8 8/9 8/10 8/11
1 2 1 4 4 2 3 4 1 5 4
Actual
Recommended
Goal
August 6, 2012
• Limited administrative privileges
• Enabled DEP

FIG. 4N

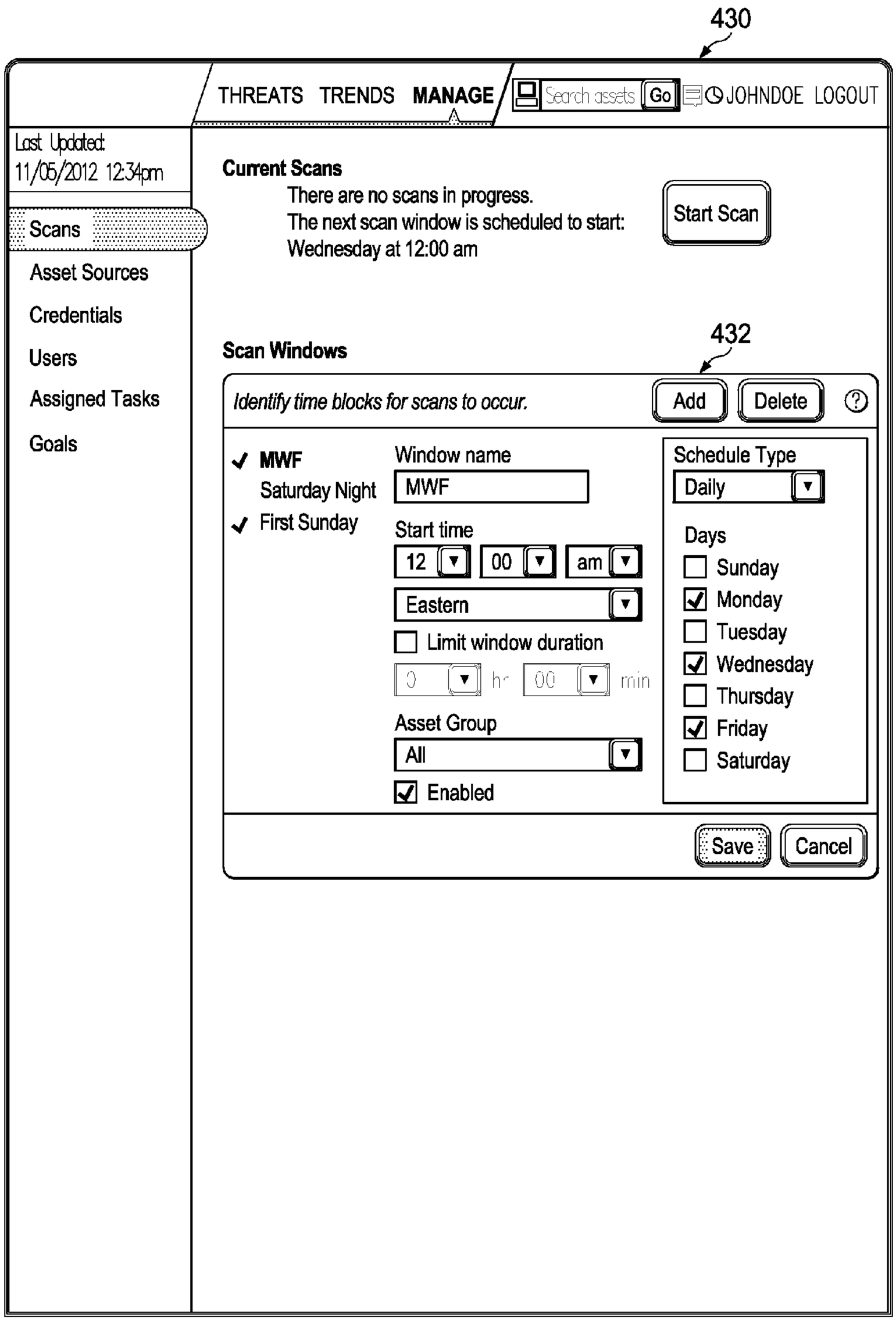

430
THREATS TRENDS MANAGE
Search assets Go
JOHNDOE LOGOUT
Last Updated:
11/05/2012 12:34pm
Scans
Asset Sources
Credentials
Users
Assigned Tasks
Goals
Current Scans
There are no scans in progress.
The next scan window is scheduled to start:
Wednesday at 12:00 am
Start Scan
Scan Windows
432
Identify time blocks for scans to occur.
Add
Delete
MWF
Saturday Night
First Sunday
Window name
MWF
Start time
12
00
am
Eastern
Limit window duration
hr
min
Asset Group
All
Enabled
Schedule Type
Daily
Days
Sunday
Monday
Tuesday
Wednesday
Thursday
Friday
Saturday
Save
Cancel

FIG. 4O

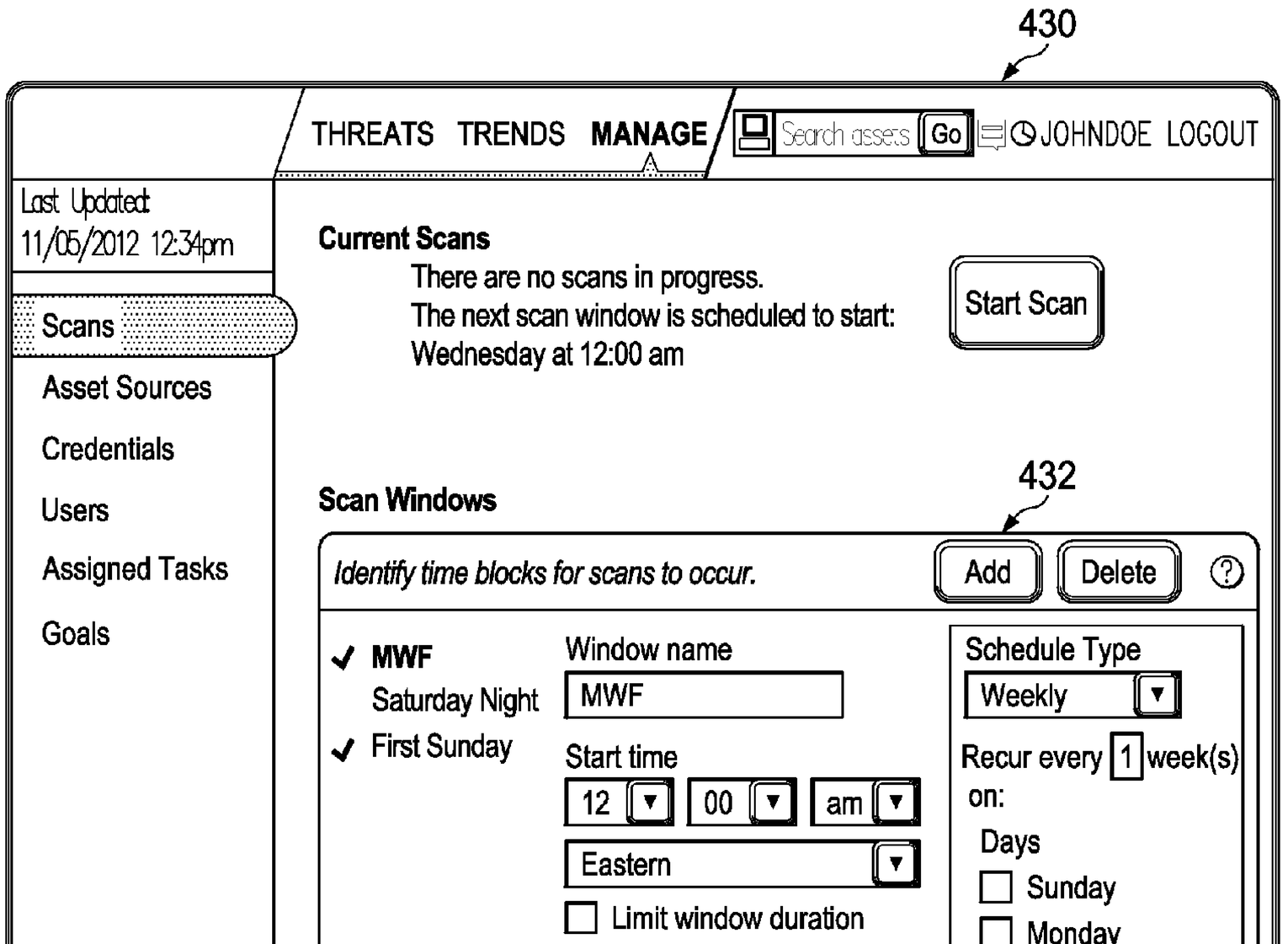

430
THREATS TRENDS MANAGE
Search assets
Go
JOHNDOE LOGOUT
Last Updated:
11/05/2012 12:34pm
Scans
Asset Sources
Credentials
Users
Assigned Tasks
Goals
Current Scans
There are no scans in progress.
The next scan window is scheduled to start:
Wednesday at 12:00 am
Start Scan
Scan Windows
432
Identify time blocks for scans to occur.
Add
Delete
MWF
Saturday Night
First Sunday
Window name
MWF
Start time
12
00
am
Eastern
Limit window duration
0
hr
00
min
Asset Group
All
Enabled
Schedule Type
Weekly
Recur every 1 week(s) on:
Days
Sunday
Monday
Tuesday
Wednesday
Thursday
Friday
Saturday
Save
Cancel

