proofpoint.

Security Awareness Training

BUSINESS INTELLIGENCE

Reporting Overview

April 2020

Table of Contents

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 • Knowledge Assessment and Training Progress*
Phishing Simulation	• Phishing Campaign Performance • Phishing User Performance • ThreatSim Campaign Overview • ThreatSim Raw Campaign Data CSV • 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
Reported Email Performance and Analysis	• Reported Email Performance • PhishAlarm Analyzer Report
Training	• Knowledge Assessment and Training Progress* • Training Assignment Performance • Training Category Performance • Training Module Performance
Users	• User Record Export • Training Report Card

* 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

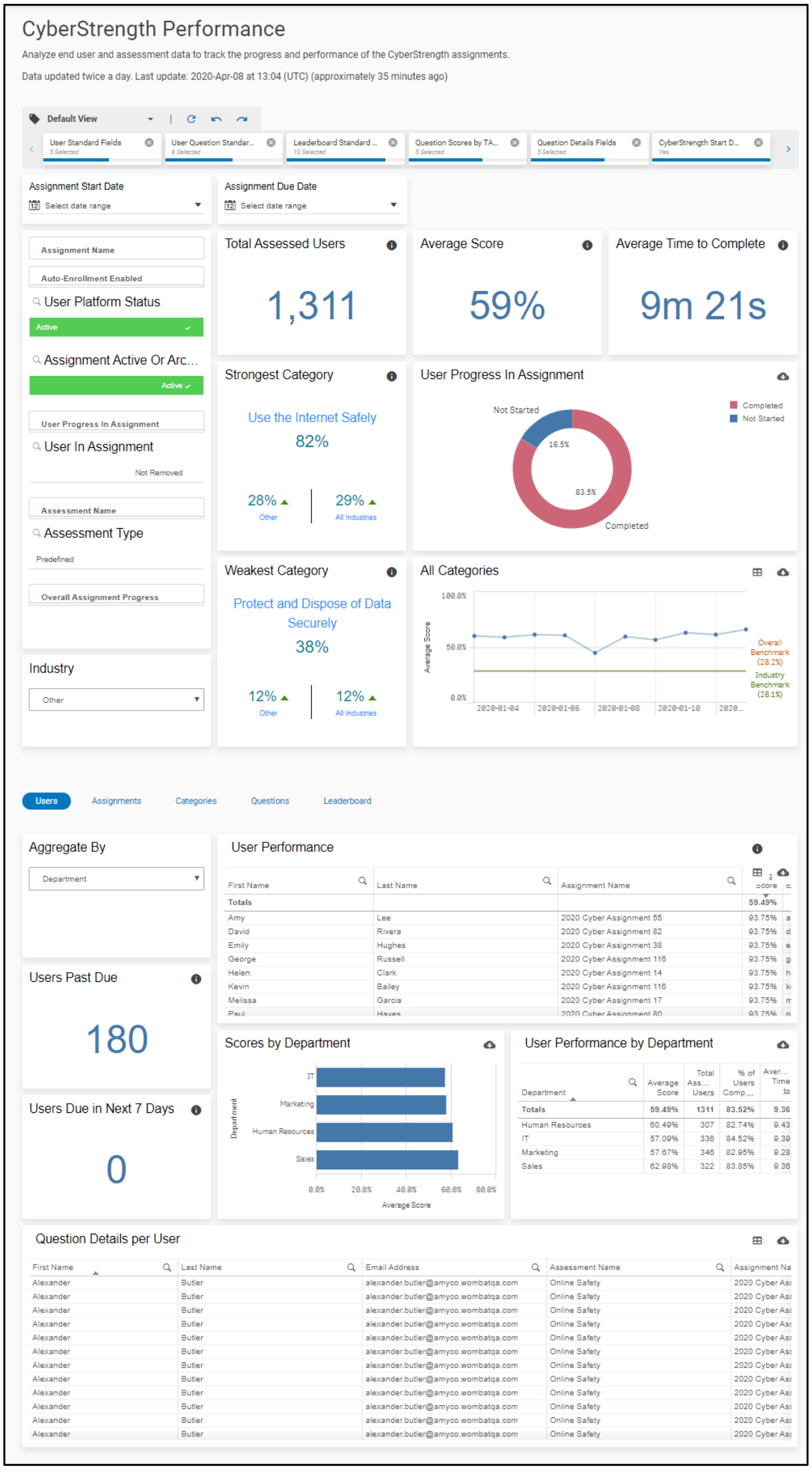
- Determine the organization's weaknesses and strengths across a range of cybersecurity areas, identify the riskiest users or business units, identify the most missed question categories, and customize programs to reduce the identified risks.
- Track user progress and performance across all CyberStrength 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.

SAMPLE CYBERSTRENGTH PERFORMANCE REPORT

(see next page)

SAMPLE CYBERSTRENGTH PERFORMANCE REPORT (CONT.)

View includes Users Tab



CyberStrength Performance

Analyze end user and assessment data to track the progress and performance of the CyberStrength assignments.

Data updated twice a day. Last update: 2020-Apr-08 at 13:04 (UTC) (approximately 35 minutes ago)

Assignment Start Date: Select date range

Assignment Due Date: Select date range

User Platform Status: Active ✓

Assignment Active Or Arc...: Active ✓

User In Assignment: Not Removed

Assessment Type: Predefined

Industry: Other

Total Assessed Users: 1,311

Average Score: 59%

Average Time to Complete: 9m 21s

Strongest Category: Use the Internet Safely 82%
28% ▲ Other | 29% ▲ All Industries

User Progress In Assignment

Weakest Category: Protect and Dispose of Data Securely 38%
12% ▲ Other | 12% ▲ All Industries

All Categories

Aggregate By: Department

User Performance

First Name	Last Name	Assignment Name	Score	E
Totals			59.49%	
Amy	Lee	2020 Cyber Assignment 55	93.75%	a
David	Rivera	2020 Cyber Assignment 82	93.75%	d
Emily	Hughes	2020 Cyber Assignment 38	93.75%	e
George	Russell	2020 Cyber Assignment 116	93.75%	g
Helen	Clark	2020 Cyber Assignment 14	93.75%	h
Kevin	Bailey	2020 Cyber Assignment 116	93.75%	k
Melissa	Garcia	2020 Cyber Assignment 17	93.75%	m
Paul	Hayes	2020 Cyber Assignment 80	93.75%	p

Users Past Due: 180

Users Due in Next 7 Days: 0

Scores by Department

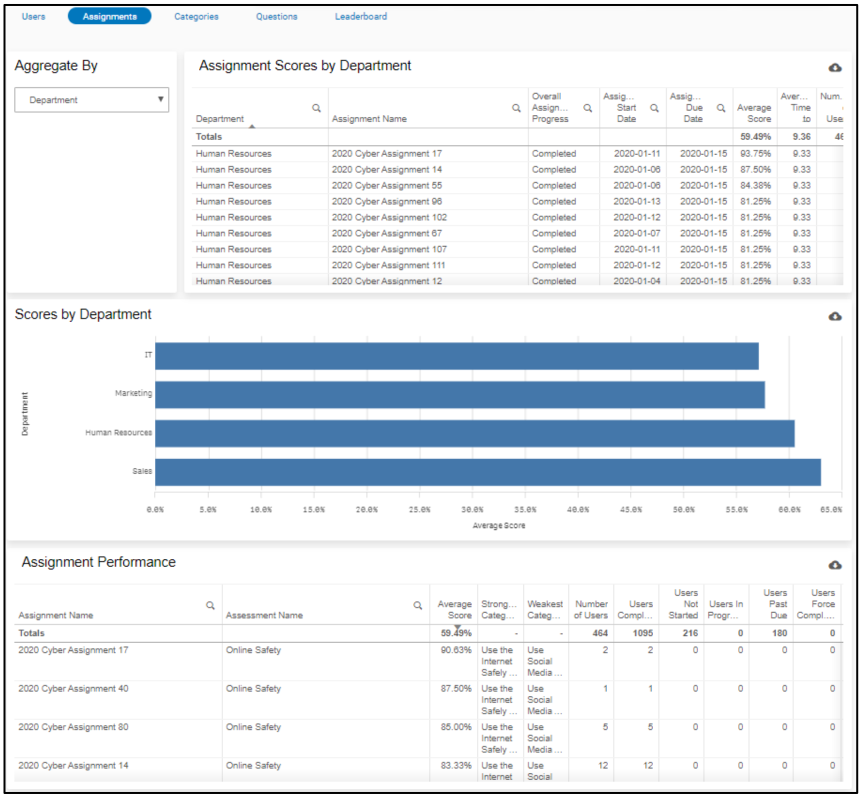
User Performance by Department

Department	Average Score	Total Ass... Users	% of Users Comp...	Aver... Time to
Totals	59.49%	1311	83.52%	9.36
Human Resources	60.49%	307	82.74%	9.43
IT	57.09%	336	84.52%	9.39
Marketing	57.67%	346	82.95%	9.28
Sales	62.98%	322	83.85%	9.36

Question Details per User

First Name	Last Name	Email Address	Assessment Name	Assignment Na
Alexander	Butler	alexander.butler@amyco.wombatqa.com	Online Safety	2020 Cyber Ass
Alexander	Butler	alexander.butler@amyco.wombatqa.com	Online Safety	2020 Cyber Ass
Alexander	Butler	alexander.butler@amyco.wombatqa.com	Online Safety	2020 Cyber Ass
Alexander	Butler	alexander.butler@amyco.wombatqa.com	Online Safety	2020 Cyber Ass
Alexander	Butler	alexander.butler@amyco.wombatqa.com	Online Safety	2020 Cyber Ass
Alexander	Butler	alexander.butler@amyco.wombatqa.com	Online Safety	2020 Cyber Ass
Alexander	Butler	alexander.butler@amyco.wombatqa.com	Online Safety	2020 Cyber Ass
Alexander	Butler	alexander.butler@amyco.wombatqa.com	Online Safety	2020 Cyber Ass
Alexander	Butler	alexander.butler@amyco.wombatqa.com	Online Safety	2020 Cyber Ass
Alexander	Butler	alexander.butler@amyco.wombatqa.com	Online Safety	2020 Cyber Ass
Alexander	Butler	alexander.butler@amyco.wombatqa.com	Online Safety	2020 Cyber Ass
Alexander	Butler	alexander.butler@amyco.wombatqa.com	Online Safety	2020 Cyber Ass

View of Assignments Tab



Aggregate By

Department

Assignment Scores by Department

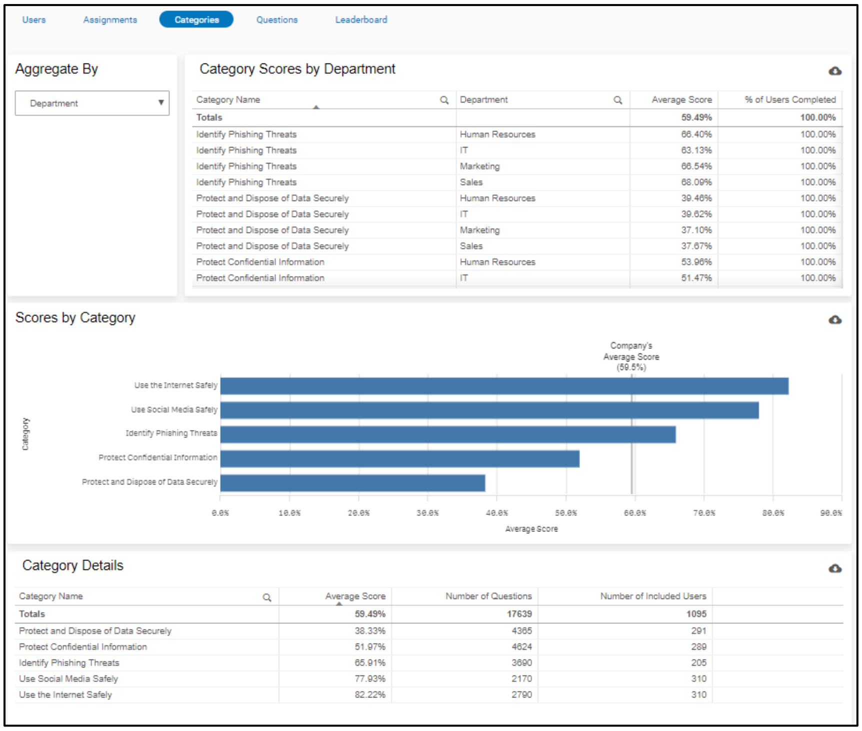
Department	Assignment Name	Overall Assign… Progress	Assig… Start Date	Assig… Due Date	Average Score	Aver… Time to	Num. Use
Totals					**59.49%**	**9.36**	**46**
Human Resources	2020 Cyber Assignment 17	Completed	2020-01-11	2020-01-15	93.75%	9.33	
Human Resources	2020 Cyber Assignment 14	Completed	2020-01-06	2020-01-15	87.50%	9.33	
Human Resources	2020 Cyber Assignment 55	Completed	2020-01-06	2020-01-15	84.38%	9.33	
Human Resources	2020 Cyber Assignment 96	Completed	2020-01-13	2020-01-15	81.25%	9.33	
Human Resources	2020 Cyber Assignment 102	Completed	2020-01-12	2020-01-15	81.25%	9.33	
Human Resources	2020 Cyber Assignment 67	Completed	2020-01-07	2020-01-15	81.25%	9.33	
Human Resources	2020 Cyber Assignment 107	Completed	2020-01-11	2020-01-15	81.25%	9.33	
Human Resources	2020 Cyber Assignment 111	Completed	2020-01-12	2020-01-15	81.25%	9.33	
Human Resources	2020 Cyber Assignment 12	Completed	2020-01-04	2020-01-15	81.25%	9.33	

Scores by Department

Assignment Performance

Assignment Name	Assessment Name	Average Score	Strong… Categ…	Weakest Categ…	Number of Users	Users Compl…	Users Not Started	Users In Progr…	Users Past Due	Users Force Compl….
Totals		**59.49%**	**-**	**-**	**464**	**1095**	**216**	**0**	**180**	**0**
2020 Cyber Assignment 17	Online Safety	90.63%	Use the Internet Safely …	Use Social Media …	2	2	0	0	0	0
2020 Cyber Assignment 40	Online Safety	87.50%	Use the Internet Safely …	Use Social Media …	1	1	0	0	0	0
2020 Cyber Assignment 80	Online Safety	85.00%	Use the Internet Safely …	Use Social Media …	5	5	0	0	0	0
2020 Cyber Assignment 14	Online Safety	83.33%	Use the Internet	Use Social	12	12	0	0	0	0

View of Categories Tab



Aggregate By

Department

Category Scores by Department

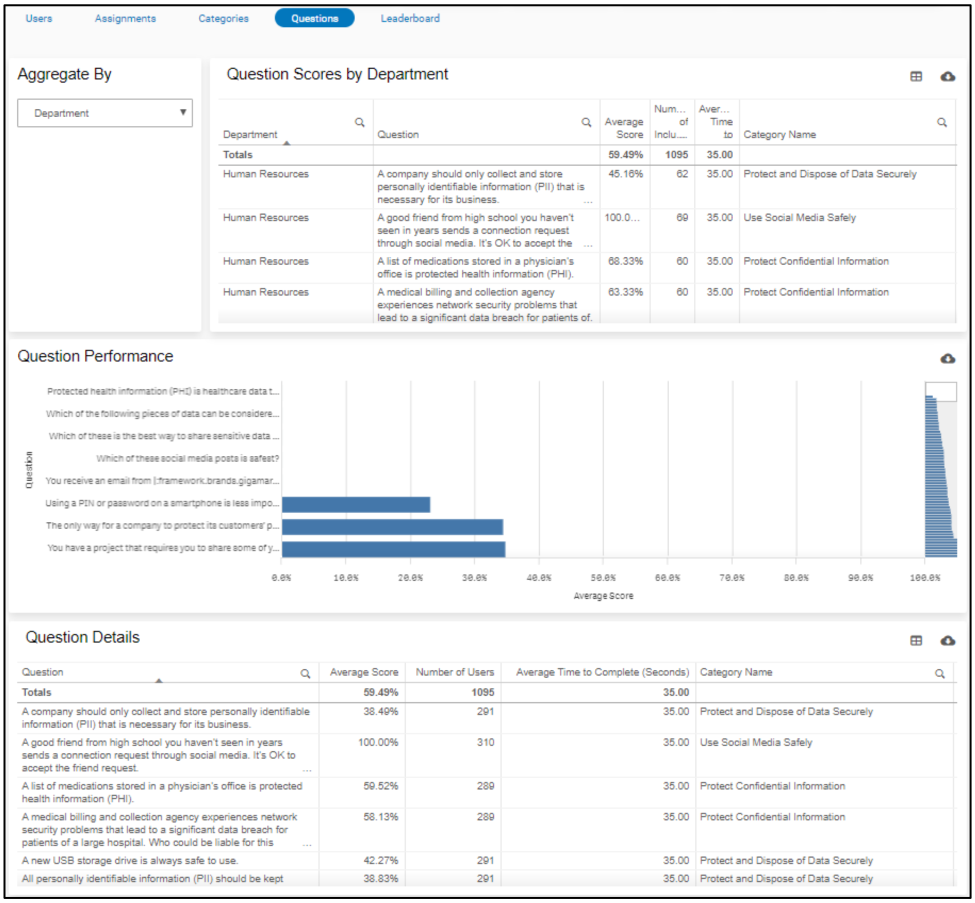
Category Name	Department	Average Score	% of Users Completed
Totals		**59.49%**	**100.00%**
Identify Phishing Threats	Human Resources	66.40%	100.00%
Identify Phishing Threats	IT	63.13%	100.00%
Identify Phishing Threats	Marketing	66.54%	100.00%
Identify Phishing Threats	Sales	68.09%	100.00%
Protect and Dispose of Data Securely	Human Resources	39.46%	100.00%
Protect and Dispose of Data Securely	IT	39.62%	100.00%
Protect and Dispose of Data Securely	Marketing	37.10%	100.00%
Protect and Dispose of Data Securely	Sales	37.67%	100.00%
Protect Confidential Information	Human Resources	53.96%	100.00%
Protect Confidential Information	IT	51.47%	100.00%

