Business Intelligence Reports Library

A list of currently available reports within our Security Education Platform.
(May 2018)

Our full-featured business intelligence capabilities deliver the robust reporting component of our Continuous Training Methodology, which emphasizes the role of measurement and analysis. We offer in-depth reporting features for all products within our Security Education Platform, and they allow you to benchmark, track, and trend user knowledge; evaluate progress; and gauge ROI.

It's critical that you be able to gauge your employees' cybersecurity awareness and knowledge levels, as well as the associated risk to your organization. You can view your data in in multiple formats that provide high-level views, as well as granular insights. You can easily analyze data within the platform and export reports to share progress and results with other stakeholders, perform more detailed analysis, and evaluate metrics alongside other security events. Platform administrators have the ability to:

- dynamically filter data using dozens of parameters, including date range, campaign type, and training status;
- add and remove table columns, as well as aggregate by custom properties;
- save multiple data views;
- export to multiple formats — XLS, CSV, PDF, and (in some instances) PNG, JPG, and SVG;
- download and print reports; and
- use our Automated Reporting feature to automatically schedule delivery of reports to stakeholders

Following you will find lists and descriptions of the reports that are currently available for each of our products. You can learn more about our portfolio of security awareness training products and services by visiting our website at www.wombatsecurity.com.

ThreatSim Phishing Simulations

ThreatSim® Phishing Simulations allow you to assess your organizations' vulnerability to malicious link-based, attachment-based, and data entry-based emails without exposing your network to an actual attack. A Teachable Moment is delivered to each user who interacts with your phishing tests, raising awareness in the moment and setting the stage for follow-up training.

Reports

- **All Email Campaigns History** – Provides statistical details about each campaign, including visibility into past, current, and pending simulations.
- **Campaign Comparison** – Compares the performance of multiple simulated phishing campaigns. Administrators have the opportunity to compare performance levels of campaigns based on overall failure rates, and by individual events (views, clicks, attachment opens, and/or data submissions). Campaigns of similar types (e.g. drive by phishing) and different types (e.g. attachment) can be compared side-by-side on the same report, giving at-a-glance insight into the most effective campaigns and campaign types.
- **Campaign Details** – Allows administrators to aggregate the results of multiple campaigns and view the overall performance results together, as well as see how individuals performed in each campaign they received. The report provides a display of each user who was part of a campaign, and how many times each user viewed, clicked, opened an attachment, and/or submitted data.
- **Campaign Overview** – Displays general campaign information as well as incident response data such as time-to-click, time-to-open, time-to-report, number of clicks, number of vulnerable users, and number of acknowledged users.
- **Endpoints** – Indicates the types of devices (desktop vs. mobile), operating systems, browsers, and browser versions that were used by employees who interacted with a campaign. Also reports on out-of-date and potentially vulnerable third-party plug-ins, including like Adobe Flash, QuickTime, and Windows Media Player (via the optional Weak Network Egress feature).
- **Geographic Distribution** – Displays worldwide mapping of user activity per campaign, which helps identify anomalies in regions with high levels of susceptibility.
- **Recent Campaigns** – Provides an at-a-glance view into the short-term phishing performance of an organization via a graphical display of campaigns and associated user activity. Information displayed in the report includes the following:
  - Click rate
  - Multiple clicks
  - Opened messages
  - No response
  - Users who reported the simulated attack
  - Browser vulnerabilities
  - Compromised users (i.e., those who provided their credentials to a fake site)
  - Weak Network Egress data, which shows the users who clicked from non-enterprise networks or networks with permissive egress rules
  - Users who acknowledged viewing the Teachable Moment

- **User Failure Summary** – Allows administrators to analyze users' interactions with simulated phishing attack campaigns. It can be used to analyze the causes of single failures as well as identify repeat offenders. Key features include the following:
  - Metrics around how many times "repeat offender" users have fallen for simulated attacks (for example, 20 users who have failed two times, 40 who have failed three times, 7 users who have failed four times).
  - Opportunity to analyze failure rates by campaign type (drive-by/link, attachment, and data entry) and identify the campaigns with the highest failure rates.
  - Aggregation of results by user property. Any property that is assigned in the user database can be used in the report, and administrators have the flexibility to segment the data based on any of the assigned properties.
  - Charts and tables that display the campaign email templates that generated the most failures across campaigns and templates.
  - The ability to segment results by any defined user properties. Some examples include department, office location, or manager.
  - Three tabular views of the raw data
  - Performance of each user
  - Number of campaigns the user exhibited bad behavior
  - Number of failures by campaign type
  - Each user's custom properties
  - User failures by template
  - View of aggregated results
- **User Failure Summary Light** – This streamlined, simplified version of our User Failure Summary report allows administrators to quickly get the insights they need into the performance of end users in simulated phishing attack campaigns.
- **Users** – Shows detailed and complete user activity, including clicks, opens, and reported phish. Also identifies out-of-date third-party browser plug-ins; detection of endpoints (via the optional Weak Network Egress feature); displays browsers, IP addresses and operating systems.

