# Table of Contents

## Overview
- Knowledge Assessment Reports ................................................................. 3
  - CyberStrength Performance Report ............................................................. 3
  - Knowledge Assessment and Training Progress Report ............................... 7

## Phishing Simulation Reports ................................................................. 9
- Phishing Campaign Performance Report ...................................................... 9
- Phishing User Performance Report .............................................................. 12
- ThreatSim Campaign Overview Report ......................................................... 14
- ThreatSim Reports on Individual Campaign Details ...................................... 15
- ThreatSim Raw Campaign Data CSV Reports .............................................. 18
- ThreatSim USB Campaign Details Report .................................................. 19

## Reported Email Performance and Analysis ........................................... 20
- PhishAlarm Analyzer Report ........................................................................ 20
- Reported Email Performance Report .......................................................... 21

## Training Reports .................................................................................... 23
- Knowledge Assessment & Training Progress Report .................................... 23
- Training Assignment Performance Report ................................................. 23
- Training Category Performance Report ....................................................... 25
- Training Module Performance Report ......................................................... 28
- Training Report Card .................................................................................. 32

## Users ........................................................................................................ 33
- User Record Export Report ......................................................................... 33
OVERVIEW

Proofpoint’s **Security Education Platform** captures each employee’s interaction with our simulated attacks, knowledge assessments, and interactive training. This means that security officers quickly have detailed information about not only who completed which assignments, but also in which topics they are strong or weak, and how they have improved over time. All user data can be characterized, filtered, and reported using administrator-defined fields, such as job function, geographic location, department, hire date, and role.

Administrators can export reports to various output formats, such as Excel and CSV, to easily share results with interested parties. Reports can be generated any time. Additionally, with our Scheduled Export feature, you can automatically send reports to managers and administrators to track progress, gauge results, and plan accordingly. This feature allows administrators to define recipients, frequency, time, and format of the report output, which aids in sharing the responsibility of driving completion of assessment training. For an LMS implementation, user performance data and results for our training modules are based on the reporting capabilities of the LMS system used.

Below is a summary of reports available in the Security Education Platform. For more details about each report, please refer to the sections that follow in the guide.

### Reports

| Knowledge Assessment                      | • CyberStrength Performance Report |
|                                         | • Knowledge Assessment and Training Progress Report* |
| Phishing Simulation                      | • Phishing Campaign Performance Report |
|                                         | • Phishing User Performance Report |
|                                         | • ThreatSim Campaign Overview Report |
|                                         | • ThreatSim Raw Campaign Data CSV Report |
|                                         | • ThreatSim Reports on Individual Campaign Details |
|                                         | o All Email Campaigns History |
|                                         | o Individual Campaign Overview |
|                                         | o Geographic Distribution |
|                                         | o Endpoints |
|                                         | o Users |
|                                         | • ThreatSim USB Campaign Details Report |
| Reported Email Performance and Analysis  | • Reported Email Performance Report |
|                                         | • PhishAlarm Analyzer Report |
| Training                                | • Knowledge Assessment and Training Progress Report* |
|                                         | • Training Assignment Performance Report |
|                                         | • Training Category Performance Report |
|                                         | • Training Module Performance Report |
|                                         | • Training Report Card |
| Users                                   | User Record Export Report |

* Report pertains to both areas.
KNOWLEDGE ASSESSMENT REPORTS

The reports in this section pertain to CyberStrength assessments. They include:

- CyberStrength Performance Report
- Knowledge Assessment & Training Progress Report

CYBERSTRENGTH PERFORMANCE REPORT

OBJECTIVE

The CyberStrength Performance Report displays a comprehensive array of user and assessment data so that organizations can track the progress and performance of their CyberStrength assignments.

BENEFITS

- Track the progress and performance of the organization’s cybersecurity initiatives.
- Quickly identify security risk at the organization, department, and user level or any other defined custom grouping.
- Benchmark the organization’s performance data against the same or other industries, other Proofpoint customers, and the organization itself over time to gauge results and develop an action plan to improve or maintain a competitive edge.

FEATURES

- Determine the organization’s weaknesses and strengths across a range of cybersecurity areas, identify the riskiest users or business units, identify the most missed question categories, and customize programs to reduce the identified risks.
- Track user progress and performance across all CyberStrength assignments.
- Compare company performance against the same or other industries, Proofpoint customers, and the organization itself over time.
- Display aggregate and detail-level data per assessment, user, category, and other customizable properties.
- Export options: Excel and CSV.

SCREENSHOT OF CYBERSTRENGTH PERFORMANCE REPORT

(see next page)
SCREENSHOT OF CYBERSTRENGTH PERFORMANCE REPORT (CONT.)

View includes Users Tab
View of Assignments Tab

View of Categories Tab
View of Questions Tab

- **Aggregate By**
  - Department

- **Question Performance**
  - Question: A company should only collect and store personally identifiable information (PII) that is necessary for its business.
  - Performance:
    - Department: XYZ
    - Performance: 50.52%
    - Number of Users: 20
    - Average Time to Complete (Seconds): 35.00
  - Question: A good friend from high school you haven’t seen in years sends a connection request through social media. It’s OK to accept the friend request.
  - Performance:
    - Department: ABC
    - Performance: 80.60%
    - Number of Users: 20
    - Average Time to Complete (Seconds): 35.00

- **Question Scores by Department**
  - Department: Human Resources
    - Question: A company should only collect and store personally identifiable information (PII) that is necessary for its business.
    - Score: 50.52%
  - Department: Human Resources
    - Question: A good friend from high school you haven’t seen in years sends a connection request through social media. It’s OK to accept the friend request.
    - Score: 80.60%

View of Leaderboard Tab

- **User Ranking**
  - Rank 1: Daniel Reed
carol.green@mydomain1.com
  - Rank 2: Carol Green
carol.green@mydomain1.com
  - Rank 3: Gary Peterson
gary.peterson@mydomain2.com
  - Rank 4: Jack Richardson
  - Rank 5: Scott Coss
  - Rank 6: Thomas Morgan
  - Rank 7: Angela Bennett
  - Rank 8: Karen Stewart
  - Rank 9: Laura Edwards
  - Rank 10: Helen Lee
  - Rank 11: Betty Adams
  - Rank 12: Carol Green
carol.green@mydomain1.com
  - Rank 13: Jennifer Diaz
  - Rank 14: Kathleen Green
  - Rank 15: Jessica Williams
  - Rank 16: Ryan Diaz
  - Rank 17: Donna Stewart
da donna.stewart@mydomain3.com
  - Rank 18: Karen Carter
innovate@barlow@mydomain4.com

User ranking is determined by the User’s score on the assignment, then the number of days to complete the assignment.
KNOWLEDGE ASSESSMENT AND TRAINING PROGRESS REPORT

OBJECTIVES

The Knowledge Assessment and Training Progress Report displays results and information regarding end users’ progress completing CyberStrength assessments and training modules. It lists the assignment and module completion status for all users by percentage Completed, In Progress, and Not Started.