Scores by Category

Category Details

Category Name	Average Score	Number of Questions	Number of Included Users
Totals	**59.49%**	**17639**	**1095**
Protect and Dispose of Data Securely	38.33%	4365	291
Protect Confidential Information	51.97%	4624	289
Identify Phishing Threats	65.91%	3690	205
Use Social Media Safely	77.93%	2170	310
Use the Internet Safely	82.22%	2790	310

View of Questions Tab



Question Scores by Department

Department	Question	Average Score	Num… of Inclu….	Aver… Time to	Category Name
Totals		59.49%	1095	35.00	
Human Resources	A company should only collect and store personally identifiable information (PII) that is necessary for its business. …	45.16%	62	35.00	Protect and Dispose of Data Securely
Human Resources	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 …	100.0…	69	35.00	Use Social Media Safely
Human Resources	A list of medications stored in a physician's office is protected health information (PHI).	68.33%	60	35.00	Protect Confidential Information
Human Resources	A medical billing and collection agency experiences network security problems that lead to a significant data breach for patients of.	63.33%	60	35.00	Protect Confidential Information

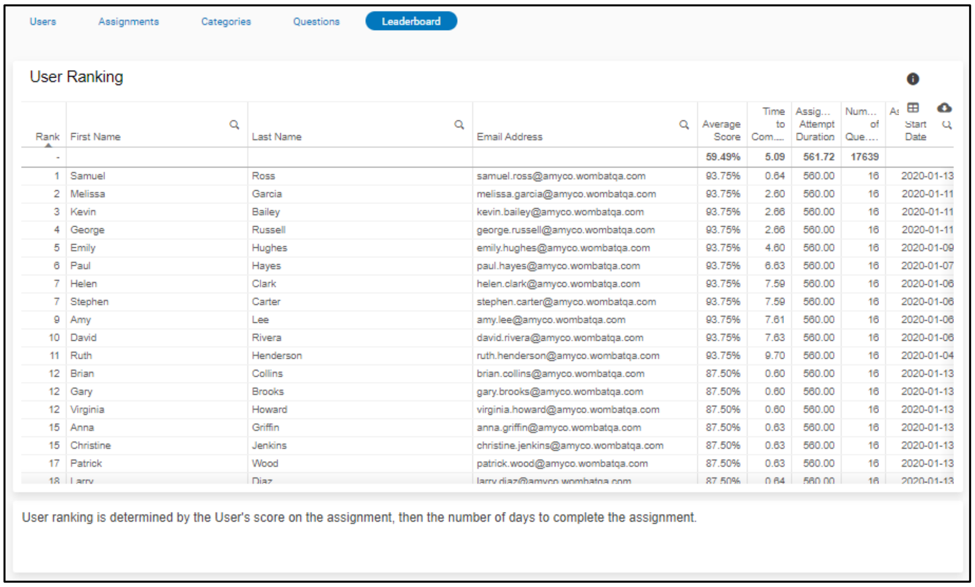
Question Performance

Protected health information (PHI) is healthcare data t…
Which of the following pieces of data can be considere…
Which of these is the best way to share sensitive data …
Which of these social media posts is safest?
You receive an email from [:framework.brands.gigamar…
Using a PIN or password on a smartphone is less impo…
The only way for a company to protect its customers' p…
You have a project that requires you to share some of y…
Question
0.0%
10.0%
20.0%
30.0%
40.0%
50.0%
60.0%
70.0%
80.0%
90.0%
100.0%
Average Score

Question Details

Question	Average Score	Number of Users	Average Time to Complete (Seconds)	Category Name
Totals	59.49%	1095	35.00	
A company should only collect and store personally identifiable information (PII) that is necessary for its business.	38.49%	291	35.00	Protect and Dispose of Data Securely
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. …	100.00%	310	35.00	Use Social Media Safely
A list of medications stored in a physician's office is protected health information (PHI).	59.52%	289	35.00	Protect Confidential Information
A medical billing and collection agency experiences network security problems that lead to a significant data breach for patients of a large hospital. Who could be liable for this …	58.13%	289	35.00	Protect Confidential Information
A new USB storage drive is always safe to use.	42.27%	291	35.00	Protect and Dispose of Data Securely
All personally identifiable information (PII) should be kept	38.83%	291	35.00	Protect and Dispose of Data Securely

View of Leaderboard Tab



User Ranking

Rank	First Name	Last Name	Email Address	Average Score	Time to Com….	Assig… Attempt Duration	Num… of Que….	As	Start Date
-				59.49%	5.09	561.72	17639		
1	Samuel	Ross	samuel.ross@amyco.wombatqa.com	93.75%	0.64	560.00	16		2020-01-13
2	Melissa	Garcia	melissa.garcia@amyco.wombatqa.com	93.75%	2.60	560.00	16		2020-01-11
3	Kevin	Bailey	kevin.bailey@amyco.wombatqa.com	93.75%	2.66	560.00	16		2020-01-11
4	George	Russell	george.russell@amyco.wombatqa.com	93.75%	2.66	560.00	16		2020-01-11
5	Emily	Hughes	emily.hughes@amyco.wombatqa.com	93.75%	4.60	560.00	16		2020-01-09
6	Paul	Hayes	paul.hayes@amyco.wombatqa.com	93.75%	6.63	560.00	16		2020-01-07
7	Helen	Clark	helen.clark@amyco.wombatqa.com	93.75%	7.59	560.00	16		2020-01-06
7	Stephen	Carter	stephen.carter@amyco.wombatqa.com	93.75%	7.59	560.00	16		2020-01-06
9	Amy	Lee	amy.lee@amyco.wombatqa.com	93.75%	7.61	560.00	16		2020-01-06
10	David	Rivera	david.rivera@amyco.wombatqa.com	93.75%	7.63	560.00	16		2020-01-06
11	Ruth	Henderson	ruth.henderson@amyco.wombatqa.com	93.75%	9.70	560.00	16		2020-01-04
12	Brian	Collins	brian.collins@amyco.wombatqa.com	87.50%	0.60	560.00	16		2020-01-13
12	Gary	Brooks	gary.brooks@amyco.wombatqa.com	87.50%	0.60	560.00	16		2020-01-13
12	Virginia	Howard	virginia.howard@amyco.wombatqa.com	87.50%	0.60	560.00	16		2020-01-13
15	Anna	Griffin	anna.griffin@amyco.wombatqa.com	87.50%	0.63	560.00	16		2020-01-13
15	Christine	Jenkins	christine.jenkins@amyco.wombatqa.com	87.50%	0.63	560.00	16		2020-01-13
17	Patrick	Wood	patrick.wood@amyco.wombatqa.com	87.50%	0.63	560.00	16		2020-01-13
18	Larry	Diaz	larry.diaz@amyco.wombatqa.com	87.50%	0.64	560.00	16		2020-01-13

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.

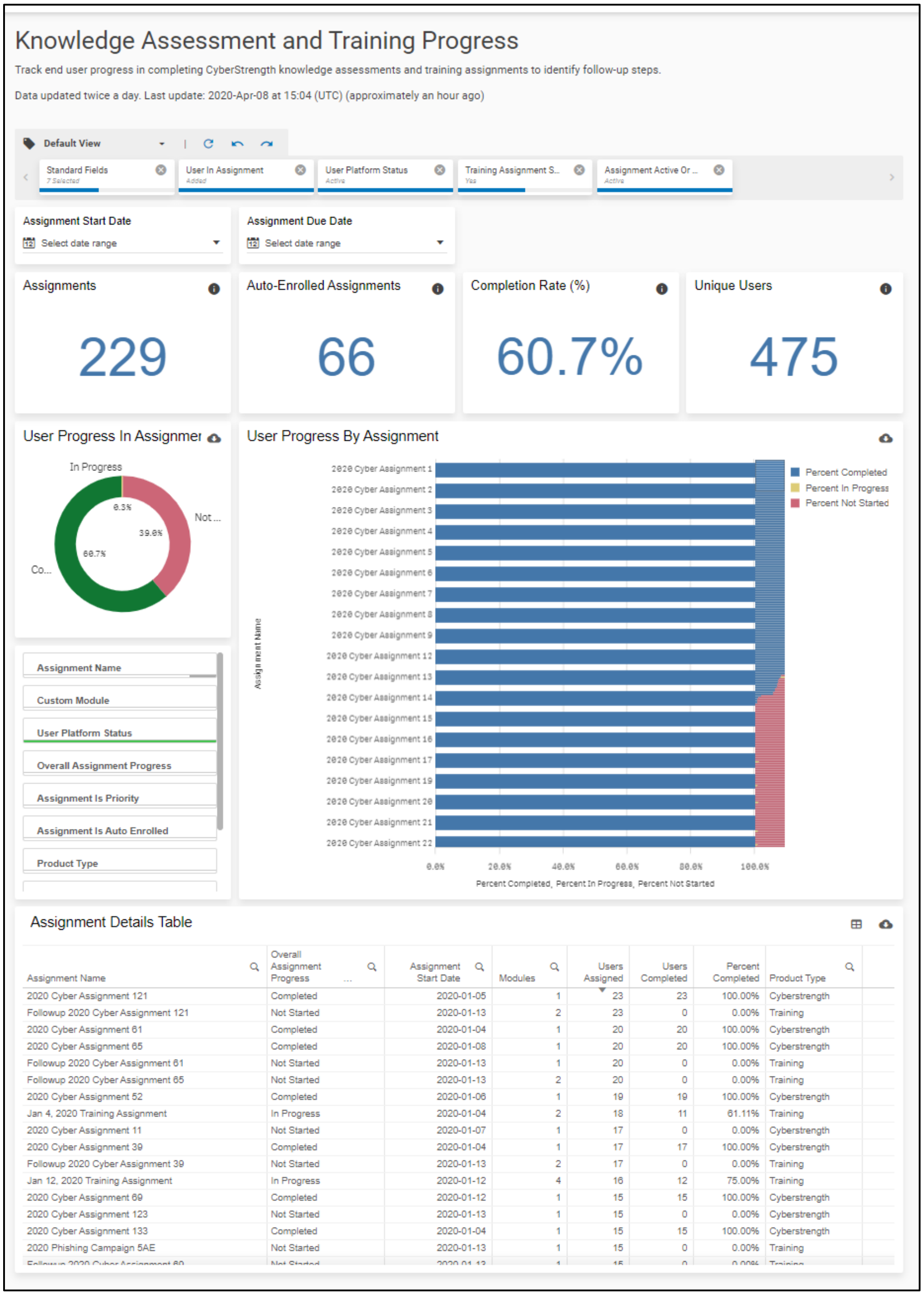
BENEFITS

- 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

SAMPLE KNOWLEDGE ASSESSMENT AND TRAINING PROGRESS REPORT



Knowledge Assessment and Training Progress

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

Data updated twice a day. Last update: 2020-Apr-08 at 15:04 (UTC) (approximately an hour ago)

Default View

Standard Fields: 7 Selected | User In Assignment: Added | User Platform Status: Active | Training Assignment S...: Yes | Assignment Active Or ...: Active

Assignment Start Date: Select date range

Assignment Due Date: Select date range

Assignments: 229

Auto-Enrolled Assignments: 66

Completion Rate (%): 60.7%

Unique Users: 475

User Progress In Assignmer

Assignment Name
Custom Module
User Platform Status
Overall Assignment Progress
Assignment Is Priority
Assignment Is Auto Enrolled
Product Type

User Progress By Assignment

Assignment Details Table

Assignment Name	Overall Assignment Progress	Assignment Start Date	Modules	Users Assigned	Users Completed	Percent Completed	Product Type
2020 Cyber Assignment 121	Completed	2020-01-05	1	23	23	100.00%	Cyberstrength
Followup 2020 Cyber Assignment 121	Not Started	2020-01-13	2	23	0	0.00%	Training
2020 Cyber Assignment 61	Completed	2020-01-04	1	20	20	100.00%	Cyberstrength
2020 Cyber Assignment 65	Completed	2020-01-08	1	20	20	100.00%	Cyberstrength
Followup 2020 Cyber Assignment 61	Not Started	2020-01-13	1	20	0	0.00%	Training
Followup 2020 Cyber Assignment 65	Not Started	2020-01-13	2	20	0	0.00%	Training
2020 Cyber Assignment 52	Completed	2020-01-06	1	19	19	100.00%	Cyberstrength
Jan 4, 2020 Training Assignment	In Progress	2020-01-04	2	18	11	61.11%	Training
2020 Cyber Assignment 11	Not Started	2020-01-07	1	17	0	0.00%	Cyberstrength
2020 Cyber Assignment 39	Completed	2020-01-04	1	17	17	100.00%	Cyberstrength
Followup 2020 Cyber Assignment 39	Not Started	2020-01-13	2	17	0	0.00%	Training
Jan 12, 2020 Training Assignment	In Progress	2020-01-12	4	16	12	75.00%	Training
2020 Cyber Assignment 69	Completed	2020-01-12	1	15	15	100.00%	Cyberstrength
2020 Cyber Assignment 123	Not Started	2020-01-13	1	15	0	0.00%	Cyberstrength
2020 Cyber Assignment 133	Completed	2020-01-04	1	15	15	100.00%	Cyberstrength
2020 Phishing Campaign 5AE	Not Started	2020-01-13	1	15	0	0.00%	Training
Followup 2020 Cyber Assignment 69	Not Started	2020-01-13	1	15	0	0.00%	Training

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

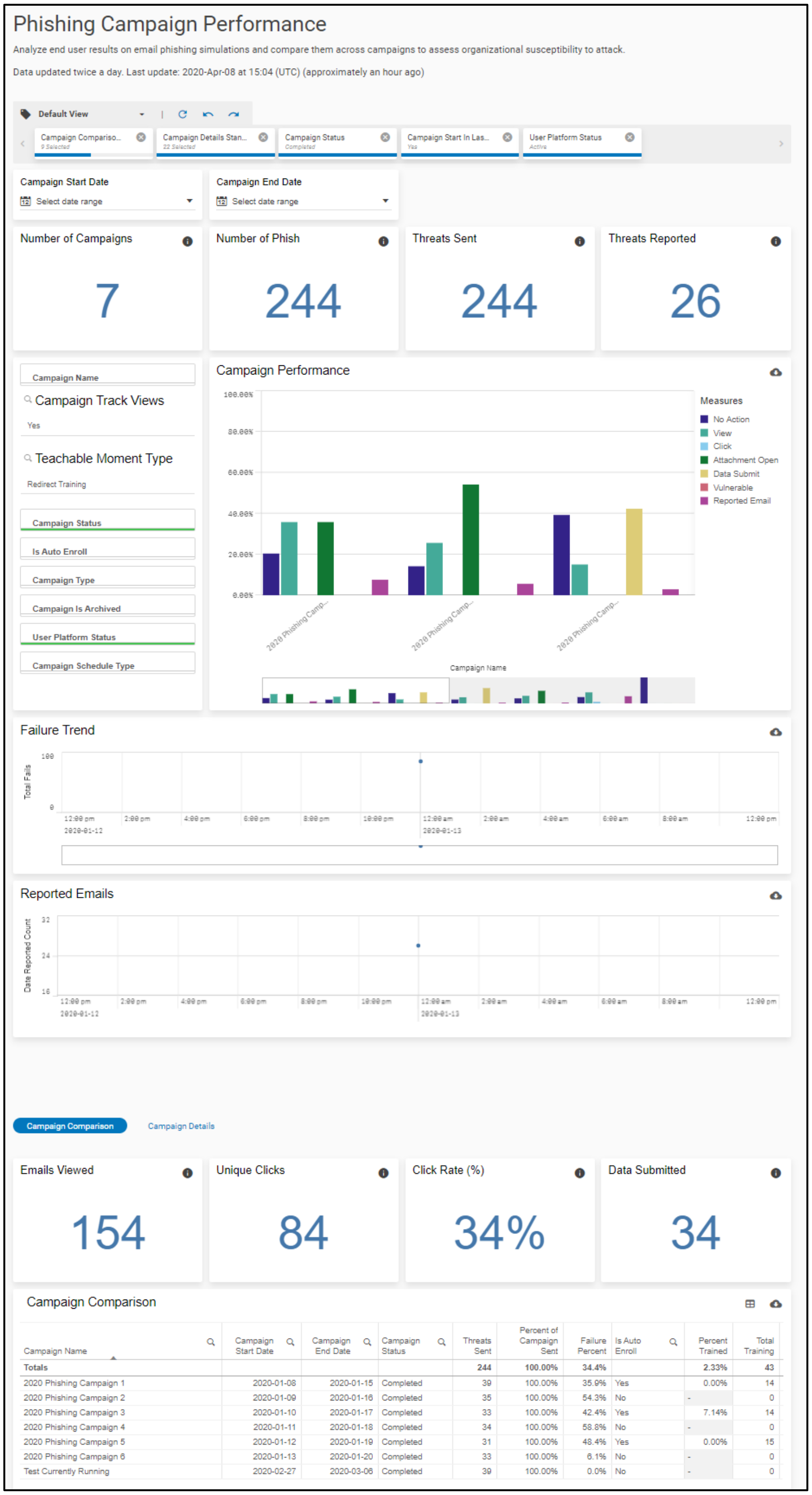
- Determine at the campaign- and user-level which campaign types end users are most vulnerable to so that additional campaigns can be developed and implemented.
- Drill-down to the user-level details to enable deeper analysis.
- Track phishing failure performance over time and use the trends to determine 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, threat emails sent, and threat 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, and 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

SAMPLE PHISHING CAMPAIGN PERFORMANCE REPORT

View includes Campaign Comparison Tab



Phishing Campaign Performance

Analyze end user results on email phishing simulations and compare them across campaigns to assess organizational susceptibility to attack.