FIG. 4P

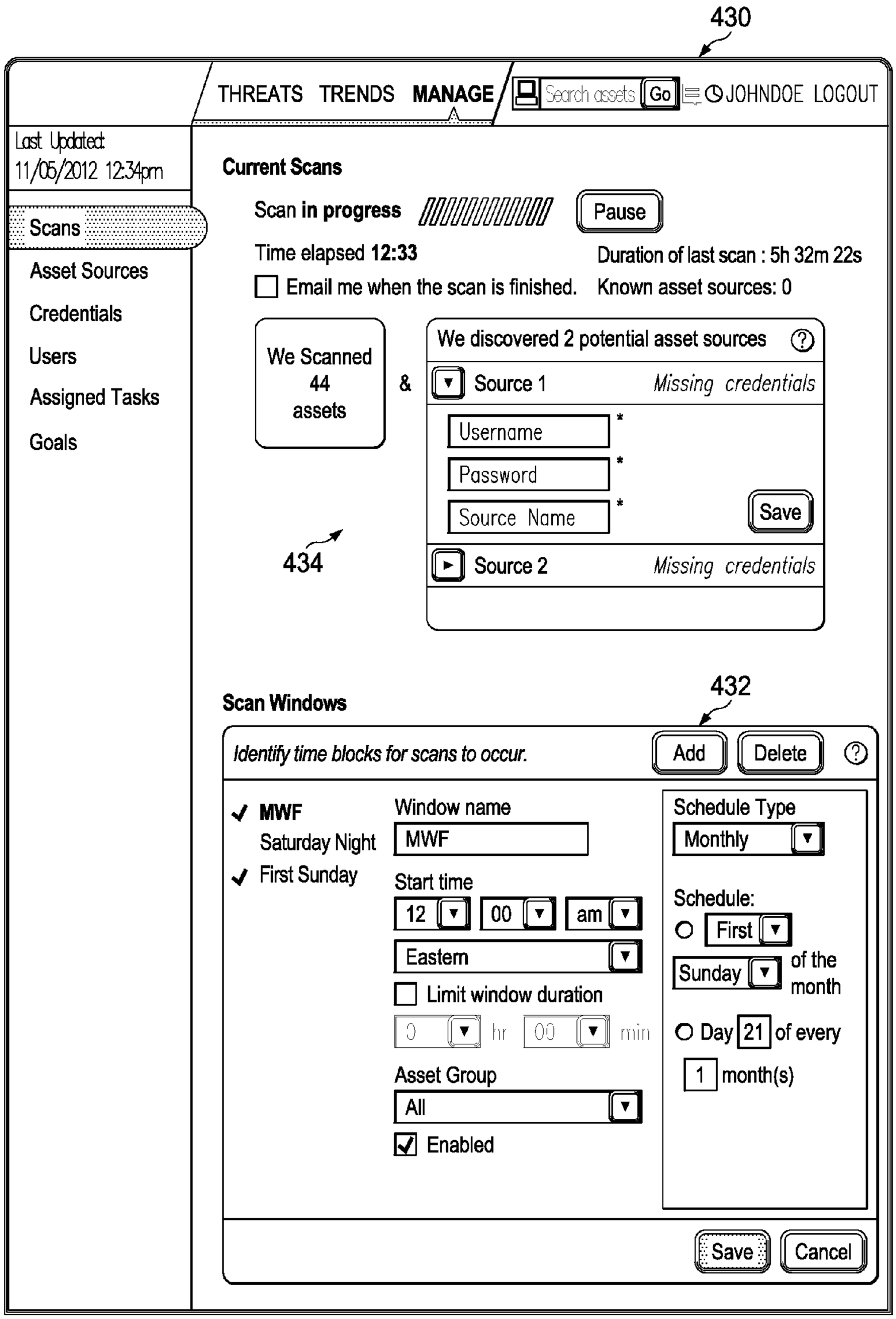

430
THREATS TRENDS MANAGE
Search assets Go
JOHNDOE LOGOUT
Last Updated:
11/05/2012 12:34pm
Scans
Asset Sources
Credentials
Users
Assigned Tasks
Goals
Current Scans
Scan in progress
Pause
Time elapsed 12:33
Duration of last scan : 5h 32m 22s
Email me when the scan is finished.
Known asset sources: 0
We Scanned 44 assets
&
We discovered 2 potential asset sources
Source 1
Missing credentials
Username
Password
Source Name
Save
Source 2
Missing credentials
434
Scan Windows
432
Identify time blocks for scans to occur.
Add
Delete
MWF
Saturday Night
First Sunday
Window name
MWF
Start time
12
00
am
Eastern
Limit window duration
0
hr
00
min
Asset Group
All
Enabled
Schedule Type
Monthly
Schedule:
First
Sunday
of the month
Day 21 of every
1 month(s)
Save
Cancel

FIG. 4Q

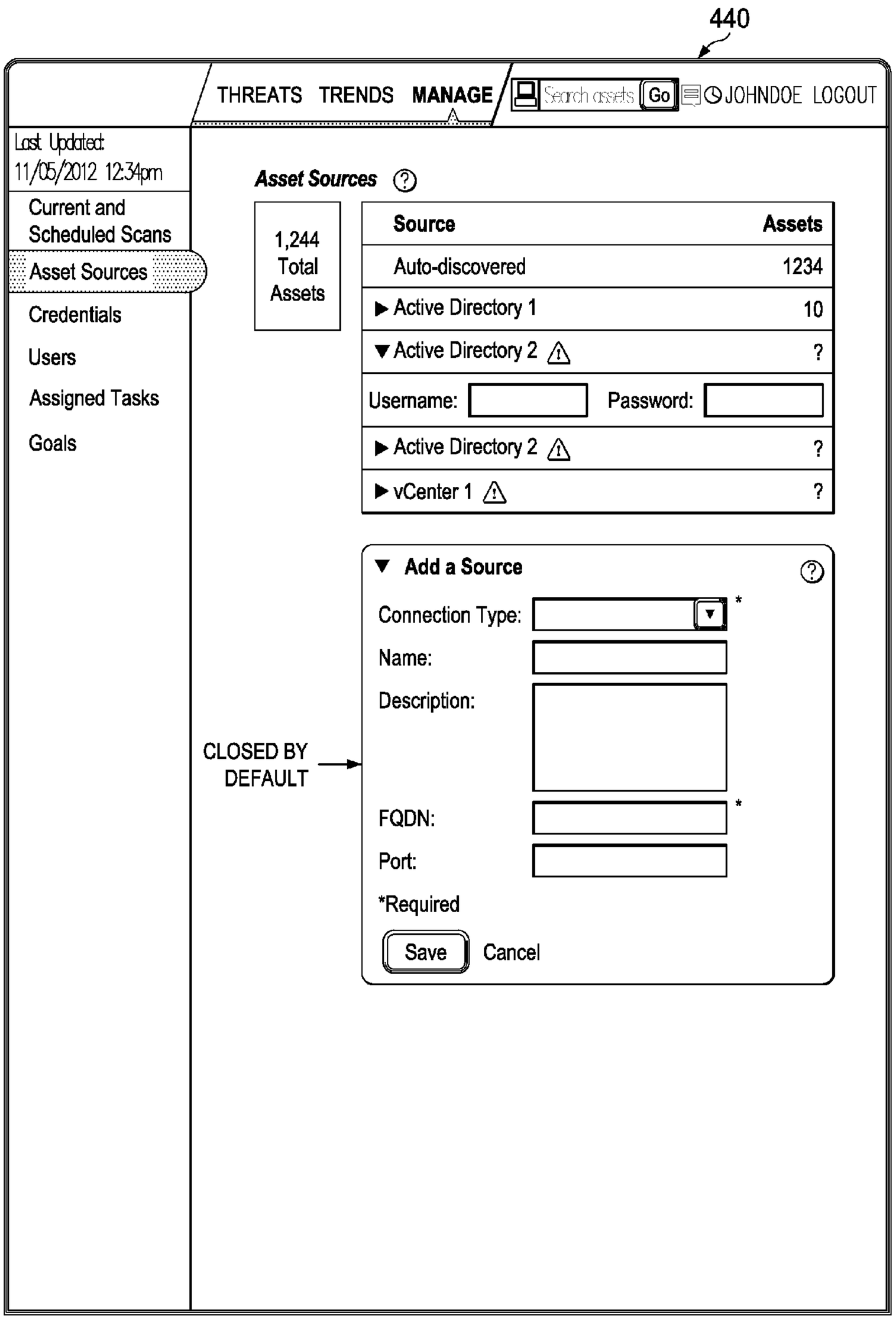

440
THREATS TRENDS MANAGE
Search assets Go
JOHNDOE LOGOUT
Last Updated: 11/05/2012 12:34pm
Current and Scheduled Scans
Asset Sources
Credentials
Users
Assigned Tasks
Goals
Asset Sources
1,244 Total Assets
Source
Assets
Auto-discovered 1234
▶ Active Directory 1 10
▼ Active Directory 2 ?
Username:
Password:
▶ Active Directory 2 ?
▶ vCenter 1 ?
CLOSED BY DEFAULT
▼ Add a Source
Connection Type: *
Name:
Description:
FQDN: *
Port:
*Required
Save
Cancel

FIG. 4R

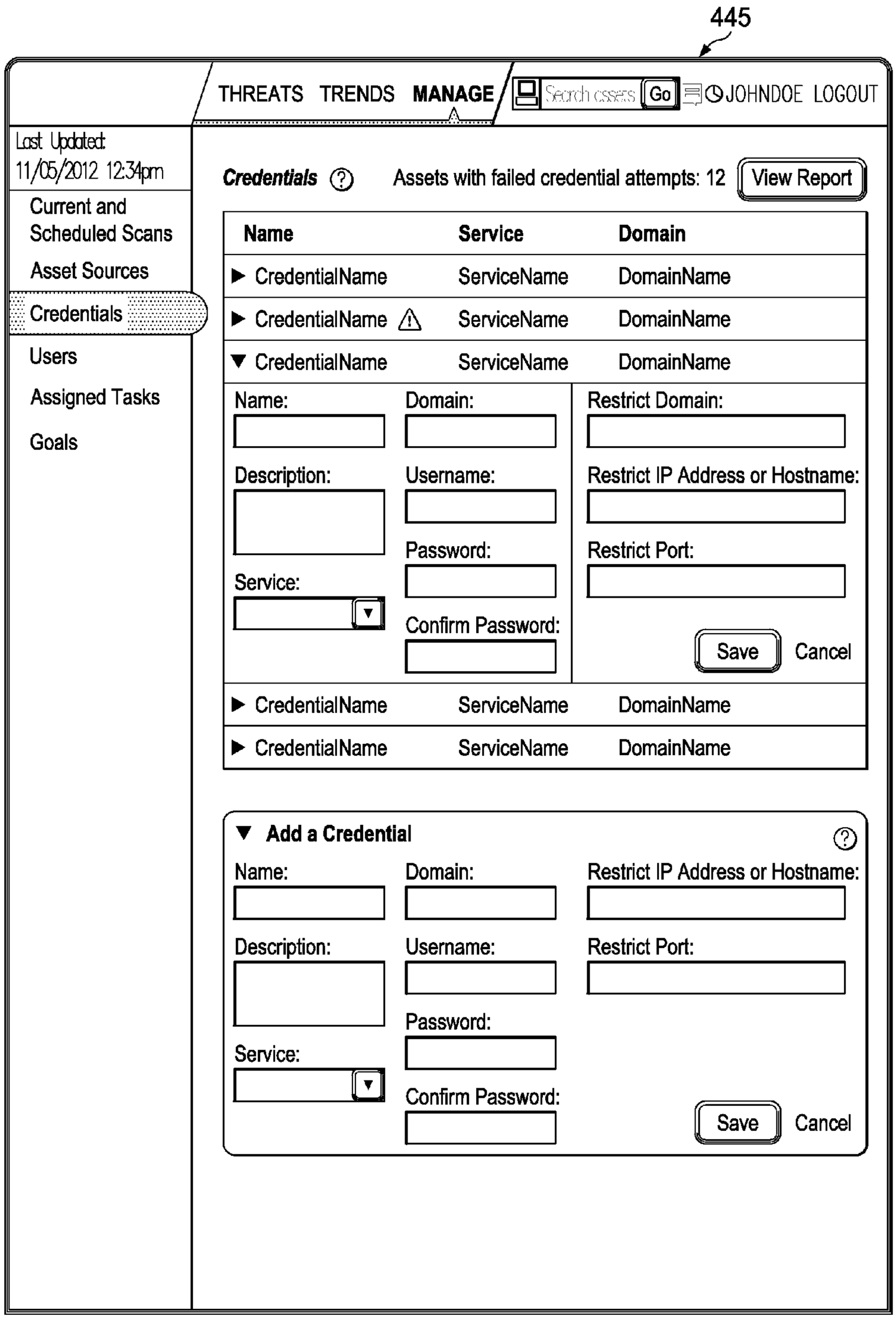

445
THREATS TRENDS MANAGE
Search assets
Go
JOHNDOE LOGOUT
Last Updated:
11/05/2012 12:34pm
Current and Scheduled Scans
Asset Sources
Credentials
Users
Assigned Tasks
Goals
Credentials
Assets with failed credential attempts: 12
View Report
Name
Service
Domain
CredentialName
ServiceName
DomainName
Name:
Domain:
Restrict Domain:
Description:
Username:
Restrict IP Address or Hostname:
Password:
Restrict Port:
Service:
Confirm Password:
Save
Cancel
Add a Credential