BENEFITS

- Quickly compare completion rates across training assignments to determine which assignments require additional action to drive them to completion.
- Track all users’ progress on all CyberStrength assessments and training assignments in a single report, gauging their effectiveness at completing assignments.
- At-a-glance view of overall results and status of training assignments.
- Ability to drill-down to assignment-level details.

KEY FEATURES

- Provides a variety of filtering options, such as by assignment, start/due date, overall assignment progress, user assignment progress, and auto enrollment assignments.
- Flexibility to select which data fields to include or exclude from the table to meet specific analysis needs.
- Displays key performance indicators for the total number of training modules, categories, correct responses, and incorrect responses.
- Displays user progress by assignment as well as assignment details.
- Results can be compared across assignments, with the ability to include or exclude deleted assignments, deleted users, and users removed from the assignments.
- Displays users’ progress in CyberStrength assessments and training assignments.
- Displays completion percentage per module that is part of an assignment.
- One-page display of all numbers and percentage details about a specific assignment and the modules included in it.
- Multiple assignments can be displayed and compared at one time.
- Export options: Excel and CSV
Knowledge Assessment and Training Progress

Track user progress in completing CyberStrength knowledge assessments and training assignments to identify follow-up steps.

Data updated daily. Last update: 2020-Jan-29 at 23:29 (UTC) (20 hours ago)

Assignment Details Table

<table>
<thead>
<tr>
<th>Assignment</th>
<th>Overall Assignment Progress</th>
<th>Start Date</th>
<th>User Assignments</th>
<th>Users Completed</th>
<th>Percent Completed</th>
<th>Product Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>2020 Cyber Assignment 1</td>
<td>Completed</td>
<td>2020-01-01</td>
<td>1</td>
<td>1</td>
<td>100.00%</td>
<td>CyberStrength</td>
</tr>
<tr>
<td>2020 Cyber Assignment 2</td>
<td>Completed</td>
<td>2020-01-02</td>
<td>1</td>
<td>1</td>
<td>100.00%</td>
<td>CyberStrength</td>
</tr>
<tr>
<td>2020 Cyber Assignment 3</td>
<td>Not Started</td>
<td>2020-01-03</td>
<td>1</td>
<td>0</td>
<td>0.00%</td>
<td>Training</td>
</tr>
<tr>
<td>Followup 2020 Cyber Assignment 1</td>
<td>Not Started</td>
<td>2020-01-04</td>
<td>2</td>
<td>2</td>
<td>100.00%</td>
<td>CyberStrength</td>
</tr>
<tr>
<td>2020 Cyber Assignment 4</td>
<td>Completed</td>
<td>2020-01-05</td>
<td>1</td>
<td>1</td>
<td>100.00%</td>
<td>CyberStrength</td>
</tr>
<tr>
<td>2020 Cyber Assignment 5</td>
<td>Completed</td>
<td>2020-01-06</td>
<td>1</td>
<td>1</td>
<td>100.00%</td>
<td>CyberStrength</td>
</tr>
<tr>
<td>2020 Cyber Assignment 6</td>
<td>Completed</td>
<td>2020-01-07</td>
<td>1</td>
<td>1</td>
<td>100.00%</td>
<td>CyberStrength</td>
</tr>
<tr>
<td>2020 Cyber Assignment 7</td>
<td>Completed</td>
<td>2020-01-08</td>
<td>1</td>
<td>1</td>
<td>100.00%</td>
<td>CyberStrength</td>
</tr>
<tr>
<td>2020 Cyber Assignment 8</td>
<td>Completed</td>
<td>2020-01-09</td>
<td>1</td>
<td>1</td>
<td>100.00%</td>
<td>CyberStrength</td>
</tr>
<tr>
<td>2020 Cyber Assignment 9</td>
<td>Completed</td>
<td>2020-01-10</td>
<td>1</td>
<td>1</td>
<td>100.00%</td>
<td>CyberStrength</td>
</tr>
<tr>
<td>2020 Cyber Assignment 10</td>
<td>Completed</td>
<td>2020-01-11</td>
<td>1</td>
<td>1</td>
<td>100.00%</td>
<td>CyberStrength</td>
</tr>
<tr>
<td>2020 Cyber Assignment 11</td>
<td>Completed</td>
<td>2020-01-12</td>
<td>1</td>
<td>1</td>
<td>100.00%</td>
<td>CyberStrength</td>
</tr>
<tr>
<td>2020 Cyber Assignment 12</td>
<td>Completed</td>
<td>2020-01-13</td>
<td>1</td>
<td>1</td>
<td>100.00%</td>
<td>CyberStrength</td>
</tr>
<tr>
<td>2020 Cyber Assignment 13</td>
<td>Completed</td>
<td>2020-01-14</td>
<td>1</td>
<td>1</td>
<td>100.00%</td>
<td>CyberStrength</td>
</tr>
<tr>
<td>2020 Cyber Assignment 14</td>
<td>Completed</td>
<td>2020-01-15</td>
<td>1</td>
<td>1</td>
<td>100.00%</td>
<td>CyberStrength</td>
</tr>
<tr>
<td>2020 Cyber Assignment 15</td>
<td>Completed</td>
<td>2020-01-16</td>
<td>1</td>
<td>1</td>
<td>100.00%</td>
<td>CyberStrength</td>
</tr>
<tr>
<td>2020 Cyber Assignment 16</td>
<td>Completed</td>
<td>2020-01-17</td>
<td>1</td>
<td>1</td>
<td>100.00%</td>
<td>CyberStrength</td>
</tr>
<tr>
<td>2020 Cyber Assignment 17</td>
<td>Completed</td>
<td>2020-01-18</td>
<td>1</td>
<td>1</td>
<td>100.00%</td>
<td>CyberStrength</td>
</tr>
<tr>
<td>2020 Cyber Assignment 18</td>
<td>Completed</td>
<td>2020-01-19</td>
<td>1</td>
<td>1</td>
<td>100.00%</td>
<td>CyberStrength</td>
</tr>
<tr>
<td>2020 Cyber Assignment 19</td>
<td>Completed</td>
<td>2020-01-20</td>
<td>1</td>
<td>1</td>
<td>100.00%</td>
<td>CyberStrength</td>
</tr>
<tr>
<td>2020 Cyber Assignment 20</td>
<td>Completed</td>
<td>2020-01-21</td>
<td>1</td>
<td>1</td>
<td>100.00%</td>
<td>CyberStrength</td>
</tr>
</tbody>
</table>
PHISHING SIMULATION REPORTS

The reports in this section pertain to ThreatSim phishing campaigns. They include:

- Phishing Campaign Performance Report
- Phishing User Performance Report
- ThreatSim Campaign Overview Report
- ThreatSim Reports on Individual Campaign Details
- ThreatSim Raw Campaign Data CSV Reports
- ThreatSim USB Campaign Details Report

PHISHING CAMPAIGN PERFORMANCE REPORT

OBJECTIVES

The Phishing Campaign Performance Report aggregates the results of multiple phishing campaigns, reflects overall performance results, displays failure trends, and shows how individuals performed in each campaign received. Administrators can compare campaign performance level trends based on overall failure rates and individual events (such as, email viewed, link clicked, attachment opened).