Data updated twice a day. Last update: 2020-Apr-08 at 15:04 (UTC) (approximately an hour ago)

Default View
Campaign Compariso... 9 Selected
Campaign Details Stan... 22 Selected
Campaign Status Completed
Campaign Start In Las... Yes
User Platform Status Active

Campaign Start Date: Select date range

Campaign End Date: Select date range

Number of Campaigns: 7

Number of Phish: 244

Threats Sent: 244

Threats Reported: 26

Campaign Name

Campaign Track Views: Yes

Teachable Moment Type: Redirect Training

Campaign Performance

Failure Trend

Reported Emails

Emails Viewed: 154

Unique Clicks: 84

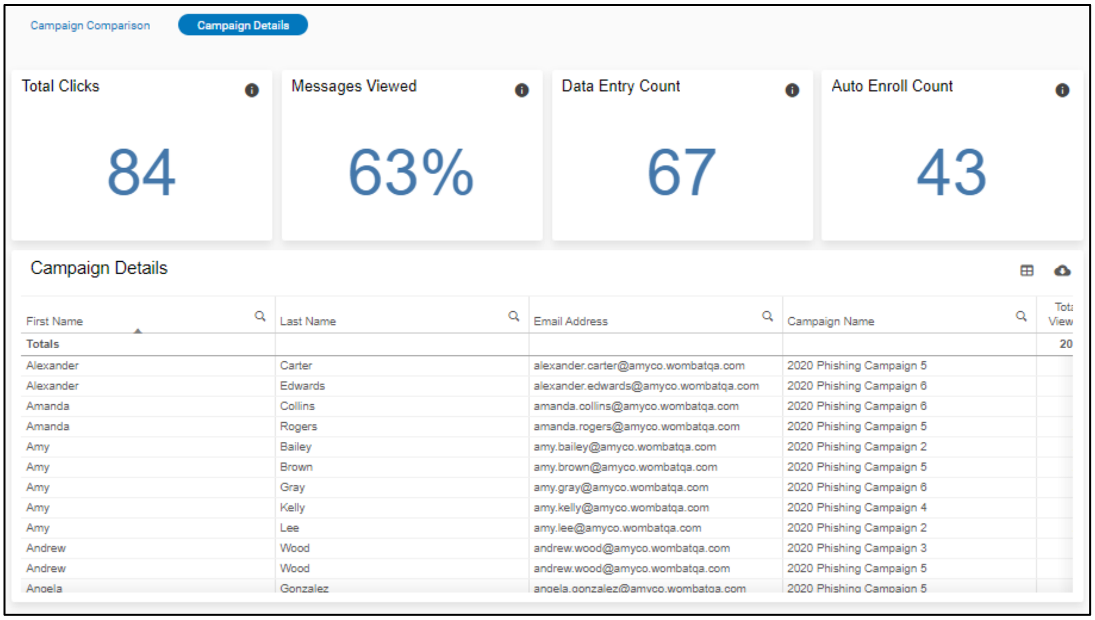
Click Rate (%): 34%

Data Submitted: 34

Campaign Comparison

Campaign Name	Campaign Start Date	Campaign End Date	Campaign Status	Threats Sent	Percent of Campaign Sent	Failure Percent	Is Auto Enroll	Percent Trained	Total Training
Totals				**244**	**100.00%**	**34.4%**		**2.33%**	**43**
2020 Phishing Campaign 1	2020-01-08	2020-01-15	Completed	39	100.00%	35.9%	Yes	0.00%	14
2020 Phishing Campaign 2	2020-01-09	2020-01-16	Completed	35	100.00%	54.3%	No	-	0
2020 Phishing Campaign 3	2020-01-10	2020-01-17	Completed	33	100.00%	42.4%	Yes	7.14%	14
2020 Phishing Campaign 4	2020-01-11	2020-01-18	Completed	34	100.00%	58.8%	No	-	0
2020 Phishing Campaign 5	2020-01-12	2020-01-19	Completed	31	100.00%	48.4%	Yes	0.00%	15
2020 Phishing Campaign 6	2020-01-13	2020-01-20	Completed	33	100.00%	6.1%	No	-	0
Test Currently Running	2020-02-27	2020-03-06	Completed	39	100.00%	0.0%	No	-	0

View of Campaign Details Tab



Total Clicks
84

Messages Viewed
63%

Data Entry Count
67

Auto Enroll Count
43

Campaign Details

First Name	Last Name	Email Address	Campaign Name	Tot: View
Totals				20
Alexander	Carter	alexander.carter@amyco.wombatqa.com	2020 Phishing Campaign 5	
Alexander	Edwards	alexander.edwards@amyco.wombatqa.com	2020 Phishing Campaign 6	
Amanda	Collins	amanda.collins@amyco.wombatqa.com	2020 Phishing Campaign 6	
Amanda	Rogers	amanda.rogers@amyco.wombatqa.com	2020 Phishing Campaign 5	
Amy	Bailey	amy.bailey@amyco.wombatqa.com	2020 Phishing Campaign 2	
Amy	Brown	amy.brown@amyco.wombatqa.com	2020 Phishing Campaign 5	
Amy	Gray	amy.gray@amyco.wombatqa.com	2020 Phishing Campaign 6	
Amy	Kelly	amy.kelly@amyco.wombatqa.com	2020 Phishing Campaign 4	
Amy	Lee	amy.lee@amyco.wombatqa.com	2020 Phishing Campaign 2	
Andrew	Wood	andrew.wood@amyco.wombatqa.com	2020 Phishing Campaign 3	
Andrew	Wood	andrew.wood@amyco.wombatqa.com	2020 Phishing Campaign 5	
Angela	Gonzalez	angela.gonzalez@amyco.wombatqa.com	2020 Phishing Campaign 5	

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.

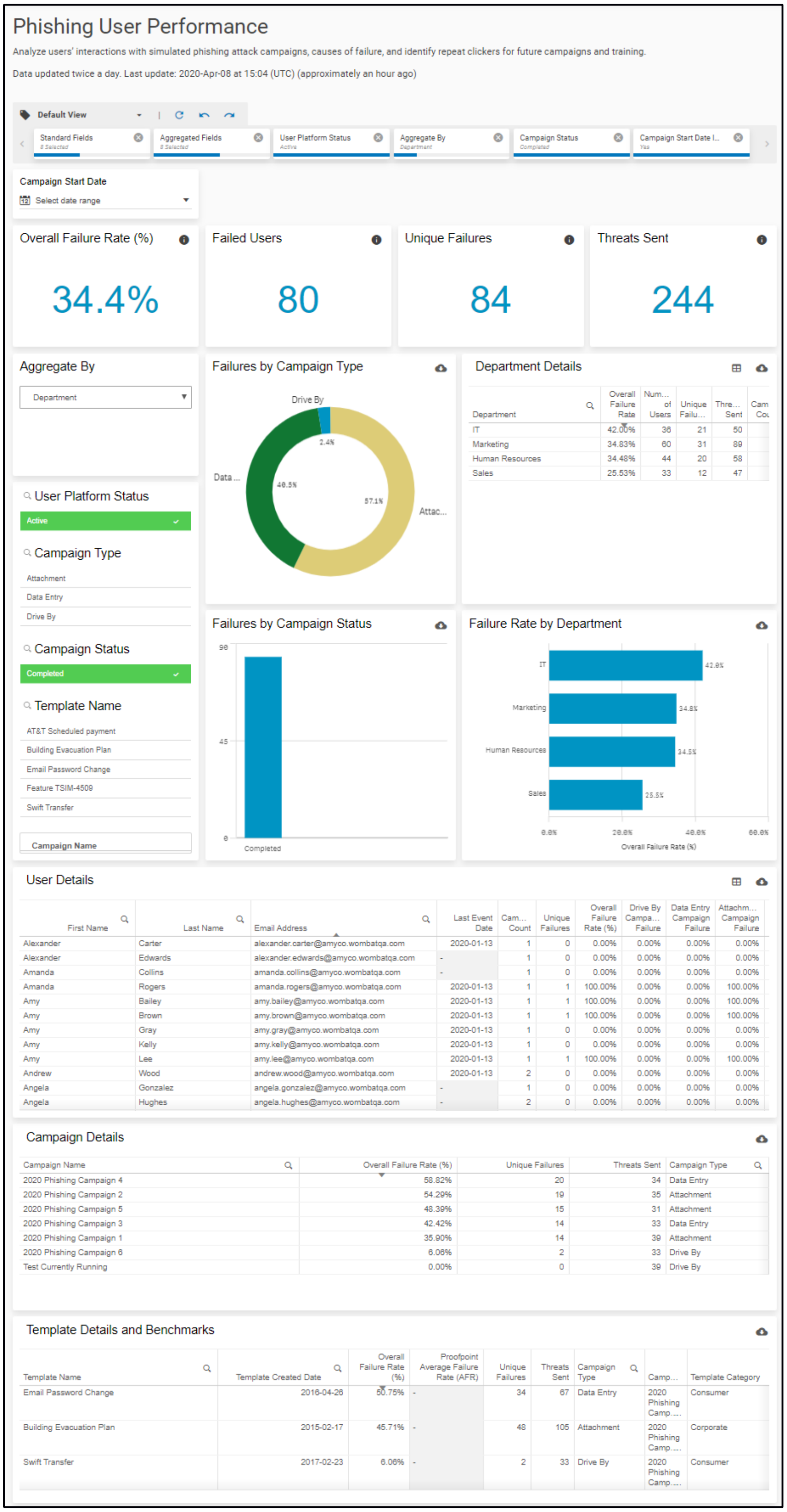
KEY FEATURES

- 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.

SAMPLE PHISHING USER PERFORMANCE REPORT

(see next page)

SAMPLE PHISHING USER PERFORMANCE REPORT (CONT.)



Phishing User Performance

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

Data updated twice a day. Last update: 2020-Apr-08 at 15:04 (UTC) (approximately an hour ago)

Campaign Start Date

Select date range

Overall Failure Rate (%)	Failed Users	Unique Failures	Threats Sent
34.4%	80	84	244

Aggregate By

Department

User Platform Status

- Active ✓

Campaign Type

- Attachment
- Data Entry
- Drive By

Campaign Status

- Completed ✓

Template Name

- AT&T Scheduled payment
- Building Evacuation Plan
- Email Password Change
- Feature TSIM-4509
- Swift Transfer

Campaign Name

Failures by Campaign Type

Department Details

Department	Overall Failure Rate	Num... of Users	Unique Failu...	Thre... Sent	Cam Cou
IT	42.00%	36	21	50	
Marketing	34.83%	60	31	89	
Human Resources	34.48%	44	20	58	
Sales	25.53%	33	12	47	

Failures by Campaign Status

Failure Rate by Department

User Details

First Name	Last Name	Email Address	Last Event Date	Cam... Count	Unique Failures	Overall Failure Rate (%)	Drive By Campa... Failure	Data Entry Campaign Failure	Attachm... Campaign Failure
Alexander	Carter	alexander.carter@amyco.wombatqa.com	2020-01-13	1	0	0.00%	0.00%	0.00%	0.00%
Alexander	Edwards	alexander.edwards@amyco.wombatqa.com	-	1	0	0.00%	0.00%	0.00%	0.00%
Amanda	Collins	amanda.collins@amyco.wombatqa.com	-	1	0	0.00%	0.00%	0.00%	0.00%
Amanda	Rogers	amanda.rogers@amyco.wombatqa.com	2020-01-13	1	1	100.00%	0.00%	0.00%	100.00%
Amy	Bailey	amy.bailey@amyco.wombatqa.com	2020-01-13	1	1	100.00%	0.00%	0.00%	100.00%
Amy	Brown	amy.brown@amyco.wombatqa.com	2020-01-13	1	1	100.00%	0.00%	0.00%	100.00%
Amy	Gray	amy.gray@amyco.wombatqa.com	2020-01-13	1	0	0.00%	0.00%	0.00%	0.00%
Amy	Kelly	amy.kelly@amyco.wombatqa.com	2020-01-13	1	0	0.00%	0.00%	0.00%	0.00%
Amy	Lee	amy.lee@amyco.wombatqa.com	2020-01-13	1	1	100.00%	0.00%	0.00%	100.00%
Andrew	Wood	andrew.wood@amyco.wombatqa.com	2020-01-13	2	0	0.00%	0.00%	0.00%	0.00%
Angela	Gonzalez	angela.gonzalez@amyco.wombatqa.com	-	1	0	0.00%	0.00%	0.00%	0.00%
Angela	Hughes	angela.hughes@amyco.wombatqa.com	-	2	0	0.00%	0.00%	0.00%	0.00%

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 2	54.29%	19	35	Attachment
2020 Phishing Campaign 5	48.39%	15	31	Attachment
2020 Phishing Campaign 3	42.42%	14	33	Data Entry
2020 Phishing Campaign 1	35.90%	14	39	Attachment
2020 Phishing Campaign 6	6.06%	2	33	Drive By
Test Currently Running	0.00%	0	39	Drive By

Template Details and Benchmarks

Template Name	Template Created Date	Overall Failure Rate (%)	Proofpoint Average Failure Rate (AFR)	Unique Failures	Threats Sent	Campaign Type	Camp...	Template Category
Email Password Change	2016-04-26	50.75%	-	34	67	Data Entry	2020 Phishing Camp....	Consumer
Building Evacuation Plan	2015-02-17	45.71%	-	48	105	Attachment	2020 Phishing Camp....	Corporate
Swift Transfer	2017-02-23	6.06%	-	2	33	Drive By	2020 Phishing Camp....	Consumer

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)

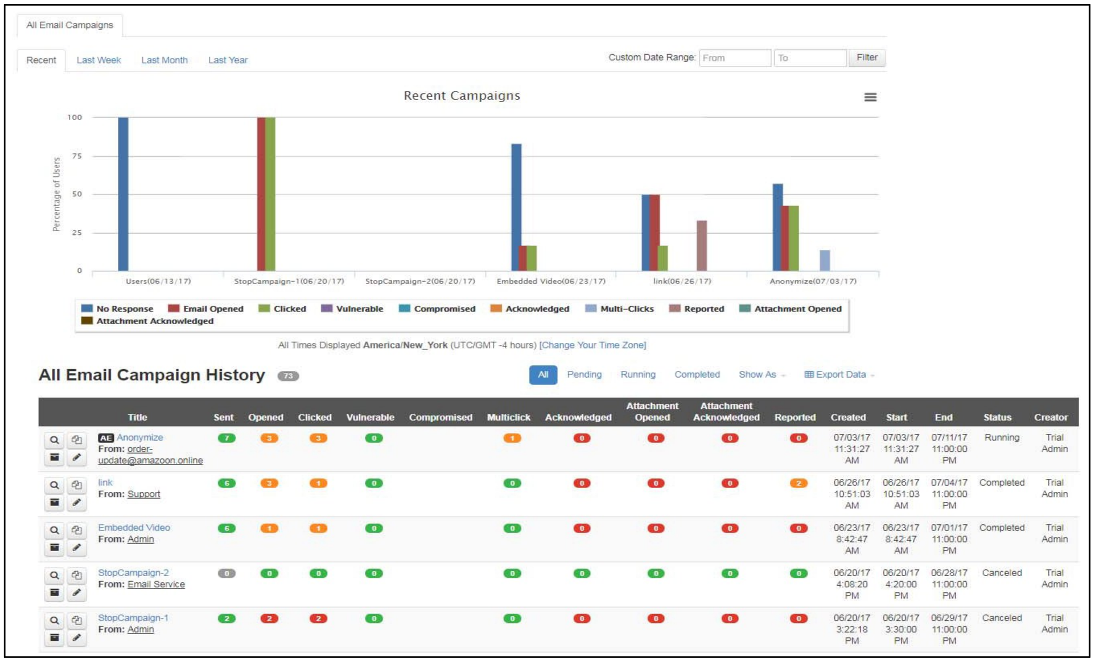
BENEFITS

- 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 option: CSV

SAMPLE THREATSIM CAMPAIGN OVERVIEW REPORT



All Times Displayed America/New_York (UTC/GMT -4 hours) [Change Your Time Zone]

All Email Campaign History 73

	Title	Sent	Opened	Clicked	Vulnerable	Compromised	Multiclick	Acknowledged	Attachment Opened	Attachment Acknowledged	Reported	Created	Start	End	Status	Creator
	AE Anonymize From: order-update@amazoon.online	7	3	3	0		1	0	0	0	0	07/03/17 11:31:27 AM	07/03/17 11:31:27 AM	07/11/17 11:00:00 PM	Running	Trial Admin
	link From: Support	6	3	1	0		0	0	0	0	2	06/26/17 10:51:03 AM	06/26/17 10:51:03 AM	07/04/17 11:00:00 PM	Completed	Trial Admin
	Embedded Video From: Admin	6	1	1	0		0	0	0	0	0	06/23/17 8:42:47 AM	06/23/17 8:42:47 AM	07/01/17 11:00:00 PM	Completed	Trial Admin
	StopCampaign-2 From: Email Service	0	0	0	0		0	0	0	0	0	06/20/17 4:08:20 PM	06/20/17 4:20:00 PM	06/28/17 11:00:00 PM	Canceled	Trial Admin
	StopCampaign-1 From: Admin	2	2	2	0		0	0	0	0	0	06/20/17 3:22:18 PM	06/20/17 3:30:00 PM	06/29/17 11:00:00 PM	Canceled	Trial Admin

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.