FIG. 4S

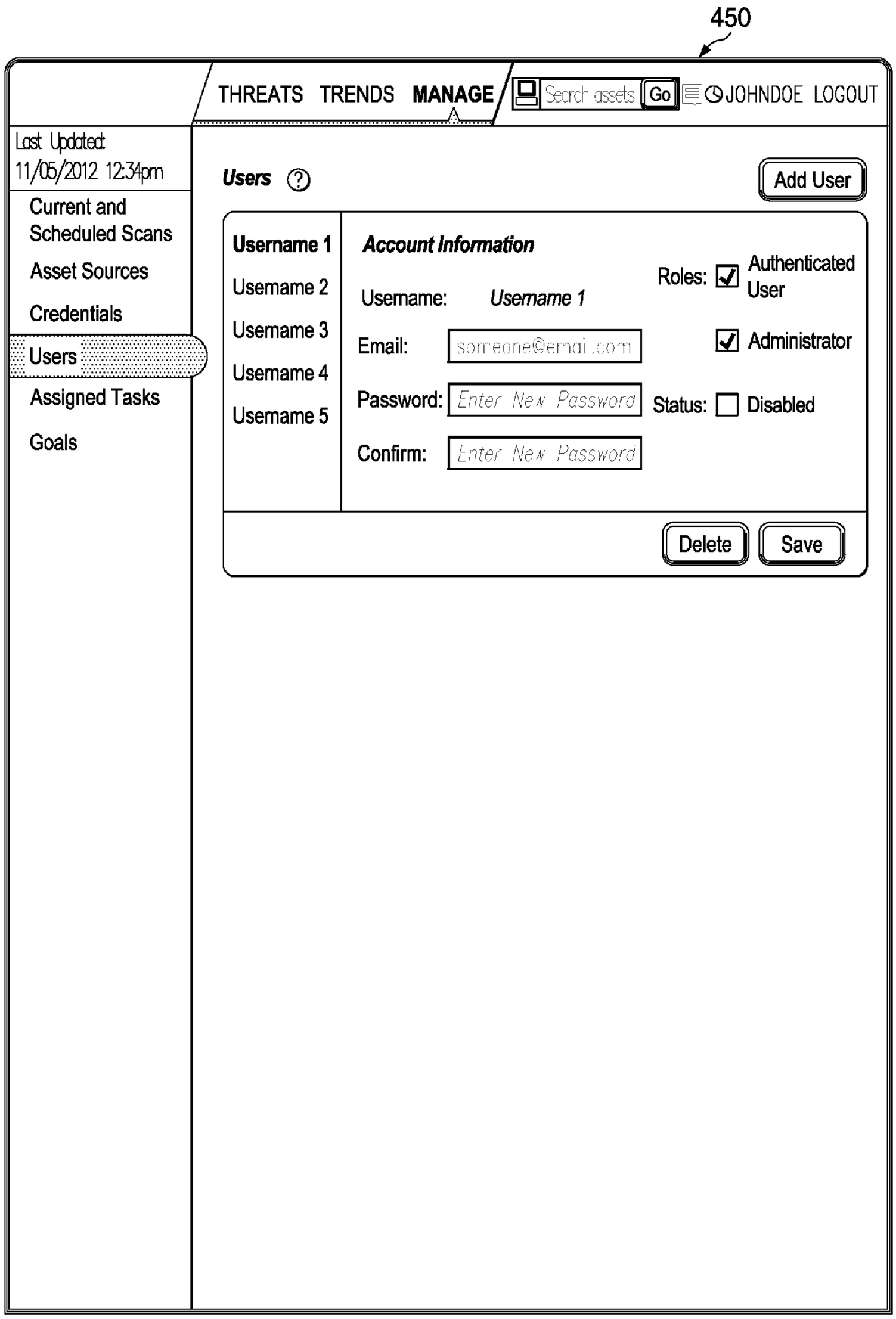

450
THREATS TRENDS MANAGE
Search assets
Go
JOHNDOE LOGOUT
Last Updated: 11/05/2012 12:34pm
Current and Scheduled Scans
Asset Sources
Credentials
Users
Assigned Tasks
Goals
Users
Add User
Username 1
Username 2
Username 3
Username 4
Username 5
Account Information
Username: Username 1
Email: someone@email.com
Password: Enter New Password
Confirm: Enter New Password
Roles: Authenticated User
Administrator
Status: Disabled
Delete
Save

FIG. 4T

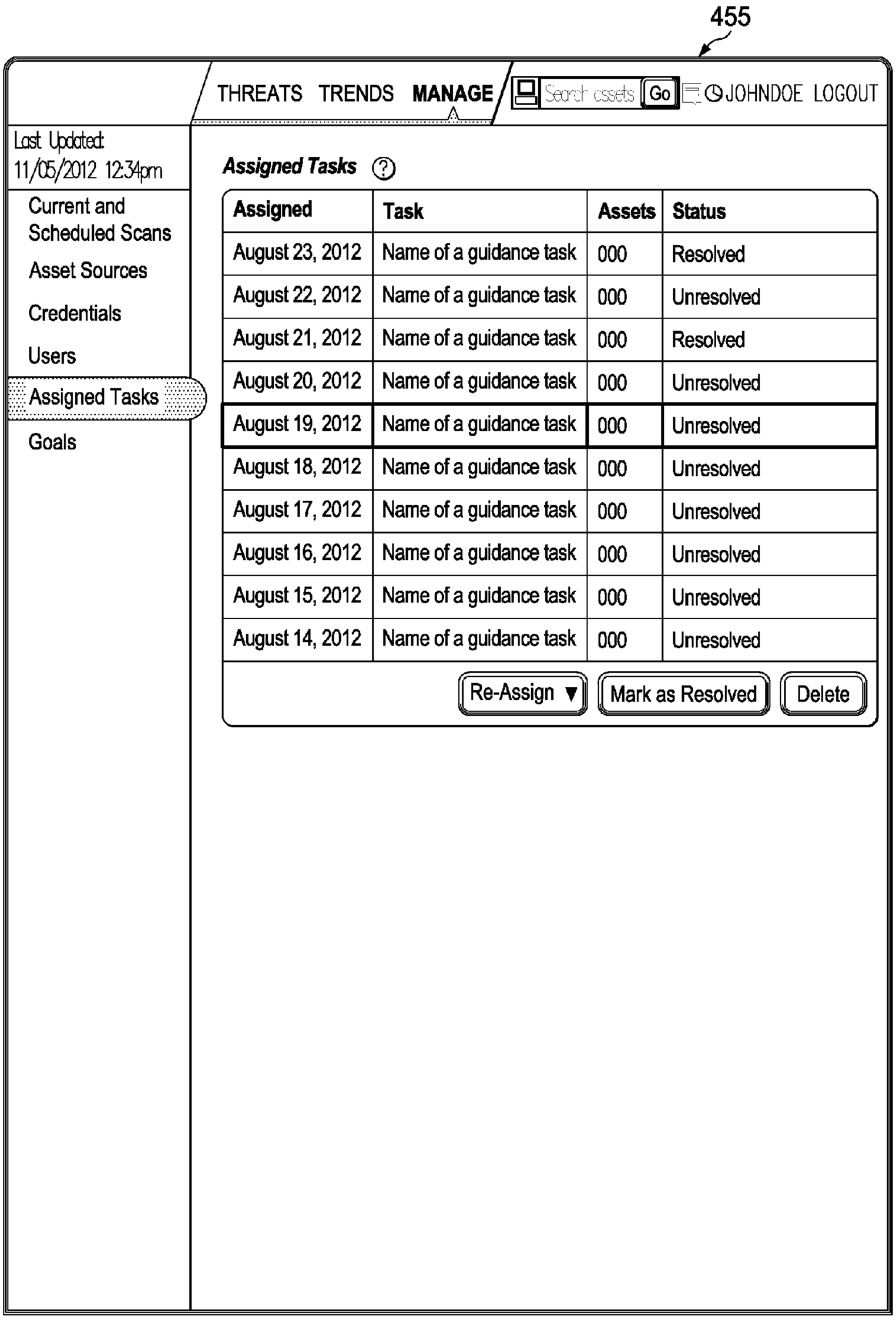

455
THREATS TRENDS MANAGE
Search assets
Go
JOHNDOE LOGOUT
Last Updated: 11/05/2012 12:34pm
Current and Scheduled Scans
Asset Sources
Credentials
Users
Assigned Tasks
Goals
Assigned Tasks
Assigned
Task
Assets
Status
August 23, 2012
Name of a guidance task
000
Resolved
August 22, 2012
Name of a guidance task
000
Unresolved
August 21, 2012
Name of a guidance task
000
Resolved
August 20, 2012
Name of a guidance task
000
Unresolved
August 19, 2012
Name of a guidance task
000
Unresolved
August 18, 2012
Name of a guidance task
000
Unresolved
August 17, 2012
Name of a guidance task
000
Unresolved
August 16, 2012
Name of a guidance task
000
Unresolved
August 15, 2012
Name of a guidance task
000
Unresolved
August 14, 2012
Name of a guidance task
000
Unresolved
Re-Assign
Mark as Resolved
Delete

