proofpoint®

Security Awareness Training

BUSINESS INTELLIGENCE

Reporting Overview

February 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 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
	  ○ All Email Campaigns History
	  ○ Individual Campaign Overview
	  ○ Geographic Distribution
	  ○ Endpoints
	  ○ 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

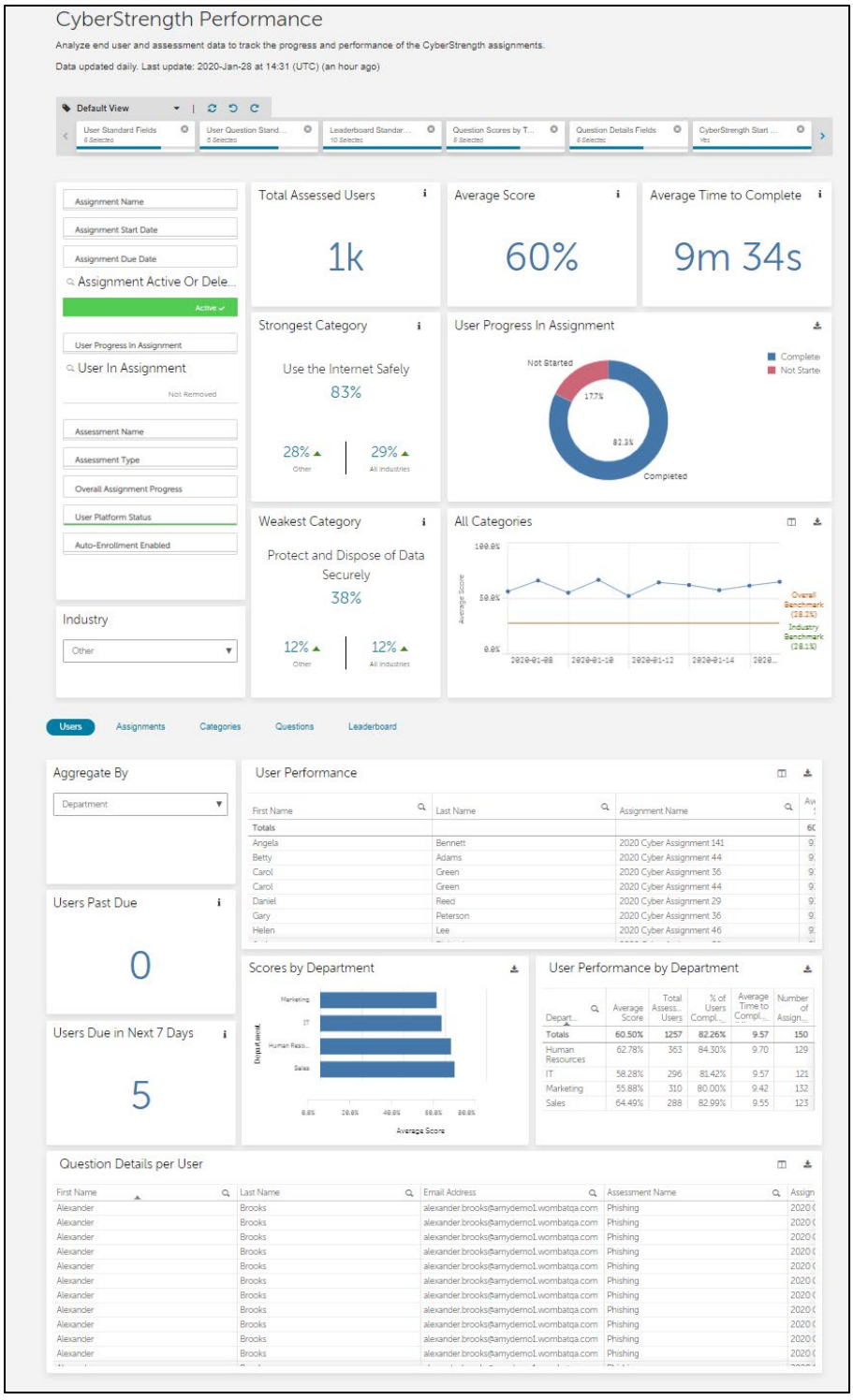
- Determine the organization's weaknesses and strengths across a range of cybersecurity areas, identify the riskiest users or business units, identify the most missed question categories, and customize programs to reduce the identified risks.
- Track user progress and performance across all CyberStrength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

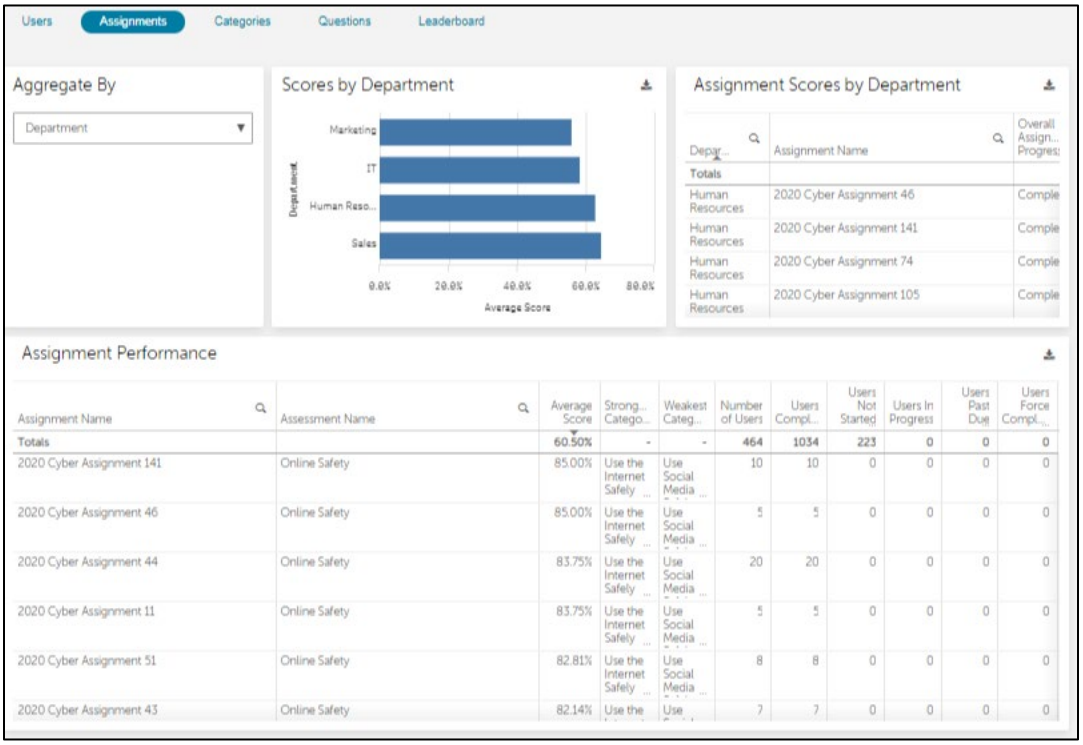
(see next page)

SCREENSHOT OF CYBERSTRENGTH PERFORMANCE REPORT (CONT.)