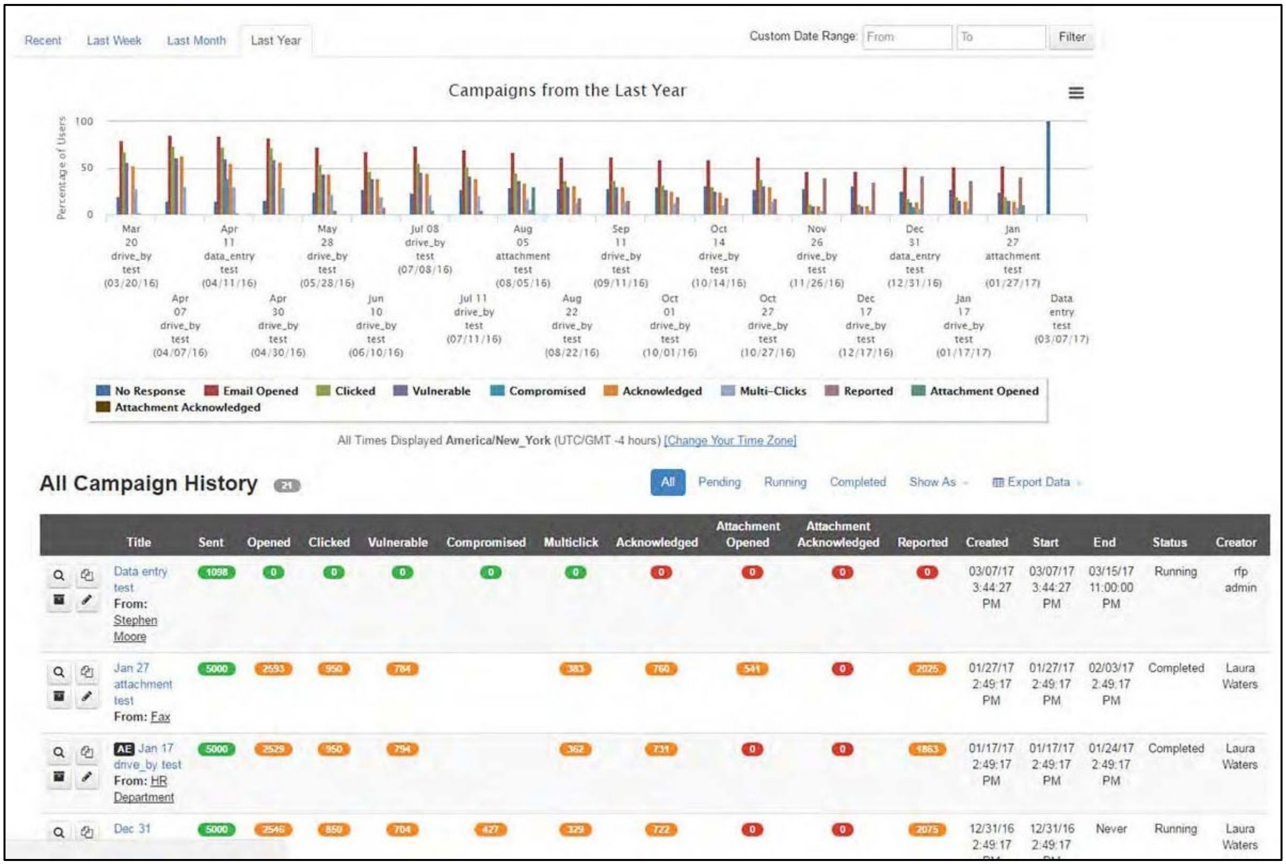
BENEFIT

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

SAMPLE THREATSIM INDIVIDUAL CAMPAIGN DETAILS REPORTS

All Campaigns History Report

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


Recent
Last Week
Last Month
Last Year
Custom Date Range: From
To
Filter
Campaigns from the Last Year
Percentage of Users
100
50
0
Mar 20 drive_by test (03/20/16)
Apr 07 drive_by test (04/07/16)
Apr 11 data_entry test (04/11/16)
Apr 30 drive_by test (04/30/16)
May 28 drive_by test (05/28/16)
Jun 10 drive_by test (06/10/16)
Jul 08 drive_by test (07/08/16)
Jul 11 drive_by test (07/11/16)
Aug 05 attachment test (08/05/16)
Aug 22 drive_by test (08/22/16)
Sep 11 drive_by test (09/11/16)
Oct 01 drive_by test (10/01/16)
Oct 14 drive_by test (10/14/16)
Oct 27 drive_by test (10/27/16)
Nov 26 drive_by test (11/26/16)
Dec 17 drive_by test (12/17/16)
Dec 31 data_entry test (12/31/16)
Jan 17 drive_by test (01/17/17)
Jan 27 attachment test (01/27/17)
Data entry test (03/07/17)
No Response
Email Opened
Clicked
Vulnerable
Compromised
Acknowledged
Multi-Clicks
Reported
Attachment Opened
Attachment Acknowledged

All Times Displayed America/New_York (UTC/GMT -4 hours) [Change Your Time Zone]

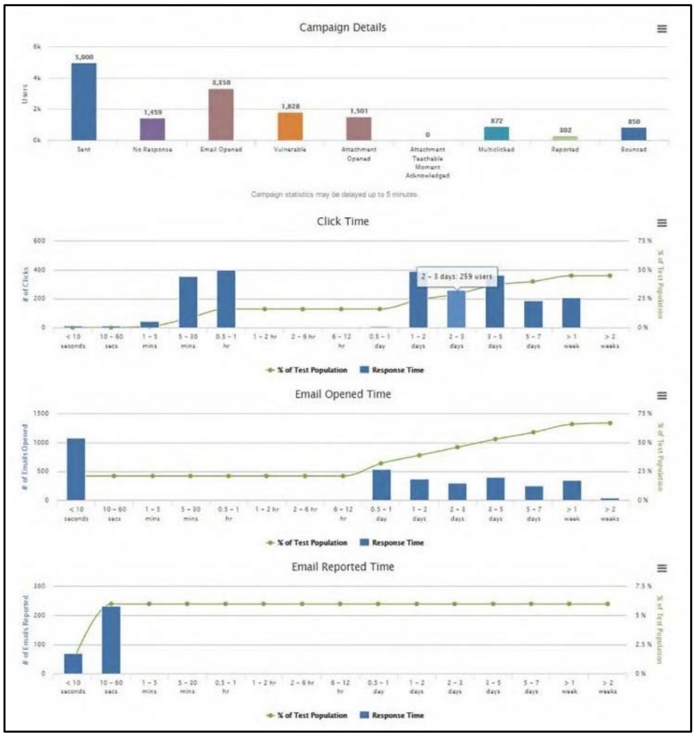
All Campaign History 21

All
Pending
Running
Completed
Show As
Export Data

Title	Sent	Opened	Clicked	Vulnerable	Compromised	Multiclick	Acknowledged	Attachment Opened	Attachment Acknowledged	Reported	Created	Start	End	Status	Creator
Data entry test From: Stephen Moore	1098	0	0	0	0	0	0	0	0	0	03/07/17 3:44:27 PM	03/07/17 3:44:27 PM	03/15/17 11:00:00 PM	Running	rfp admin
Jan 27 attachment test From: Fax	5000	2593	950	784		383	760	541	0	2025	01/27/17 2:49:17 PM	01/27/17 2:49:17 PM	02/03/17 2:49:17 PM	Completed	Laura Waters
AE Jan 17 drive_by test From: HR Department	5000	2529	950	794		362	731	0	0	1863	01/17/17 2:49:17 PM	01/17/17 2:49:17 PM	01/24/17 2:49:17 PM	Completed	Laura Waters
Dec 31	5000	2546	850	704	427	329	722	0	0	2075	12/31/16 2:49:17	12/31/16 2:49:17	Never	Running	Laura Waters

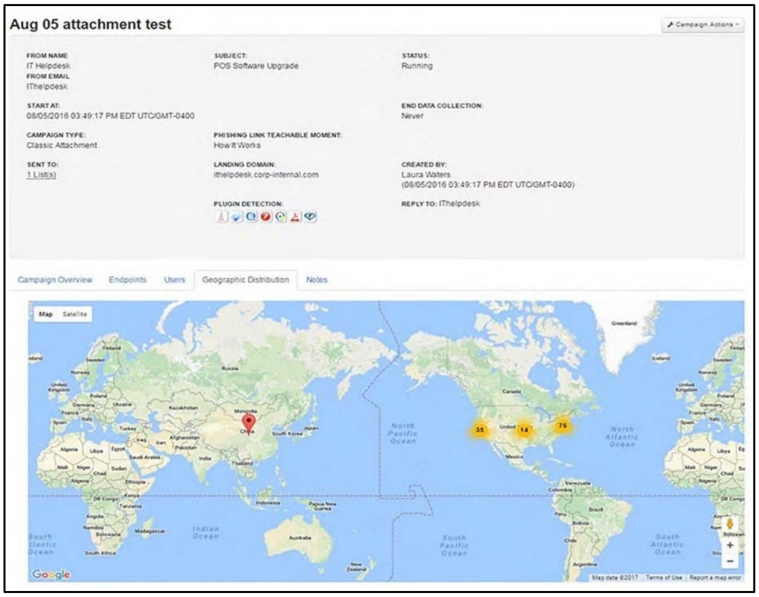
Individual Campaign Overview Report

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.



Aug 05 attachment test

FROM NAME
IT Helpdesk
FROM EMAIL
IThelpdesk

SUBJECT:
POS Software Upgrade

STATUS:
Running

START AT:
08/05/2016 03:49:17 PM EDT UTC/GMT-0400

END DATA COLLECTION:
Never

CAMPAIGN TYPE:
Classic Attachment

PHISHING LINK TEACHABLE MOMENT:
How It Works

SENT TO:
1 List(s)

LANDING DOMAIN:
ithelpdesk.corp-internal.com

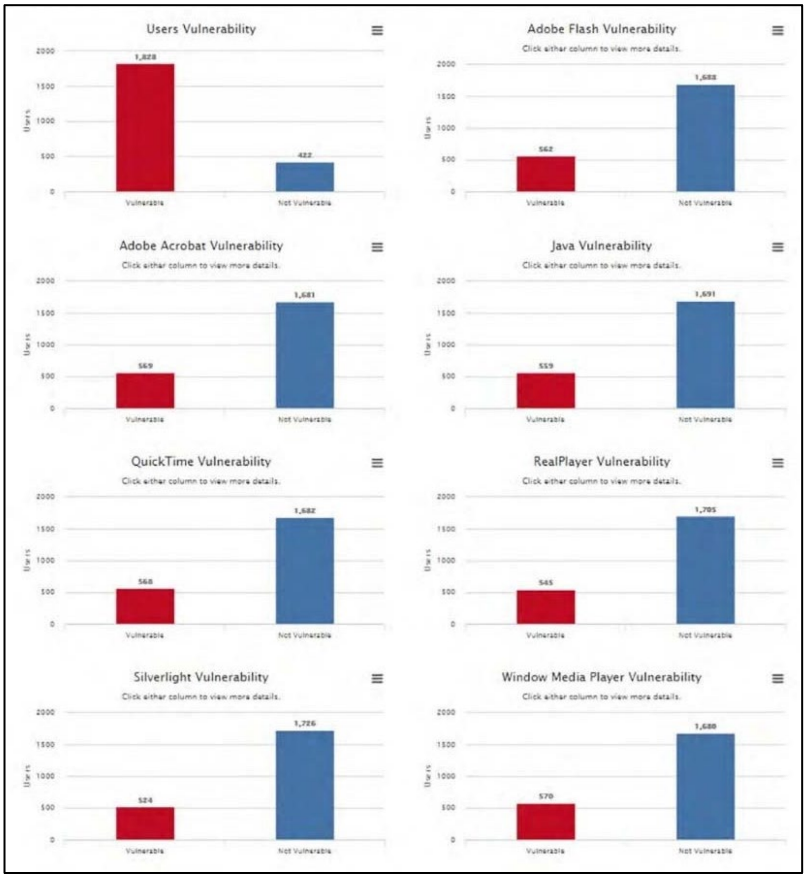
CREATED BY:
Laura Waters
(08/05/2016 03:49:17 PM EDT UTC/GMT-0400)

PLUGIN DETECTION:

REPLY TO: IThelpdesk

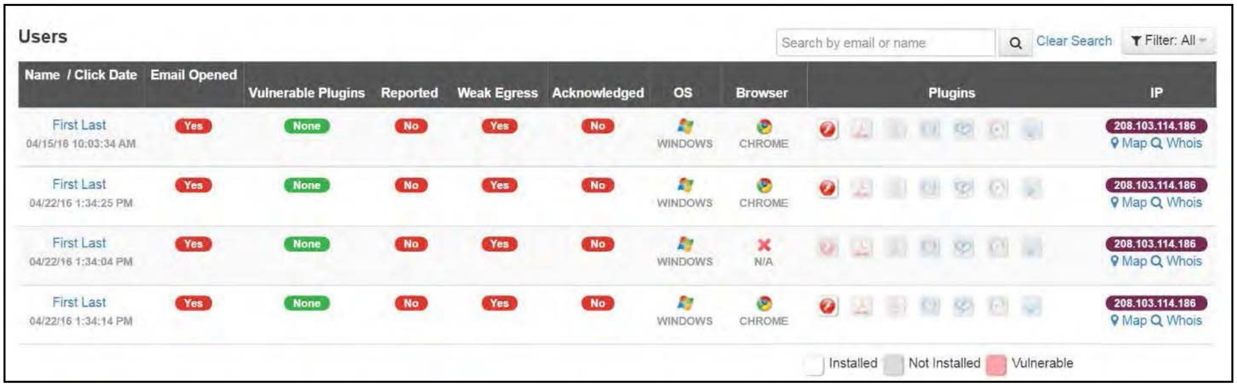
Endpoints Report

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).



Name / Click Date	Email Opened	Vulnerable Plugins	Reported	Weak Egress	Acknowledged	OS	Browser	Plugins	IP
First Last 04/15/16 10:03:34 AM	Yes	None	No	Yes	No	WINDOWS	CHROME		208.103.114.186 Map Whois
First Last 04/22/16 1:34:25 PM	Yes	None	No	Yes	No	WINDOWS	CHROME		208.103.114.186 Map Whois
First Last 04/22/16 1:34:04 PM	Yes	None	No	Yes	No	WINDOWS	✕ N/A		208.103.114.186 Map Whois
First Last 04/22/16 1:34:14 PM	Yes	None	No	Yes	No	WINDOWS	CHROME		208.103.114.186 Map Whois

□ Installed ▨ Not Installed 🟥 Vulnerable

THREATSIM RAW CAMPAIGN DATA CSV REPORTS

OBJECTIVE

The ThreatSim Raw Campaign Data CSV reports provide 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

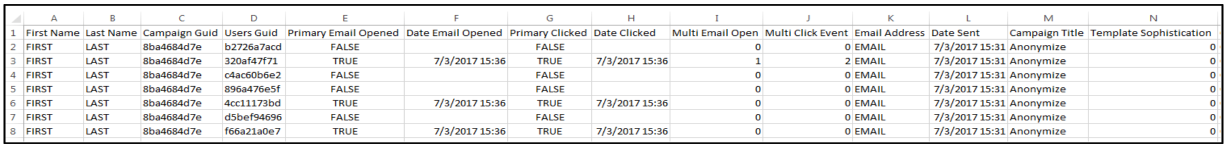
Simple export of comprehensive ThreatSim data for quick and easy import into the organization's preferred analysis tool for evaluation.

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 option: CSV

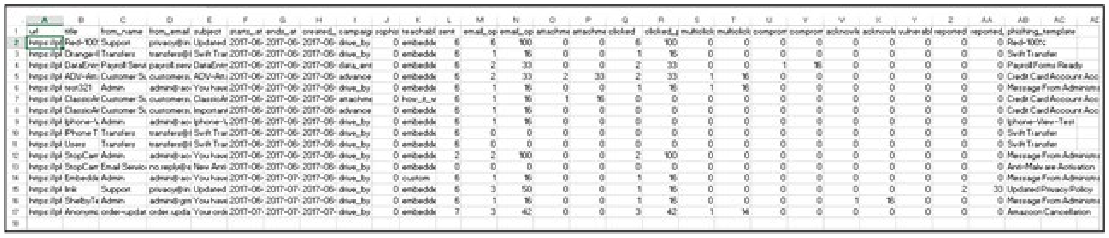
SAMPLE THREATSIM RAW CAMPAIGN DATA CSV REPORTS

Campaign Overview CSV Report



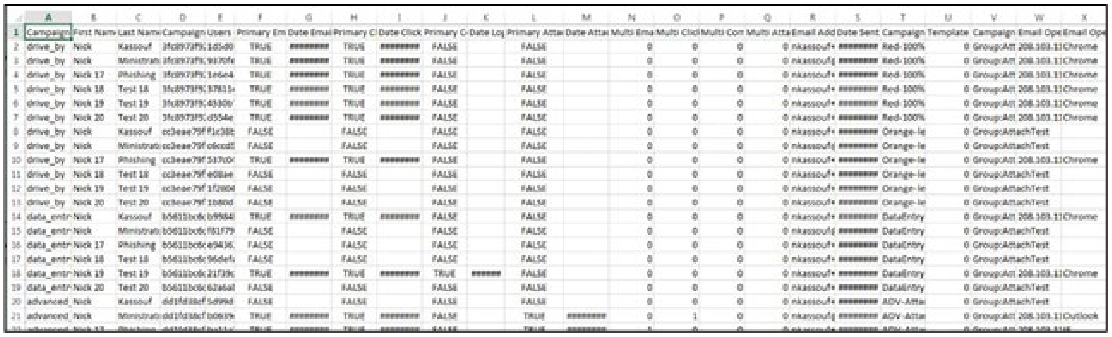
	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	First Name	Last Name	Campaign Guid	Users Guid	Primary Email Opened	Date Email Opened	Primary Clicked	Date Clicked	Multi Email Open	Multi Click Event	Email Address	Date Sent	Campaign Title	Template Sophistication
2	FIRST	LAST	8ba4684d7e	b2726a7acd	FALSE		FALSE		0	0	EMAIL	7/3/2017 15:31	Anonymize	0
3	FIRST	LAST	8ba4684d7e	320af47f71	TRUE	7/3/2017 15:36	TRUE	7/3/2017 15:36	1	2	EMAIL	7/3/2017 15:31	Anonymize	0
4	FIRST	LAST	8ba4684d7e	c4ac60b6e2	FALSE		FALSE		0	0	EMAIL	7/3/2017 15:31	Anonymize	0
5	FIRST	LAST	8ba4684d7e	896a476e5f	FALSE		FALSE		0	0	EMAIL	7/3/2017 15:31	Anonymize	0
6	FIRST	LAST	8ba4684d7e	4cc11173bd	TRUE	7/3/2017 15:36	TRUE	7/3/2017 15:36	0	0	EMAIL	7/3/2017 15:31	Anonymize	0
7	FIRST	LAST	8ba4684d7e	d5bef94696	FALSE		FALSE		0	0	EMAIL	7/3/2017 15:31	Anonymize	0
8	FIRST	LAST	8ba4684d7e	f66a21a0e7	TRUE	7/3/2017 15:36	TRUE	7/3/2017 15:36	0	0	EMAIL	7/3/2017 15:31	Anonymize	0