FIG. 4U

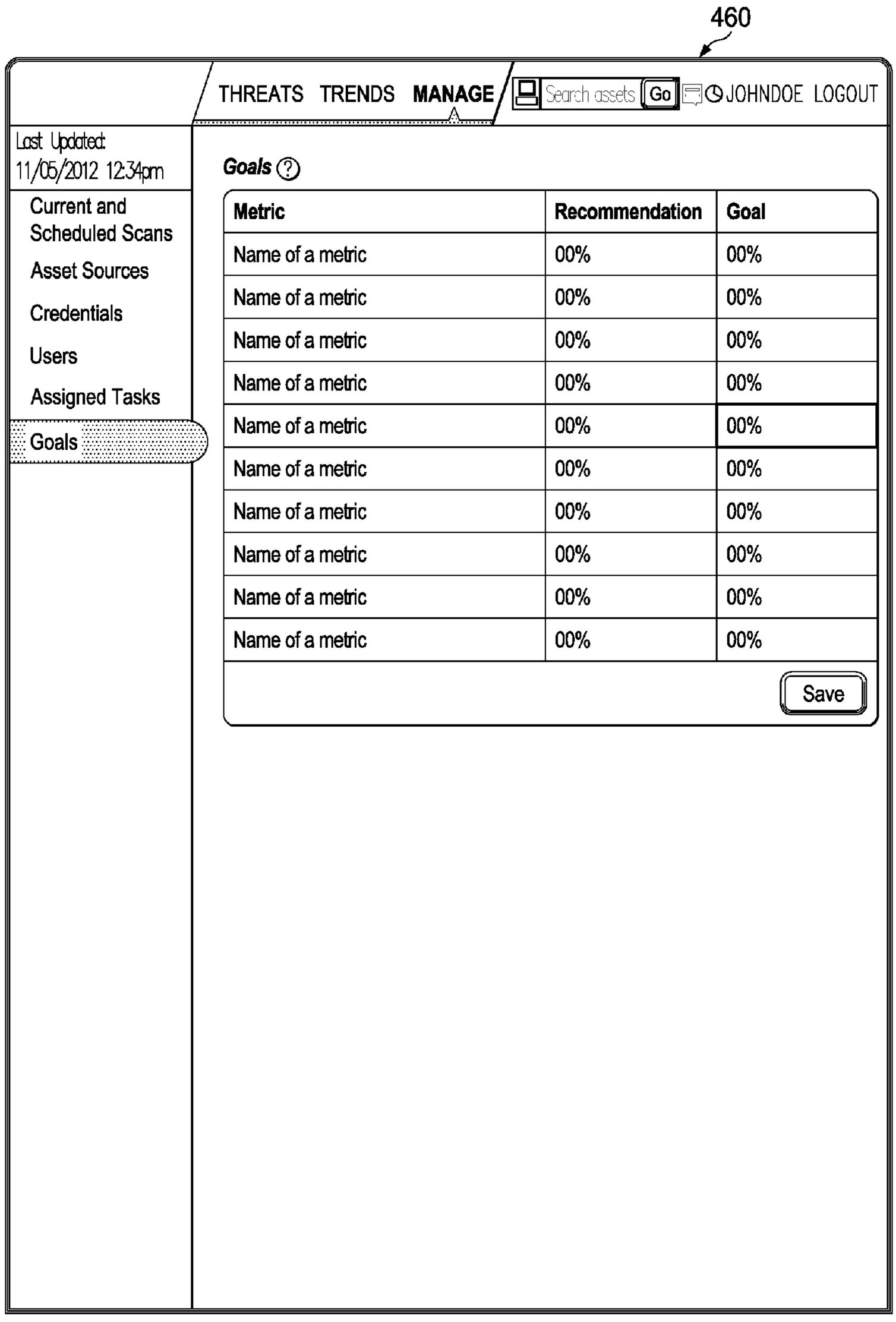

460
THREATS TRENDS MANAGE
Search assets
Go
JOHNDOE LOGOUT
Last Updated:
11/05/2012 12:34pm
Current and Scheduled Scans
Asset Sources
Credentials
Users
Assigned Tasks
Goals
Goals
Metric
Recommendation
Goal
Name of a metric
00%
00%
Save

FIG. 4V

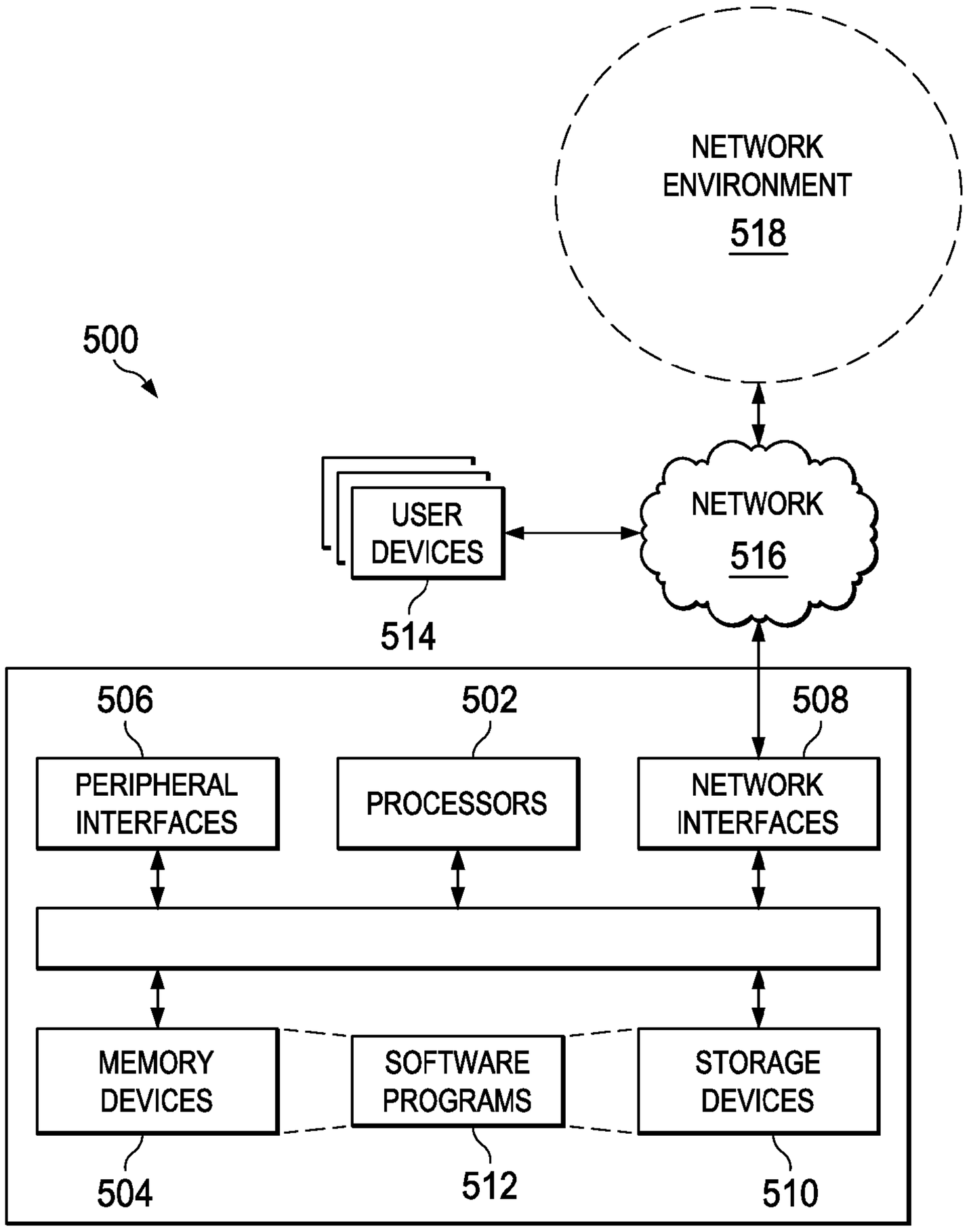

NETWORK ENVIRONMENT
518
500
USER DEVICES
514
NETWORK
516
506
502
508
PERIPHERAL INTERFACES
PROCESSORS
NETWORK INTERFACES
MEMORY DEVICES
SOFTWARE PROGRAMS
STORAGE DEVICES
504
512
510

FIG. 5

# SYSTEMS AND METHODS FOR ASSESSING SECURITY FOR A NETWORK OF ASSETS AND PROVIDING RECOMMENDATIONS

## CROSS-REFERENCE TO RELATED APPLICATIONS

This application is related to U.S. patent application Ser. No. 13/899,093 filed May 21, 2013, entitled "SYSTEMS AND METHODS FOR DETERMINING AN OBJECTIVE SECURITY ASSESSMENT FOR A NETWORK OF ASSETS" by HD Moore, Roy Donald Hodgman, Dana Elizabeth Wolf, and Matthew Robert Hathaway, the disclosure of which is incorporated by reference herein in its entirety.

## BACKGROUND

In today's distributed computing environments, security is of the utmost importance. Due to the rise of wide-area public networks, users have unlimited access to content, e.g. data, files, applications, programs, etc., from a variety of sources. Additionally, the users' connection to the public networks provides a window for malicious entities to attack the users' computing systems. Malicious entities utilize this ease of accessibility and anonymity to attack the users. For example, the malicious entities can plant viruses, Trojans, or other malicious agents in publicly available content in order to attack the users' computing systems and steal sensitive information from the users and can attack the users' system remotely across the public networks.

To identify security risks in computing systems and networks, users and administrators employ vulnerability assessment and security assessment tools. These tools can identify vulnerabilities in computing systems and networks but only provide discrete information about the vulnerabilities (i.e. that a vulnerability exists). Accordingly, the tools do not provide any assessment of the vulnerabilities within the context of the overall network security.

## BRIEF DESCRIPTION OF THE DRAWINGS

Various features of the implementations can be more fully appreciated, as the same become better understood with reference to the following detailed description of the implementations when considered in connection with the accompanying figures, in which:

FIGS. **1**A and **1**B illustrate an example of a network environment in which an overall security assessment can be performed, according to various implementations;

FIG. **2** illustrates an example of a process for determining an overall security assessment of a network environment, according to various implementations;

FIG. **3** illustrates an example of a process for determining an overall security score for a network environment, according to various implementations;

FIGS. **4**A-**4**V illustrates examples of interfaces that can be used to communicate with a security assessment tool, according to various implementations; and

FIG. **5** illustrates an example of a computer device, according to various implementations.

## DETAILED DESCRIPTION

For simplicity and illustrative purposes, the principles of the present teachings are described by referring mainly to examples of various implementations thereof. However, one of ordinary skill in the art would readily recognize that the same principles are equally applicable to, and can be implemented in, all types of information and systems, and that any such variations do not depart from the true spirit and scope of the present teachings. Moreover, in the following detailed description, references are made to the accompanying figures, which illustrate specific examples of various implementations. Electrical, mechanical, logical and structural changes can be made to the examples of the various implementations without departing from the spirit and scope of the present teachings. The following detailed description is, therefore, not to be taken in a limiting sense and the scope of the present teachings is defined by the appended claims and their equivalents.

According to implementations, systems and methods are directed to providing an overall security assessment of a network of computer assets. In implementations, a security assessment tool can determine computer assets in a network and provide an overall security score for the network. The overall security score can represent an objective measure of the security of the network that considers potential security threats to the computer assets, counter measures deployed in the network to address the potential security threats, and the effectiveness of the counter measures. Based on the overall security assessment, the security assessment tool can provide recommendations for improving the security of the network.

FIGS. **1**A and **1**B illustrate an example of a network environment **100**, in which a security assessment can be performed, according to various implementations. While FIGS. **1**A and **1**B illustrate various components contained in the network environment **100**, FIGS. **1**A and **1**B illustrate one example of a network environment and additional components can be added and existing components can be removed.