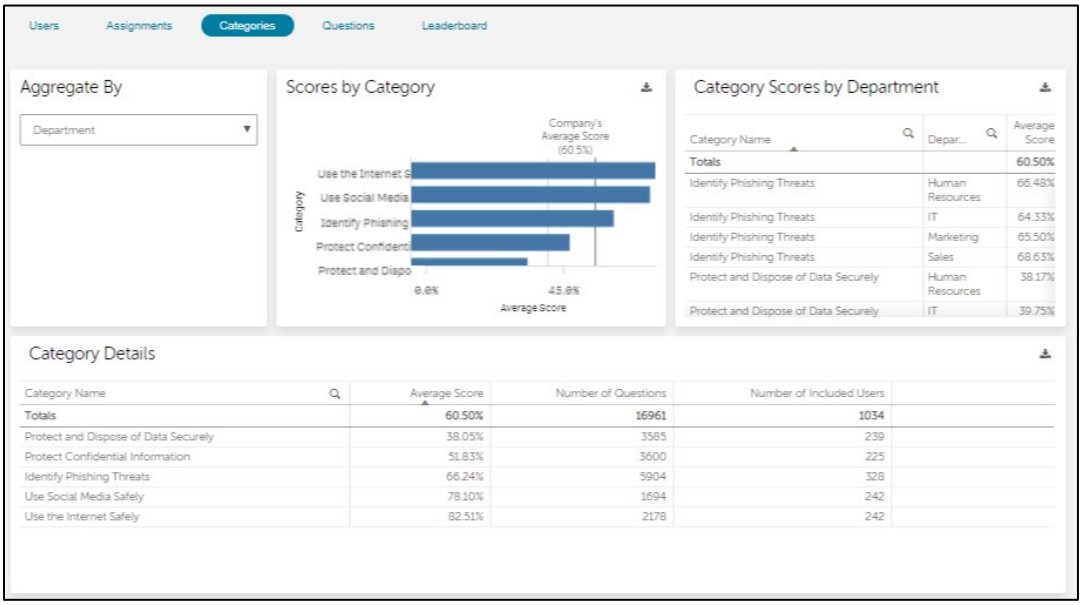
View includes Users Tab



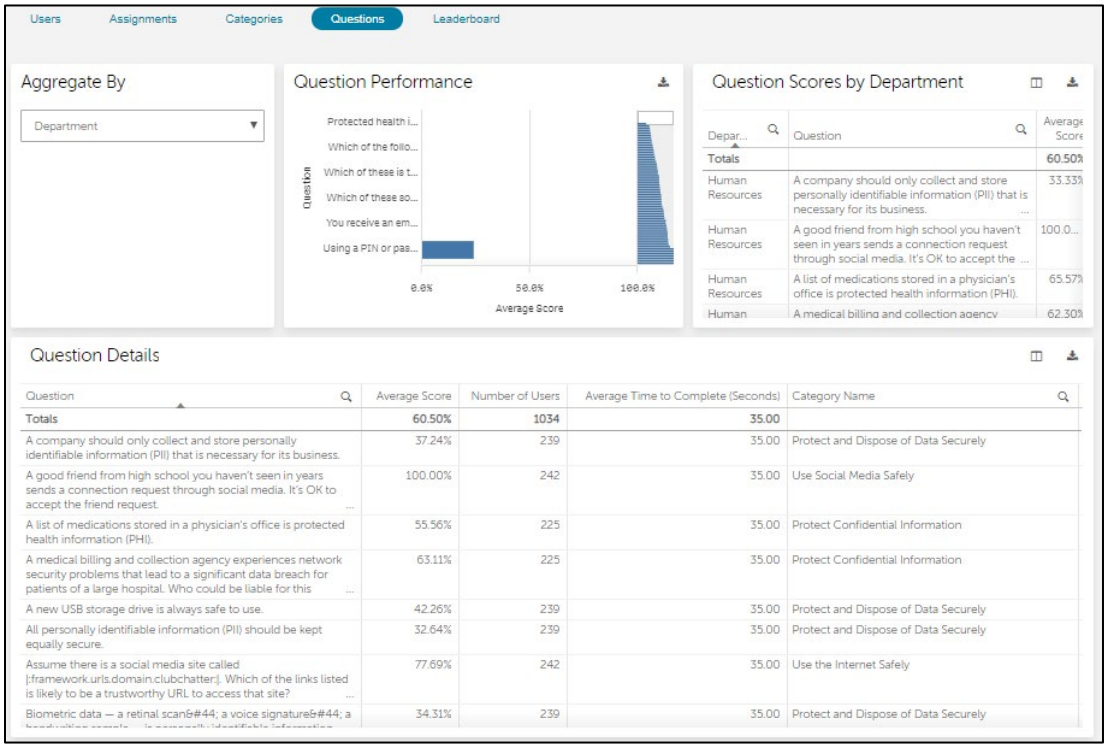
View of Assignments Tab



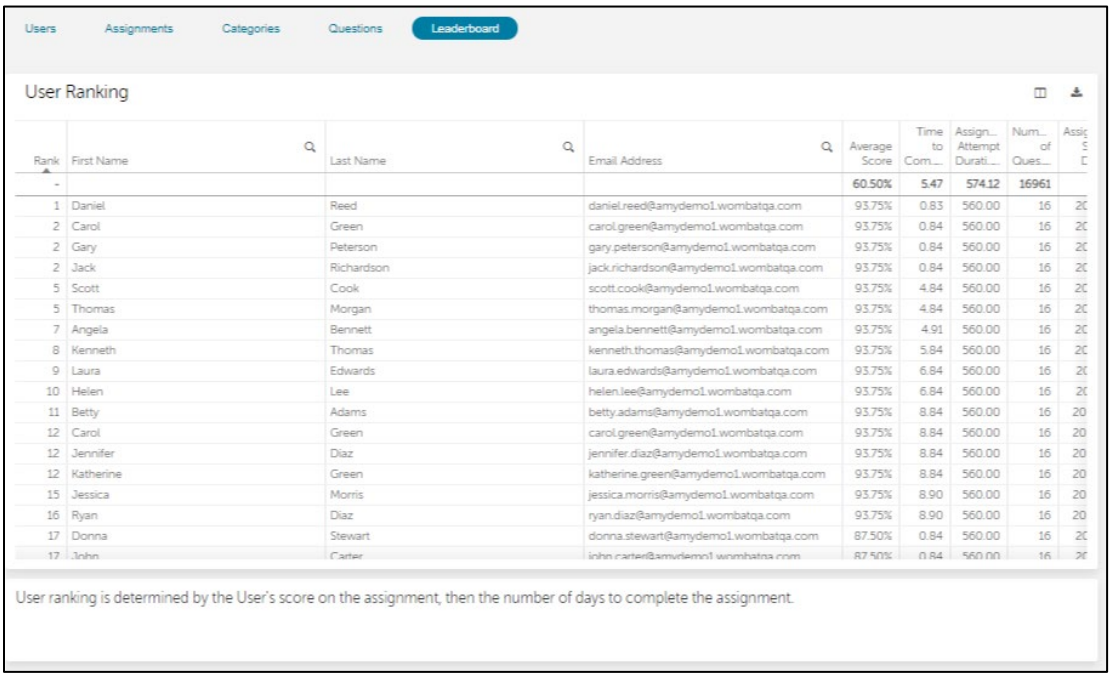
View of Categories Tab



View of Questions Tab



View of Leaderboard Tab



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.

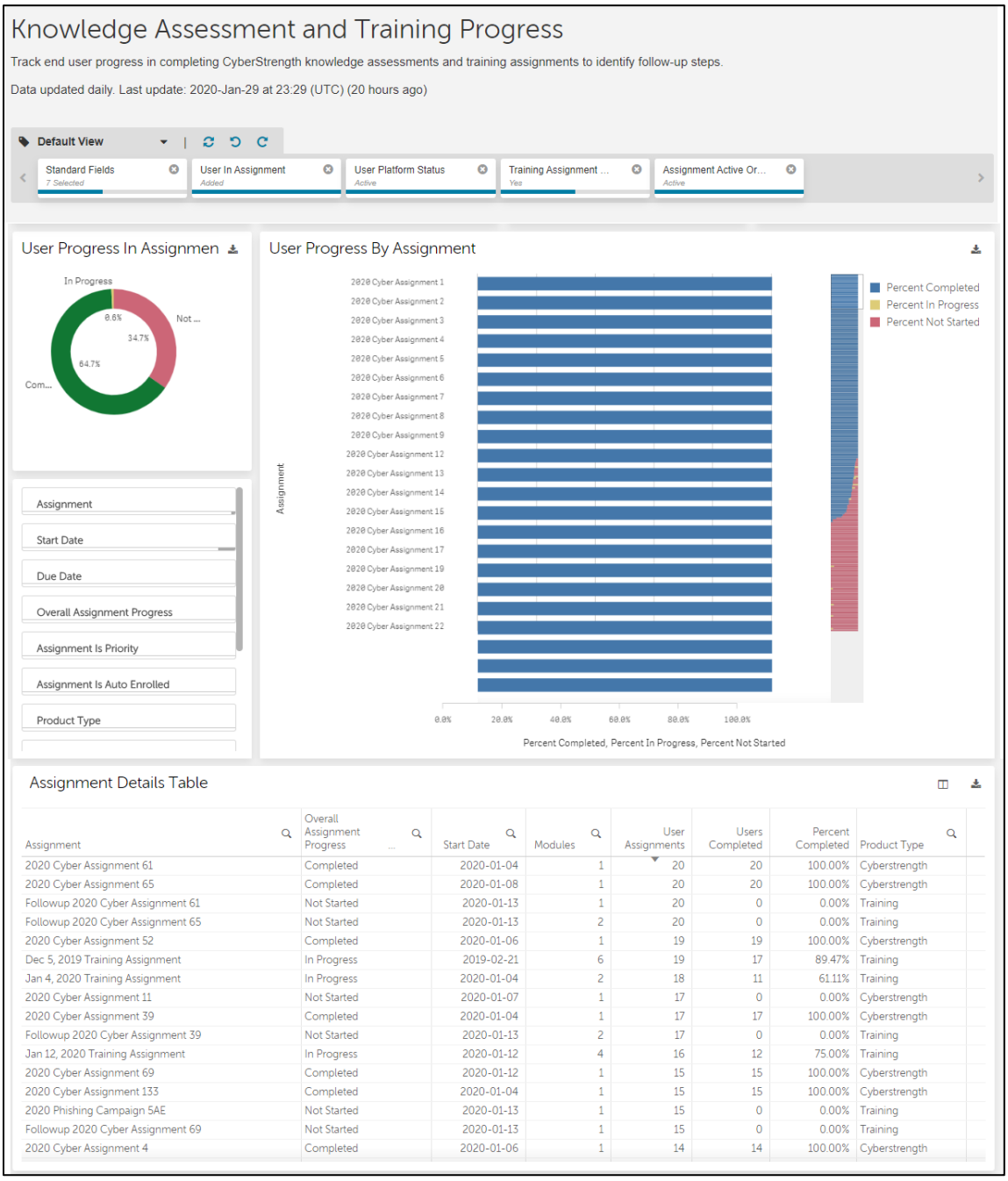
BENEFITS

- 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

SCREENSHOT OF KNOWLEDGE ASSESSMENT AND TRAINING PROGRESS REPORT



Assignment	Overall Assignment Progress	Start Date	Modules	User Assignments	Users Completed	Percent Completed	Product Type
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
Dec 5, 2019 Training Assignment	In Progress	2019-02-21	6	19	17	89.47%	Training
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 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
2020 Cyber Assignment 4	Completed	2020-01-06	1	14	14	100.00%	Cyberstrength

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

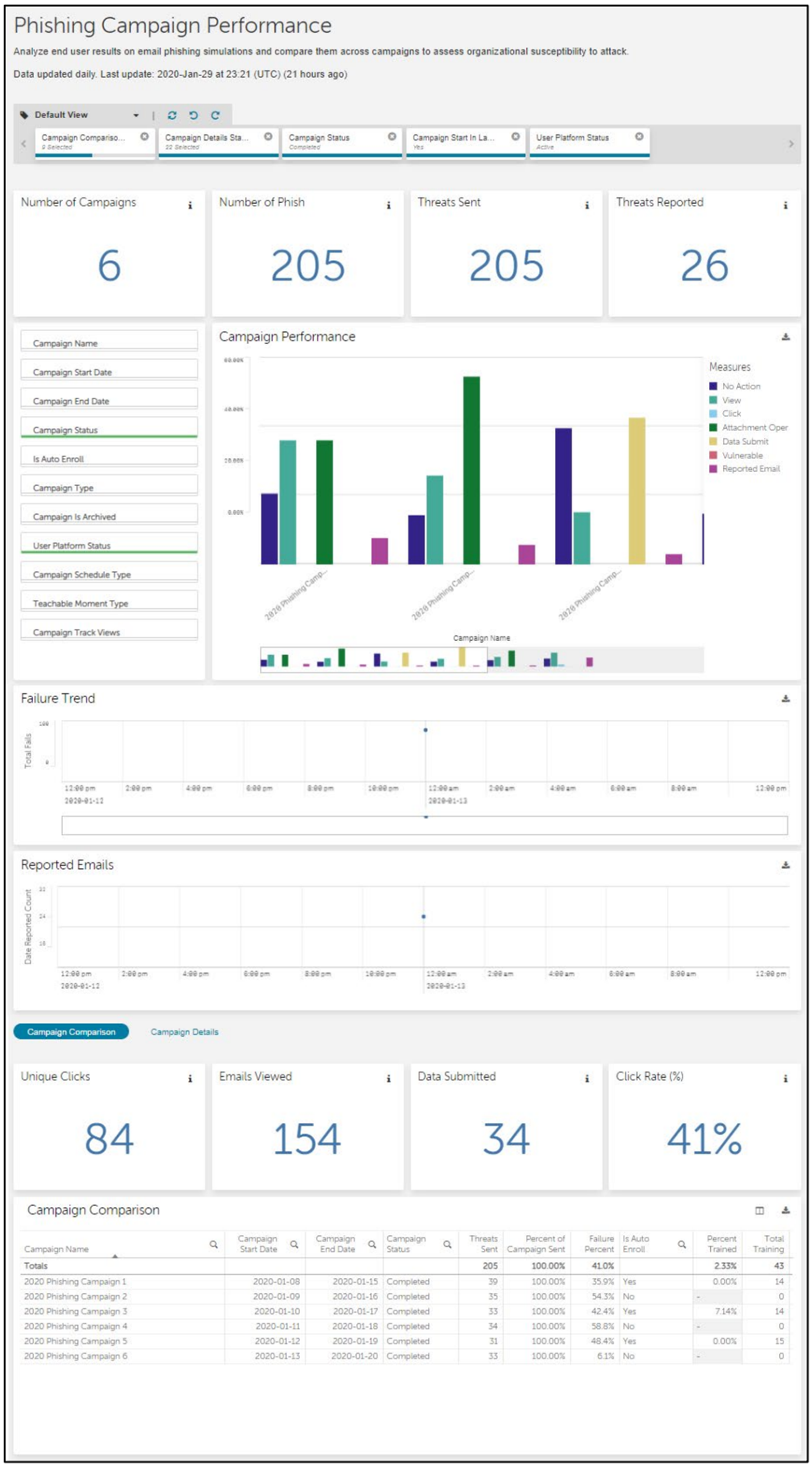
- Determine at the campaign- and user-level which campaign types end users are most vulnerable to so that additional campaigns can be developed and implemented.
- Drill-down to the user-level details to enable deeper analysis.
- Track phishing failure performance over time and use the trends to determine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