Campaign History CSV Report



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	AA	AB
1	url	title	from_name	from_email	subject	starts_at	ends_at	created_	campaign	sophis	teachabl	sent	email_op	email_op	attachme	attachme	clicked	clicked_p	multiclick	multiclick	comprom	comprom	acknowle	acknowle	vulnerabl	reported	reported_	phishing_template
2	https://pl	Red-100	Support	privacy@in	Updated	2017-06-	2017-06-	2017-06-	drive_by	0	embedde	6	6	100	0	0	6	100	0	0	0	0	0	0	0	0	0	Red-100%
3	https://pl	Orange-l	Transfers	transfers@	Swift Trar	2017-06-	2017-06-	2017-06-	drive_by	0	embedde	6	1	16	0	0	1	16	0	0	0	0	0	0	0	0	0	Swift Transfer
4	https://pl	DataEntr	Payroll Serv	payroll.serv	DataEntr	2017-06-	2017-06-	2017-06-	data_ent	0	embedde	6	2	33	0	0	2	33	0	0	1	16	0	0	0	0	0	Payroll Forms Ready
5	https://pl	ADV-Att	Customer S	customers	ADV-Att	2017-06-	2017-06-	2017-06-	advance	0	embedde	6	2	33	2	33	2	33	1	16	0	0	0	0	0	0	0	Credit Card Account Acc
6	https://pl	test321	Admin	admin@aci	You have	2017-06-	2017-06-	2017-06-	drive_by	0	embedde	6	1	16	0	0	1	16	1	16	0	0	0	0	0	0	0	Message From Administ
7	https://pl	ClassicAt	Customer S	customers	ClassicAt	2017-06-	2017-06-	2017-06-	attachme	0	how_it_w	6	1	16	1	16	0	0	0	0	0	0	0	0	0	0	0	Credit Card Account Acc
8	https://pl	ClassicAt	Customer S	customers	Important	2017-06-	2017-06-	2017-06-	advance	0	embedde	6	1	16	0	0	0	0	0	0	0	0	0	0	0	0	0	Credit Card Account Acc
9	https://pl	iphone-V	Admin	admin@aci	iphone-V	2017-06-	2017-06-	2017-06-	drive_by	0	embedde	6	1	16	0	0	0	0	0	0	0	0	0	0	0	0	0	iphone-View-Test
10	https://pl	iPhone T	Transfers	transfers@	Swift Trar	2017-06-	2017-06-	2017-06-	drive_by	0	embedde	6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Swift Transfer
11	https://pl	Users	Transfers	transfers@	Swift Trar	2017-06-	2017-06-	2017-06-	drive_by	0	embedde	6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Swift Transfer
12	https://pl	StopCam	Admin	admin@aci	You have	2017-06-	2017-06-	2017-06-	drive_by	0	embedde	2	2	100	0	0	2	100	0	0	0	0	0	0	0	0	0	Message From Administ
13	https://pl	StopCam	Email Servic	no.reply@e	New Ant	2017-06-	2017-06-	2017-06-	drive_by	0	embedde	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Anti-Malware Activation
14	https://pl	Embedde	Admin	admin@aci	You have	2017-06-	2017-07-	2017-06-	drive_by	0	custom	6	1	16	0	0	1	16	0	0	0	0	0	0	0	0	0	Message From Administ
15	https://pl	link	Support	privacy@in	Updated	2017-06-	2017-07-	2017-06-	drive_by	0	embedde	6	3	50	0	0	1	16	0	0	0	0	0	0	0	2	33	Updated Privacy Policy
16	https://pl	ShelbyT	Admin	admin@gm	You have	2017-06-	2017-07-	2017-06-	drive_by	0	embedde	6	1	16	0	0	1	16	0	0	0	0	1	16	0	0	0	Message From Administ
17	https://pl	Anonymi	order-updat	order.upda	Your ord	2017-07-	2017-07-	2017-07-	drive_by	0	embedde	7	3	42	0	0	3	42	1	14	0	0	0	0	0	0	0	Amazon Cancellation
18																												

Campaign Details CSV Report



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
1	Campaign	First Nam	Last Nam	Campaign	Users	Primary Em	Date Emai	Primary C	Date Click	Primary C	Date Log	Primary Atta	Date Atta	Multi Ema	Multi Clicl	Multi Com	Multi Atta	Email Add	Date Sent	Campaign	Template	Campaign	Email Ope	Email Ope
2	drive_by	Nick	Kassouf	3fc8973f9(	1d5d0	TRUE	########	TRUE	########	FALSE		FALSE		0	0	0	0	nkassouf+	########	Red-100%	0	Group:Att	208.103.1	Chrome
3	drive_by	Nick	Ministrat	3fc8973f9(	9170fe	TRUE	########	TRUE	########	FALSE		FALSE		0	0	0	0	nkassouf@	########	Red-100%	0	Group:Att	208.103.1	Chrome
4	drive_by	Nick 17	Phishing	3fc8973f9(	1e6e4	TRUE	########	TRUE	########	FALSE		FALSE		0	0	0	0	nkassouf+	########	Red-100%	0	Group:Att	208.103.1	Chrome
5	drive_by	Nick 18	Test 18	3fc8973f9(	17815	TRUE	########	TRUE	########	FALSE		FALSE		0	0	0	0	nkassouf+	########	Red-100%	0	Group:Att	208.103.1	Chrome
6	drive_by	Nick 19	Test 19	3fc8973f9(	43306	TRUE	########	TRUE	########	FALSE		FALSE		0	0	0	0	nkassouf+	########	Red-100%	0	Group:Att	208.103.1	Chrome
7	drive_by	Nick 20	Test 20	3fc8973f9(	d554e	TRUE	########	TRUE	########	FALSE		FALSE		0	0	0	0	nkassouf+	########	Red-100%	0	Group:Att	208.103.1	Chrome
8	drive_by	Nick	Kassouf	cc3eae79f	f1c38	FALSE		FALSE		FALSE		FALSE		0	0	0	0	nkassouf+	########	Orange-le	0	Group:AttachTest		
9	drive_by	Nick	Ministrat	cc3eae79f	c6cod	FALSE		FALSE		FALSE		FALSE		0	0	0	0	nkassouf@	########	Orange-le	0	Group:AttachTest		
10	drive_by	Nick 17	Phishing	cc3eae79f	537c0	TRUE	########	TRUE	########	FALSE		FALSE		0	0	0	0	nkassouf+	########	Orange-le	0	Group:Att	208.103.1	Chrome
11	drive_by	Nick 18	Test 18	cc3eae79f	e08ae	FALSE		FALSE		FALSE		FALSE		0	0	0	0	nkassouf+	########	Orange-le	0	Group:AttachTest		
12	drive_by	Nick 19	Test 19	cc3eae79f	1f2804	FALSE		FALSE		FALSE		FALSE		0	0	0	0	nkassouf+	########	Orange-le	0	Group:AttachTest		
13	drive_by	Nick 20	Test 20	cc3eae79f	1b80d	FALSE		FALSE		FALSE		FALSE		0	0	0	0	nkassouf+	########	Orange-le	0	Group:AttachTest		
14	data_entr	Nick	Kassouf	b5611bc6c	b9984	TRUE	########	TRUE	########	FALSE		FALSE		0	0	0	0	nkassouf+	########	DataEntry	0	Group:Att	208.103.1	Chrome
15	data_entr	Nick	Ministrat	b5611bc6c	f81f79	FALSE		FALSE		FALSE		FALSE		0	0	0	0	nkassouf@	########	DataEntry	0	Group:AttachTest		
16	data_entr	Nick 17	Phishing	b5611bc6c	e9436	FALSE		FALSE		FALSE		FALSE		0	0	0	0	nkassouf+	########	DataEntry	0	Group:AttachTest		
17	data_entr	Nick 18	Test 18	b5611bc6c	96def	FALSE		FALSE		FALSE		FALSE		0	0	0	0	nkassouf+	########	DataEntry	0	Group:AttachTest		
18	data_entr	Nick 19	Test 19	b5611bc6c	21f39	TRUE	########	TRUE	########	TRUE	######	FALSE		0	0	0	0	nkassouf+	########	DataEntry	0	Group:Att	208.103.1	Chrome
19	data_entr	Nick 20	Test 20	b5611bc6c	62a6a	FALSE		FALSE		FALSE		FALSE		0	0	0	0	nkassouf+	########	DataEntry	0	Group:AttachTest		
20	advanced_	Nick	Kassouf	dd1fd38cf	5d99d	FALSE		FALSE		FALSE		FALSE		0	0	0	0	nkassouf+	########	ADV-Attac	0	Group:AttachTest		
21	advanced_	Nick	Ministrat	dd1fd38cf	b0639	TRUE	########	TRUE	########	FALSE		TRUE	########	0	1	0	0	nkassouf@	########	ADV-Attac	0	Group:Att	208.103.1	Outlook
22	advanced_	Nick 17	Phishing	dd1fd38cf	[illegible]	TRUE	########	TRUE	########	FALSE		TRUE	########	1	0	0	0	nkassouf+	########	ADV-Attac	0	Group:Att	208.103.1	[illegible]

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.

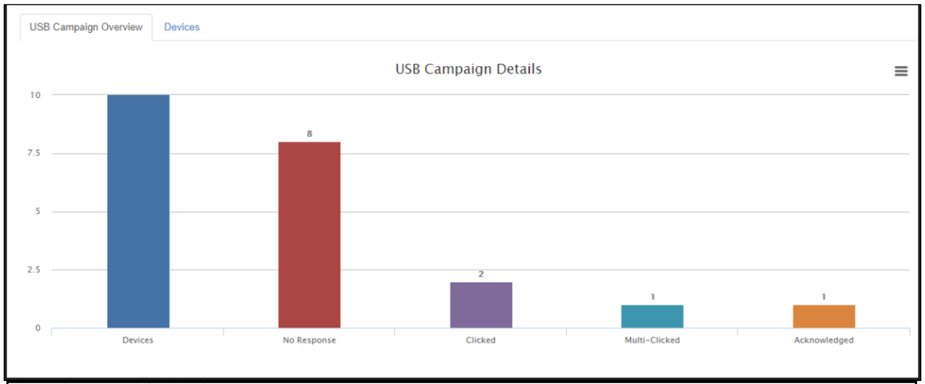
BENEFITS

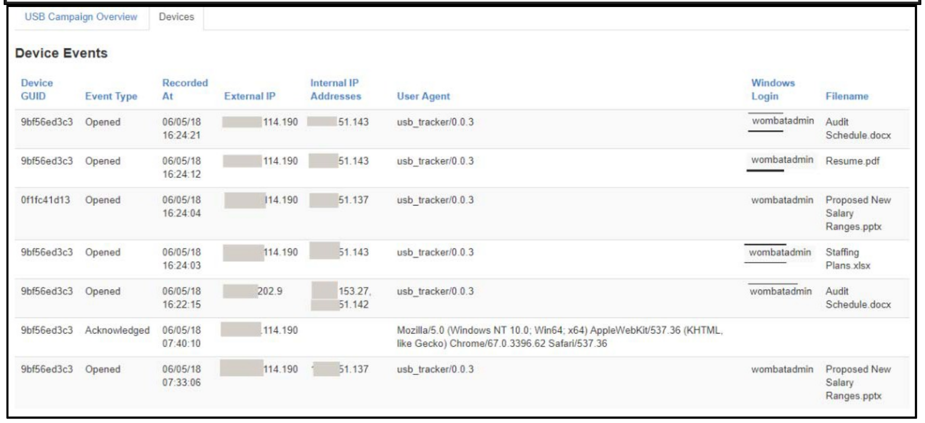
- Examine the organization's recent USB campaigns and performance at a glance, analyze the details, and determine the next steps in cybersecurity training programs.
- View USB campaign results and determine which campaigns are most effective for the organization.

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.

SAMPLE THREATSIM USB CAMPAIGN DETAILS REPORT





Device Events

Device GUID	Event Type	Recorded At	External IP	Internal IP Addresses	User Agent	Windows Login	Filename
9bf56ed3c3	Opened	06/05/18 16:24:21	[redacted]114.190	[redacted]51.143	usb_tracker/0.0.3	wombatadmin	Audit Schedule.docx
9bf56ed3c3	Opened	06/05/18 16:24:12	[redacted]114.190	[redacted]51.143	usb_tracker/0.0.3	wombatadmin	Resume.pdf
0f1fc41d13	Opened	06/05/18 16:24:04	[redacted]14.190	[redacted]51.137	usb_tracker/0.0.3	wombatadmin	Proposed New Salary Ranges.pptx
9bf56ed3c3	Opened	06/05/18 16:24:03	[redacted]114.190	[redacted]51.143	usb_tracker/0.0.3	wombatadmin	Staffing Plans.xlsx
9bf56ed3c3	Opened	06/05/18 16:22:15	[redacted]202.9	[redacted]153.27, [redacted]51.142	usb_tracker/0.0.3	wombatadmin	Audit Schedule.docx
9bf56ed3c3	Acknowledged	06/05/18 07:40:10	[redacted]114.190		Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.62 Safari/537.36		
9bf56ed3c3	Opened	06/05/18 07:33:06	[redacted]114.190	[redacted]51.137	usb_tracker/0.0.3	wombatadmin	Proposed New Salary Ranges.pptx

REPORTED EMAIL PERFORMANCE & ANALYSIS REPORTS

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

- PhishAlarm Analyzer Results Report
- Reported Email Performance Report

PHISHALARM ANALYZER RESULTS REPORT

OBJECTIVE

The PhishAlarm Analyzer Results 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.

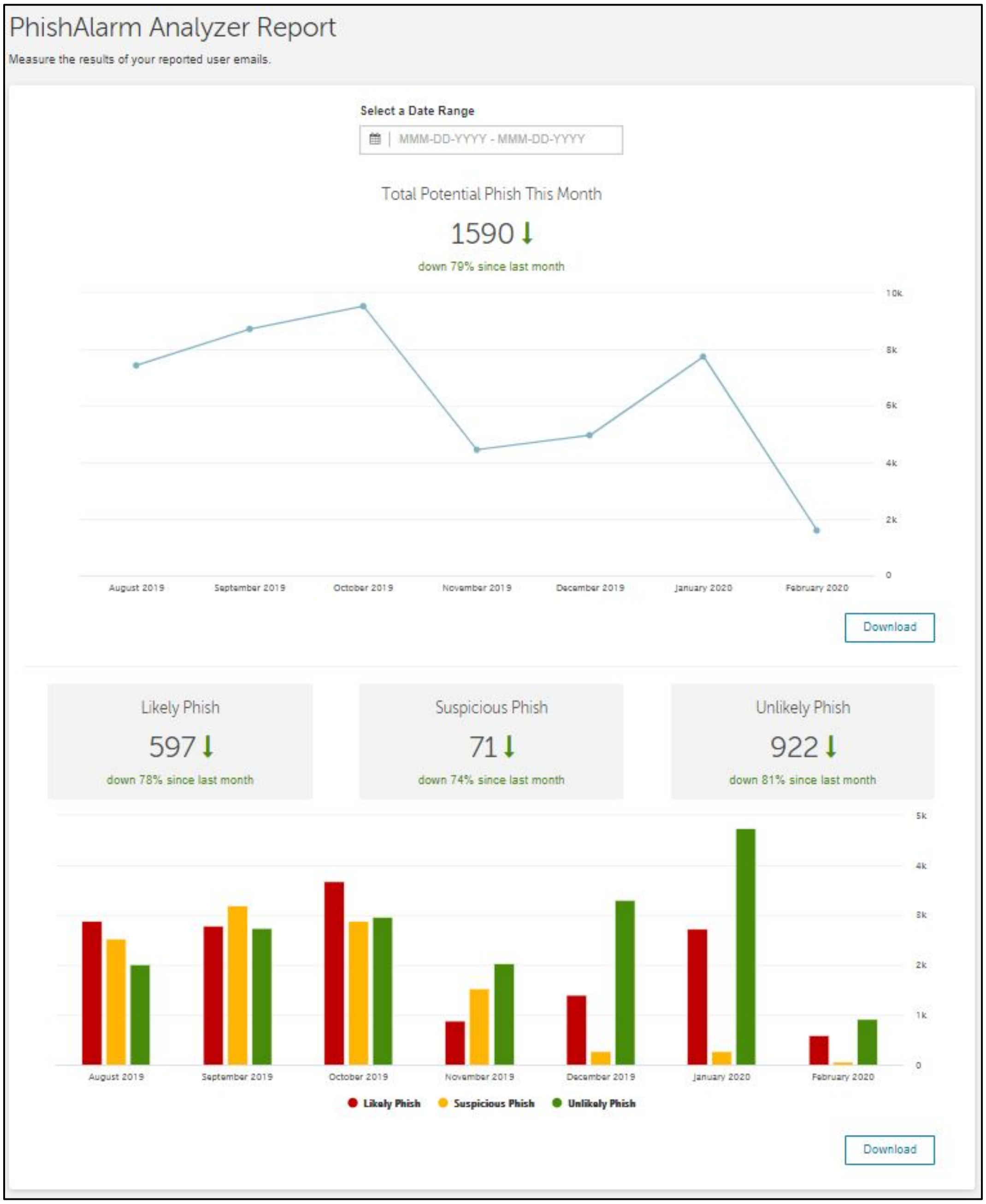
KEY FEATURES

- 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 option: CSV

SAMPLE PHISHALARM ANALYZER RESULTS REPORT

(see next page)

SAMPLE PHISHALARM ANALYZER RESULTS REPORT (CONT.)



PhishAlarm Analyzer Report

Measure the results of your reported user emails.

Select a Date Range

MMM-DD-YYYY - MMM-DD-YYYY

Total Potential Phish This Month

1590 ↓

down 79% since last month

Likely Phish

597 ↓

down 78% since last month

Suspicious Phish

71 ↓

down 74% since last month

Unlikely Phish

922 ↓

down 81% since last month

REPORTED EMAIL PERFORMANCE REPORT

OBJECTIVE

The Reported Email 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.

