Part 3: Evaluation

SECURITY BOOT CAMP

An actionable test security workbook for educators and organizations delivering online exams.

WELCOME!

In the age of ubiquitous remote online testing, it is more essential than ever to ensure security, prevent cheating and theft, and lock down the validity and trustworthiness of your exams.

Even with the use of high-quality proctors, it's still possible for test takers to subvert the rules, steal test content, and gain an unfair advantage. The online testing environment provides an especially fertile breeding ground for such behavior.

That's where the **Security Boot Camp** comes in. This workbook series will highlight key test security concepts and provide actionable worksheets and resources to help you understand and apply these concepts to your program so you can make sound decisions for your security.

On page 3, you'll find **eight steps for improving the security of online tests.** This list serves as the outline for all three of the Security Boot Camp workbooks. In **Part 3** of the Security Boot Camp, you'll learn all about the **Evaluation** stage of the test security cycle. Quality assurance spot-checking, patrolling the web for stolen intellectual property, and deep data diving are three key ways to evaluate the health of your items and tests.

So dust off that stylus or fire up that printer, give your trusted team members a call, and follow along. It's time to head to Security Boot Camp!

8 STEPS TO TAKE RIGHT NOW TO IMPROVE SECURITY FOR YOUR ONLINE TESTS

PART 1: PREPARATION WORKBOOK

CREATE A SECURITY PLAN 1

PUBLICIZE YOUR SECURITY MEASURES 2

PART 2: TECHNOLOGY WORKBOOK

EVALUATE YOUR ONLINE TESTING SOLUTION 3

LEVERAGE SECURE ITEM TYPES 4

TURN YOUR ITEM POOL INTO AN ITEM OCEAN 5

PART 3: EVALUATION WORKBOOK

CONDUCT A QUALITY ASSURANCE CHECK 6

YOU ARE HERE

SEARCH THE WEB FOR TEST CONTENT 7

REVIEW YOUR TEST DATA 8

BACKGROUND

MODULE 6: CONDUCTING A QUALITY ASSURANCE CHECK

MODULE 7: SEARCHING THE WEB FOR STOLEN CONTENT

MODULE 8: REVIEWING YOUR TESTING DATA

An Open Letter to the World of Online Testing

from Dr. David Foster
CEO of Caveon Test Security

Hi there,

In just a few short weeks, the COVID-19 pandemic has upended nearly every aspect of our lives, including the way important testing is done. For those students, teachers, professors, candidates, testing organizations, and testing service vendors who have had their plans for taking or giving tests disrupted, I want to offer this message of optimism. Your exams can still be taken and administered securely, even during a pandemic.

Nationwide quarantines and social distancing measures have made it so we can no longer take tests in classrooms, at testing centers, or in other locations. To solve this problem, testing organizations are quickly introducing new solutions that will allow individuals to test online from their own homes. These methods often rely on the use of online proctors to keep those tests secure.

Let me state that I am a wholehearted advocate for this type of online testing. In 2006, I proposed the concept of online proctoring—also referred to as remote proctoring—at the annual conference of the Association of Test Publishers. In 2013, I reviewed the services of several new online proctoring vendors, comparing them on the security features. Two years later, Caveon published its security *Standards for Online Proctoring*, providing a way to evaluate the professionalism of any remote proctoring service. For any program considering the move to online testing, and wishing to create or use an online proctoring solution, I would recommend those two publications and others available on the Caveon website.

However, I need to add a word of caution. Online proctoring is far from a security panacea. Although well-designed proctoring systems—online or onsite—provide some useful security features, tests remain vulnerable to a number of significant security threats that will undermine the test's soundness and trustworthiness.

I repeat—when you put your exams online, even if you are using a competent method of remote proctoring, the two *most dangerous* test security threats remain: **proctors cannot detect when individuals are stealing your test content, and they cannot stop individuals who are cheating by using pre-knowledge.** If these threats cannot be detected by online proctors or proctors working at testing centers, then they are free to do extensive damage.

Let me explain these threats in more detail (without all the industry jargon).

#1: Theft of Test Content.