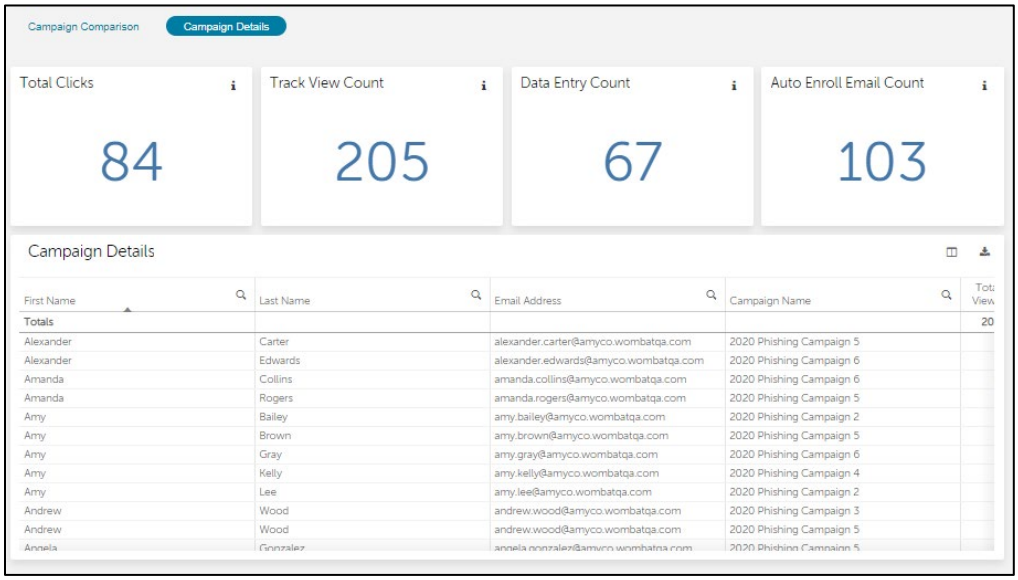
SCREENSHOT OF PHISHING CAMPAIGN PERFORMANCE REPORT

View with Campaign Comparison Report



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				205	100.00%	41.0%		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

View of Campaign Details Tab



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.

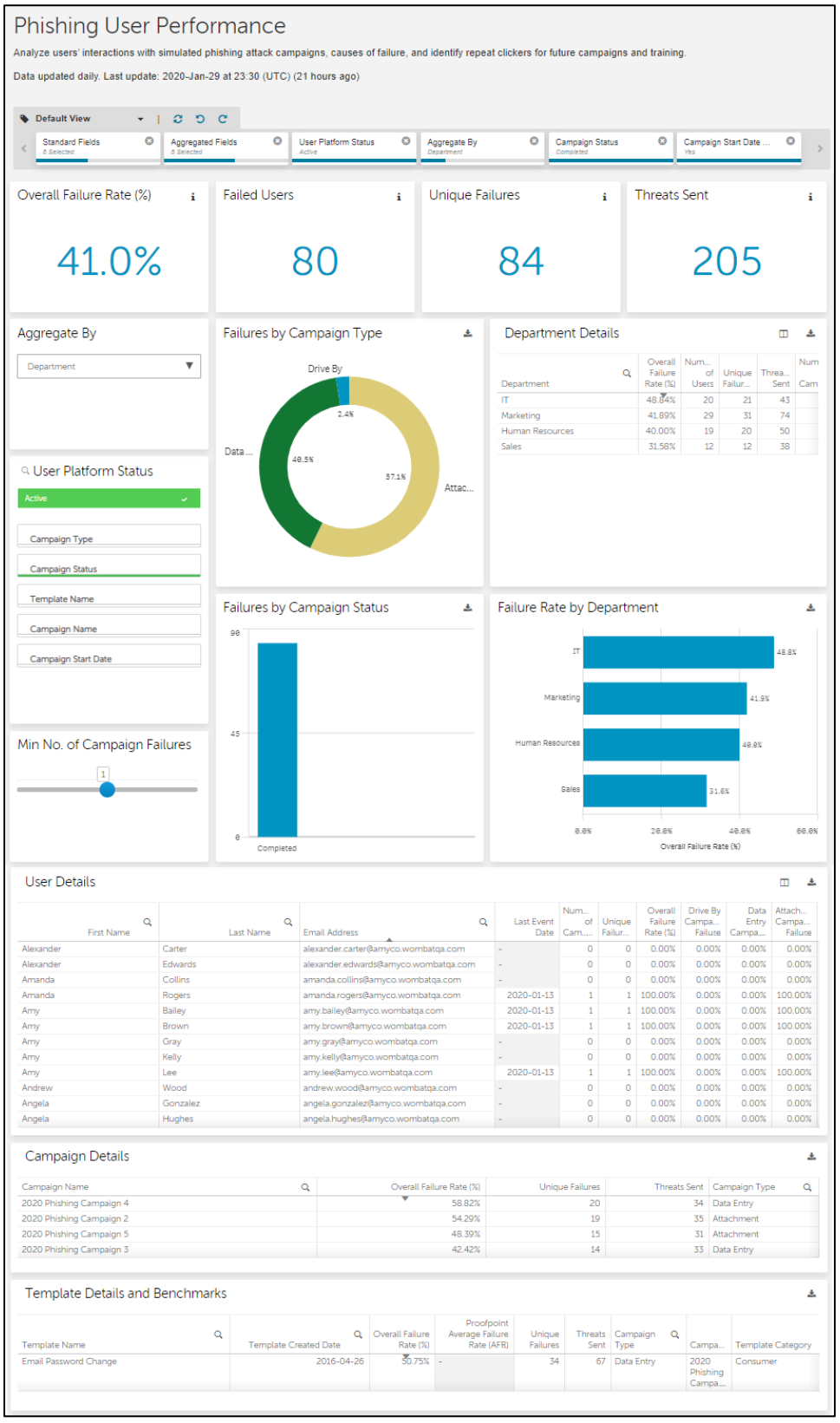
KEY FEATURES

- 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.)



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)

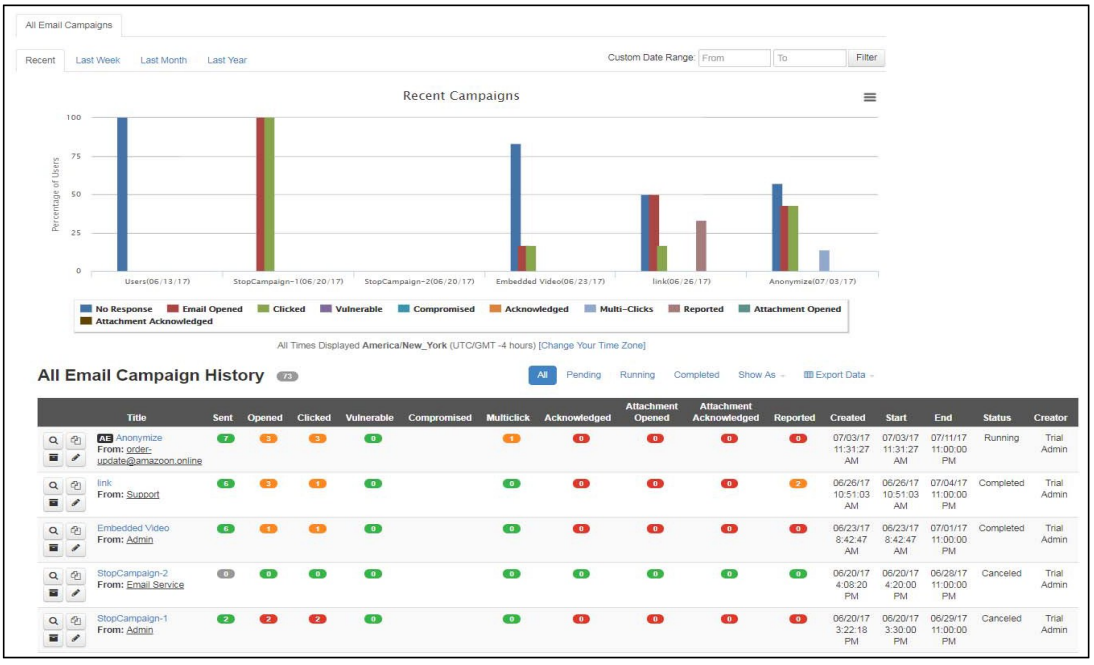
BENEFITS

- 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.