As illustrated in FIG. **1**A, the network environment **100** can represent the computer systems and network hardware of public or private entities, such as governmental agencies, individuals, businesses, partnerships, companies, corporations, etc., utilized to support the entities. The network environment **100** can include a number of computer assets **102**. The computer assets **102** can be connected by one or more local area networks **104** and one or more wide area network **106**. In implementations, a security assessment tool **108** can be configured to assess the security of the network environment **100** and provide an overall security score for the network environment **100**.

The computer assets **102** can include any type of conventional computer systems that are operating with the network environment **100** or supporting the network environment **100**. For example, the network environment **100** can include various types of servers, such as file servers, web servers, application servers, database servers, email servers and the like, that provide services within the network environment **100**. Likewise, for example, the computer assets **102** can include laptop computers, desktop computers, tablet computers, mobile phones, and the like used by the personnel of the entities.

Additionally, for example, the computer assets **102** can include other hardware and computer systems that support the network environment **100**. For example, the computer assets **102** can include gateways, routers, wireless access points, firewalls, and the like that support any type of communications networks, such as the local area network **104** and the wide area networks **106**, to allow the computing systems in the network environment **100** to communicate. In any of the examples, the computer systems in the network environment **100** can include hardware resources, such as processors,

memory, network hardware, storage devices, and the like, and software resources, such as operating systems (OS), application programs, and the like.

In addition to physical computer systems, the computer assets **102** can include virtualized computer systems, such as virtual machines (VM). A VM can be a virtualized computer system, or a software implementation of a computer system layered on top of any of physical computer system. The VM's access to the underlying computer system can be controlled through a hypervisor or virtual machine monitor. The VMs can provide for multiple and/or different operating system environments to run concurrently on a single computer system.

While several examples of the computer assets **102** have been described above, the computer assets **102** can include any system, whether physical or virtual, that performs computing processes in the network environment **100**. Additionally, the computer assets **102** in the network environment **100** can be located at any location, whether located at single geographic location or remotely located from each other. For example, the network environment **100** can represent the computer assets **102** of a company that is located in multiple geographic locations. As such, one or more of the computer assets **102** can be located at one location (e.g. one office of the company) and one or more of the computer assets **102** can be located at one or more different locations (e.g. satellite offices of the company).

In implementations, the security assessment tool **108** can be configured to assess the overall security of the network environment **100**. The security assessment tool **108** can be configured to identify the computer assets **102** of the network environment **100**. Once identified, the security assessment tool **108** can be configured to determine the security information of the network environment **100** and the computer assets **102**. Based on the security information, the security assessment tool **108** can be configured to determine potential security threats to the network environment **100** and the computer assets **102**. Likewise, based on the security information, the security assessment tool **108** can be configured to determine counter measures that are deployed in the network environment **100** and deployed on the computer assets **102** to address the potential security threats. Based on the effectiveness of the deployed counter measures, the security assessment tool **108** can be configured to provide an overall assessment of the security of the network environment **100**. Based on the overall security assessment, the security assessment tool **108** can be configured to provide recommendations for improving the security of the network environment **100**.

As described herein, a security threat can be any process, method, technique, algorithm, condition, software program, policy, and the like that can be utilized to compromise the security of the network environment **100**. For example, a security threat can include known threat vectors for computer assets **102** and the network environment **100**, such as known malware, known exploits, known viruses, and the like. A counter measure can include processes, techniques, methods, algorithms, conditions, policies, software programs and the like that can be implemented in the network environment **100** to address potential security threats.

Security information can include any information about the structure of the network environment **100** and any information about the computer assets **102**. For example, the security information can include security details of the network environment **100**, such as security polices of the network environment **100**, details of computer assets **102** (e.g. firewalls) providing security in the network environment **100**, and the like. Likewise, for example, the security information can include security details of the computer assets **102**, such as the configuration of the computer assets **102**, system setting of the computer assets **102**, software programs including security software programs installed on the computer assets **102**, security settings of the computer assets **102**, configuration policies of the computer assets **102**, security policies of the computer assets **102**, access information for the computer assets **102**, and details of software programs installed on the computer assets.

In implementation, the security assessment tool **108** can be configured as a software program that is capable of being stored on and executed by a computer system, whether part of the network environment **100** or external to the network environment **100**. The security assessment tool **108** can be written in a variety of programming languages, such as JAVA, C++, Python code, Visual Basic, hypertext markup language (HTML), extensible markup language (XML), and the like to accommodate a variety of operating systems, computing system architectures, etc. FIG. **1**B illustrates a more detailed view of the security assessment tool **108**. As illustrated, the security assessment tool **108** can be configured as a standalone software program and can include a scanner **110**, a threat model **112**, a score module **114**, and one or more interfaces **116**. While FIG. **1**B illustrates the components as being part of the security assessment tool **108**, the components can be separate software programs that communicate with the security assessment tool **108**. Likewise, the security assessment tool **108**, itself, can be a component of another software program.

The scanner **110** can include one or more software modules or tools that can scan the network environment **100** and the computer assets **102**. The scanner **110** can be configured to determine the structure of the network environment **100** and identify the computer assets **102**. Likewise, the scanner **110** can be configured to determine the security information for the network environment **100**. Accordingly, the scanner **110** can be configured to include the necessary logic, commands, algorithms, and code to scan the network environment **100** and to communicate computer assets **102**. For example, the scanner **110** can include various types of network scanners and vulnerability scanners, such as NeXpose™ or Metasploit™ from Rapid7, LLC.

The threat model **112** can be a listing of known security threats to network environments. The threat model **112** can include the identification of the known security threats and details of the security threats. The details can include the types of the computer assets **102** that are vulnerable to the known security threats, the affect of the known security threats, one or more counter measures that address the known security threats, and the like.

The score model **114** can include the necessary logic, commands, algorithms, and code utilized by the security assessment tool **108** to determine the overall security assessments and provide recommendations as described herein. The score model **114** can include a listing of the counter measures to security threats and a weighting value associated with each of the counter measures. The weighting value can represent the effectiveness of a particular counter measure.

The security assessment tool **108** can also include an interface **116**. The interface **116** can be configured to allow one or more users to interact with the security assessment tool **108**. The interface **116** can be configured to provide one or more graphical user interfaces (GUIs) and/or command-line interfaces to allow a user to interact with the security assessment tool **108**. Likewise, the interface **116** can be configured to provide one or more application programming interfaces (APIs) to allow other software programs to interact with the

security assessment tool **108**. As described herein, the security assessment tool **108** will be described with reference to a user interacting with the security assessment tool **108**. In implementations, a user can include a one or more persons and/or one or more software programs that can interact with the security assessment tool **108**.

In implementations, a user can utilize the interface **116** interact with the security assessment tool **108** to perform the overall security assessment. The user can utilize the interface **116** to initiate a security assessment of the network environment **100**. The user can utilize the interface **116** to enter information about the network environment **100** and the computer assets **102**. For example, the user can enter information about the structure of the network environment **100** such as network addresses of the network environment **100**. Likewise, for example, the user can enter information about the computer assets **102**, such as identification of the computer assets **102**, access information for the computer assets **102**, and the like. The security assessment tool **108**, for example, the scanner **110**, can utilize the information provided by the user when identifying the computer assets **102** and when determining the security information for the network environment **100**.

The security assessment tool **108** can utilize the interface **116** to output the results of the overall security assessment. The results can include the security score relative to the potential security threats and the overall security score determined by the security assessment tool **108**. The results can also include one or more recommendations for improving the security score relative to the potential security threats and the overall security score. For example, the one or more recommendations can include deploying a new counter measure, changing a security setting of the computer assets **102**, changing a system setting of the computer assets **102**, changing a security policy of the computer systems **102**, updating software of the computer assets **102**, installing security software on the computer assets **102**, and improving access information for the computer assets **102**.

As illustrated, the security assessment tool **108** can be configured to access one or more security resources **118**. The security resources **118** can be a source, whether internal or external to the network environment **100**, that provides information about security threats and counter measures. For example, the security resources **118** can include security experts, security forums, security literature, empirical security testing platforms, and the like. Likewise, for example, the security resource **118** can include the user of the security assessment tool **108**. The security assessment tool **108** can utilize the security resources **118** to generate and update the threat model **112**. The security assessment tool **108** can also utilize the security resources **118** to generate and update the score model **114**. For example, the security assessment tool **108** can utilize the security resources **118** to determine effectiveness metrics for the counter measures. The effectiveness metrics can be utilized to determine and update the weighting values for the counter measures.

FIG. **2** illustrates an example of a process **200** for assessing the security of the network environment **100**, according to various implementations. The illustrated stages of the process **200** are examples and that any of the illustrated stages can be removed, additional stages can be added, and the order of the illustrated stages can be changed.

As illustrated, at **202**, the process can begin. At **204**, the security assessment tool **108** can determine the computer assets **102** in the network environment **100**. The security assessment tool **108** can scan the network environment **100** to identify the computer assets **102** in the network environment **100**. Likewise, the security assessment tool **108** can receive an identification of computer assets **102** from a user of the security assessment tool **108**. Additionally, the security assessment tool **108** can receive, from a user, information about the network environment **100** and the computer assets **102** to assist in scanning the network environment **100**.

In **206**, the security assessment tool **108** can determine an actual deployment of counter measures on the computer assets. To determine the actual deployment of the counter measurers, the security assessment tool **108** can determine security information of the network environment **100**. The security assessment tool **108** can scan the network environment **100** and the computer assets **102** to identify security information. Likewise, the security assessment tool **108** can receive the security information from a user of the security assessment tool **108**. Additionally, the security assessment tool **108** can receive, from a user, information about the network environment **100** and the computer assets **102** to assist in scanning the network environment **100**.

The security information can include any information about the structure of the network environment **100** and any information about the computer assets **102**. For example, the security information can include security details of the network environment **100**, such as security polices of the network environment **100**, details of computer assets **102** (e.g. firewalls) providing security in the network environment **100**, and the like. Likewise, for example, the security information can include security details of the computer assets **102**, such as the configuration of the computer assets **102**, system setting of the computer assets **102**, software programs including security software programs installed on the computer assets **102**, security settings of the computer assets **102**, configuration policies of the computer assets **102**, security policies of the computer assets **102**, access information for the computer assets **102**, and details of software programs installed on the computer assets.

Once the security information is determined, the security assessment tool **108** can determine potential security threats to the network and determine counter measures to address the potential security threats. Based on the security information, the security assessment tool **108** can examine the threat model **112** to identify the potential security threats to the network environment **100**. Additionally, from the threat model **112**, the security assessment tool **108** can identify counter measure that can address the potential security threats to the network environment **100**.

For example, based on the type and configurations of computer assets **102**, the security assessment tool **108** can determine potential security threats. For instance, if one or more of the computer assets **102** are running a particular OS or a particular software program, the security assessment tool **108** can determine any potential security threats and any counter measures that are applicable to the particular OS or software program. Likewise, for instance, if one or more of the computer assets **102** are connected to a public network (e.g. the internet), the security assessment tool **108** can determine any potential security threats and any counter measures that are associated with public networks.