BENEFITS

- Determine at the campaign- and user-level which campaign types end users are most vulnerable to so that additional campaigns can be developed and implemented.
- Drill-down to the user-level details to enable deeper analysis.
- Track phishing failure performance over time and use the trends to determine the organization’s optimal security awareness training programs.
- Compare campaigns types alongside each other to gain at-a-glance insight into the most effective campaigns and campaign types.

KEY FEATURES

- Provides a variety of filtering options, such as by campaign type and status, start and end date range, and include/exclude archived campaigns.
- Flexibility to select which data fields to include or exclude from the table to meet specific analysis needs.
- Displays key performance indicators for number of campaigns, number of phish, emails sent, and emails reported.
- Provides details about each current and past campaign as well as the participating end users.
- Shows user behavior statistics for individual campaigns, such as how many times each user viewed, clicked, opened an attachment, and/or submitted data.
- Compares performance results of different campaigns, whether of the same type or different type.
- Displays the failure trend of campaigns and number of reported emails of a campaign over time.
- Export options: Excel and CSV
SCREENSHOT OF PHISHING CAMPAIGN PERFORMANCE REPORT

View with Campaign Comparison Report

Phishing Campaign Performance

Analysis and case results on email phishing simulations are compared against campaigns and across campaigns to assess organizational susceptibility to attack.


Number of Campaigns: 6
Number of Phish: 205
Threats Sent: 205
Threats Reported: 26

Campaign Performance

Failure Trend

Reported Emails

Unique Clicks: 84
Emails Viewed: 154
Data Submitted: 34
Click Rate (%): 41

Campaign Comparison

© 2020 Proofpoint, Inc. Private and confidential.
### View of Campaign Details Tab

<table>
<thead>
<tr>
<th>First Name</th>
<th>Last Name</th>
<th>Email Address</th>
<th>Campaign Name</th>
<th>Total Views</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alexander</td>
<td>Carter</td>
<td><a href="mailto:alexander.carter@bryanco.workspa.com">alexander.carter@bryanco.workspa.com</a></td>
<td>2020 Phishing Campaign 5</td>
<td></td>
</tr>
<tr>
<td>Amanda</td>
<td>Collins</td>
<td><a href="mailto:amanda.collins@bryanco.workspa.com">amanda.collins@bryanco.workspa.com</a></td>
<td>2020 Phishing Campaign 6</td>
<td></td>
</tr>
<tr>
<td>Amanda</td>
<td>Rogers</td>
<td><a href="mailto:amanda.rogers@bryanco.workspa.com">amanda.rogers@bryanco.workspa.com</a></td>
<td>2020 Phishing Campaign 7</td>
<td></td>
</tr>
<tr>
<td>Amy</td>
<td>Bailey</td>
<td><a href="mailto:amy.bailey@bryanco.workspa.com">amy.bailey@bryanco.workspa.com</a></td>
<td>2020 Phishing Campaign 8</td>
<td></td>
</tr>
<tr>
<td>Amy</td>
<td>Brown</td>
<td><a href="mailto:amy.brown@bryanco.workspa.com">amy.brown@bryanco.workspa.com</a></td>
<td>2020 Phishing Campaign 9</td>
<td></td>
</tr>
<tr>
<td>Amy</td>
<td>Gray</td>
<td><a href="mailto:amy.gray@bryanco.workspa.com">amy.gray@bryanco.workspa.com</a></td>
<td>2020 Phishing Campaign 10</td>
<td></td>
</tr>
<tr>
<td>Amy</td>
<td>Kelly</td>
<td><a href="mailto:amy.kelly@bryanco.workspa.com">amy.kelly@bryanco.workspa.com</a></td>
<td>2020 Phishing Campaign 11</td>
<td></td>
</tr>
<tr>
<td>Amy</td>
<td>Lee</td>
<td><a href="mailto:amy.lee@bryanco.workspa.com">amy.lee@bryanco.workspa.com</a></td>
<td>2020 Phishing Campaign 12</td>
<td></td>
</tr>
<tr>
<td>Andrew</td>
<td>Wood</td>
<td><a href="mailto:andrew.wood@bryanco.workspa.com">andrew.wood@bryanco.workspa.com</a></td>
<td>2020 Phishing Campaign 13</td>
<td></td>
</tr>
<tr>
<td>Brenda</td>
<td></td>
<td><a href="mailto:brenda@bryanco.workspa.com">brenda@bryanco.workspa.com</a></td>
<td>2020 Phishing Campaign 14</td>
<td></td>
</tr>
</tbody>
</table>

- **Total Clicks**: 84
- **Tracking View Count**: 205
- **Data Entry Count**: 67
- **Auto Enroll Email Count**: 103
PHISHING USER PERFORMANCE REPORT

OBJECTIVE

The Phishing User Performance Report analyzes users’ interactions with simulated phishing attack campaigns, causes of single failures, and identifies repeat offenders.

BENEFITS

- Assists in identifying simulated phishing attack campaigns, campaign types, and templates that might be more effective than others within their organization.
- Focus on the phishing risk at the campaign, department, and individual user level to identify and tailor security awareness training programs.
- Instantly identify riskiest users and repeat offenders to perform immediate corrective action.

KEY FEATURES

- Displays detailed charts showing results and statistical information about users who fell for the phishing campaigns.
- Compares results of campaigns grouped by most failed users, templates, campaigns, departments, as well as any other groupings uploaded into the Platform.
- Shows repeat offenders who can be grouped and targeted for additional training.
- Outlines the comparisons of failure results for different users, departments, templates, campaigns and campaign types all in one report.
- Export options: Excel and CSV.

SCREENSHOT OF PHISHING USER PERFORMANCE REPORT

(see next page)
SCREENSHOT OF PHISHING USER PERFORMANCE REPORT (CONT.)