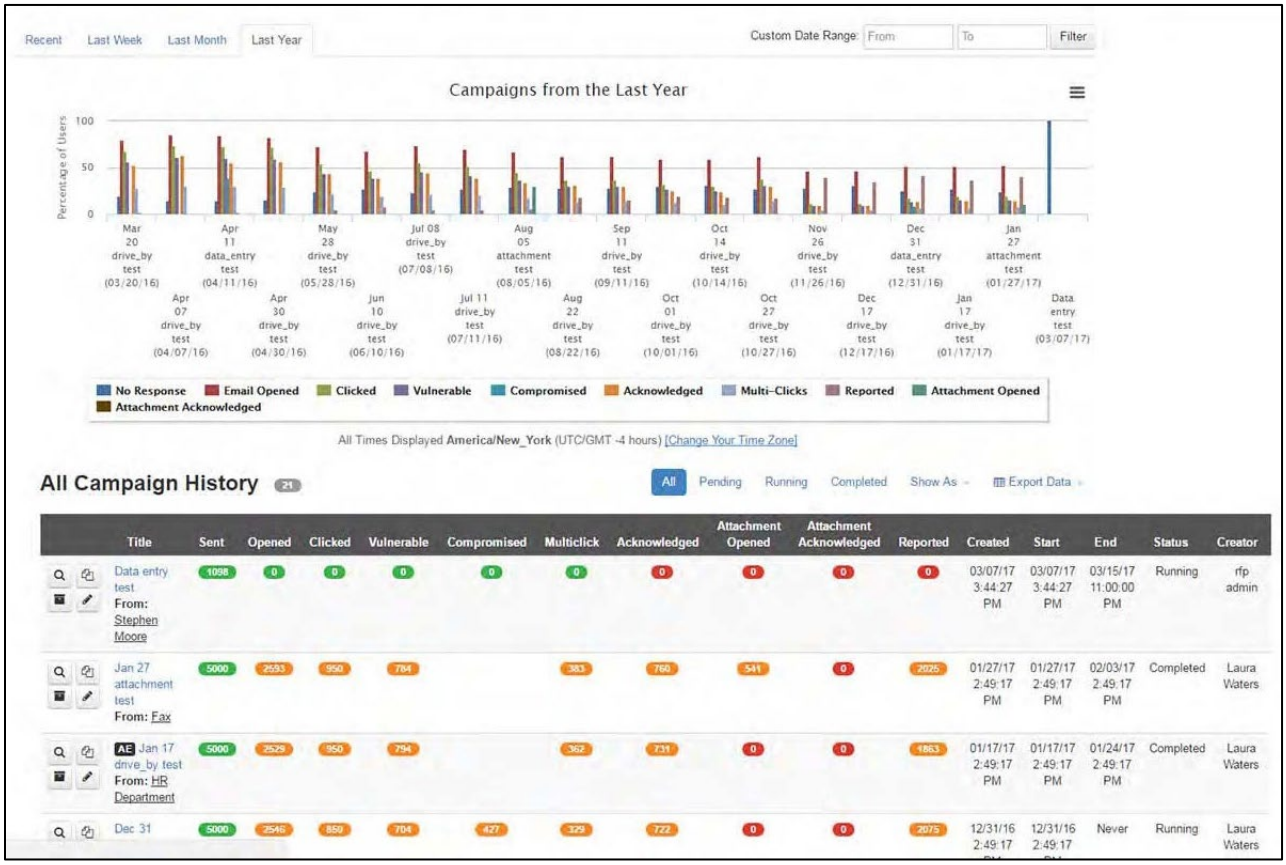
BENEFIT

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.

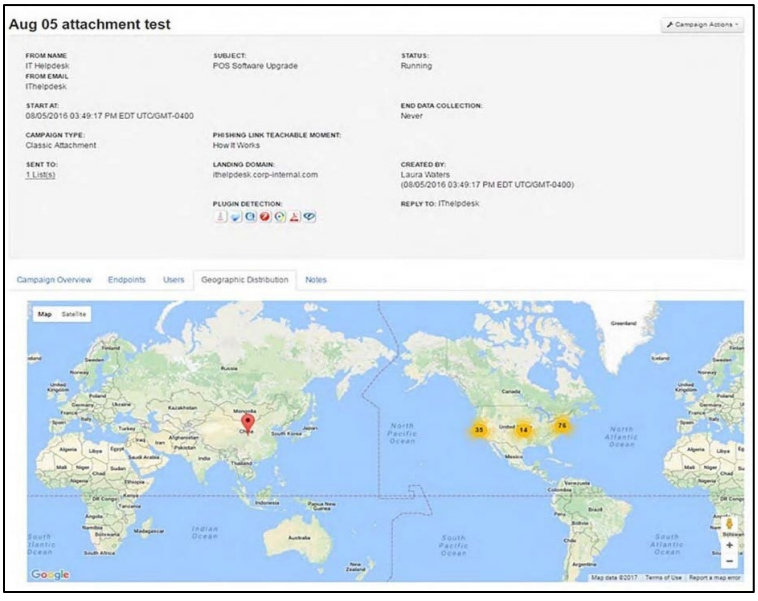


Individual Campaign Overview Report

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.

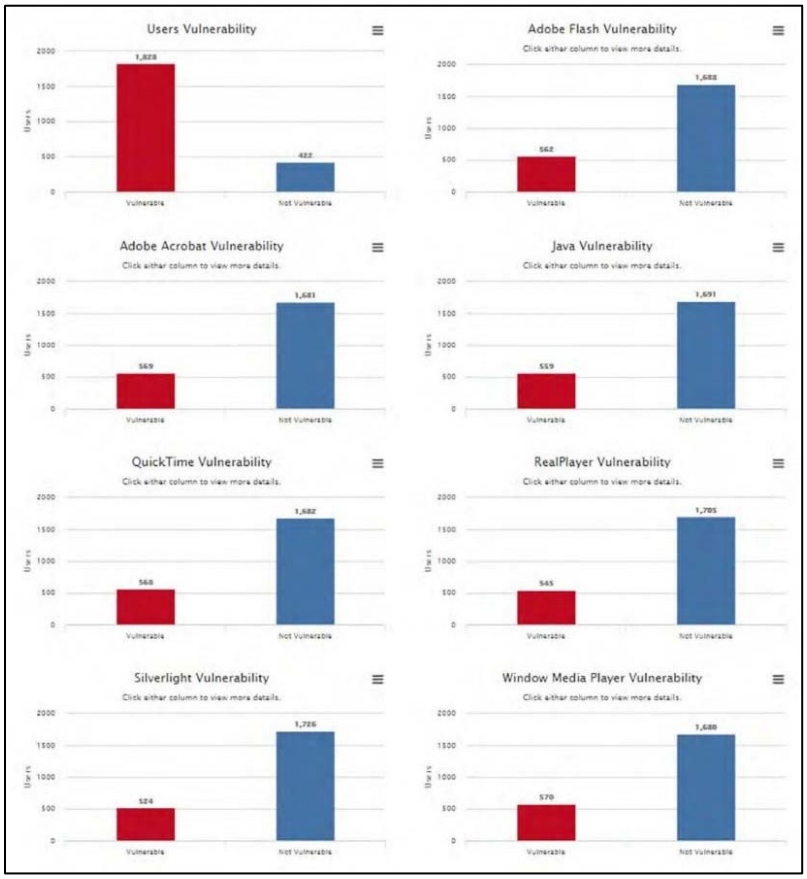
Geographic Distribution Report

Displays worldwide mapping of user activity per campaign, which helps identify anomalies in the organization's data regions with high levels of susceptibility.



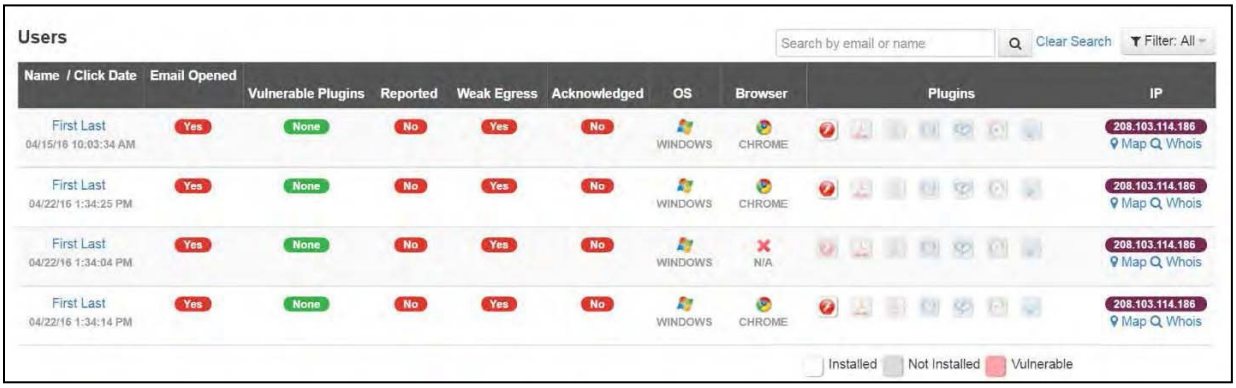
Endpoints Report

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

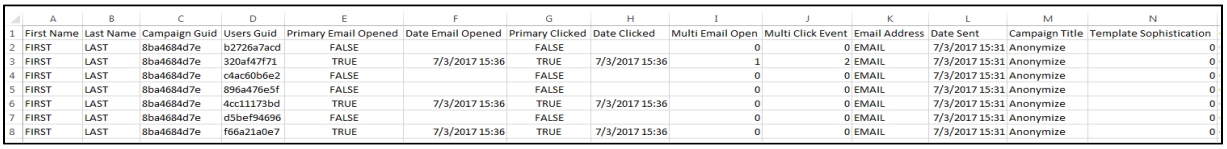
Simple export of comprehensive ThreatSim data for quick and easy import into the organization's preferred analysis tool for evaluation.

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.

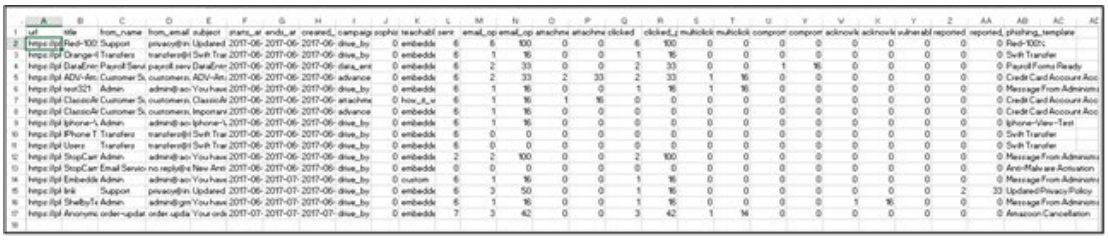
SCREENSHOTS OF THREATSIM RAW CAMPAIGN DATA CSV REPORTS

Campaign Overview CSV Report

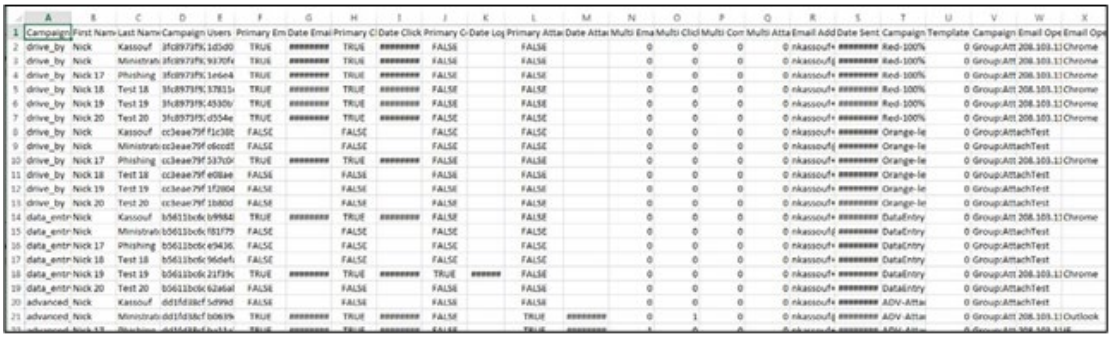


	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	First Name	Last Name	Campaign Guid	Users Guid	Primary Email Opened	Date Email Opened	Primary Clicked	Date Clicked	Multi Email Open	Multi Click Event	Email Address	Date Sent	Campaign Title	Template Sophistication
2	FIRST	LAST	8ba4684d7e	b2726a7acd	FALSE		FALSE		0	0	EMAIL	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



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.