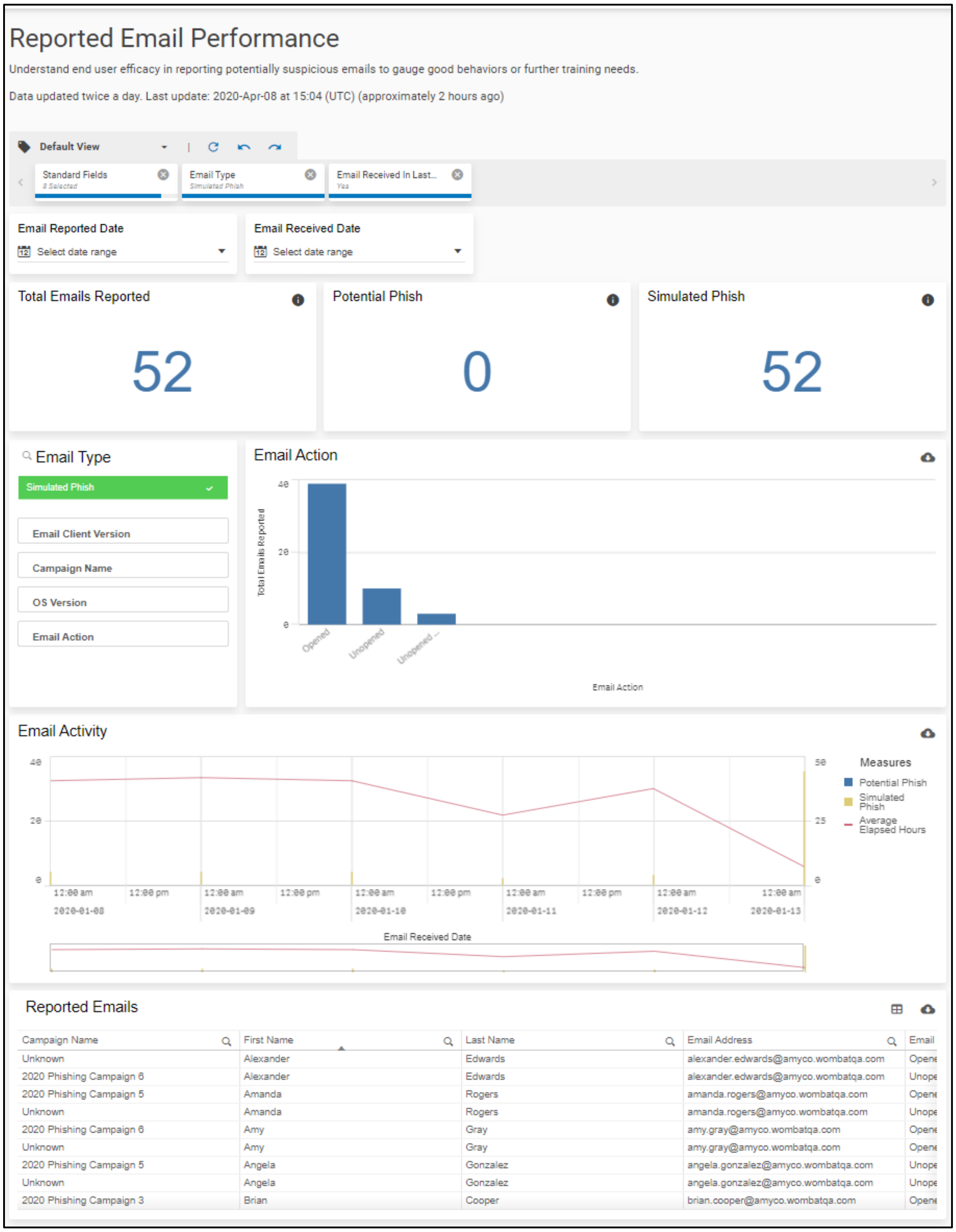
KEY FEATURES

- 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, and simulated phish.
- 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

SAMPLE REPORTED EMAIL PERFORMANCE REPORT

(see next page)

SAMPLE REPORTED EMAIL PERFORMANCE REPORT (CONT.)



Reported Email Performance

Understand end user efficacy in reporting potentially suspicious emails to gauge good behaviors or further training needs.

Data updated twice a day. Last update: 2020-Apr-08 at 15:04 (UTC) (approximately 2 hours ago)

Default View

Standard Fields: 8 Selected

Email Type: Simulated Phish

Email Received In Last...: Yes

Email Reported Date: Select date range

Email Received Date: Select date range

Total Emails Reported: 52

Potential Phish: 0

Simulated Phish: 52

Email Type

- Simulated Phish ✓
- Email Client Version
- Campaign Name
- OS Version
- Email Action

Reported Emails

Campaign Name	First Name	Last Name	Email Address	Email
Unknown	Alexander	Edwards	alexander.edwards@amyco.wombatqa.com	Opene
2020 Phishing Campaign 6	Alexander	Edwards	alexander.edwards@amyco.wombatqa.com	Unope
2020 Phishing Campaign 5	Amanda	Rogers	amanda.rogers@amyco.wombatqa.com	Opene
Unknown	Amanda	Rogers	amanda.rogers@amyco.wombatqa.com	Unope
2020 Phishing Campaign 6	Amy	Gray	amy.gray@amyco.wombatqa.com	Opene
Unknown	Amy	Gray	amy.gray@amyco.wombatqa.com	Opene
2020 Phishing Campaign 5	Angela	Gonzalez	angela.gonzalez@amyco.wombatqa.com	Unope
Unknown	Angela	Gonzalez	angela.gonzalez@amyco.wombatqa.com	Unope
2020 Phishing Campaign 3	Brian	Cooper	brian.cooper@amyco.wombatqa.com	Opene

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

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.

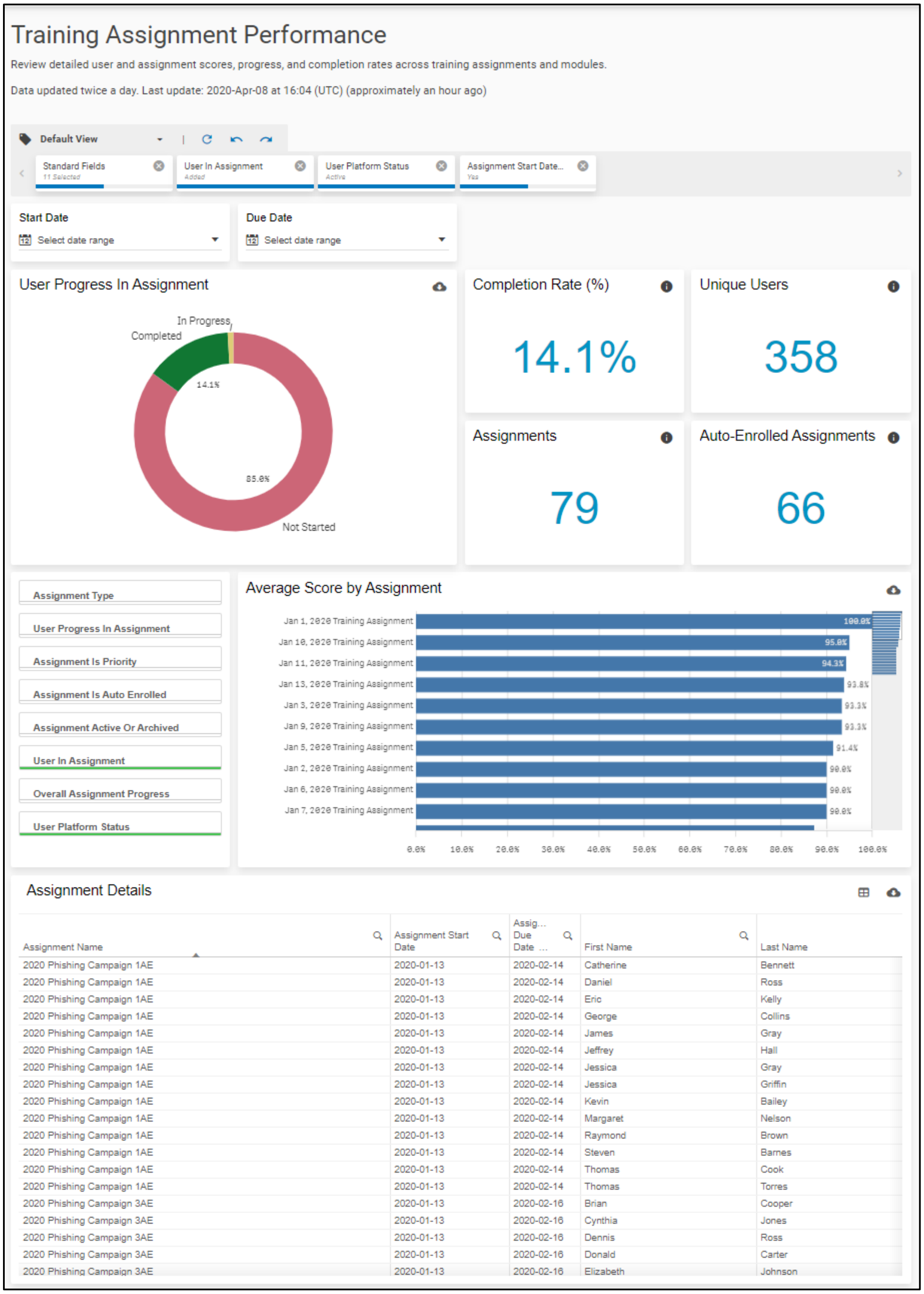
KEY FEATURES

- 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.

SAMPLE TRAINING ASSIGNMENT PERFORMANCE REPORT

(see next page)

SAMPLE TRAINING ASSIGNMENT PERFORMANCE REPORT (CONT.)



Training Assignment Performance

Review detailed user and assignment scores, progress, and completion rates across training assignments and modules.

Data updated twice a day. Last update: 2020-Apr-08 at 16:04 (UTC) (approximately an hour ago)

Default View

Standard Fields: 11 Selected
User In Assignment: Added
User Platform Status: Active
Assignment Start Date...: Yes

Start Date: Select date range
Due Date: Select date range

User Progress In Assignment

Completion Rate (%): 14.1%

Unique Users: 358

Assignments: 79

Auto-Enrolled Assignments: 66

Assignment Type
User Progress In Assignment
Assignment Is Priority
Assignment Is Auto Enrolled
Assignment Active Or Archived
User In Assignment
Overall Assignment Progress
User Platform Status

Average Score by Assignment

Jan 1, 2020 Training Assignment
100.0%
Jan 10, 2020 Training Assignment
95.0%
Jan 11, 2020 Training Assignment
94.3%
Jan 13, 2020 Training Assignment
93.8%
Jan 3, 2020 Training Assignment
93.3%
Jan 9, 2020 Training Assignment
93.3%
Jan 5, 2020 Training Assignment
91.4%
Jan 2, 2020 Training Assignment
90.0%
Jan 6, 2020 Training Assignment
90.0%
Jan 7, 2020 Training Assignment
90.0%
0.0%
10.0%
20.0%
30.0%
40.0%
50.0%
60.0%
70.0%
80.0%
90.0%
100.0%

Assignment Details

Assignment Name	Assignment Start Date	Assig... Due Date ...	First Name	Last Name
2020 Phishing Campaign 1AE	2020-01-13	2020-02-14	Catherine	Bennett
2020 Phishing Campaign 1AE	2020-01-13	2020-02-14	Daniel	Ross
2020 Phishing Campaign 1AE	2020-01-13	2020-02-14	Eric	Kelly
2020 Phishing Campaign 1AE	2020-01-13	2020-02-14	George	Collins
2020 Phishing Campaign 1AE	2020-01-13	2020-02-14	James	Gray
2020 Phishing Campaign 1AE	2020-01-13	2020-02-14	Jeffrey	Hall
2020 Phishing Campaign 1AE	2020-01-13	2020-02-14	Jessica	Gray
2020 Phishing Campaign 1AE	2020-01-13	2020-02-14	Jessica	Griffin
2020 Phishing Campaign 1AE	2020-01-13	2020-02-14	Kevin	Bailey
2020 Phishing Campaign 1AE	2020-01-13	2020-02-14	Margaret	Nelson
2020 Phishing Campaign 1AE	2020-01-13	2020-02-14	Raymond	Brown
2020 Phishing Campaign 1AE	2020-01-13	2020-02-14	Steven	Barnes
2020 Phishing Campaign 1AE	2020-01-13	2020-02-14	Thomas	Cook
2020 Phishing Campaign 1AE	2020-01-13	2020-02-14	Thomas	Torres
2020 Phishing Campaign 3AE	2020-01-13	2020-02-16	Brian	Cooper
2020 Phishing Campaign 3AE	2020-01-13	2020-02-16	Cynthia	Jones
2020 Phishing Campaign 3AE	2020-01-13	2020-02-16	Dennis	Ross
2020 Phishing Campaign 3AE	2020-01-13	2020-02-16	Donald	Carter
2020 Phishing Campaign 3AE	2020-01-13	2020-02-16	Elizabeth	Johnson

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

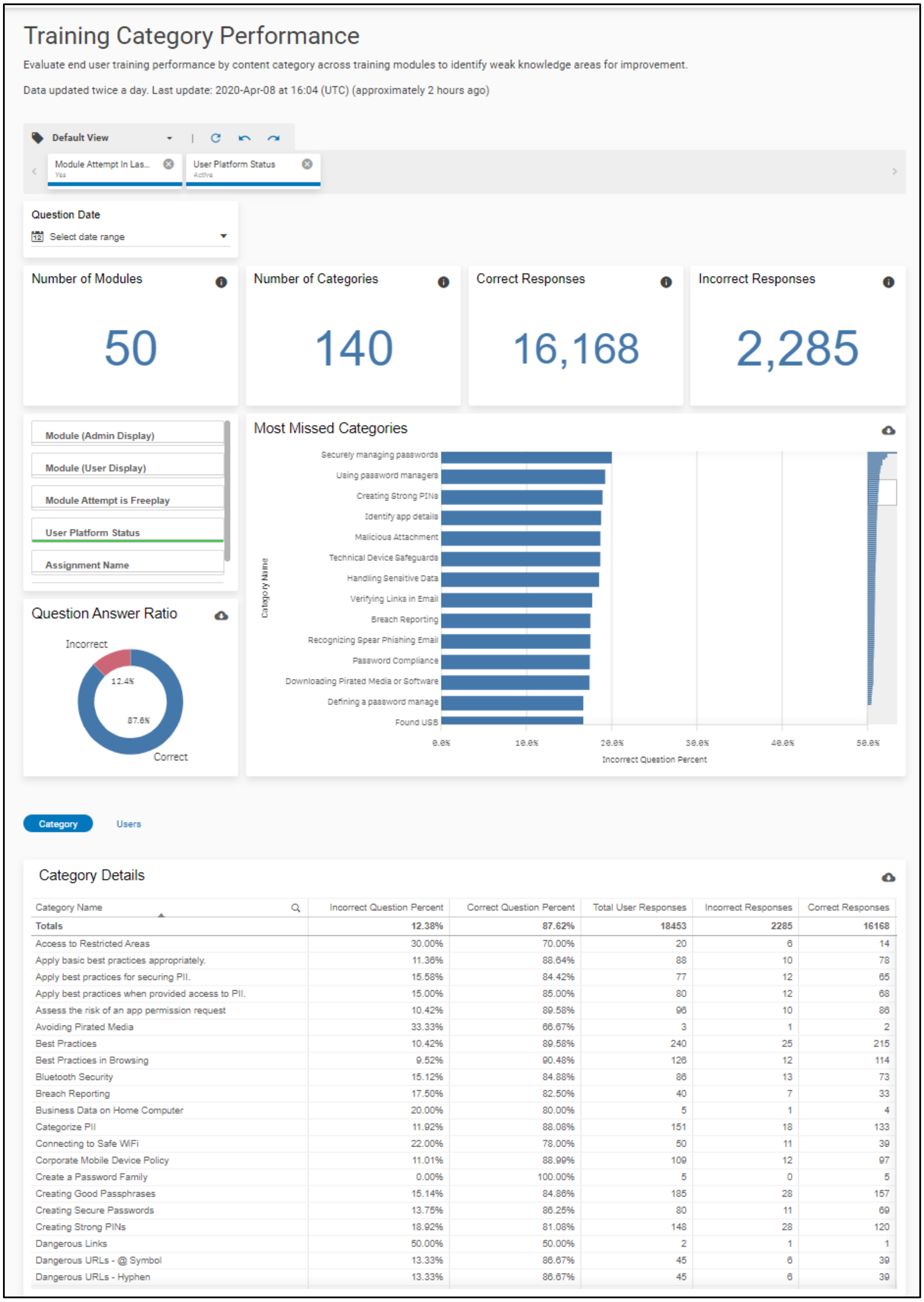
- Provides a variety of filtering options, such as by training module name, date, assignment, and include/exclude deleted users.
- Flexibility to select which data fields to include or exclude from the table to meet specific analysis needs.
- Displays key performance indicators for the total number of 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

SAMPLE TRAINING CATEGORY PERFORMANCE REPORT

(see next page)

SAMPLE TRAINING CATEGORY PERFORMANCE REPORT (CONT.)

View includes Category Tab



Training Category Performance

Evaluate end user training performance by content category across training modules to identify weak knowledge areas for improvement.