Phishing User Performance

Analyze users' interactions with simulated phishing attack campaigns, causes of failure, and identify repeat attackers for future campaigns and training.

Data updated daily. Last update: 2020-01-29 at 23:36 (UTC) (21 hours ago)

Overall Failure Rate (%)

41.0%

Failed Users

80

Unique Failures

84

Threats Sent

205

Aggregate By

Department

Department Details

Department | Overall Failure Rate (%) | Unique Failures
--- | --- | ---
IT | 0% | 0
Marketing | 0% | 0
Human Resources | 0% | 0
Sales | 0% | 0

User Platform Status

Active

Campaign Type

Campaign Status

Campaign Name

Campaign Start Date

Min No. of Campaign Failures

User Details

First Name | Last Name | Email Address | Number of Unique Failures | Overall Failure Rate (%) | Data Entry | Attach. Campaign
--- | --- | --- | --- | --- | --- | ---
Alexander | Carter | alexander.carter@phishing.com | 0 | 0% | 0 | 0
Alexander | Edwards | alexander.edwards@phishing.com | 0 | 0% | 0 | 0
Amanda | Cobbs | amanda.cobbs@phishing.com | 0 | 0% | 0 | 0
Amanda | Rogers | amanda.rogers@phishing.com | 0 | 0% | 0 | 0
Amy | Bailey | amy.bailey@phishing.com | 1 | 100% | 1 | 1
Amy | Brown | amy.brown@phishing.com | 1 | 100% | 1 | 1
Amy | Gray | amy.gray@phishing.com | 0 | 0% | 0 | 0
Amy | Kelly | amy.kelly@phishing.com | 0 | 0% | 0 | 0
Amy | Lee | amy.lee@phishing.com | 0 | 0% | 0 | 0
Andrew | Wood | andrew.wood@phishing.com | 0 | 0% | 0 | 0
Angela | Gonzalez | angela.gonzalez@phishing.com | 0 | 0% | 0 | 0
Angela | Hughes | angela.hughes@phishing.com | 0 | 0% | 0 | 0

Campaign Details

Campaign Name | Overall Failure Rate (%) | Unique Failures | Threats Sent | Campaign Type
--- | --- | --- | --- | ---
2020 Phishing Campaign 4 | 58.82% | 20 | 34 | Data Entry
2020 Phishing Campaign 5 | 42.20% | 19 | 24 | Attachment
2020 Phishing Campaign 6 | 46.39% | 13 | 20 | Attachment
2020 Phishing Campaign 7 | 42.42% | 24 | 20 | Data Entry

Template Details and Benchmarks

Template Name | Template Created Date | Overall Failure Rate (%) | Predicted Average Failure Rate (%) | Unique Failures | Threats Sent | Campaign Type | Template Category
--- | --- | --- | --- | --- | --- | --- | ---
Email Template Change | 2020-01-29 | 55% | 75% | 0 | 0 | Data Entry | 2020 Phishing Campaign
THREATSIM CAMPAIGN OVERVIEW REPORT

OBJECTIVE

The ThreatSim Campaign Overview Report provides an at-a-glance view into the short-term phishing performance of simulated phishing campaigns and associated user activity. Information displayed includes:

- Click rate
- Multiple clicks
- No response
- Open messages
- Attachment opened
- Users who reported the mock phish
- Users who acknowledged viewing the Teachable Moment
- Browser vulnerabilities
- Compromised users (provided credentials to a fake site)

BENEFITS

- Quickly view the organization’s recent phishing campaign performance, analyze trends, and determine next steps in your program.
- Scan campaign results side-by-side and determine which campaigns are most effective for the organization.

KEY FEATURES

- Provides a bar chart of campaigns detailing and comparing the results with the ability to display campaigns over a period of up to a year.
- Displays a list of all the campaigns, overall results, create, start and end dates, status, and creator of each campaign. They can be filtered by status, shown as numbers or percentages.
- Export in CSV only.

SCREENSHOT OF THREATSIM CAMPAIGN OVERVIEW REPORT
THREATSIM REPORTS ON INDIVIDUAL CAMPAIGN DETAILS

OBJECTIVE

Within the ThreatSim Campaign Overview Report, each campaign can be accessed to provide administrators with statistical details in a variety of reports. Refer to the reports below.

BENEFIT

Easily analyze comprehensive details of each campaign to determine riskiest users, geography, IP addresses, devices (desktop vs mobile), and browser plug-in vulnerabilities.

SCREENSHOTS OF REPORTS

All Campaigns History Report

Provides statistical details about each campaign, including visibility into past, current, and pending campaigns.

[Image of screenshot showing campaigns from the last year and all campaign history report]

© 2020 Proofpoint, Inc. Private and confidential.
Individual Campaign Overview Report
Displays relevant incident response data such as time-to-click, time-to-open, time-to-report, time-to-open attachments, user clicks vs. no responses, vulnerable vs. non-vulnerable users, compromised vs. non-compromised users, and acknowledged vs. non-acknowledged users. Option to print Executive Summary.

Geographic Distribution Report
Displays worldwide mapping of user activity per campaign, which helps identify anomalies in the organization’s data regions with high levels of susceptibility.
Endpoints Report
Indicates the types of devices (desktop vs. mobile), operating systems, browsers, and browser versions that were used by employees who fell for a mock phishing email. Also reports on out-of-date and potentially vulnerable third-party plug-ins (via the optional Weak Network Egress feature).

Users Report
Shows detailed and complete user activity, including clicks, opens, and reported phish. Also identifies out-of-date third-party browser plug-ins and detection of off-end points (via the optional Weak Network Egress feature).
THREATSIM RAW CAMPAIGN DATA CSV REPORTS

OBJECTIVE

The ThreatSim Raw Campaign Data CSV Report provides user and user’s equipment details that are not available in other reports, reflecting all information available on campaigns in one report. Administrators can export all campaign data and build custom charts based on desired fields and stats.

BENEFIT

Simple export of comprehensive ThreatSim data for quick and easy import into the organization’s preferred analysis tool for evaluation.

KEY FEATURES

- Located under the campaign overview page under Export Data > Campaign History.
- Provides raw data of all campaigns within a selected range, which enables administrators to manipulate and create different charts from the results.
- Displays details about campaigns such as campaign title, type, template used, from name and from email fields, summarized results, and many other fields.
- Export in CSV only.

SCREENSHOTS OF THREATSIM RAW CAMPAIGN DATA CSV REPORTS

Campaign Overview CSV Report

Campaign History CSV Report

Campaign Details CSV Report
THREATSIM USB CAMPAIGN DETAILS REPORT

OBJECTIVE

The ThreatSim USB Campaign Details Report shows the number of USB devices that were accessed and the IP addresses of the users who fell for the USB drop.