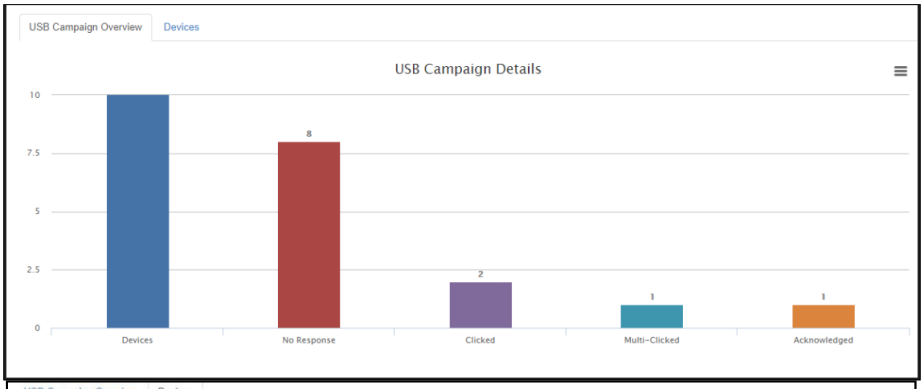
BENEFITS

- 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



USB Campaign Overview | Devices

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]114.190	[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 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

SCREENSHOT OF PHISHALARM ANALYZER REPORT (CONT.)

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.

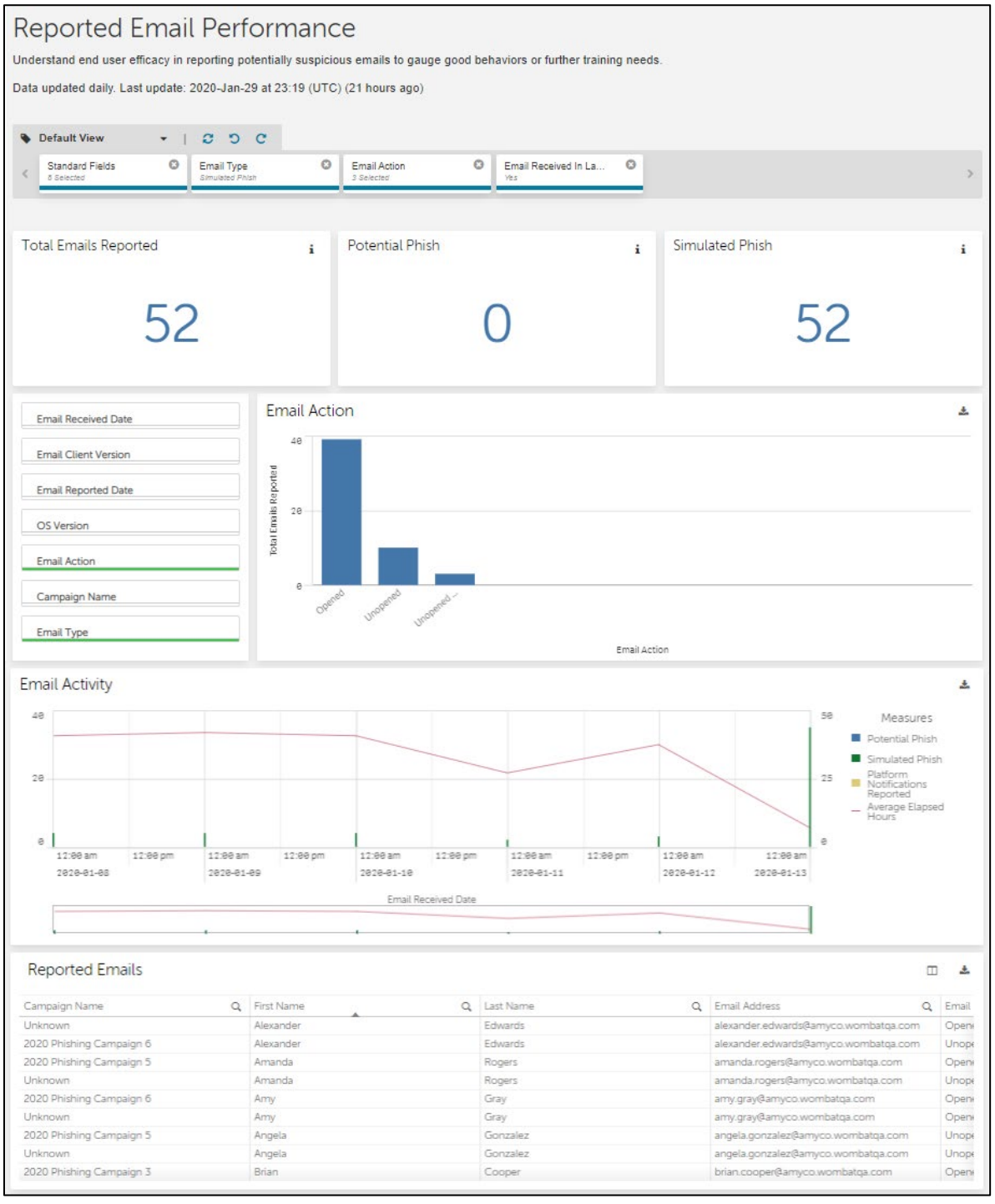
BENEFITS

- 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



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.

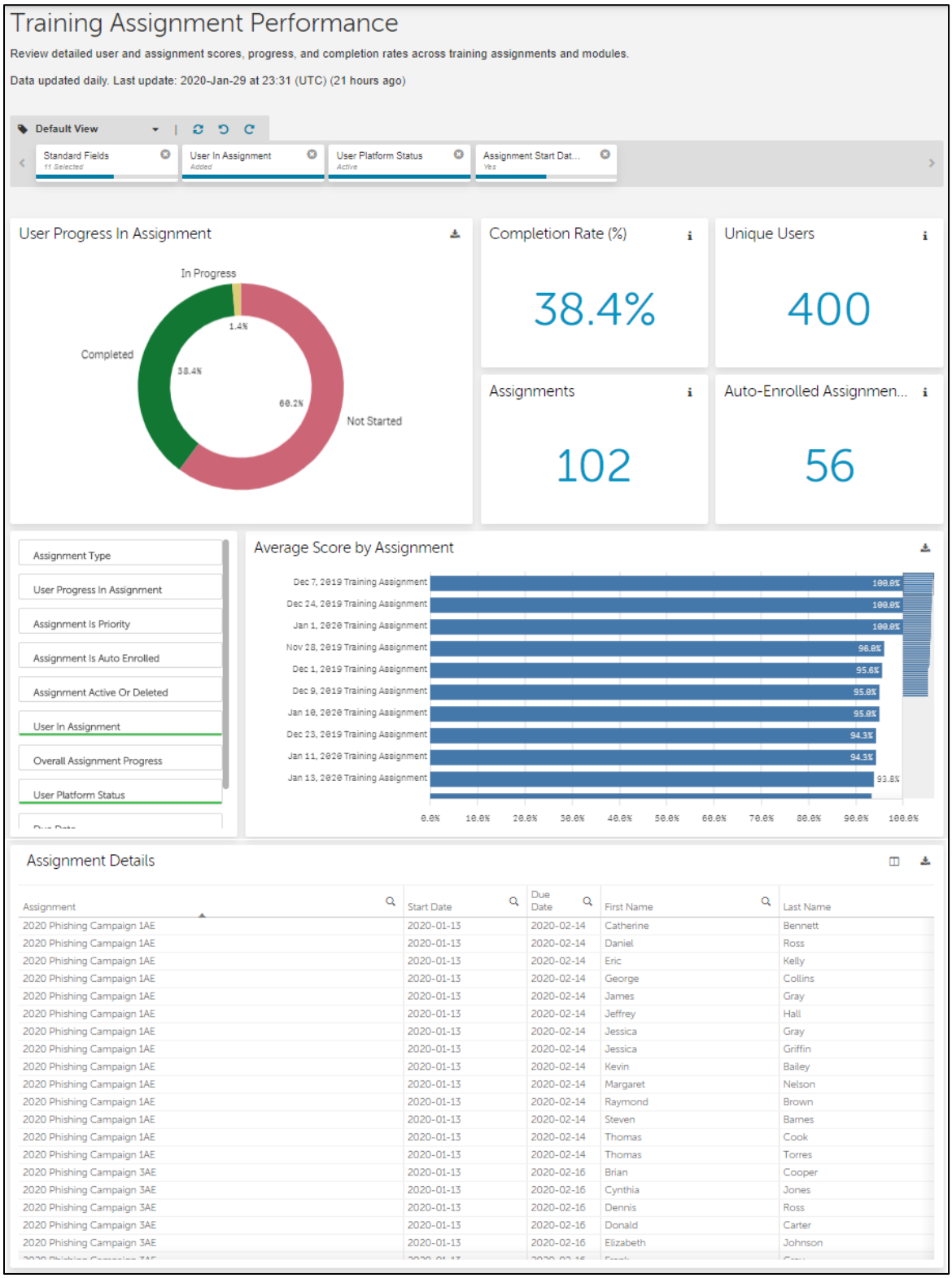
BENEFITS

- 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.