PhishAlarm and PhishAlarm Analyzer

Our PhishAlarm® email client add-in allows your employees to report suspicious messages to security and incident response teams with a single mouse click. An optional companion to our PhishAlarm email reporting tool, PhishAlarm Analyzer enables faster remediation of threats by using machine learning to prioritize suspicious emails and provide information for incident response teams to investigate threats.

Reports

- **PhishAlarm Reported Emails** – Identifies which users reported which types of emails, and whether an end user successfully spotted a simulated or potential phishing email. The report shows the information reported via the PhishAlarm button, including the following details:
  - The email type (ThreatSim simulated phish or a potential real phish)
  - First name, last name, and email address of the end user who reported the message
  - The time the email was sent
  - The time the email was reported

- **PhishAlarm Analyzer Threat 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.

CyberStrength Knowledge Assessments

Our CyberStrength® Knowledge Assessments provide the ability to assess end-user understanding of a range of pertinent cybersecurity topics, including phishing and social engineering attacks, password best practices, mobile device safeguards, and more. Administrators can build knowledge assessments using our library of 150+ questions, create their own custom questions, and choose from ten Predefined CyberStrength options that help to streamline the administrative process.

Reports

- **Assessment Report** – Shows the overall status of CyberStrength assignments, aggregating user data to identify the strengths and weaknesses in users' cybersecurity knowledge and provides visibility if auto-enroll was assigned. Charts illustrate the top-scoring content areas as well, the highest scoring groups across all participants, and benchmark lines that compare your company's performance against others in your industry, and across all Wombat customers.

- **Risk Report** – Offers the ability to drill down into detailed information about a range of assessment results, including scores by group, lowest overall score by group, most missed questions, lowest scores by person, and benchmarking against your industry as well as all Wombat customers. This analysis can be used to tailor follow-up training efforts and focus on the training topics that are most needed by employees.

- **User Details Report** - Provides the deepest level of detail of users' performance on CyberStrength assessments. For each user, see each question, the answer they selected, the time they spent on the question, your company's average performance, and more.

ThreatSim Smishing and USB Simulations

Our ThreatSim Smishing and USB Simulations can help gauge your employees' understanding of the dangers associated with SMS/text phishing (smishing) and USB-based attacks. These unique assessments can protect corporate systems from malware, spyware, and other dangerous software.

Reports

- **Smishing Campaign** – Provides an at-a-glance view of data points related to the simulated smishing attack, including the users who fell for the attack and how many people viewed and clicked the message.
- **USB Campaign** – Shows the number of USB devices that were accessed and the IP addresses of the users who fell for the simulated USB drop.
- **Responses per USB Device** – Displays the number of unique responses per USB device planted around the workplace. This data can be used to determine which areas of an organization — and which employees — were more likely to pick up and use an untested/unauthorized USB drive.

Interactive Training Modules

We offer a library of more than 25 training modules which cover a wide range of cybersecurity and compliance-related topics. Education is critical to behavior change, and we design our interactive modules based on industry-proven Learning Science Principles to deliver training that engages end users, imparts actionable knowledge, and improves overall security postures. Customizable Training Jackets allow the insertion of content specific to an organization, as well as policy acknowledgements and training completion certificates.

Our business intelligence features go well beyond "completed/not completed" tracking and present more detailed, actionable metrics related to employee training assignment results.

Reports

- **Assignment Comparison** – Shows both a simple top-ten bar chart of assignments and a data table of assignments illustrating completion rates and other statistics.
- **Assignment Details** – Shows the details of how each user is progressing within an assignment and includes each user who was assigned training. A pie chart displays the status of each user in an assignment, and a bar chart shows the completion rate of each module within the assignment.
- **Assignment Status** – Gives a snapshot of 5 to 25 assignments, side-by-side, for selected dates. A bar chart and table display the percentage of users who have completed, are in progress on, or have not started and assignment.
- **Assignment User Details** – A companion to the Assignment Comparison report, this report provides comprehensive user-level information for training assignments. Offers the ability to drill down to the user level and module level and view a number of data points, including a user's module score percentage, time to complete the module, and total questions answered. There is also a chart view that shows the overall user progress against any assignments showing in the data set.
- **Module Completion Summary** – Tracks all end-user interactions with the training modules, including status, score and duration of attempts.
- **Module Performance** – Shows the average score for each module, as well as the module score for each user. A chart view highlights the top 25 user scores.
- **Most Missed Categories** – Identifies topic areas users are having the most trouble with in our training modules. Drill down category by category to view individual user performance.
- **Policy Acknowledgement** – Offers a detailed view of learners who have responded to a policy acknowledgement statement that was added to a training module through our Training Jacket feature. Two chart views show the status of policy acknowledgment responses.
- **Training Leaderboard** – Allows creation and sharing of refined, dashboard-like views of users' training module performance. Administrators can quickly identify the top performers, completion progress, and best-performing departments. The report also includes an exportable table that ranks all users with a formula that uses completion time and module scores across any combination of training modules.
- **User Report Cards** – Provides visibility of all single user activity, including scores for specific modules and a cumulative performance rating. Gives visibility into results over time and helps to identify users who could benefit from additional training.