BENEFITS

- Examine the organization’s recent USB campaigns and performance at a glance, analyze the details, and determine the next steps in cybersecurity training programs.
- View USB campaign results and determine which campaigns are most effective for the organization.

KEY FEATURES

- Provides the number of USBs that had no response, one-click or multi-clicked responses, and the total number of users who acknowledged the Teachable Moment.
- Displays details about the USBs within each campaign, USB unique ID, external and internal IP addresses of users’ PCs as well as the Windows login used on the PC.
- Lists the filename the user fell for and clicked on.
- Shows the event types and when an event took place.
- Export options: PNG, JPEG, SVG and PDF.

SCREENSHOT OF THREATSIM USB CAMPAIGN DETAILS REPORT
REPORTED EMAIL PERFORMANCE AND ANALYSIS

The reports in this section pertain to PhishAlarm and PhishAlarm Analyzer. They include:

- PhishAlarm Analyzer Report
- Reported Email Performance Report

PHISHALARM ANALYZER REPORT

OBJECTIVE

The PhishAlarm Analyzer Report shows the number of reported threats identified over time (hours, day, weeks, months, quarters). Results are displayed for the three classification categories – “Likely a Phish,” “Suspicious,” and “Not Likely a Phish” – for all email domains analyzed by PhishAlarm Analyzer.

BENEFITS

- Quickly review the total number, types, and trends of phishing emails reported for a given period so you can gauge the effectiveness of your awareness and training of reporting suspected phish.
- Evaluate users’ ability to identify and report actual phishing emails and track performance over time.

KEY FEATURES

- Provides the total number of phishing emails reported monthly.
- Shows the trend of reported emails over a specific date range.
- Assists in identifying the overall understanding of cybersecurity topics within an organization based on the emails reported as well as the trend of the type of emails reported.
- Breaks down the number of emails reported, per category.
- Export in CSV only.

SCREENSHOT OF PHISHALARM ANALYZER REPORT

© 2020 Proofpoint, Inc. Private and confidential.
REPORTED EMAIL PERFORMANCE REPORT

OBJECTIVE

The Reported Emails Performance Report displays the information reported by end users via the PhishAlarm button. It lists the users’ names and email addresses, type of email (simulated phish, training email, or potential phish), action taken by end users (opened, unopened with preview, or unopened), associated phishing campaign name, and time elapsed to report potential phish. Additional information, such as the end users’ operating system and email client version, can also be displayed.

BENEFITS

- Gauge end users’ ability to identify phishing emails and their responsiveness to reporting phish to determine further training needs.
- Identify most active and accurate phish reporters for rewards and recognition.

KEY FEATURES

- Provides a variety of filtering options, such as email type, email action taken by users, and campaign name.
- Flexibility to select which data fields to include or exclude from the table to meet specific analysis needs.
- Displays key performance indicators for the total emails reported, potential phish, simulated phish, and platform notifications.
- Displays detailed results on who reported the email, the type of email reported (simulated phish, potential phish, or training email), the action taken by the end user (opened, unopened, or unopened with preview), and the associated phishing campaign.
- Provides an elapsed time stamp between the receipt of the email and the time reported.
- Specifies end users’ operating system and email client version.
- Export options: Excel and CSV
Screenshot of Reported Emails Performance Report

Reported Email Performance
Understand end user efficacy in reporting potentially suspicious emails to gauge good behaviors or further training needs.
Data updated daily. Last update: 2020-Jan-29 at 23:16 (UTC) (21 hours ago)

Total Emails Reported: 52
Potential Phish: 0
Simulated Phish: 52

Email Activity

Reported Emails

© 2020 Proofpoint, Inc. Private and confidential.
TRAINING REPORTS

The reports in this section pertain to Training modules. They include:

- Knowledge Assessment & Training Progress Report
- Training Assignment Performance Report
- Training Category Performance Report
- Training Module Performance Report
- Training Report Card

KNOWLEDGE ASSESSMENT & TRAINING PROGRESS REPORT

Refer to Knowledge Assessment and Training Progress Report under Knowledge Assessment.

TRAINING ASSIGNMENT PERFORMANCE REPORT

OBJECTIVE

The Training Assignment Performance Report provides comprehensive user-level information for training assignments. Administrators can drill down to the user-level and module-level to view several data points, including standard information such as user module score percentage, time to complete the module, and total questions answered.

BENEFITS

- Easily view and analyze detailed user-level results, progress, and completion rates across training assignments and modules.
- Use gathered information to notify users who have not completed assignments, identify poorly performing users for further training, and identify top performing users for rewards and recognition.

KEY FEATURES

- View detailed results about progress and assignment completions for users within an assignment.
- Flexibility to select and display different column headers within the report, to see progress by different departments, regions, or other properties.
- Administrators can include or exclude deleted assignments, deleted users, and users removed from assignments in their view.
- Ability to create and save different views based on Administrator’s preferences.
- Export options: Excel and CSV.
TRAINING CATEGORY PERFORMANCE REPORT

OBJECTIVE
The Training Category Performance Report tracks the questions and topics end users are having the most trouble with based on the training assignments they have completed. By highlighting weaknesses, an organization can more effectively focus on training efforts.

BENEFIT
Quickly pinpoint the most missed categories across training modules or by individual module so that security awareness training programs can be implemented to focus on those areas for improvement.

KEY FEATURES
- Provides a variety of filtering options, such as by training module name, date, assignment, and include/exclude deleted users.
- Flexibility to select which data fields to include or exclude from the table to meet specific analysis needs.
- Displays key performance indicators for the total number of training modules, categories, correct responses, and incorrect responses.
- Clearly identifies the most missed training categories in a bar chart.
- Ability to view per category details on percentage and total number of incorrect and correct questions and total user responses.
- Ability to view user-level details on how many questions were answered correctly and incorrectly, the corresponding category, module, and assignment names, and the module and assignment completion dates.
- Results include topics in modules taken as part of an assignment and as a standalone (Free Play).
- Export options: Excel and CSV

SCREENSHOT OF TRAINING CATEGORY PERFORMANCE REPORT
(see next page)
SCREENSHOT OF TRAINING CATEGORY PERFORMANCE REPORT (CONT.)