Then, the security assessment tool **108** can determine an actual deployment of the counter measures in the network. Based on the security information and potential security threats, the security assessment tool **108** can determine which counter measures are actually deployed in the network environment **100** and on the computer assets **102**. The security assessment tool **108** can determine which of counter mea-

sures are deployed and the coverage of the counter measures (e.g. on which computer assets **102** are the counter measures deployed).

In **208**, the security assessment tool **108** can determine an overall security score for the network based on the actual deployment of the counter measures, potential security threats, and an effectiveness of the counter measures. The security assessment tool **108** can determine the overall security score based on potential security threats to the network environment **100**, the actual deployment of the counter measures in the network environment **100**, and effectiveness on the deployed counter measures. The overall security score can include security scores for different security threats. The security score for each security threat can reflect the actual deployment of counter measures for each counter measure and the effectiveness of the deployed counter measures. The overall security score can be the combination of the security scores for each potential security threat.

The security score for each potential security threat and the overall security score can be a numerical value that represents the overall security score for the network environment **100**, where a higher numerical value represents better security relative to lower numerical values. For example, the security score for each potential security threat and overall security score can be a numerical value between "0" and "10," where "0" represents no security for potential security threats and "10" represents complete coverage for the potential security threats. For instance, if for a particular security threat, the network environment **100** has deployed, on 100% of the computer assets **102**, a counter measure that is 50% effective in mitigating a the particular security threat. In this instance, the security assessment tool **108** can determine that the overall security score is 5.

The above describes an example of the general process for determining the overall security score. A complete description of examples of determining the security score can be found in the related application, U.S. patent application Ser. No. 13/899,093 filed May 21, 2013, entitled "SYSTEMS AND METHODS FOR DETERMINING AN OBJECTIVE SECURITY ASSESSMENT FOR A NETWORK OF ASSETS" by HD Moore, Roy Donald Hodgman, Dana Elizabeth Wolf, and Matthew Robert Hathaway, the disclosure of which is incorporated by reference herein in its entirety.

In **210**, the security assessment tool **108** can determine recommendations for improving the overall security score. The recommendations can include any actions, procedures, processes, and the like for improving the security score relative to the potential security threats and the overall security score. For example, the one or more recommendations can include deploying a new counter measure, changing a security setting of the computer assets **102**, changing a system setting of the computer assets **102**, changing a security policy of the computer systems **102**, updating software of the computer assets **102**, installing security software on the computer assets **102**, and improving access information for the computer assets **102**.

In **212**, the security assessment tool **108** can output the overall security score and the recommendations for the network environment **100**. For example, the security assessment tool **108** can output the security score for each potential security threat and overall security score via the interface **116**. The security assessment tool **108** can output the value of the security score for each potential security threat and overall security score in addition to recommendations to improve the overall security score.

In **214**, the security assessment tool **108** can repeat the process above, over time, to determine new overall security scores. As new security threats arise, computer assets are added and removed from the network, new counter measures are determined, and as new counter measured are deployed, the security assessment tool **108** can determine new security score for each potential security threat and a new overall security score. Likewise, the security assessment tool **108** can determine impact of the changes on the new scores.

In **216**, the security assessment tool **108** can perform trending analysis over time. The trending analysis can be any procedure or process that determines how the security assessment changes over time. For example, the security assessment tool **108** can track the change in the overall security (or security scores for potential threats), over time, and output a graph or other indication of the changes over time. Likewise, for example, the security assessment tool **108** can track the change in deployment of counter measures, over time, and output a graph or other indication of the changes over time.

In **218**, the process can end, repeat, or return to any point.

FIG. **3** illustrates an example of a process **300** for determining an overall security score and implementing recommendations, according to various implementations. The illustrated stages of the process **300** are examples and that any of the illustrated stages can be removed, additional stages can be added, and the order of the illustrated stages can be changed.

As illustrated, at **302**, the process can begin. In **304**, the security assessment tool **108** can initially determine computer assets in a computer network and counter measures deployed on the computer assets. For example, when the security assessment tool **108** first examines the network environment **100**, the security assessment tool **108** can determine the computer assets and security information for the network environment **100**. The security assessment tool **108** can determine the computer assets and security information according to the procedures as discussed above in FIG. **2**.

In **306**, the security assessment tool **108** can determine the overall security score and the recommendations based on the initial determination. The overall security scores can represent the initial overall security scores before performing any of the recommendations. The security assessment tool **108** can determine the overall security score based on the actual deployment of the counter measures, the potential security threats to the network environment, and an effectiveness of the counter measures according to the procedures as discussed above in FIG. **2**.

The recommendations can include any actions, procedures, processes, and the like for improving the security score relative to the potential security threats and the overall security score. For example, the one or more recommendations can include deploying a new counter measure, changing a security setting of the computer assets **102**, changing a system setting of the computer assets **102**, changing a security policy of the computer systems **102**, updating software of the computer assets **102**, installing security software on the computer assets **102**, and improving access information for the computer assets **102**.

In **308**, one or more of the recommendations can be implemented in the network environment **100**. The recommendations can be implemented by the security assessment tool **108**. For example, the security assessment tool **108** can access the computer assets and perform the recommended action, such as deploying a new counter measure, changing a security setting of the computer assets **102**, changing a system setting of the computer assets **102**, changing a security policy of the computer systems **102**, updating software of the computer assets **102**, installing security software on the computer assets **102**, and improving access information for the computer assets **102**.

Likewise, a user or other computer system in the network environment **100** can implement the one or more recommendations. If performed by the user, the security assessment tool **108** can output an identification of the one or more recommendations and instructions for performing the one or more recommendations. For example, if the recommendation is changing a security setting of a particular computer asset **102**, the security assessment tool **108** can output an identification of the particular computer asset **102**, an identification of the security setting to be changed, and instructions for changing the security setting. Based on the output identification and instructions, the user can implement the one or more recommendations.

After the initial assessment, the security assessment tool **108** can perform the security assessment over time to determine have the overall security score changes relative to changes in the network environment **100**. In **310**, the security assessment tool **108** can determine a change in computer assets in a network, change in counter measures deployed, or change in potential security threats. The security assessment tool **108** can rescan the computer assets **102** and determine new security information and changes in the security information. Likewise, the security assessment tool **108** can determine if computer assets **102** have been removed and added. Additionally, the user of the security assessment tool **108** can enter new security information, changes in the security information, and changes in the computer assets **102**. Additionally, the security assessment tool **108** can determine, by examining the threat model **112**, new security threats, changes to existing security threats, new counter measures, and changes to existing counter measures.

In **312**, the security assessment tool **108** can determine a new overall security score and the new recommendations for improving the security score. The overall security scores can represent the initial overall security scores before performing any of the recommendations. The security assessment tool **108** can determine the overall security score based on the actual deployment of the counter measures, the potential security threats to the network environment, and an effectiveness of the counter measures according to the procedures as discussed above in FIG. **2**.

The recommendations can include any actions, procedures, processes, and the like for improving the security score relative to the potential security threats and the overall security score. For example, the one or more recommendations can include deploying a new counter measure, changing a security setting of the computer assets **102**, changing a system setting of the computer assets **102**, changing a security policy of the computer systems **102**, updating software of the computer assets **102**, installing security software on the computer assets **102**, and improving access information for the computer assets **102**.

In **314**, one or more of the new recommendation can be implemented. The new recommendations can be implemented by the security assessment tool **108**. For example, the security assessment tool **108** can access the computer assets and perform the recommended action, such as deploying a new counter measure, changing a security setting of the computer assets **102**, changing a system setting of the computer assets **102**, changing a security policy of the computer systems **102**, updating software of the computer assets **102**, installing security software on the computer assets **102**, and improving access information for the computer assets **102**.

Likewise, a user or other computer system in the network environment **100** can implement the one or more new recommendations. If performed by the user, the security assessment tool **108** can output an identification of the one or more recommendations and instructions for performing the one or more recommendations. For example, if the recommendation is adding a new counter measure, the security assessment tool **108** can output an identification of the counter measure, an identification of the computer assets affected by the new counter measure, and instructions for adding the new counter measure. Based on the output identification and instructions, the user can implement the one or more recommendations.

In **316**, the security assessment tool **108** can repeat the process over time as conditions in the network environment **100** change. The security assessment tool **108** can automatically repeat the process at predefined times or at the predetermined internals. Likewise, the security assessment tool **108** can repeat the process at the request of a user or other computer system.

In **318**, the security assessment tool **108** can perform trending analysis over time. The trending analysis can be any procedure or process that determines how the security assessment changes over time. For example, the security assessment tool **108** can track the change in the overall security (or security scores for potential threats), over time, and output a graph or other indication of the changes over time. Likewise, for example, the security assessment tool **108** can track the change in deployment of counter measures, over time, and output a graph or other indication of the changes over time.

In **320**, the process can end, repeat, or return to any point.

FIGS. **4**A-**4**V illustrate examples GUIs provided by the interface **116** that can be used to communicate with the security assessment tool **108**. The examples of the GUI, as described below, can be provided locally at a computer system executing the security assessment tool **108**, such as displayed on a display. Additionally, the examples of the GUI, as described below, can be provided remotely to computer system, for example, in the form of web pages. Likewise, the examples of the GUIs can be provided via one or more application programming interfaces (APIs) to allow other software programs to interact with the security assessment tool **108**.

As illustrated in FIG. **4**A, the security assessment tool **108** can provide a GUI **400**. In this example, the GUI **400** can allow a user to enter information about themselves that allows the security assessment tool **108** to create an account with the security assessment tool **108**. The GUI **400** can include a window **401** that allows a user to provide their name, a user name, a password, and an email address. The security assessment tool **108** can utilize the account to grant access to the user, store preferences of the user, and the like. Once the account is created, the user can utilize fields and widgets **402** to access the security assessment tool **108** using the username and password.

Once the user has created an account, the security assessment tool **108** can provide a GUI **405** as illustrated in FIG. **4**B. The GUI **405** can allow the user to initiate a scan of the network environment **400**, for example the initial scan of the network environment **400**. The GUI **405** can include fields **406** that allow the user to enter information about the network environment **100**, such as the domain credentials of the network environment **100** that allow the security assessment tool **108** to access the network environment **100**. The GUI **405** can also include a widget **407** that causes the security assessment tool **108** to initiate the scan. During the scan, the security assessment tool **108** can determine the computer assets **102** in the network environment **100** and the security information of the computer assets **102**. As illustrated in FIG. **4**C, the security assessment tool **108** can provide, during the scan, a GUI **408** that shows the progress of the scan.