SCREENSHOT OF TRAINING ASSIGNMENT PERFORMANCE REPORT



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

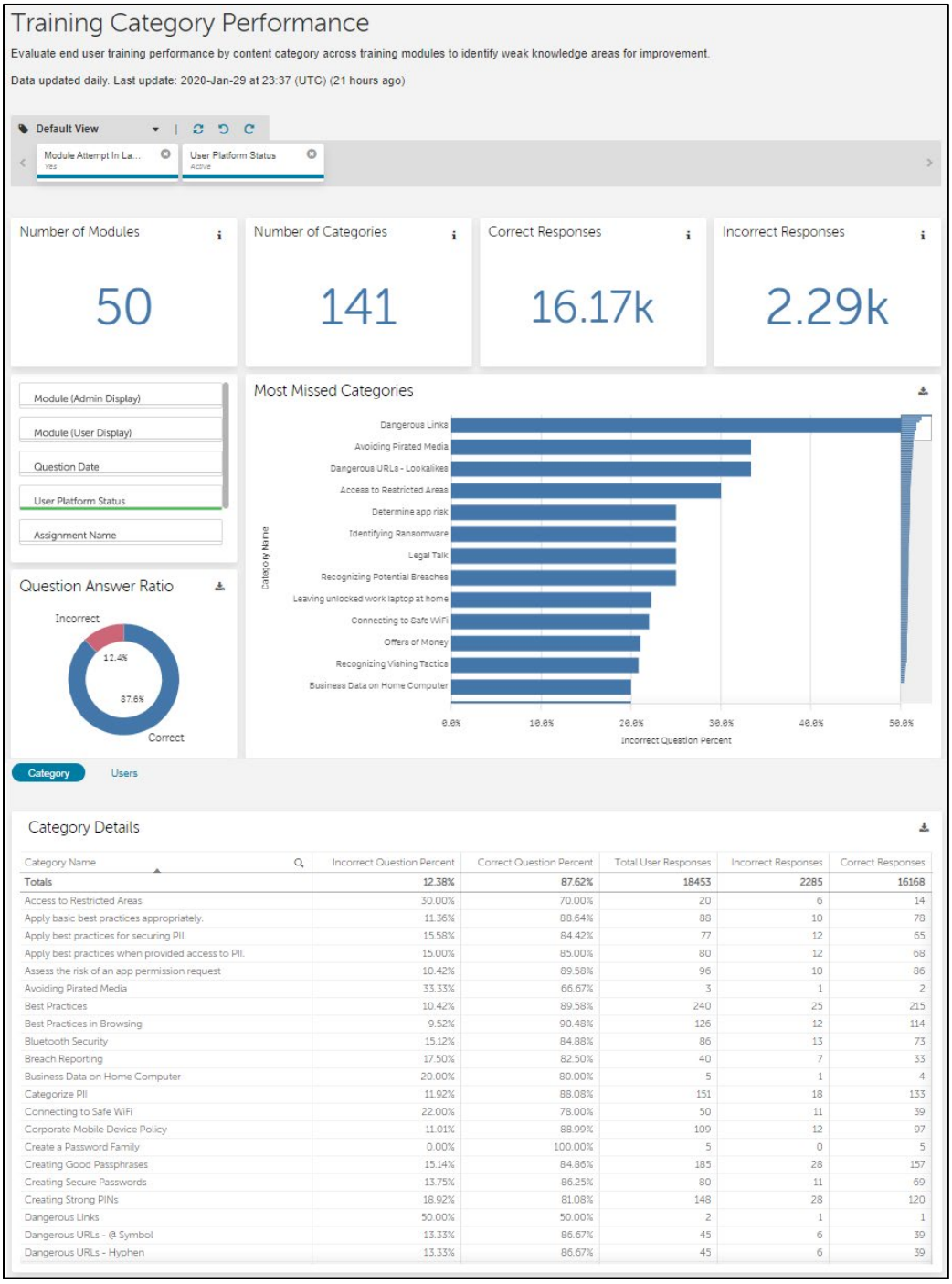
- Provides a variety of filtering options, such as by training module name, date, assignment, and include/exclude deleted users.
- Flexibility to select which data fields to include or exclude from the table to meet specific analysis needs.
- Displays key performance indicators for the total number of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

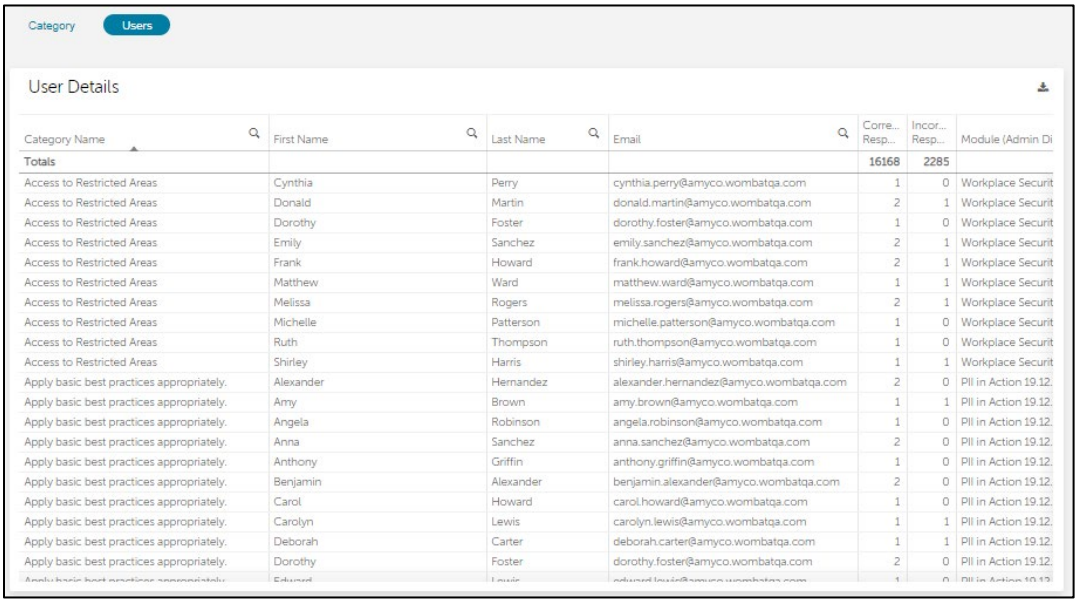
(see next page)

SCREENSHOT OF TRAINING CATEGORY PERFORMANCE REPORT (CONT.)

View includes Category Tab



View of Users Tab



Category Name	First Name	Last Name	Email	Corre... Resp...	Incor... Resp...	Module (Admin Di
Totals				16168	2285	
Access to Restricted Areas	Cynthia	Perry	cynthia.perry@amyco.wombatqa.com	1	0	Workplace Securit
Access to Restricted Areas	Donald	Martin	donald.martin@amyco.wombatqa.com	2	1	Workplace Securit
Access to Restricted Areas	Dorothy	Foster	dorothy.foster@amyco.wombatqa.com	1	0	Workplace Securit
Access to Restricted Areas	Emily	Sanchez	emily.sanchez@amyco.wombatqa.com	2	1	Workplace Securit
Access to Restricted Areas	Frank	Howard	frank.howard@amyco.wombatqa.com	2	1	Workplace Securit
Access to Restricted Areas	Matthew	Ward	matthew.ward@amyco.wombatqa.com	1	1	Workplace Securit
Access to Restricted Areas	Melissa	Rogers	melissa.rogers@amyco.wombatqa.com	2	1	Workplace Securit
Access to Restricted Areas	Michelle	Patterson	michelle.patterson@amyco.wombatqa.com	1	0	Workplace Securit
Access to Restricted Areas	Ruth	Thompson	ruth.thompson@amyco.wombatqa.com	1	0	Workplace Securit
Access to Restricted Areas	Shirley	Harris	shirley.harris@amyco.wombatqa.com	1	1	Workplace Securit
Apply basic best practices appropriately.	Alexander	Hernandez	alexander.hernandez@amyco.wombatqa.com	2	0	PII in Action 19.12.
Apply basic best practices appropriately.	Amy	Brown	amy.brown@amyco.wombatqa.com	1	1	PII in Action 19.12.
Apply basic best practices appropriately.	Angela	Robinson	angela.robinson@amyco.wombatqa.com	1	0	PII in Action 19.12.
Apply basic best practices appropriately.	Anna	Sanchez	anna.sanchez@amyco.wombatqa.com	2	0	PII in Action 19.12.
Apply basic best practices appropriately.	Anthony	Griffin	anthony.griffin@amyco.wombatqa.com	1	0	PII in Action 19.12.
Apply basic best practices appropriately.	Benjamin	Alexander	benjamin.alexander@amyco.wombatqa.com	2	0	PII in Action 19.12.
Apply basic best practices appropriately.	Carol	Howard	carol.howard@amyco.wombatqa.com	1	0	PII in Action 19.12.
Apply basic best practices appropriately.	Carolyn	Lewis	carolyn.lewis@amyco.wombatqa.com	1	1	PII in Action 19.12.
Apply basic best practices appropriately.	Deborah	Carter	deborah.carter@amyco.wombatqa.com	1	1	PII in Action 19.12.
Apply basic best practices appropriately.	Dorothy	Foster	dorothy.foster@amyco.wombatqa.com	2	0	PII in Action 19.12.
Apply basic best practices appropriately.	Edward	Lewis	edward.lewis@amyco.wombatqa.com	1	0	PII in Action 19.12.

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

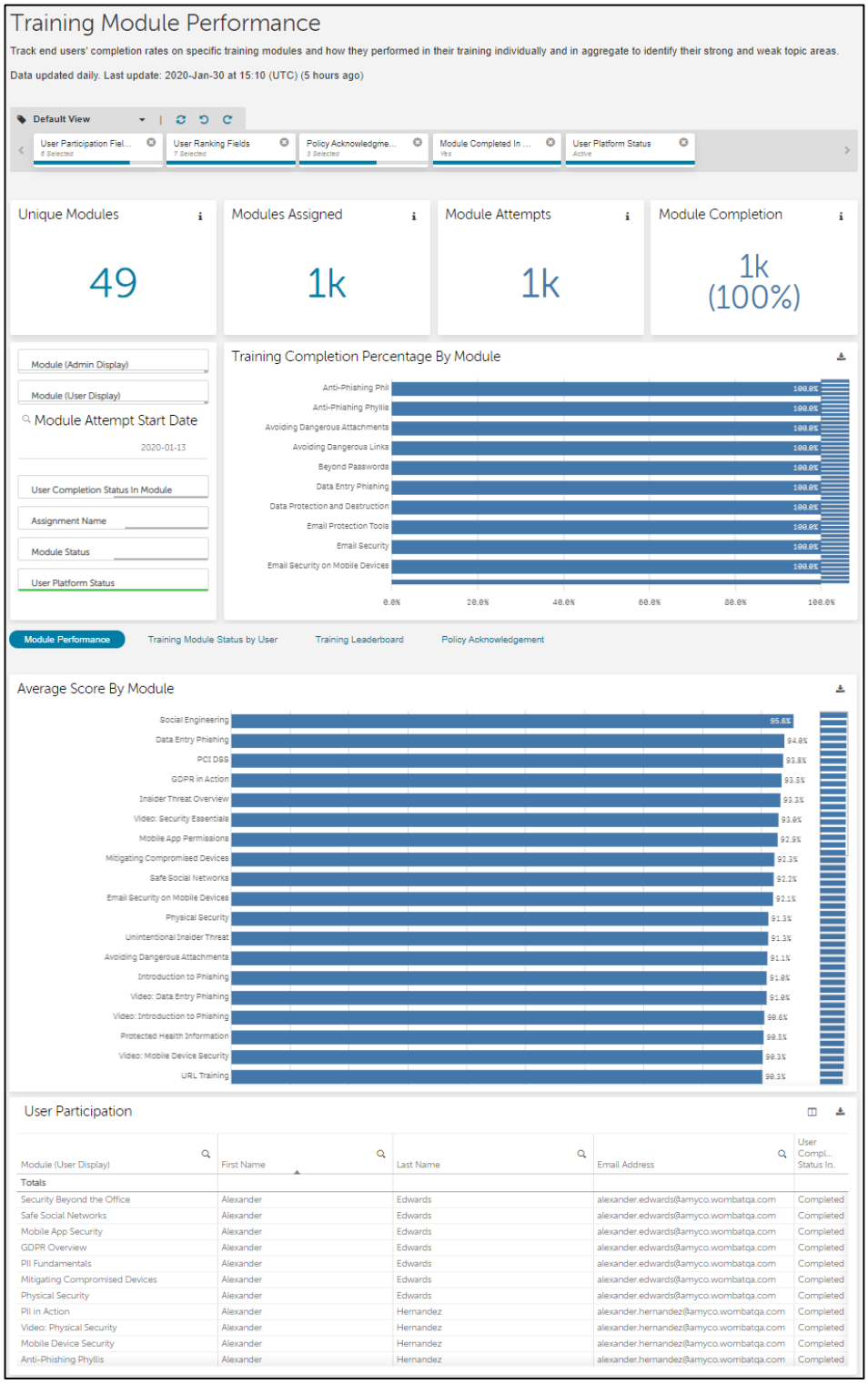
- Easily view and monitor users' training module completion status, completion rate, and scores.
- Identify cybersecurity awareness topics where individuals are strongest and weakest so that future training programs can be tailored accordingly.
- View training completion percentage and average score 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