View includes Category Tab
# View of Users Tab

| Category Name                  | First Name | Last Name | Email                        | Role             | User ID
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Access to Restricted Areas</td>
<td>Cynthia</td>
<td>Perry</td>
<td><a href="mailto:cynthia.perry@amyo.com">cynthia.perry@amyo.com</a></td>
<td>Workplace Security</td>
<td>1</td>
</tr>
<tr>
<td>Access to Restricted Areas</td>
<td>Donald</td>
<td>Martin</td>
<td><a href="mailto:donald.martin@amyo.com">donald.martin@amyo.com</a></td>
<td>Workplace Security</td>
<td>2</td>
</tr>
<tr>
<td>Access to Restricted Areas</td>
<td>Dorothy</td>
<td>Foster</td>
<td><a href="mailto:dorothy.foster@amyo.com">dorothy.foster@amyo.com</a></td>
<td>Workplace Security</td>
<td>1</td>
</tr>
<tr>
<td>Access to Restricted Areas</td>
<td>Emily</td>
<td>Sanchez</td>
<td><a href="mailto:emily.sanchez@amyo.com">emily.sanchez@amyo.com</a></td>
<td>Workplace Security</td>
<td>2</td>
</tr>
<tr>
<td>Access to Restricted Areas</td>
<td>Frank</td>
<td>Howard</td>
<td><a href="mailto:frank.howard@amyo.com">frank.howard@amyo.com</a></td>
<td>Workplace Security</td>
<td>2</td>
</tr>
<tr>
<td>Access to Restricted Areas</td>
<td>Matthew</td>
<td>Wood</td>
<td><a href="mailto:matthew.wood@amyo.com">matthew.wood@amyo.com</a></td>
<td>Workplace Security</td>
<td>1</td>
</tr>
<tr>
<td>Access to Restricted Areas</td>
<td>Michael</td>
<td>Petterson</td>
<td><a href="mailto:michael.petterson@amyo.com">michael.petterson@amyo.com</a></td>
<td>Workplace Security</td>
<td>2</td>
</tr>
<tr>
<td>Access to Restricted Areas</td>
<td>Ruth</td>
<td>Thompson</td>
<td><a href="mailto:ruth.thompson@amyo.com">ruth.thompson@amyo.com</a></td>
<td>Workplace Security</td>
<td>1</td>
</tr>
<tr>
<td>Apply basic best practices appropriately</td>
<td>Alexander</td>
<td>Hernandez</td>
<td><a href="mailto:alexander.hernandez@amyo.com">alexander.hernandez@amyo.com</a></td>
<td>P11 in Action 15.12</td>
<td>2</td>
</tr>
<tr>
<td>Apply basic best practices appropriately</td>
<td>Amy</td>
<td>Brown</td>
<td><a href="mailto:amy.brown@amyo.com">amy.brown@amyo.com</a></td>
<td>P11 in Action 15.12</td>
<td>1</td>
</tr>
<tr>
<td>Apply basic best practices appropriately</td>
<td>Angela</td>
<td>Robinson</td>
<td><a href="mailto:angela.robinson@amyo.com">angela.robinson@amyo.com</a></td>
<td>P11 in Action 15.12</td>
<td>1</td>
</tr>
<tr>
<td>Apply basic best practices appropriately</td>
<td>Anna</td>
<td>Sanchez</td>
<td><a href="mailto:anna.sanchez@amyo.com">anna.sanchez@amyo.com</a></td>
<td>P11 in Action 15.12</td>
<td>2</td>
</tr>
<tr>
<td>Apply basic best practices appropriately</td>
<td>Anthony</td>
<td>Griffin</td>
<td><a href="mailto:anthony.griffin@amyo.com">anthony.griffin@amyo.com</a></td>
<td>P11 in Action 15.12</td>
<td>1</td>
</tr>
<tr>
<td>Apply basic best practices appropriately</td>
<td>Benjamin</td>
<td>Reander</td>
<td><a href="mailto:benjamin.reander@amyo.com">benjamin.reander@amyo.com</a></td>
<td>P11 in Action 15.12</td>
<td>3</td>
</tr>
<tr>
<td>Apply basic best practices appropriately</td>
<td>Carol</td>
<td>Howard</td>
<td><a href="mailto:carol.howard@amyo.com">carol.howard@amyo.com</a></td>
<td>P11 in Action 15.12</td>
<td>1</td>
</tr>
<tr>
<td>Apply basic best practices appropriately</td>
<td>Carolyn</td>
<td>Lavis</td>
<td><a href="mailto:carolyn.lavis@amyo.com">carolyn.lavis@amyo.com</a></td>
<td>P11 in Action 15.12</td>
<td>1</td>
</tr>
<tr>
<td>Apply basic best practices appropriately</td>
<td>Deborah</td>
<td>Curry</td>
<td><a href="mailto:deborah.curry@amyo.com">deborah.curry@amyo.com</a></td>
<td>P11 in Action 15.12</td>
<td>1</td>
</tr>
<tr>
<td>Apply basic best practices appropriately</td>
<td>Dorothy</td>
<td>Fowler</td>
<td><a href="mailto:dorothy.fowler@amyo.com">dorothy.fowler@amyo.com</a></td>
<td>P11 in Action 15.12</td>
<td>2</td>
</tr>
</tbody>
</table>
TRAINING MODULE PERFORMANCE REPORT

OBJECTIVES

The Training Module Performance Report displays results and information for Training modules. It tracks individual completion rates and attempts for specific or multiple modules, whether part of an assignment or not, in addition to capturing whether the user responded to a policy acknowledgment statement added through our Training Jacket feature. The report displays average scores for each module, in addition to individual user’s scores. It also tracks and ranks completion rates for individuals and departments to help determine best performing groups.

BENEFITS

- Easily view and monitor users’ training module completion status, completion rate, and scores.
- Identify cybersecurity awareness topics where individuals are strongest and weakest so that future training programs can be tailored accordingly.
- View training completion percentage and average score by module.
- Review detailed scores for each module and compare results across modules.
- Clearly identify users who have acknowledged, declined, or took no action on the company-specified policy acknowledgment to comply with organizational policies.
- Quickly identify leaderboard data showing best performing individuals or departments on training module assignment completion time and scores for rewards and recognition and, conversely, identify lower performing individuals or departments to determine action plans for improvement.

KEY FEATURES

- Provides a variety of filtering options, such as by module name, status, and attempt start date as well as user completion status.
- Flexibility to select which data fields to include or exclude from the table to meet specific analysis needs.
- Displays key performance indicators for the number of modules, assigned modules, attempts and completion.
- Provides detailed results about which users attempted or completed a specific module as part of an assignment or standalone (Free Play).
- Tracks user-level scores on modules taken within or outside of an assignment.
- Displays an overall acceptance rate percentage as well as a breakdown of who accepted, declined, or took no action on the Policy Acknowledgement inserted in a Training Jacket of the modules.
- Provides an exportable Leaderboard table that ranks all users with a formula that uses completion time and module scores across any combination of training modules.
- Reflects a score distribution for users who are part of an assignment.
- Export options: Excel and CSV
SCREENSHOT OF TRAINING MODULE USER REPORT

View includes Module Performance Tab

Training Module Performance
Track end users' completion rates on specific training modules and how they performed in their training individually and in aggregate to identify their strong and weak topic areas.