Data updated twice a day. Last update: 2020-Apr-08 at 16:04 (UTC) (approximately 2 hours ago)

Number of Modules: 50

Number of Categories: 140

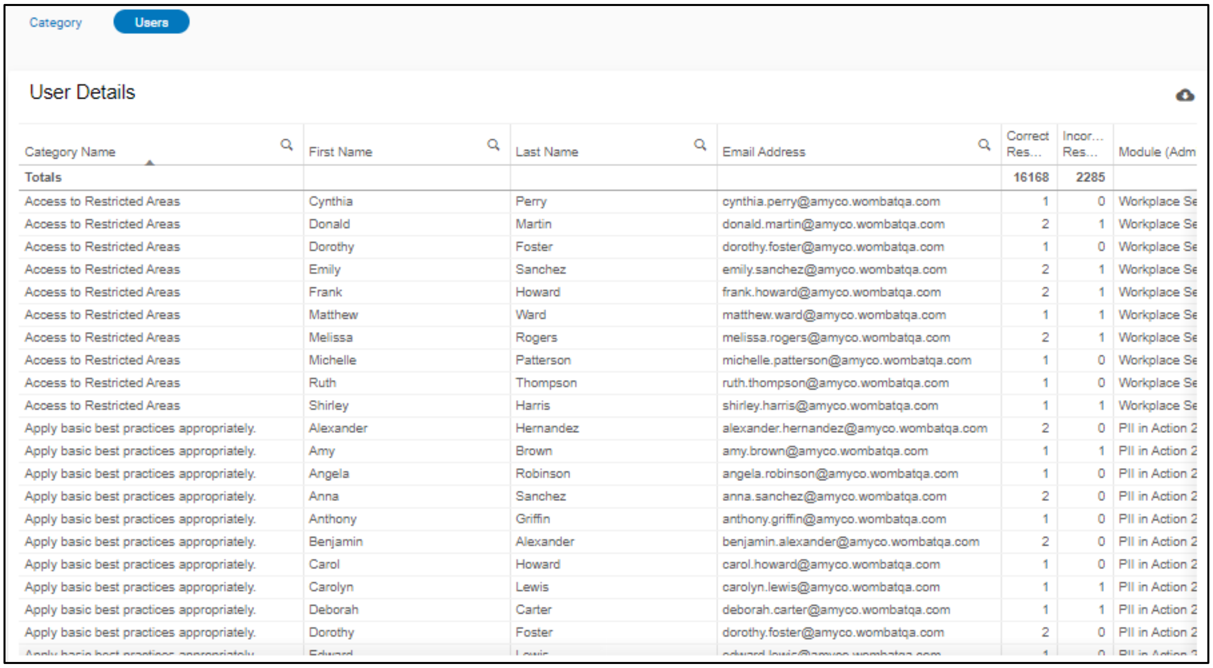
Correct Responses: 16,168

Incorrect Responses: 2,285

Category Details

Category Name	Incorrect Question Percent	Correct Question Percent	Total User Responses	Incorrect Responses	Correct Responses
Totals	**12.38%**	**87.62%**	**18453**	**2285**	**16168**
Access to Restricted Areas	30.00%	70.00%	20	6	14
Apply basic best practices appropriately.	11.36%	88.64%	88	10	78
Apply best practices for securing PII.	15.58%	84.42%	77	12	65
Apply best practices when provided access to PII.	15.00%	85.00%	80	12	68
Assess the risk of an app permission request	10.42%	89.58%	96	10	86
Avoiding Pirated Media	33.33%	66.67%	3	1	2
Best Practices	10.42%	89.58%	240	25	215
Best Practices in Browsing	9.52%	90.48%	126	12	114
Bluetooth Security	15.12%	84.88%	86	13	73
Breach Reporting	17.50%	82.50%	40	7	33
Business Data on Home Computer	20.00%	80.00%	5	1	4
Categorize PII	11.92%	88.08%	151	18	133
Connecting to Safe WiFi	22.00%	78.00%	50	11	39
Corporate Mobile Device Policy	11.01%	88.99%	109	12	97
Create a Password Family	0.00%	100.00%	5	0	5
Creating Good Passphrases	15.14%	84.86%	185	28	157
Creating Secure Passwords	13.75%	86.25%	80	11	69
Creating Strong PINs	18.92%	81.08%	148	28	120
Dangerous Links	50.00%	50.00%	2	1	1
Dangerous URLs - @ Symbol	13.33%	86.67%	45	6	39
Dangerous URLs - Hyphen	13.33%	86.67%	45	6	39

View of Users Tab



User Details

Category Name	First Name	Last Name	Email Address	Correct Res…	Incor… Res…	Module (Adm
Totals				**16168**	**2285**	
Access to Restricted Areas	Cynthia	Perry	cynthia.perry@amyco.wombatqa.com	1	0	Workplace Se
Access to Restricted Areas	Donald	Martin	donald.martin@amyco.wombatqa.com	2	1	Workplace Se
Access to Restricted Areas	Dorothy	Foster	dorothy.foster@amyco.wombatqa.com	1	0	Workplace Se
Access to Restricted Areas	Emily	Sanchez	emily.sanchez@amyco.wombatqa.com	2	1	Workplace Se
Access to Restricted Areas	Frank	Howard	frank.howard@amyco.wombatqa.com	2	1	Workplace Se
Access to Restricted Areas	Matthew	Ward	matthew.ward@amyco.wombatqa.com	1	1	Workplace Se
Access to Restricted Areas	Melissa	Rogers	melissa.rogers@amyco.wombatqa.com	2	1	Workplace Se
Access to Restricted Areas	Michelle	Patterson	michelle.patterson@amyco.wombatqa.com	1	0	Workplace Se
Access to Restricted Areas	Ruth	Thompson	ruth.thompson@amyco.wombatqa.com	1	0	Workplace Se
Access to Restricted Areas	Shirley	Harris	shirley.harris@amyco.wombatqa.com	1	1	Workplace Se
Apply basic best practices appropriately.	Alexander	Hernandez	alexander.hernandez@amyco.wombatqa.com	2	0	PII in Action 2
Apply basic best practices appropriately.	Amy	Brown	amy.brown@amyco.wombatqa.com	1	1	PII in Action 2
Apply basic best practices appropriately.	Angela	Robinson	angela.robinson@amyco.wombatqa.com	1	0	PII in Action 2
Apply basic best practices appropriately.	Anna	Sanchez	anna.sanchez@amyco.wombatqa.com	2	0	PII in Action 2
Apply basic best practices appropriately.	Anthony	Griffin	anthony.griffin@amyco.wombatqa.com	1	0	PII in Action 2
Apply basic best practices appropriately.	Benjamin	Alexander	benjamin.alexander@amyco.wombatqa.com	2	0	PII in Action 2
Apply basic best practices appropriately.	Carol	Howard	carol.howard@amyco.wombatqa.com	1	0	PII in Action 2
Apply basic best practices appropriately.	Carolyn	Lewis	carolyn.lewis@amyco.wombatqa.com	1	1	PII in Action 2
Apply basic best practices appropriately.	Deborah	Carter	deborah.carter@amyco.wombatqa.com	1	1	PII in Action 2
Apply basic best practices appropriately.	Dorothy	Foster	dorothy.foster@amyco.wombatqa.com	2	0	PII in Action 2
Apply basic best practices appropriately.	Edward	Lewis	edward.lewis@amyco.wombatqa.com	1	0	PII in Action 2

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

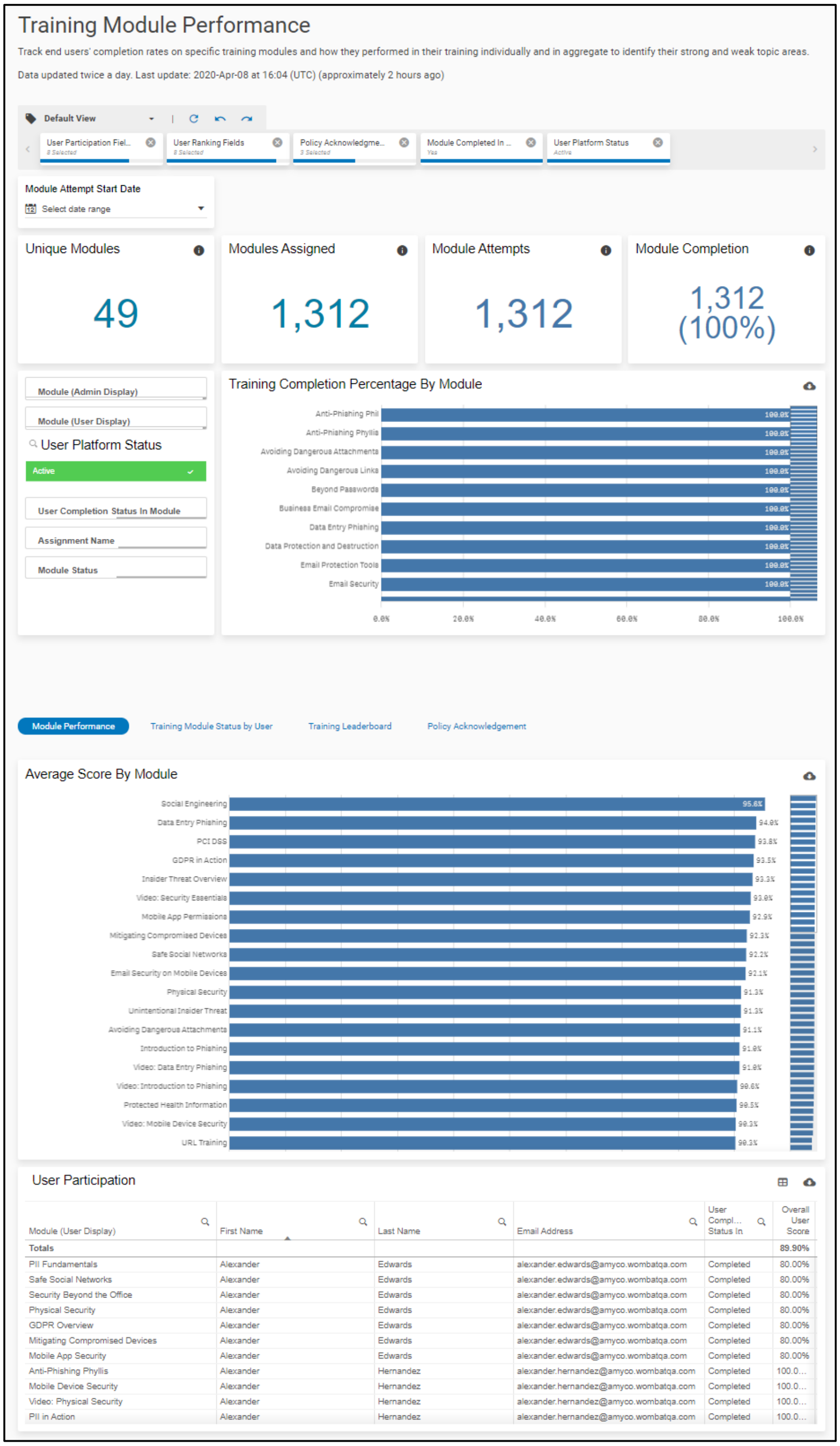
- Provides a variety of filtering options, such as by module name, status, and attempt start date as well as user completion status.
- Flexibility to select which data fields to include or exclude from the table to meet specific analysis needs.
- Displays key performance indicators for the number of 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

SAMPLE TRAINING MODULE PERFORMANCE REPORT

(see next page)

SAMPLE TRAINING MODULE PERFORMANCE REPORT (CONT.)

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 twice a day. Last update: 2020-Apr-08 at 16:04 (UTC) (approximately 2 hours ago)

Default View

- User Participation Fiel... — 8 Selected
- User Ranking Fields — 8 Selected
- Policy Acknowledgme... — 3 Selected
- Module Completed In ... — Yes
- User Platform Status — Active

Module Attempt Start Date: Select date range

Unique Modules	Modules Assigned	Module Attempts	Module Completion
49	1,312	1,312	1,312 (100%)

Module (Admin Display)

Module (User Display)

User Platform Status: Active ✓

User Completion Status In Module

Assignment Name

Module Status

Training Completion Percentage By Module

Anti-Phishing Phil 100.0%
Anti-Phishing Phyllis 100.0%
Avoiding Dangerous Attachments 100.0%
Avoiding Dangerous Links 100.0%
Beyond Passwords 100.0%
Business Email Compromise 100.0%
Data Entry Phishing 100.0%
Data Protection and Destruction 100.0%
Email Protection Tools 100.0%
Email Security 100.0%
0.0%
20.0%
40.0%
60.0%
80.0%
100.0%

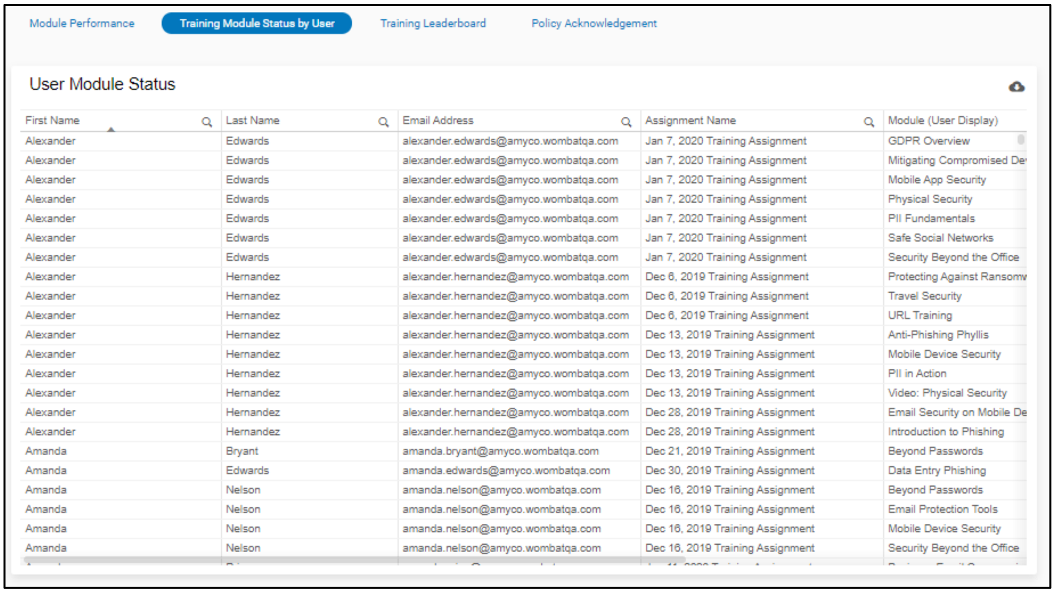
Average Score By Module

Social Engineering 95.6%
Data Entry Phishing 94.0%
PCI DSS 93.8%
GDPR in Action 93.5%
Insider Threat Overview 93.3%
Video: Security Essentials 93.0%
Mobile App Permissions 92.9%
Mitigating Compromised Devices 92.3%
Safe Social Networks 92.2%
Email Security on Mobile Devices 92.1%
Physical Security 91.3%
Unintentional Insider Threat 91.3%
Avoiding Dangerous Attachments 91.1%
Introduction to Phishing 91.0%
Video: Data Entry Phishing 91.0%
Video: Introduction to Phishing 90.6%
Protected Health Information 90.5%
Video: Mobile Device Security 90.3%
URL Training 90.3%

User Participation

Module (User Display)	First Name	Last Name	Email Address	User Compl... Status In	Overall User Score
Totals					89.90%
PII Fundamentals	Alexander	Edwards	alexander.edwards@amyco.wombatqa.com	Completed	80.00%
Safe Social Networks	Alexander	Edwards	alexander.edwards@amyco.wombatqa.com	Completed	80.00%
Security Beyond the Office	Alexander	Edwards	alexander.edwards@amyco.wombatqa.com	Completed	80.00%
Physical Security	Alexander	Edwards	alexander.edwards@amyco.wombatqa.com	Completed	80.00%
GDPR Overview	Alexander	Edwards	alexander.edwards@amyco.wombatqa.com	Completed	80.00%
Mitigating Compromised Devices	Alexander	Edwards	alexander.edwards@amyco.wombatqa.com	Completed	80.00%
Mobile App Security	Alexander	Edwards	alexander.edwards@amyco.wombatqa.com	Completed	80.00%
Anti-Phishing Phyllis	Alexander	Hernandez	alexander.hernandez@amyco.wombatqa.com	Completed	100.0...
Mobile Device Security	Alexander	Hernandez	alexander.hernandez@amyco.wombatqa.com	Completed	100.0...
Video: Physical Security	Alexander	Hernandez	alexander.hernandez@amyco.wombatqa.com	Completed	100.0...
PII in Action	Alexander	Hernandez	alexander.hernandez@amyco.wombatqa.com	Completed	100.0...

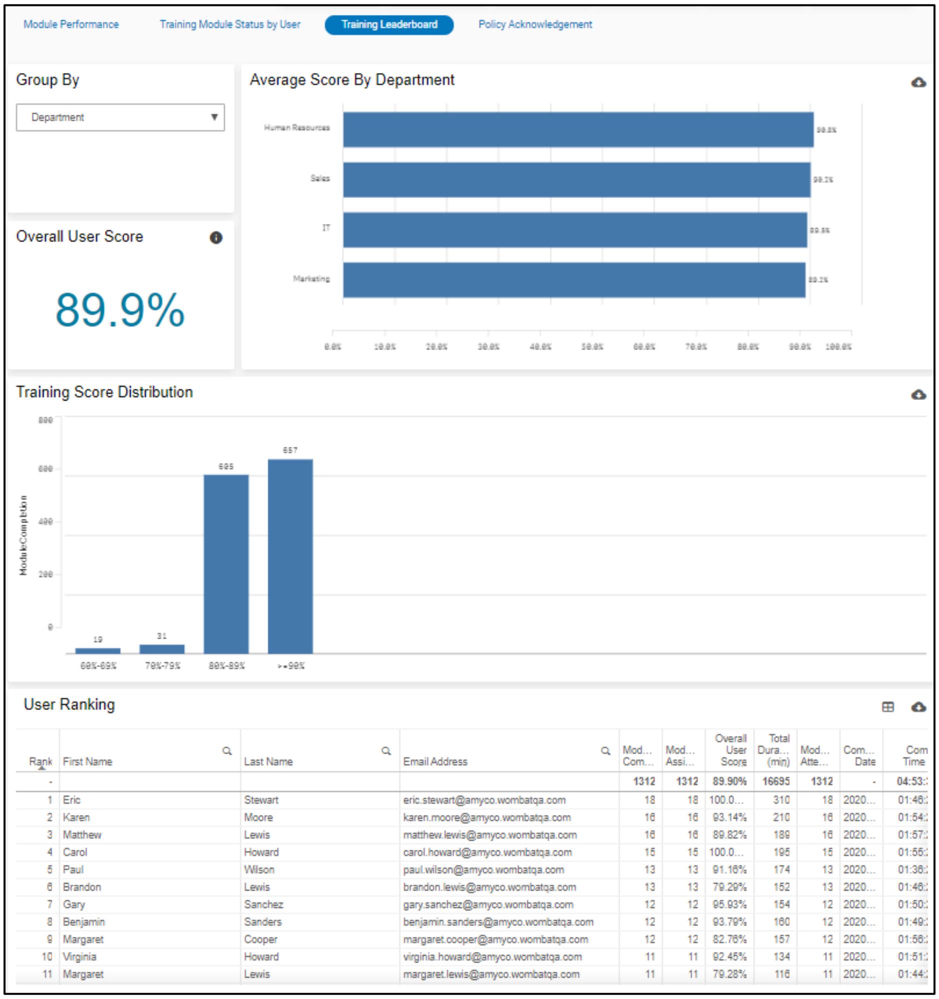
View of Training Module Status by User Tab