The first of these threats is the sure theft of test content (your test questions and answers) by individuals using hidden cameras. These are the kind of cameras that can be concealed in a button, the frame of eyeglasses, a lapel pin, or simply appear to be part of the fabric of a shirt. They are capable of recording an entire test session in high-resolution digital video. They are inexpensive, widely available, and easy to set up and use.

Even though a proctor might be closely monitoring an individual taking an exam, if that individual is motivated to steal test questions (to share with a friend or sell online), they will be able to easily steal the entire test—with no risk of being caught! That information can then be easily shared with someone in the neighboring room, apartment, or even on another continent.

#2: Cheating Using Pre-knowledge.

The second threat that cannot be detected by proctoring is cheating on the test using pre-knowledge of the test content. The term "pre-knowledge" is used to describe any information gained about the content of the exam prior to testing. For example, a test taker could purchase the answers to test questions online and memorize them before taking the exam. This form of cheating follows the theft of content described above.

A person with access to the stolen content can cheat confidently and effectively, knowing in advance all the questions and their answers. No proctor, however diligent, can tell the difference between an honest test taker and one who has gained an unfair advantage through pre-knowledge.

As a test security company, we have established practical and actionable solutions for all test security threats, including the two described above. We freely share and discuss test security solutions when we attend conferences, conduct webinars, and through other resources available on our website. Our mission at Caveon is to keep *every* exam safe and the test scores valid and trustworthy for important decisions. At this time, if you are curious about adopting online testing and want to safely navigate these dangerous waters, please visit the website and request a free consultation. We are here to help.

To be clear, I'm not advocating that you abandon your goal of online testing or proctoring your tests. **I believe online testing is the future of this industry and has tremendous potential, but only if it is done *securely*.** I simply want to help make this transition as painless as possible by making you aware of the very dangerous threats that jeopardize your exams *before* they arise and help you understand that viable solutions do in fact exist.

Sincerely,

David Foster

David F. Foster
Chairman & CEO
Caveon Test Security

LOOKING AHEAD

- What are some things you can do to make your tests more secure right away? (Pages 3, 10, 21, 31)
- How can you know when your tests need more (or better) security? (Page 23, 34)
- What indicators can shed light on the health of your program? (Page 33)

MODULE 6

CONDUCT A QUALITY ASSURANCE CHECK

QUESTIONS YOU MAY HAVE

- What elements of my program can I run through a quality assurance check? (Pages 13, 14, 15)
- How can I build a rubric for QA checks? (Page 15)
- When should I consider conducting QA? (Page 11)

QA TERMS AND CONCEPTS

Quality Assurance (QA)
The maintenance of a desired level of quality in a service or product, especially by means of attention to every stage of the process of delivery or production.

Recorded Test Sessions
If a remote test session is proctored via a webcam, the audiovisual recording of that test session is a recorded test session.

User Experience (UX)
In testing, the end user is the test taker, so the testing UX is the process by which a test taker is registered, authenticated, admitted, and administered the test.

Remote Testing
Testing that is conducted online, without requiring the test taker to be present at a testing center. Remote testing can be either proctored or unproctored.

Proctoring
The process of observing test takers during test administration. This can include examinee authentication, and can take place in-person or remotely.

Audit(or)
An audit is the process by which a person (auditor) observes and conducts a standardized evaluation of specified elements of a testing program.

ENSURING QUALITY FOR TESTS THAT ARE DELIVERED REMOTELY

MARC WEINSTEIN

As Vice President of Caveon Investigative Services and Chief Privacy Officer, Marc maintains a laser focus on the security and defensibility of tests. He's an expert in quality assurance for all types of high-stakes test administrations, including remote testing.

When transitioning to online remote-proctored testing, it is critical to identify vulnerabilities in your systems, personnel, practices, and policies. Gaps in your security, however small, can chip away at the trustworthiness of your tests, so it's important to take periodic stock of the major elements of your online testing program.