Data updated daily. Last update: 2020-Jan-30 at 15:15 (UTC) (8 hours ago)

- Unique Modules: 49
- Modules Assigned: 1k
- Module Attempts: 1k
- Module Completion: 1k (100%)

Training Completion Percentage By Module

Average Score By Module

User Participation
**View of Training Module Status by User Tab**

<table>
<thead>
<tr>
<th>First Name</th>
<th>Last Name</th>
<th>Email Address</th>
<th>Assignment Name</th>
<th>Module(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alexander</td>
<td>Edwards</td>
<td><a href="mailto:alexander.edwards@proofpoint.com">alexander.edwards@proofpoint.com</a></td>
<td>Training Assignment</td>
<td>IP Discovery</td>
</tr>
<tr>
<td>Alexander</td>
<td>Edwards</td>
<td><a href="mailto:alexander.edwards@proofpoint.com">alexander.edwards@proofpoint.com</a></td>
<td>Training Assignment</td>
<td>Phishing</td>
</tr>
<tr>
<td>Alexander</td>
<td>Edwards</td>
<td><a href="mailto:alexander.edwards@proofpoint.com">alexander.edwards@proofpoint.com</a></td>
<td>Training Assignment</td>
<td>Social Media</td>
</tr>
<tr>
<td>Alexander</td>
<td>Edwards</td>
<td><a href="mailto:alexander.edwards@proofpoint.com">alexander.edwards@proofpoint.com</a></td>
<td>Training Assignment</td>
<td>Security BD</td>
</tr>
<tr>
<td>Alexander</td>
<td>Edwards</td>
<td><a href="mailto:alexander.edwards@proofpoint.com">alexander.edwards@proofpoint.com</a></td>
<td>Training Assignment</td>
<td>Privacy Set</td>
</tr>
<tr>
<td>Alexander</td>
<td>Edwards</td>
<td><a href="mailto:alexander.edwards@proofpoint.com">alexander.edwards@proofpoint.com</a></td>
<td>Training Assignment</td>
<td>Protecting</td>
</tr>
<tr>
<td>Alexander</td>
<td>Edwards</td>
<td><a href="mailto:alexander.edwards@proofpoint.com">alexander.edwards@proofpoint.com</a></td>
<td>Training Assignment</td>
<td>Device Security</td>
</tr>
<tr>
<td>Alexander</td>
<td>Edwards</td>
<td><a href="mailto:alexander.edwards@proofpoint.com">alexander.edwards@proofpoint.com</a></td>
<td>Training Assignment</td>
<td>Malware Analysis</td>
</tr>
<tr>
<td>Alexander</td>
<td>Edwards</td>
<td><a href="mailto:alexander.edwards@proofpoint.com">alexander.edwards@proofpoint.com</a></td>
<td>Training Assignment</td>
<td>Awareness</td>
</tr>
<tr>
<td>Alexander</td>
<td>Edwards</td>
<td><a href="mailto:alexander.edwards@proofpoint.com">alexander.edwards@proofpoint.com</a></td>
<td>Training Assignment</td>
<td>Anti Phishing</td>
</tr>
<tr>
<td>Alexander</td>
<td>Edwards</td>
<td><a href="mailto:alexander.edwards@proofpoint.com">alexander.edwards@proofpoint.com</a></td>
<td>Training Assignment</td>
<td>Anti Malware</td>
</tr>
<tr>
<td>Alexander</td>
<td>Edwards</td>
<td><a href="mailto:alexander.edwards@proofpoint.com">alexander.edwards@proofpoint.com</a></td>
<td>Training Assignment</td>
<td>Vendor Management</td>
</tr>
<tr>
<td>Alexander</td>
<td>Edwards</td>
<td><a href="mailto:alexander.edwards@proofpoint.com">alexander.edwards@proofpoint.com</a></td>
<td>Training Assignment</td>
<td>Mobile Data</td>
</tr>
<tr>
<td>Alexander</td>
<td>Edwards</td>
<td><a href="mailto:alexander.edwards@proofpoint.com">alexander.edwards@proofpoint.com</a></td>
<td>Training Assignment</td>
<td>Cloud Data</td>
</tr>
<tr>
<td>Alexander</td>
<td>Edwards</td>
<td><a href="mailto:alexander.edwards@proofpoint.com">alexander.edwards@proofpoint.com</a></td>
<td>Training Assignment</td>
<td>Data Breach</td>
</tr>
<tr>
<td>Alexander</td>
<td>Edwards</td>
<td><a href="mailto:alexander.edwards@proofpoint.com">alexander.edwards@proofpoint.com</a></td>
<td>Training Assignment</td>
<td>Data Entry</td>
</tr>
<tr>
<td>Amanda</td>
<td>Bryant</td>
<td><a href="mailto:amanda.bryant@proofpoint.com">amanda.bryant@proofpoint.com</a></td>
<td>Training Assignment</td>
<td>Beyond Pay</td>
</tr>
<tr>
<td>Amanda</td>
<td>Nelson</td>
<td><a href="mailto:amanda.nelson@proofpoint.com">amanda.nelson@proofpoint.com</a></td>
<td>Training Assignment</td>
<td>Beyond Pay</td>
</tr>
<tr>
<td>Amanda</td>
<td>Nelson</td>
<td><a href="mailto:amanda.nelson@proofpoint.com">amanda.nelson@proofpoint.com</a></td>
<td>Training Assignment</td>
<td>Beyond Pay</td>
</tr>
<tr>
<td>Amanda</td>
<td>Nelson</td>
<td><a href="mailto:amanda.nelson@proofpoint.com">amanda.nelson@proofpoint.com</a></td>
<td>Training Assignment</td>
<td>Beyond Pay</td>
</tr>
<tr>
<td>Amanda</td>
<td>Nelson</td>
<td><a href="mailto:amanda.nelson@proofpoint.com">amanda.nelson@proofpoint.com</a></td>
<td>Training Assignment</td>
<td>Beyond Pay</td>
</tr>
<tr>
<td>Amanda</td>
<td>Nelson</td>
<td><a href="mailto:amanda.nelson@proofpoint.com">amanda.nelson@proofpoint.com</a></td>
<td>Training Assignment</td>
<td>Beyond Pay</td>
</tr>
</tbody>
</table>