After the scan in complete, the security assessment tool **108** can determine the overall security assessment for the

network environment **100** and display the results in a GUI **410**, as illustrate din FIG. **4**D-**4**L. As illustrated in FIG. **4**D, the GUI **410** can include fields **411** that display the overall security score and the security scores for each potential security threat. The GUI **410** can also include fields **412** that display the number of computer assets **102** in the network environment **100** scanned and the change in the number of computer assets **102** scanned since the last scan. The GUI **410** also includes a window **413** that displays the potential security threats and the actual coverage of the counter measures. As illustrated, the window **413** can include a description of the counter measures and a graphic (bar meter) that shows the potential security threats and the actual coverage actual deployment of the counter measures addressing the security threat. The graphic can include slider bars that allow a user to set a goal for the actual coverage actual deployment of the counter measures. The window **413** can also include a graphic that shows the change in the actual deployment of the counter measures since the last scan. The GUI **410** can also include a window **414** that shows the recommendations for improving the security scores. The GUI **410** can also include a window **415** that shows details of the computer assets **102**, such as network address, user, type of system, and the risk of the computer asset **102** relative to the potential security threats.

Further, as illustrated in FIG. **4**E, the window **413** can be interact to allow the user to view additional details on more or more of the potential security threats. As illustrated, a user can expand a particular potential security threat to view each counter measure deployed. As illustrated in FIG. **4**F, the window **413**, **414**, and **415** can also be linked. If a user selects a potential threat in window **413**, the recommendations displayed in the window **414** can be sorted for the selected potential security threat, and the computer assets **102** displayed in the window **415** can be the computer assets affected by the selected potential security threat. As illustrated in FIG. **4**G and FIG. **4**I, the window **415** can also be interactive. A user can select a computer asset **102** to view additional details of the computer asset **102** (windows **417** and **418**). As illustrated in FIG. **4**H, the window **414** can also be interactive. The user can select a particular recommendation in the window **414**, and the security assessment tool **108** can display a window **416**. The window **416** can show detailed instructions for implementing the recommendation. The GUI **410** can also include widgets **419**, **420**, and **421** that also the user to view setup tips, progress of an ongoing scan, and specify computer assets **102** to scan, respectively.

The security assessment tool **108** can also allow a user to search for computer assets **102**. FIG. **4**M illustrates a window **422** of a search performed on a network address range "202.160.183.x".

As described above, the security assessment tool **108** can perform trending analysis. FIG. **4**N illustrates an example of a trending analysis performed by the security assessment tool **108**. As illustrated, the security assessment tool **108** can provide a GUI **425**. The GUI **425** can include a graph that shows the trends of the security assessment, for example, change in deployment of a counter measure. As discussed above, the user can use the interface to manage the security assessment tool **108**. FIGS. **40**-**4**Q illustrate a GUI **430** that can be utilized to schedule scans by the security assessment tool **108**. As illustrated, the GUI **430** can include a window **432** that allows a user to specify the details of automatic scan to be performed by the security assessment tool **108**. The GUI **430** can also include fields that display the progress of scan in progress. FIGS. **4**R-**4**V illustrate other GUI that can be used to management to process of the security assessment tool **108**. FIGS. **4**R and **4**S illustrate GUIs **440** and **445** that can be utilized to enter information about the computer assets **102**. FIG. **4**T illustrates a GUI **450** that can be utilized to manage the account information of the user's of the security assessment tool **108**. FIGS. **4**U and **4**V illustrate GUIs **455** and **460** that can be utilized to assign task to users and set goals.

FIG. **5** illustrates an example of a hardware configuration for a computing device **500** implementing the security assessment tool **108** that can be used to perform one or more of the processes described above. While FIG. **5** illustrates various components contained in the computing device **500**, FIG. **5** illustrates one example of a computing device and additional components can be added and existing components can be removed.

As illustrated in FIG. **5**, the computing device **500** can include one or more processors **502** of varying core configurations and clock frequencies. The computing device **500** can also include one or more memory devices **504** that serve as a main memory during the operation of the computing device **500**. For example, during operation, a copy of the security assessment tool **108** can be stored in the one or more memory devices **504**. The computing device **500** can also include one or more peripheral interfaces **506**, such as keyboards, mice, touchpads, computer screens, touchscreens, etc., for enabling human interaction with and manipulation of the computing device **500**.

The computing device **500** can also include one or more network interfaces **508** for communicating via one or more networks, such as Ethernet adapters, wireless transceivers, or serial network components, for communicating over wired or wireless media using protocols. The computing device **500** can also include one or more storage device **510** of varying physical dimensions and storage capacities, such as flash drives, hard drives, random access memory, etc., for storing data, such as images, files, and program instructions for execution by the one or more processors **502**.

Additionally, the computing device **500** can include one or more software programs **512**, such as the security assessment tool **108**. The one or more software programs **512** can include instructions that cause the one or more processors **502** to perform the processes described herein. Copies of the one or more software programs **512** can be stored in the one or more memory devices **504** and/or on in the one or more storage devices **510**. Likewise, the data, for example, utilized by one or more software programs **512** can be stored in the one or more memory devices **504** and/or on in the one or more storage devices **510**.

In implementations, the computing device **500** can communicate with one or more remote user devices **514** and a network environment **518**, such as the network environment **100**, via a network **516**. The one or more remote user devices **514** can be any types of conventional computing devices. For example, the one or more user devices **514** can be desktops, laptops, servers, etc., or mobile devices, such as smart telephones, tablet computers, cellular telephones, personal digital assistants, etc. The network **516** can be any type of network, such as a local area network, a wide-area network, a virtual private network, the Internet, an intranet, an extranet, a public switched telephone network, an infrared network, a wireless network, and any combination thereof. The network **516** can support communications using any of a variety of commercially-available protocols, such as TCP/IP, OSI, FTP, UPnP, NFS, CIFS, and AppleTalk. The network **516** can be, for example, a local area network, a wide-area network, a virtual private network, the Internet, an intranet, an extranet, a public switched telephone network, an infrared network, a wireless network, and any combination thereof.

In implementations, the computing device **500** can exchange data with the one or more user devices **514** and the network environment **518** over the network **516**. For example, the computing device **500** can receive requests to perform security assessments and receive data regarding the security assessment requests.

The computing device **500** and the security assessment tool **108** can be implemented as part of at least one service or Web service, such as may be part of a service-oriented architecture. For example, the computing device **500** can exchange data with the one or more user devices **514** during operation of the at least one service or Web service. Services such as Web services can communicate using any appropriate type of messaging, such as by using messages in extensible markup language (XML) format and exchanged using an appropriate protocol such as SOAP (derived from the "Simple Object Access Protocol"). Processes provided or executed by such services can be written in any appropriate language, such as the Web Services Description Language (WSDL). Using a language such as WSDL allows for functionality such as the automated generation of client-side code in various SOAP frameworks.

In implementations the computing device **500** can be utilized as part of a Web server architecture. In the Web server architecture, the computing device **500** can run any of a variety of server or mid-tier applications, including HTTP servers, FTP servers, CGI servers, data servers, Java servers, and business application servers. The computing device **500** also can be capable of executing programs or scripts in response requests from the one or more remote user devices **514**, such as by executing one or more Web applications that may be implemented as one or more scripts or programs written in any programming language, such as Java®, C, C# or C++, or any scripting language, such as Perl, Python, or TCL, as well as combinations thereof. The computing device **500** can also include database servers, including without limitation those commercially available from Oracle®, Microsoft®, Sybase®, and IBM®.

The computing device **500** can include a variety of data stores and other memory and storage media as discussed above. These can reside in a variety of locations, such as on a storage medium local to (and/or resident in) one or more of the computers or remote from any or all of the computers across the network. In some implementations, information can reside in a storage-area network ("SAN") familiar to those skilled in the art. Similarly, any necessary files for performing the functions attributed to the computers, servers, or other network devices may be stored locally and/or remotely, as appropriate.

In implementations, the components of the computing device **500** as described above need not be enclosed within a single enclosure or even located in close proximity to one another. Those skilled in the art will appreciate that the above-described componentry are examples only, as the computing device **500** can include any type of hardware componentry, including any necessary accompanying firmware or software, for performing the disclosed implementations. The computing device **500** can also be implemented in part or in whole by electronic circuit components or processors, such as application-specific integrated circuits (ASICs) or field-programmable gate arrays (FPGAs).

Certain implementations described above can be performed as a computer applications or programs. The computer program can exist in a variety of forms both active and inactive. For example, the computer program can exist as one or more software programs, software modules, or both that can be comprised of program instructions in source code, object code, executable code or other formats; firmware program(s); or hardware description language (HDL) files. Any of the above can be embodied on a computer readable medium, which include computer readable storage devices and media, and signals, in compressed or uncompressed form. Examples of computer readable storage devices and media include conventional computer system RAM (random access memory), ROM (read-only memory), EPROM (erasable, programmable ROM), EEPROM (electrically erasable, programmable ROM), and magnetic or optical disks or tapes. Examples of computer readable signals, whether modulated using a carrier or not, are signals that a computer system hosting or running the present teachings can be configured to access, including signals downloaded through the Internet or other networks. Concrete examples of the foregoing include distribution of executable software program(s) of the computer program on a CD-ROM or via Internet download. In a sense, the Internet itself, as an abstract entity, is a computer readable medium. The same is true of computer networks in general.

While the teachings have been described with reference to examples of the implementations thereof, those skilled in the art will be able to make various modifications to the described implementations without departing from the true spirit and scope. The terms and descriptions used herein are set forth by way of illustration only and are not meant as limitations. In particular, although the method has been described by examples, the steps of the method may be performed in a different order than illustrated or simultaneously. Furthermore, to the extent that the terms "including", "includes", "having", "has", "with", or variants thereof are used in either the detailed description and the claims, such terms are intended to be inclusive in a manner similar to the term "comprising." As used herein, the terms "one or more of" and "at least one of" with respect to a listing of items such as, for example, A and B, means A alone, B alone, or A and B. Further, unless specified otherwise, the term "set" should be interpreted as "one or more." Also, the term "couple" or "couples" is intended to mean either an indirect or direct connection. Thus, if a first device couples to a second device, that connection may be through a direct connection, or through an indirect connection via other devices, components, and connections.

What is claimed is:

**1**. A computer-implemented method for determining an objective security assessment for a network, the method comprising:

determining computer assets in the network;

determining an actual deployment of counter measures associated with the network, wherein the counter measures address potential security threats to the network;

determining, by a processor, an overall security score for the network based at least in part on the actual deployment of the counter measures and an effectiveness of the counter measures;

determining at least one recommendation for improving the overall security score; and

outputting the at least one recommendation and the overall security score,

wherein the overall security score comprises a security score of each of the counter measures associated with the computer assets, the security score of each of the counter measures being based at least in part on an actual effectiveness score that represents the actual deployment of each of the counter measures and a possible effectiveness score that represents a possible deployment of each of the counter measures, and

wherein outputting the at least one recommendation and the overall security score further comprises outputting the security score of each of the counter measures deployed on the computer assets.

**2**. The computer-implemented method of claim **1**, the method further comprising:

determining, at a later time, a change in the actual deployment of the counter measures; and

determining a new overall security score for the network based at least in part on the change in the actual deployment and the effectiveness of the counter measures.

**3**. The computer-implemented method of claim **2**, the method further comprising:

outputting the new overall security score;

outputting a change in the new overall security score relative to the overall security score; and

outputting at least one new recommendation for improving the overall security score.