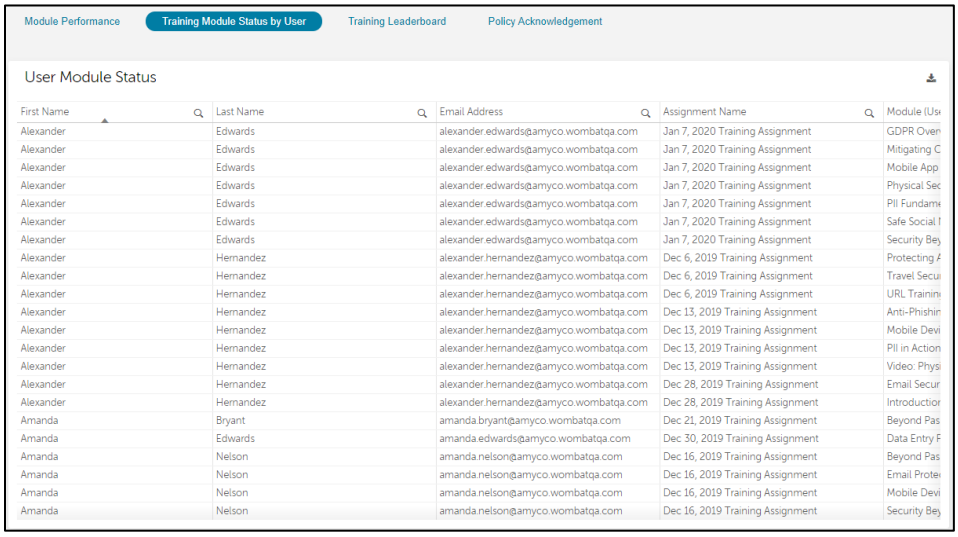
- Provides a variety of filtering options, such as by module name, status, and attempt start date as well as user completion status.
- Flexibility to select which data fields to include or exclude from the table to meet specific analysis needs.
- Displays key performance indicators for the number of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

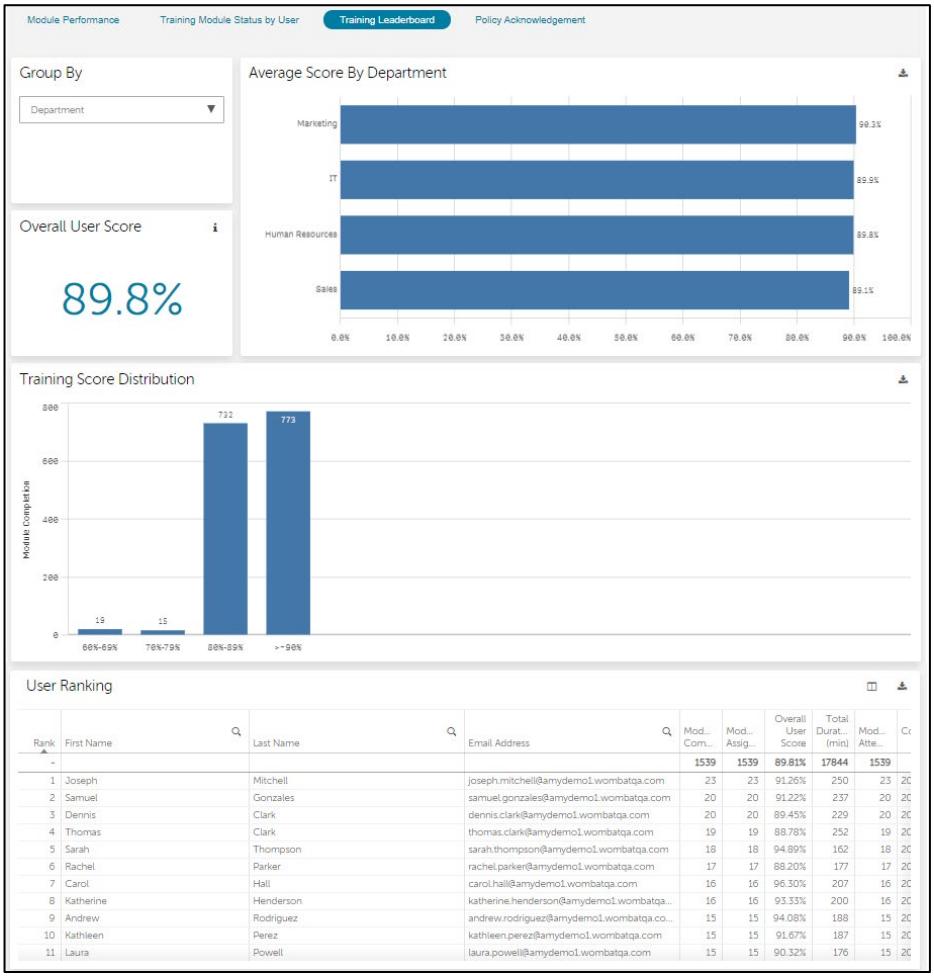


View of Training Module Status by User Tab



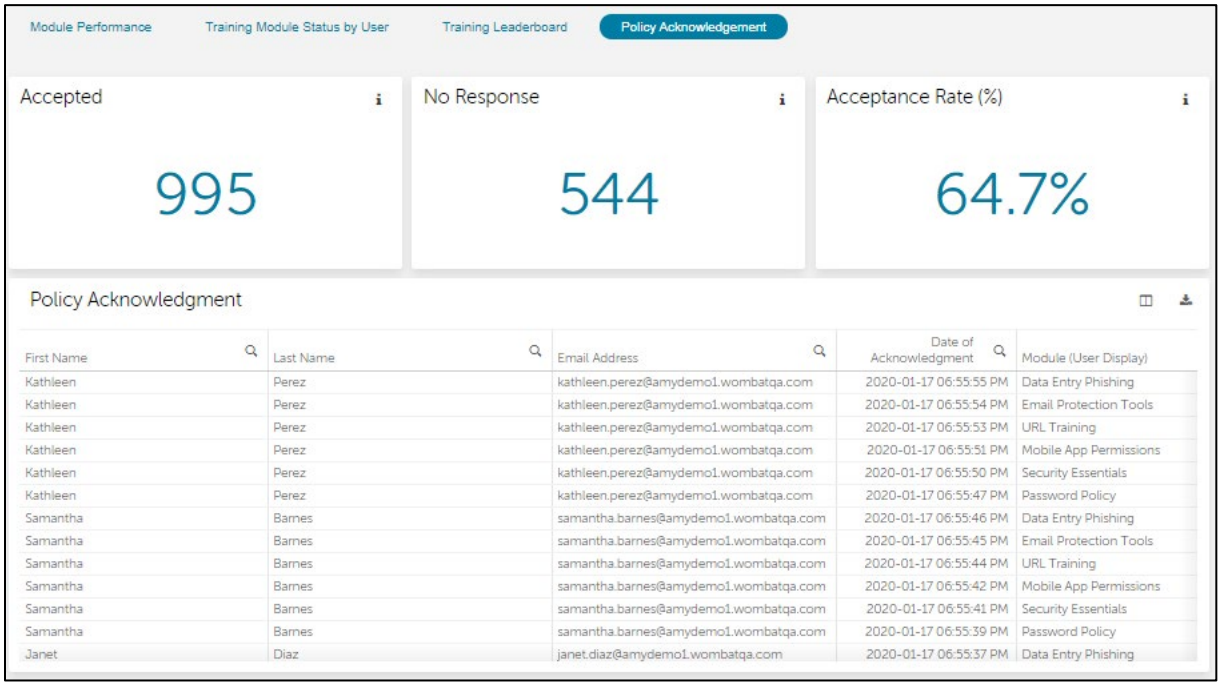
First Name	Last Name	Email Address	Assignment Name	Module (Us
Alexander	Edwards	alexander.edwards@amyco.wombatqa.com	Jan 7, 2020 Training Assignment	GDPR Over
Alexander	Edwards	alexander.edwards@amyco.wombatqa.com	Jan 7, 2020 Training Assignment	Mitigating C
Alexander	Edwards	alexander.edwards@amyco.wombatqa.com	Jan 7, 2020 Training Assignment	Mobile App
Alexander	Edwards	alexander.edwards@amyco.wombatqa.com	Jan 7, 2020 Training Assignment	Physical Sec
Alexander	Edwards	alexander.edwards@amyco.wombatqa.com	Jan 7, 2020 Training Assignment	PII Fundame
Alexander	Edwards	alexander.edwards@amyco.wombatqa.com	Jan 7, 2020 Training Assignment	Safe Social I
Alexander	Edwards	alexander.edwards@amyco.wombatqa.com	Jan 7, 2020 Training Assignment	Security Bey
Alexander	Hernandez	alexander.hernandez@amyco.wombatqa.com	Dec 6, 2019 Training Assignment	Protecting A
Alexander	Hernandez	alexander.hernandez@amyco.wombatqa.com	Dec 6, 2019 Training Assignment	Travel Secu
Alexander	Hernandez	alexander.hernandez@amyco.wombatqa.com	Dec 6, 2019 Training Assignment	URL Trainin
Alexander	Hernandez	alexander.hernandez@amyco.wombatqa.com	Dec 13, 2019 Training Assignment	Anti-Phishir
Alexander	Hernandez	alexander.hernandez@amyco.wombatqa.com	Dec 13, 2019 Training Assignment	Mobile Devi
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: Physi
Alexander	Hernandez	alexander.hernandez@amyco.wombatqa.com	Dec 28, 2019 Training Assignment	Email Secur
Alexander	Hernandez	alexander.hernandez@amyco.wombatqa.com	Dec 28, 2019 Training Assignment	Introductior
Amanda	Bryant	amanda.bryant@amyco.wombatqa.com	Dec 21, 2019 Training Assignment	Beyond Pas
Amanda	Edwards	amanda.edwards@amyco.wombatqa.com	Dec 30, 2019 Training Assignment	Data Entry F
Amanda	Nelson	amanda.nelson@amyco.wombatqa.com	Dec 16, 2019 Training Assignment	Beyond Pas
Amanda	Nelson	amanda.nelson@amyco.wombatqa.com	Dec 16, 2019 Training Assignment	Email Protec
Amanda	Nelson	amanda.nelson@amyco.wombatqa.com	Dec 16, 2019 Training Assignment	Mobile Devi
Amanda	Nelson	amanda.nelson@amyco.wombatqa.com	Dec 16, 2019 Training Assignment	Security Bey