**View of Training Leaderboard Tab**

**Average Score By Department**

<table>
<thead>
<tr>
<th>Department</th>
<th>Average Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Human Resources</td>
<td>86.00%</td>
</tr>
<tr>
<td>Sales</td>
<td>88.45%</td>
</tr>
<tr>
<td>Marketing</td>
<td>88.81%</td>
</tr>
<tr>
<td>Legal</td>
<td>88.20%</td>
</tr>
<tr>
<td>IT</td>
<td>88.82%</td>
</tr>
</tbody>
</table>

**Training Score Distribution**

- **Score by Department**
- **Overall User Score**: 89.8%

**User Ranking**

<table>
<thead>
<tr>
<th>#</th>
<th>First Name</th>
<th>Last Name</th>
<th>Email Address</th>
<th>Amount</th>
<th>Amount</th>
<th>Overall Score</th>
<th>Total Score</th>
<th>Overall Place</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Joseph</td>
<td>Mitchell</td>
<td><a href="mailto:joseph.mitchell@beyond.com">joseph.mitchell@beyond.com</a></td>
<td>1550</td>
<td>1550</td>
<td>89.85%</td>
<td>25</td>
<td>25</td>
</tr>
<tr>
<td>2</td>
<td>Tammy</td>
<td>Davis</td>
<td><a href="mailto:tammy.davis@beyond.com">tammy.davis@beyond.com</a></td>
<td>20</td>
<td>20</td>
<td>88.45%</td>
<td>20</td>
<td>20</td>
</tr>
<tr>
<td>3</td>
<td>Dean</td>
<td>Clark</td>
<td><a href="mailto:dean.clark@beyond.com">dean.clark@beyond.com</a></td>
<td>20</td>
<td>20</td>
<td>88.45%</td>
<td>20</td>
<td>20</td>
</tr>
<tr>
<td>4</td>
<td>Thomas</td>
<td>Clark</td>
<td><a href="mailto:thomas.clark@beyond.com">thomas.clark@beyond.com</a></td>
<td>10</td>
<td>10</td>
<td>88.81%</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>5</td>
<td>Sarah</td>
<td>Thompson</td>
<td><a href="mailto:sarah.thompson@beyond.com">sarah.thompson@beyond.com</a></td>
<td>15</td>
<td>15</td>
<td>88.82%</td>
<td>15</td>
<td>15</td>
</tr>
<tr>
<td>6</td>
<td>Rachel</td>
<td>Parker</td>
<td><a href="mailto:rachel.parker@beyond.com">rachel.parker@beyond.com</a></td>
<td>15</td>
<td>15</td>
<td>88.82%</td>
<td>15</td>
<td>15</td>
</tr>
<tr>
<td>7</td>
<td>Carla</td>
<td>Hall</td>
<td><a href="mailto:carla.hall@beyond.com">carla.hall@beyond.com</a></td>
<td>15</td>
<td>15</td>
<td>88.82%</td>
<td>15</td>
<td>15</td>
</tr>
<tr>
<td>8</td>
<td>Katherine</td>
<td>Henderson</td>
<td><a href="mailto:katherine.henderson@beyond.com">katherine.henderson@beyond.com</a></td>
<td>15</td>
<td>15</td>
<td>88.82%</td>
<td>15</td>
<td>15</td>
</tr>
<tr>
<td>9</td>
<td>Andrew</td>
<td>Prolong</td>
<td><a href="mailto:andrew.prolong@beyond.com">andrew.prolong@beyond.com</a></td>
<td>15</td>
<td>15</td>
<td>88.82%</td>
<td>15</td>
<td>15</td>
</tr>
<tr>
<td>10</td>
<td>Kathleen</td>
<td>Perez</td>
<td><a href="mailto:kathleen.perez@beyond.com">kathleen.perez@beyond.com</a></td>
<td>15</td>
<td>15</td>
<td>88.82%</td>
<td>15</td>
<td>15</td>
</tr>
<tr>
<td>11</td>
<td>Laura</td>
<td>Powell</td>
<td><a href="mailto:laura.powell@beyond.com">laura.powell@beyond.com</a></td>
<td>15</td>
<td>15</td>
<td>88.82%</td>
<td>15</td>
<td>15</td>
</tr>
</tbody>
</table>
View of Policy Acknowledgement Tab

<table>
<thead>
<tr>
<th>Policy Acknowledgement</th>
<th>Module (User Display)</th>
</tr>
</thead>
<tbody>
<tr>
<td>First Name</td>
<td>Last Name</td>
</tr>
<tr>
<td>Kathleen</td>
<td>Perez</td>
</tr>
<tr>
<td>Kathleen</td>
<td>Perez</td>
</tr>
<tr>
<td>Kathleen</td>
<td>Perez</td>
</tr>
<tr>
<td>Kathleen</td>
<td>Perez</td>
</tr>
<tr>
<td>Kathleen</td>
<td>Perez</td>
</tr>
<tr>
<td>Samantha</td>
<td>Barnes</td>
</tr>
<tr>
<td>Samantha</td>
<td>Barnes</td>
</tr>
<tr>
<td>Samantha</td>
<td>Barnes</td>
</tr>
<tr>
<td>Samantha</td>
<td>Barnes</td>
</tr>
<tr>
<td>Samantha</td>
<td>Barnes</td>
</tr>
<tr>
<td>Samantha</td>
<td>Barnes</td>
</tr>
<tr>
<td>Samantha</td>
<td>Barnes</td>
</tr>
<tr>
<td>Janet</td>
<td>Diaz</td>
</tr>
</tbody>
</table>
TRAINING REPORT CARD

OBJECTIVE
The Training Report Card tracks the overall progress and performance of a single user, including scores for specific modules and a cumulative performance rating.

BENEFITS

- Quickly identify users who need extra training in specific topic areas.
- Track a user’s performance over time.

KEY FEATURES

- Displays a user’s overall status and progress, for all activities, in the Platform on one page.
- Allows an administrator to see all the modules that the user completed or attempted, in two tables individually and cumulative on the same page.
- Displays all modules completed by a user (even if the user was removed from an assignment) as well as the best and most recent score for each module completed.
- Administrator can see all assignments that are assigned to a user and the status for each on one page.
- Export options: Excel and Word.

SCREENSHOT OF TRAINING REPORT CARD REPORT

---

© 2020 Proofpoint, Inc. Private and confidential.
USERS

The report in this section pertains to User records.

USER RECORD EXPORT REPORT

OBJECTIVE

The User Record Export Report provides a complete list of users and assigned attributes that were uploaded into the platform.

BENEFIT

Enables a backup copy of all users and user attributes to be saved, in the event of any potential maintenance issues.

KEY FEATURES

- Displays all your users and their attributes for reference.
- Exportable information to retain in the event of a recovery need.
- Export options: Excel and CSV.

SCREENSHOT OF USER RECORD EXPORT REPORT