User Module Status

First Name	Last Name	Email Address	Assignment Name	Module (User Display)
Alexander	Edwards	alexander.edwards@amyco.wombatqa.com	Jan 7, 2020 Training Assignment	GDPR Overview
Alexander	Edwards	alexander.edwards@amyco.wombatqa.com	Jan 7, 2020 Training Assignment	Mitigating Compromised De
Alexander	Edwards	alexander.edwards@amyco.wombatqa.com	Jan 7, 2020 Training Assignment	Mobile App Security
Alexander	Edwards	alexander.edwards@amyco.wombatqa.com	Jan 7, 2020 Training Assignment	Physical Security
Alexander	Edwards	alexander.edwards@amyco.wombatqa.com	Jan 7, 2020 Training Assignment	PII Fundamentals
Alexander	Edwards	alexander.edwards@amyco.wombatqa.com	Jan 7, 2020 Training Assignment	Safe Social Networks
Alexander	Edwards	alexander.edwards@amyco.wombatqa.com	Jan 7, 2020 Training Assignment	Security Beyond the Office
Alexander	Hernandez	alexander.hernandez@amyco.wombatqa.com	Dec 6, 2019 Training Assignment	Protecting Against Ransomw
Alexander	Hernandez	alexander.hernandez@amyco.wombatqa.com	Dec 6, 2019 Training Assignment	Travel Security
Alexander	Hernandez	alexander.hernandez@amyco.wombatqa.com	Dec 6, 2019 Training Assignment	URL Training
Alexander	Hernandez	alexander.hernandez@amyco.wombatqa.com	Dec 13, 2019 Training Assignment	Anti-Phishing Phyllis
Alexander	Hernandez	alexander.hernandez@amyco.wombatqa.com	Dec 13, 2019 Training Assignment	Mobile Device Security
Alexander	Hernandez	alexander.hernandez@amyco.wombatqa.com	Dec 13, 2019 Training Assignment	PII in Action
Alexander	Hernandez	alexander.hernandez@amyco.wombatqa.com	Dec 13, 2019 Training Assignment	Video: Physical Security
Alexander	Hernandez	alexander.hernandez@amyco.wombatqa.com	Dec 28, 2019 Training Assignment	Email Security on Mobile De
Alexander	Hernandez	alexander.hernandez@amyco.wombatqa.com	Dec 28, 2019 Training Assignment	Introduction to Phishing
Amanda	Bryant	amanda.bryant@amyco.wombatqa.com	Dec 21, 2019 Training Assignment	Beyond Passwords
Amanda	Edwards	amanda.edwards@amyco.wombatqa.com	Dec 30, 2019 Training Assignment	Data Entry Phishing
Amanda	Nelson	amanda.nelson@amyco.wombatqa.com	Dec 16, 2019 Training Assignment	Beyond Passwords
Amanda	Nelson	amanda.nelson@amyco.wombatqa.com	Dec 16, 2019 Training Assignment	Email Protection Tools
Amanda	Nelson	amanda.nelson@amyco.wombatqa.com	Dec 16, 2019 Training Assignment	Mobile Device Security
Amanda	Nelson	amanda.nelson@amyco.wombatqa.com	Dec 16, 2019 Training Assignment	Security Beyond the Office

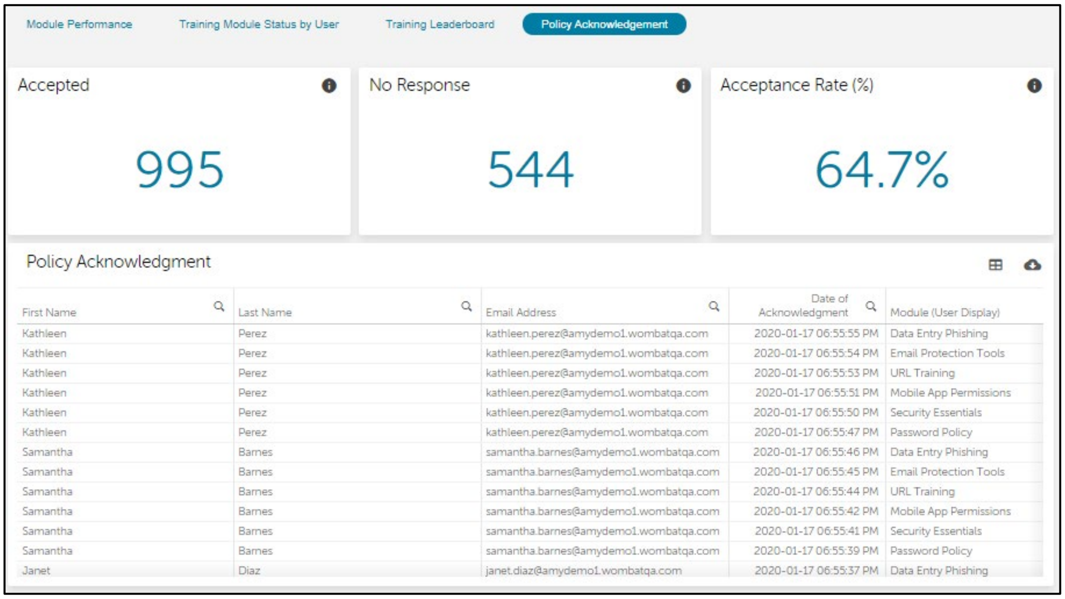
View of Training Leaderboard Tab



User Ranking

Rank	First Name	Last Name	Email Address	Mod... Com...	Mod... Assi...	Overall User Score	Total Dura... (min)	Mod... Atte...	Com... Date	Com Time
-				1312	1312	89.90%	16695	1312	-	04:53:
1	Eric	Stewart	eric.stewart@amyco.wombatqa.com	18	18	100.0...	310	18	2020...	01:46:
2	Karen	Moore	karen.moore@amyco.wombatqa.com	16	16	93.14%	210	16	2020...	01:54:
3	Matthew	Lewis	matthew.lewis@amyco.wombatqa.com	16	16	89.82%	189	16	2020...	01:57:
4	Carol	Howard	carol.howard@amyco.wombatqa.com	15	15	100.0...	195	15	2020...	01:55:
5	Paul	Wilson	paul.wilson@amyco.wombatqa.com	13	13	91.16%	174	13	2020...	01:36:
6	Brandon	Lewis	brandon.lewis@amyco.wombatqa.com	13	13	79.29%	152	13	2020...	01:46:
7	Gary	Sanchez	gary.sanchez@amyco.wombatqa.com	12	12	95.93%	154	12	2020...	01:50:
8	Benjamin	Sanders	benjamin.sanders@amyco.wombatqa.com	12	12	93.79%	160	12	2020...	01:49:
9	Margaret	Cooper	margaret.cooper@amyco.wombatqa.com	12	12	82.76%	157	12	2020...	01:56:
10	Virginia	Howard	virginia.howard@amyco.wombatqa.com	11	11	92.45%	134	11	2020...	01:51:
11	Margaret	Lewis	margaret.lewis@amyco.wombatqa.com	11	11	79.28%	116	11	2020...	01:44:

View of Policy Acknowledgement Tab



Accepted 995

No Response 544

Acceptance Rate (%) 64.7%

Policy Acknowledgment

First Name	Last Name	Email Address	Date of Acknowledgment	Module (User Display)
Kathleen	Perez	kathleen.perez@amydemo1.wombatqa.com	2020-01-17 06:55:55 PM	Data Entry Phishing
Kathleen	Perez	kathleen.perez@amydemo1.wombatqa.com	2020-01-17 06:55:54 PM	Email Protection Tools
Kathleen	Perez	kathleen.perez@amydemo1.wombatqa.com	2020-01-17 06:55:53 PM	URL Training
Kathleen	Perez	kathleen.perez@amydemo1.wombatqa.com	2020-01-17 06:55:51 PM	Mobile App Permissions
Kathleen	Perez	kathleen.perez@amydemo1.wombatqa.com	2020-01-17 06:55:50 PM	Security Essentials
Kathleen	Perez	kathleen.perez@amydemo1.wombatqa.com	2020-01-17 06:55:47 PM	Password Policy
Samantha	Barnes	samantha.barnes@amydemo1.wombatqa.com	2020-01-17 06:55:46 PM	Data Entry Phishing
Samantha	Barnes	samantha.barnes@amydemo1.wombatqa.com	2020-01-17 06:55:45 PM	Email Protection Tools
Samantha	Barnes	samantha.barnes@amydemo1.wombatqa.com	2020-01-17 06:55:44 PM	URL Training
Samantha	Barnes	samantha.barnes@amydemo1.wombatqa.com	2020-01-17 06:55:42 PM	Mobile App Permissions
Samantha	Barnes	samantha.barnes@amydemo1.wombatqa.com	2020-01-17 06:55:41 PM	Security Essentials
Samantha	Barnes	samantha.barnes@amydemo1.wombatqa.com	2020-01-17 06:55:39 PM	Password Policy
Janet	Diaz	janet.diaz@amydemo1.wombatqa.com	2020-01-17 06:55:37 PM	Data Entry Phishing

USERS

The reports in this section pertain to User records. They include:

- User Record Export
- Training Report Card

USER RECORD EXPORT

OBJECTIVE

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

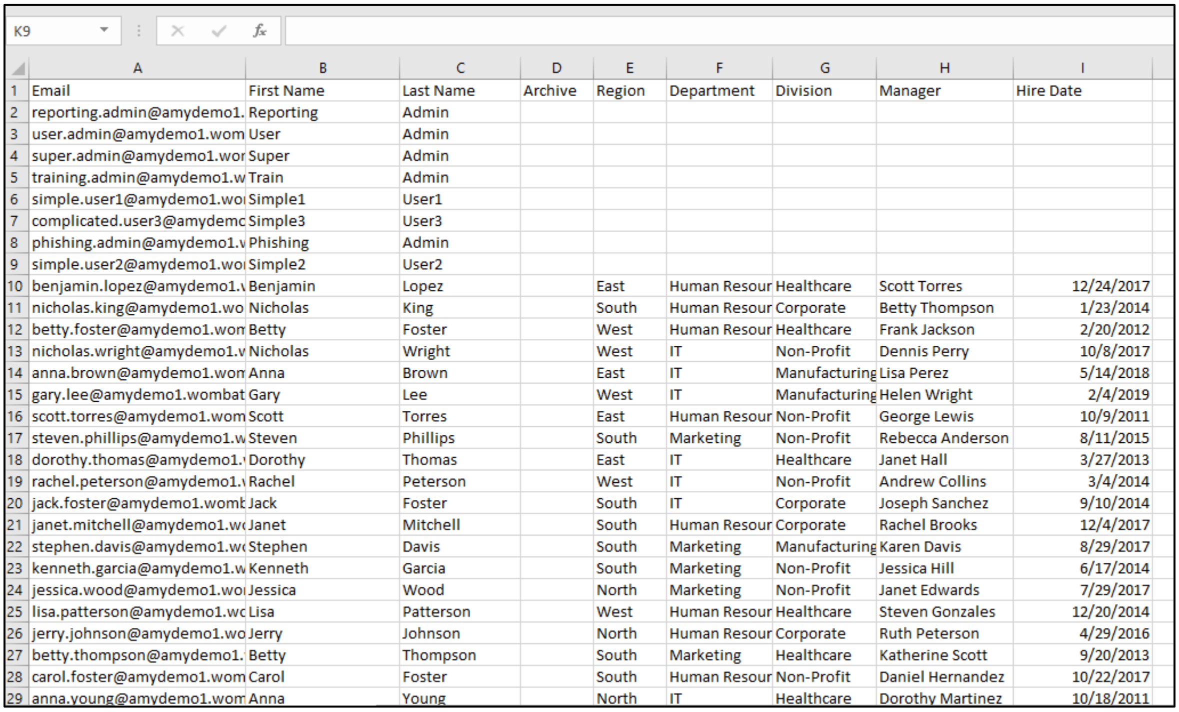
BENEFIT

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 option: CSV

SAMPLE USER RECORD EXPORT



	A	B	C	D	E	F	G	H	I
1	Email	First Name	Last Name	Archive	Region	Department	Division	Manager	Hire Date
2	reporting.admin@amydemo1.	Reporting	Admin						
3	user.admin@amydemo1.wom	User	Admin						
4	super.admin@amydemo1.wor	Super	Admin						
5	training.admin@amydemo1.w	Train	Admin						
6	simple.user1@amydemo1.wo	Simple1	User1						
7	complicated.user3@amydemc	Simple3	User3						
8	phishing.admin@amydemo1.v	Phishing	Admin						
9	simple.user2@amydemo1.wo	Simple2	User2						
10	benjamin.lopez@amydemo1.\	Benjamin	Lopez		East	Human Resour	Healthcare	Scott Torres	12/24/2017
11	nicholas.king@amydemo1.wo	Nicholas	King		South	Human Resour	Corporate	Betty Thompson	1/23/2014
12	betty.foster@amydemo1.wom	Betty	Foster		West	Human Resour	Healthcare	Frank Jackson	2/20/2012
13	nicholas.wright@amydemo1.v	Nicholas	Wright		West	IT	Non-Profit	Dennis Perry	10/8/2017
14	anna.brown@amydemo1.wom	Anna	Brown		East	IT	Manufacturing	Lisa Perez	5/14/2018
15	gary.lee@amydemo1.wombat	Gary	Lee		West	IT	Manufacturing	Helen Wright	2/4/2019
16	scott.torres@amydemo1.wom	Scott	Torres		East	Human Resour	Non-Profit	George Lewis	10/9/2011
17	steven.phillips@amydemo1.w	Steven	Phillips		South	Marketing	Non-Profit	Rebecca Anderson	8/11/2015
18	dorothy.thomas@amydemo1.	Dorothy	Thomas		East	IT	Healthcare	Janet Hall	3/27/2013
19	rachel.peterson@amydemo1.\	Rachel	Peterson		West	IT	Non-Profit	Andrew Collins	3/4/2014
20	jack.foster@amydemo1.womb	Jack	Foster		South	IT	Corporate	Joseph Sanchez	9/10/2014
21	janet.mitchell@amydemo1.wc	Janet	Mitchell		South	Human Resour	Corporate	Rachel Brooks	12/4/2017
22	stephen.davis@amydemo1.wc	Stephen	Davis		South	Marketing	Manufacturing	Karen Davis	8/29/2017
23	kenneth.garcia@amydemo1.w	Kenneth	Garcia		South	Marketing	Non-Profit	Jessica Hill	6/17/2014
24	jessica.wood@amydemo1.wo	Jessica	Wood		North	Marketing	Non-Profit	Janet Edwards	7/29/2017
25	lisa.patterson@amydemo1.wc	Lisa	Patterson		West	Human Resour	Healthcare	Steven Gonzales	12/20/2014
26	jerry.johnson@amydemo1.wo	Jerry	Johnson		North	Human Resour	Corporate	Ruth Peterson	4/29/2016
27	betty.thompson@amydemo1.	Betty	Thompson		South	Marketing	Healthcare	Katherine Scott	9/20/2013
28	carol.foster@amydemo1.wom	Carol	Foster		South	Human Resour	Non-Profit	Daniel Hernandez	10/22/2017
29	anna.young@amydemo1.wom	Anna	Young		North	IT	Healthcare	Dorothy Martinez	10/18/2011

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.

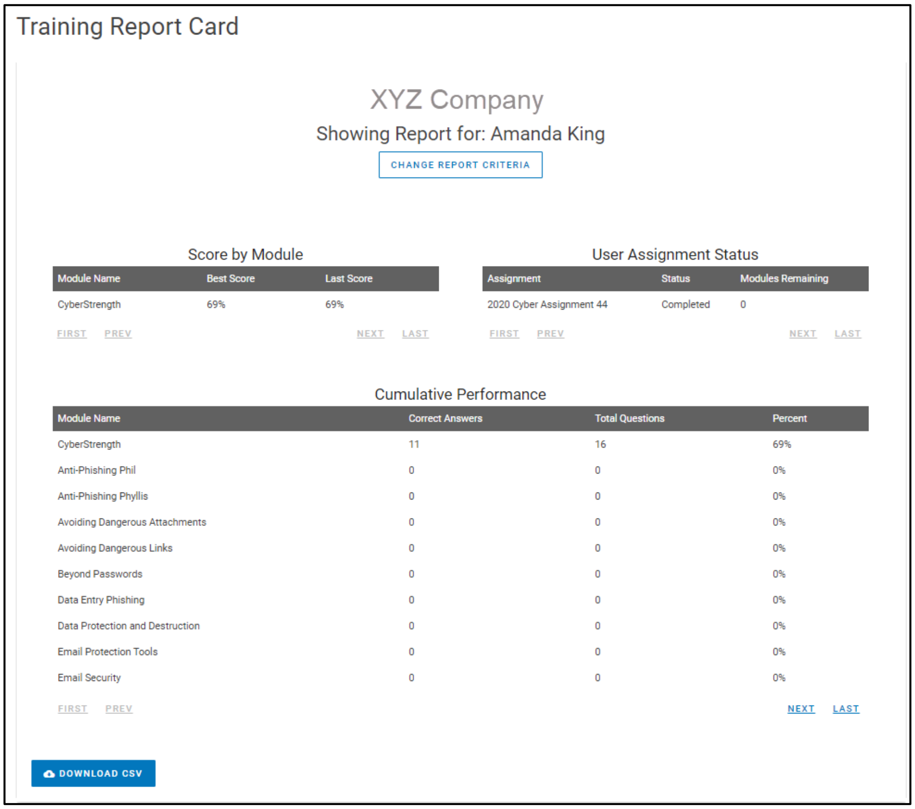
BENEFITS

- 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 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 option: CSV

SAMPLE TRAINING REPORT CARD



Training Report Card

XYZ Company

Showing Report for: Amanda King

Score by Module

Module Name	Best Score	Last Score
CyberStrength	69%	69%

User Assignment Status

Assignment	Status	Modules Remaining
2020 Cyber Assignment 44	Completed	0

Cumulative Performance

Module Name	Correct Answers	Total Questions	Percent
CyberStrength	11	16	69%
Anti-Phishing Phil	0	0	0%
Anti-Phishing Phyllis	0	0	0%
Avoiding Dangerous Attachments	0	0	0%
Avoiding Dangerous Links	0	0	0%
Beyond Passwords	0	0	0%
Data Entry Phishing	0	0	0%
Data Protection and Destruction	0	0	0%
Email Protection Tools	0	0	0%
Email Security	0	0	0%