View of Training Leaderboard Tab



Rank	First Name	Last Name	Email Address	Mod... Com...	Mod... Assig...	Overall User Score	Total Durat... (min)	Mod... Atte...	C
-				1539	1539	89.81%	17844	1539	
1	Joseph	Mitchell	joseph.mitchell@amydemo1.wombatqa.com	23	23	91.26%	250	23	20
2	Samuel	Gonzales	samuel.gonzales@amydemo1.wombatqa.com	20	20	91.22%	237	20	20
3	Dennis	Clark	dennis.clark@amydemo1.wombatqa.com	20	20	89.45%	229	20	20
4	Thomas	Clark	thomas.clark@amydemo1.wombatqa.com	19	19	88.78%	252	19	20
5	Sarah	Thompson	sarah.thompson@amydemo1.wombatqa.com	18	18	94.89%	162	18	20
6	Rachel	Parker	rachel.parker@amydemo1.wombatqa.com	17	17	88.20%	177	17	20
7	Carol	Hall	carol.hall@amydemo1.wombatqa.com	16	16	96.30%	207	16	20
8	Katherine	Henderson	katherine.henderson@amydemo1.wombatqa...	16	16	93.33%	200	16	20
9	Andrew	Rodriguez	andrew.rodriguez@amydemo1.wombatqa.co...	15	15	94.08%	188	15	20
10	Kathleen	Perez	kathleen.perez@amydemo1.wombatqa.com	15	15	91.67%	187	15	20
11	Laura	Powell	laura.powell@amydemo1.wombatqa.com	15	15	90.32%	176	15	20

View of Policy Acknowledgement Tab



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

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.

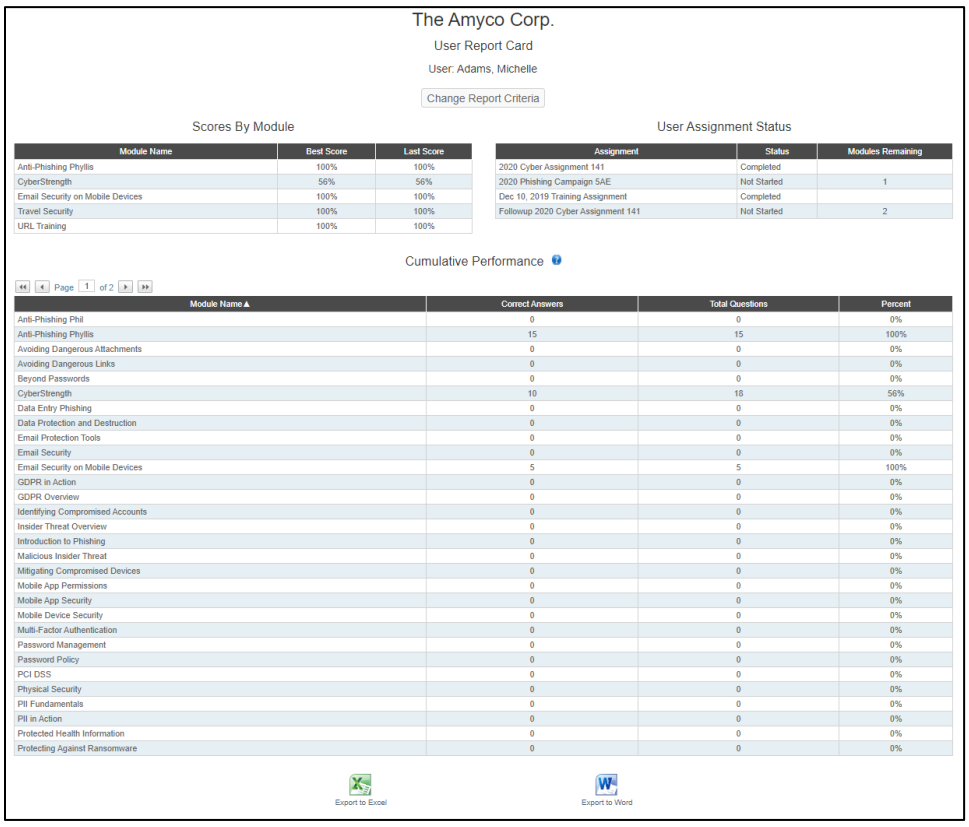
BENEFITS

- 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 options: Excel and Word.

SCREENSHOT OF TRAINING REPORT CARD REPORT



The Amyco Corp.

User Report Card

User: Adams, Michelle

Change Report Criteria

Scores By Module

Module Name	Best Score	Last Score
Anti-Phishing Phyllis	100%	100%
CyberStrength	56%	56%
Email Security on Mobile Devices	100%	100%
Travel Security	100%	100%
URL Training	100%	100%

User Assignment Status

Assignment	Status	Modules Remaining
2020 Cyber Assignment 141	Completed	
2020 Phishing Campaign 5AE	Not Started	1
Dec 10, 2019 Training Assignment	Completed	
Followup 2020 Cyber Assignment 141	Not Started	2

Cumulative Performance

Page 1 of 2

Module Name▲	Correct Answers	Total Questions	Percent
Anti-Phishing Phil	0	0	0%
Anti-Phishing Phyllis	15	15	100%
Avoiding Dangerous Attachments	0	0	0%
Avoiding Dangerous Links	0	0	0%
Beyond Passwords	0	0	0%
CyberStrength	10	18	56%
Data Entry Phishing	0	0	0%
Data Protection and Destruction	0	0	0%
Email Protection Tools	0	0	0%
Email Security	0	0	0%
Email Security on Mobile Devices	5	5	100%
GDPR in Action	0	0	0%
GDPR Overview	0	0	0%
Identifying Compromised Accounts	0	0	0%
Insider Threat Overview	0	0	0%
Introduction to Phishing	0	0	0%
Malicious Insider Threat	0	0	0%
Mitigating Compromised Devices	0	0	0%
Mobile App Permissions	0	0	0%
Mobile App Security	0	0	0%
Mobile Device Security	0	0	0%
Multi-Factor Authentication	0	0	0%
Password Management	0	0	0%
Password Policy	0	0	0%
PCI DSS	0	0	0%
Physical Security	0	0	0%
PII Fundamentals	0	0	0%
PII in Action	0	0	0%
Protected Health Information	0	0	0%
Protecting Against Ransomware	0	0	0%

Export to Excel Export to Word

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

The Amydemo1 Corp.

User Record Export

Export to Excel Export to CSV

The web version of this report shows only your first 200 users. Exporting it will include them all. The time it takes to export this report depends on your user count as well as how much you take advantage of uploading and adding custom user properties. The more users and/or properties you have the longer it will take to export this report.

Data updated: 2020-Jan-29 at 16:03 (UTC)

Page 1 of 2

emailAddress▲	firstName	lastName	Department	Division	Hire Date	Manager	Region
alexander.brooks@amydemo1.wombatqa.com	Alexander	Brooks	Marketing	Corporate	2012-07-29	Matthew Price	North
alexander.campbell@amydemo1.wombatqa.com	Alexander	Campbell	IT	Manufacturing	2016-02-29	Nancy Robinson	North
alexander.cook@amydemo1.wombatqa.com	Alexander	Cook	Human Resources	Healthcare	2012-07-28	Anthony Hill	East
amanda.barnes@amydemo1.wombatqa.com	Amanda	Barnes	Marketing	Healthcare	2017-07-11	Frank Jackson	North
amy.griffin@amydemo1.wombatqa.com	Amy	Griffin	IT	Manufacturing	2015-03-14	Nicholas Wright	East
andrew.adams@amydemo1.wombatqa.com	Andrew	Adams	Human Resources	Corporate	2014-01-03	Kenneth Garcia	South
andrew.bryant@amydemo1.wombatqa.com	Andrew	Bryant	Human Resources	Healthcare	2011-10-28	Kimberly Long	West
andrew.collins@amydemo1.wombatqa.com	Andrew	Collins	IT	Non-Profit	2014-12-22	Edward King	South
andrew.evans@amydemo1.wombatqa.com	Andrew	Evans	Marketing	Manufacturing	2016-11-15	Gregory Brooks	West
angela.bennett@amydemo1.wombatqa.com	Angela	Bennett	Human Resources	Healthcare	2018-05-13	Lisa Coleman	North
angela.evans@amydemo1.wombatqa.com	Angela	Evans	Human Resources	Healthcare	2015-02-01	Edward King	South
angela.gonzalez@amydemo1.wombatqa.com	Angela	Gonzalez	Marketing	Manufacturing	2014-11-06	Christopher Lopez	South
anna.brown@amydemo1.wombatqa.com	Anna	Brown	IT	Manufacturing	2018-05-14	Lisa Perez	East
anna.garcia@amydemo1.wombatqa.com	Anna	Garcia	Human Resources	Healthcare	2016-05-27	Jessica Morris	East
anna.hall@amydemo1.wombatqa.com	Anna	Hall	Human Resources	Manufacturing	2014-11-28	Samuel Stewart	East
anna.hill@amydemo1.wombatqa.com	Anna	Hill	Human Resources	Healthcare	2019-02-28	Alexander Cook	West
anthony.adams@amydemo1.wombatqa.com	Anthony	Adams	Sales	Healthcare	2013-12-17	Pamela Washington	North
anthony.cooper@amydemo1.wombatqa.com	Anthony	Cooper	Human Resources	Non-Profit	2014-11-20	Kathleen Price	West
anthony.foster@amydemo1.wombatqa.com	Anthony	Foster	IT	Healthcare	2018-10-31	William Griffin	North
anthony.hill@amydemo1.wombatqa.com	Anthony	Hill	Marketing	Healthcare	2018-10-04	Steven Stewart	East
ashley.green@amydemo1.wombatqa.com	Ashley	Green	Human Resources	Healthcare	2011-07-30	Samantha Howard	West