**4**. The computer-implemented method of claim **2**, wherein the change in the actual deployment corresponds to at least one of a performance of the at least one recommendation and a change in the computer assets in the network.

**5**. The computer-implemented method of claim **1**, wherein determining the assets in the computer network comprises at least one of:

scanning the network for one or more of the computer assets; and

receiving, via an interface, an identification of one or more of the computer assets.

**6**. The computer-implemented method of claim **1**, wherein determining the actual deployment of counter measures comprises:

determining security information of the computer assets, wherein the security information comprises at least one of identification of security software installed on the computer assets, vulnerabilities on the computer assets, system settings of the computer assets, security settings of the computer assets, configuration policies of the computer assets, security policies of the computer assets, access information for the computer assets, details of software installed on the computer assets, and a comparison of the access information and the security setting for the computer assets;

determining, based at least in part on the security information, at least one of the counter measures associated with the network; and

determining, based at least in part on the security information, a coverage of the at least one of the counter measures within the network.

**7**. The computer-implemented method of claim **6**, wherein determining the security information comprises at least one of:

receiving, via an interface, a portion of the security information from a user; and

automatically discovering a portion of the security information.

**8**. The computer-implemented method of claim **1**, wherein the actual effectiveness and the possible effectiveness of the counter measures is based on at least one of:

empirical testing of counter measures versus actual security threats; survey of security experts including commonly understood best practices; and results of findings by security research organizations.

**9**. The computer-implemented method of claim **1**, wherein the at least one recommendation comprises at least one of deploying a new counter measure, changing a security setting of the computer assets, changing a system setting of the computer assets, changing a security policy of the computer assets, updating software of the computer assets, installing security software on the computer assets, and improving access information for the computer assets.

**10**. The computer-implemented method of claim **1**, the method further comprising:

receiving, via an interface, a selection of the at least one recommendation; and

outputting instructions for implementing the at least one recommendation.

**11**. The computer-implemented method of claim **1**, the method further comprising:

determining an amount that each of the potential security threats contributes to the overall security score;

ranking each of the potential security threats based at least in part on one of the frequency of the threat in empirical testing, the potential impact of the threat, or likelihood of the threat succeeding to determine the amount that each of the potential security threats contributes to the overall security score; and

outputting the potential security threats ordered according to the ranking.

**12**. The computer-implemented method of claim **11**, the method further comprising:

receiving, via an interface, at least one of the potential security threats that is a priority;

re-ranking each of the potential security threats based at least in part on the at least one of the potential security threats being a priority; and

outputting the potential security threats ordered according to the re-ranking.

**13**. The computer-implemented method of claim **1**, wherein the computer assets comprises at least one of a physical computer system, physical computer hardware, and a virtual computer system.

**14**. A system for determining an objective security assessment, the system comprising:

a network interface to a network of computer assets;

one or more memory device storing instructions; and

one or more processors coupled to the network interface and the one or more memory devices, the one or more processors being configured to execute the instructions to perform a method comprising:

determining computer assets in the network;

determining an actual deployment of counter measures associated with the network, wherein the counter measures address potential security threats to the network;

determining an overall security score for the network based at least in part on the actual deployment of the counter measures and an effectiveness of the counter measures;

determining at least one recommendation for improving the overall security score; and

outputting the at least one recommendation and the overall security score,

wherein the overall security score comprises a security score of each of the counter measures associated with the computer assets, the security score of each of the counter measures being based at least in part on an actual effectiveness score that represents the actual deployment of each of the counter measures and a possible effectiveness score that represents a possible deployment of each of the counter measures, and

wherein outputting the at least one recommendation and the overall security score further comprises output-

ting the security score of each of the counter measures deployed on the computer assets.

**15**. The system of claim **14**, wherein the one or more processors are configured to execute the instructions to perform the method further comprising:

determining, at a later time, a change in the actual deployment of the counter measures; and

determining a new overall security score for the network based at least in part on the change in the actual deployment and the effectiveness of the counter measures.

**16**. The system of claim **15**, wherein the one or more processors are configured to execute the instructions to perform the method further comprising:

outputting the new overall security score;

outputting a change in the new overall security score relative to the overall security score; and

outputting at least one new recommendation for improving the overall security score.

**17**. The system of claim **15**, wherein the change in the actual deployment corresponds to at least one of a performance of the at least one recommendation and a change in the computer assets in the network.

**18**. The system of claim **14**, wherein determining the assets in the computer network comprises at least one of:

scanning the network for one or more of the computer assets; and

receiving, via an interface, an identification of one or more of the computer assets.

**19**. The system of claim **14**, wherein determining the actual deployment of counter measures comprises:

determining security information of the computer assets, wherein the security information comprises at least one of identification of security software installed on the computer assets, vulnerabilities on the computer assets, system settings of the computer assets, security settings of the computer assets, configuration policies of the computer assets, security policies of the computer assets, access information for the computer assets, details of software installed on the computer assets, and a comparison of the access information and the security setting for the computer assets;

determining, based at least in part on the security information, at least one of the counter measures associated with the network; and

determining, based at least in part on the security information, a coverage of the at least one of the counter measures within the network.

**20**. The system of claim **19**, wherein determining the security information comprises at least one of:

receiving, via an interface, a portion of the security information from a user; and

automatically discovering a portion of the security information.

**21**. The system of claim **14**, wherein the actual effectiveness and the possible effectiveness of the counter measures is based on at least one of:

empirical testing of counter measures versus actual security threats; survey of security experts including commonly understood best practices; and results of findings by security research organizations.

**22**. The system of claim **14**, wherein the at least one recommendation comprises at least one of deploying a new counter measure, changing a security setting of the computer assets, changing a system setting of the computer assets, changing a security policy of the computer assets, updating software of the computer assets, installing security software on the computer assets, and improving access information for the computer assets.

**23**. The system of claim **14**, wherein the one or more processors are configured to execute the instructions to perform the method further comprising:

receiving, via an interface, a selection of the at least one recommendation; and

outputting instructions for implementing the at least one recommendation.

**24**. The system of claim **14**, wherein the one or more processors are configured to execute the instructions to perform the method further comprising:

determining an amount that each of the potential security threats contributes to the overall security score;

ranking each of the potential security threats based at least in part on one of the frequency of the threat in empirical testing, the potential impact of the threat, or likelihood of the threat succeeding to determine the amount that each of the potential security threats contributes to the overall security score; and

outputting the potential security threats ordered according to the ranking.

**25**. The system of claim **24**, wherein the one or more processors are configured to execute the instructions to perform the method further comprising:

receiving, via an interface, at least one of the potential security threats that is a priority;

re-ranking each of the potential security threats based at least in part on the at least one of the potential security threats being a priority; and

outputting the potential security threats ordered according to the re-ranking.

**26**. The system of claim **14**, wherein the computer assets comprises at least one of a physical computer system, physical computer hardware, and a virtual computer system.

**27**. A non-transitory computer readable storage medium comprising instructions for causing one or more processors to perform a method for determining an objective security assessment for a network, the method comprising:

determining computer assets in the network;

determining, by a security assessment tool, an actual deployment of counter measures associated with the network, wherein the counter measures address potential security threats to the network;

determining, by a processor, an overall security score for the network based at least in part on the actual deployment of the counter measures and an effectiveness of the counter measures;

determining at least one recommendation for improving the overall security score; and

outputting the at least one recommendation and the overall security score,

wherein the overall security score comprises a security score of each of the counter measures associated with the computer assets, the security score of each of the counter measures being based at least in part on an actual effectiveness score that represents the actual deployment of each of the counter measures and a possible effectiveness score that represents a possible deployment of each of the counter measures, and

wherein outputting the at least one recommendation and the overall security score further comprises outputting the security score of each of the counter measures deployed on the computer assets.

**28**. The non-transitory computer readable storage medium of claim **27**, the method further comprising:

determining, at a later time, a change in the actual deployment of the counter measures; and

determining a new overall security score for the network based at least in part on the change in the actual deployment and the effectiveness of the counter measures.

**29**. The non-transitory computer readable storage medium of claim **28**, the method further comprising:

outputting the new overall security score;

outputting a change in the new overall security score relative to the overall security score; and

outputting at least one new recommendation for improving the overall security score.

**30**. The non-transitory computer readable storage medium of claim **28**, wherein the change in the actual deployment corresponds to at least one of a performance of the at least one recommendation and a change in the computer assets in the network.

**31**. The non-transitory computer readable storage medium of claim **27**, wherein determining the assets in the computer network comprises at least one of:

scanning the network for one or more of the computer assets; and

receiving, via an interface, an identification of one or more of the computer assets.

**32**. The non-transitory computer readable storage medium of claim **27**, wherein determining the actual deployment of counter measures comprises:

determining security information of the computer assets, wherein the security information comprises at least one of identification of security software installed on the computer assets, vulnerabilities on the computer assets, system settings of the computer assets, security settings of the computer assets, configuration policies of the computer assets, security policies of the computer assets, access information for the computer assets, details of software installed on the computer assets, and a comparison of the access information and the security setting for the computer assets;

determining, based at least in part on the security information, at least one of the counter measures associated with the network; and

determining, based at least in part on the security information, a coverage of the at least one of the counter measures within the network.

**33**. The non-transitory computer readable storage medium of claim **32**, wherein determining the security information comprises at least one of:

receiving, via an interface, a portion of the security information from a user; and

automatically discovering a portion of the security information.

**34**. The non-transitory computer readable storage medium of claim **27**, wherein the actual effectiveness and the possible effectiveness of the counter measures is based on at least one of:

empirical testing of counter measures versus actual security threats; survey of security experts including commonly understood best practices; and results of findings by security research organizations.

**35**. The non-transitory computer readable storage medium of claim **27**, wherein the at least one recommendation comprises at least one of deploying a new counter measure, changing a security setting of the computer assets, changing a system setting of the computer assets, changing a security policy of the computer assets, updating software of the computer assets, installing security software on the computer assets, and improving access information for the computer assets.

**36**. The non-transitory computer readable storage medium of claim **27**, the method further comprising:

receiving, via an interface, a selection of the at least one recommendation; and

outputting instructions for implementing the at least one recommendation.

**37**. The non-transitory computer readable storage medium of claim **27**, the method further comprising:

determining an amount that each of the potential security threats contributes to the overall security score;

ranking each of the potential security threats based at least in part on one of the frequency of the threat in empirical testing, the potential impact of the threat, or likelihood of the threat succeeding to determine the amount that each of the potential security threats contributes to the overall security score; and

outputting the potential security threats ordered according to the ranking.

**38**. The non-transitory computer readable storage medium of claim **37**, the method further comprising:

receiving, via an interface, at least one of the potential security threats that is a priority;

re-ranking each of the potential security threats based at least in part on the at least one of the potential security threats being a priority; and

outputting the potential security threats ordered according to the re-ranking.

**39**. The non-transitory computer readable storage medium of claim **27**, wherein the computer assets comprises at least one of a physical computer system, physical computer hardware, and a virtual computer system.

* * * * *