This can be done in a number of creative ways. For example, you can assess the quality of your systems and practices through reviewing patterns in your data (see Module 8). More specific to remote testing though are some quality assurance techniques that may be useful to you as you navigate the world of remote delivery:

- Stress testing, or "secret shopping" your remote proctoring vendor
- Moving through your test taker's workflow from their vantage point
- Auditing your recorded test sessions for patterns or anomalies

This module is designed to walk you through some basic quality assurance concepts and provide exercises to help you understand how to approach your unique quality assurance needs. But how can you tell when it's the right time to conduct a quality assurance check? There are a handful of strong indicators that you may be due:

1

YOU JUST PARTNERED WITH NEW VENDORS

If you've just begun working with a new remote proctoring vendor, you should have a neutral party perform a quality assurance audit to ensure your policies are followed to the letter.

2

YOU'RE RE-PRIORITIZING YOUR SECURITY

Are you worried that your test takers are subverting your rules? Wondering if proctors are receiving adequate training or doing a thorough enough job administering your assessments? A QA check provides powerful insights.

3

YOU'RE EVALUATING OTHER PARTS OF YOUR PROGRAM

Whether you use automated, record-and-review, or live proctoring, you might be wondering if you'd benefit from switching to another proctoring method. A QA check will help inform your decision.

4

YOU RECORD AND STORE YOUR TEST SESSIONS

Do you have hundreds of recorded test sessions but no time to review them? Record-and-review methods of proctoring can always be spot-checked by third-party auditors.

MODULE 6 · PART 1

THE BENEFITS OF QUALITY ASSURANCE

01

DETECTION

Most attempts at test theft and cheating are designed to fly under the radar of traditional security measures. Monitoring—whether remote or in-person—is an effective tool for detecting testing irregularities and security vulnerabilities that aren't visible from an exterior vantage point.

02

FEEDBACK

Do your test administrators and proctors have all the tools they need to be effective? Do your examinees have proper notice of all the rules and procedures? Gain valuable feedback about the effectiveness of your test administration and security procedures by spot-checking testing sessions.

03

IMPROVEMENT

After conducting the monitoring of your remote test administrations, you'll have a wealth of data that can help you and your team make actionable test security improvements to your program. Update policies and procedures based on trends, and ensure that your security practices always remain relevant.

04

DETERRENCE

Send a message to would-be fraudsters and test thieves that you take your test security seriously. Monitoring test administrations acts as a strong deterrent for anyone who might intentionally attempt to commit test fraud or steal your test content—and it's one more layer of security to strengthen your test program.

WHAT CAN YOU TEST FOR QUALITY?

RECORDED TEST SESSIONS

Record-and-review is a popular method of proctoring, but did you know that you can also use recorded test sessions for quality assurance—even if you don't actively proctor? If you don't have the resources to proctor or review every single test session, simply plan to audit a meaningful percentage of your recorded test sessions to conduct quality assurance.

PROCTOR CONDUCT

Have you ever thought to evaluate your proctoring solution? It's easier than you think. Whether your exams are administered online or in person, an auditor can pose as a student and make an effort to subvert the rules to stress test your proctoring security. Do proctors respond the way you'd expect them to respond? Do you need to improve training?

USER EXPERIENCE

Whether you're trying to shore up security or you're just looking to create a smooth and painless registration and testing process, you might want to run a quality assurance check on your user experience. Again posing as a candidate, an auditor can move through your test taker experience to check for security risks and steps that could use improvement..

MODULE 6 · PART 3

6 STEPS TO STARTING QUALITY ASSURANCE MONITORING

STEP 1

Set your purpose and goals.

WHY ARE WE MONITORING?

STEP 2

Determine budget and funding sources.

HOW MUCH ARE WE WILLING TO SPEND?

STEP 3

Select the parameters of your project.

WHAT ARE WE MONITORING? HOW MUCH?

STEP 4

Evaluate staffing options.

SHOULD WE OUTSOURCE OUR QUALITY ASSURANCE?

STEP 5

Develop checklists and training materials.

WHAT DO WE NEED TO GET GOING?

STEP 6

Set up periodic program reviews.

WHAT'S OUR SCHEDULE GOING FORWARD?

MODULE 6 · PART 4

QA RUBRIC BRAINSTORM

What steps need to be taken in order to implement the below components into your quality assurance plan?

QUESTION	EXAMPLES	IMPLEMENTATION
What elements of your program are you interested in/capable of putting through a quality assurance check?	• Proctor conduct • Tests, items, and forms • Test-takers' experiences • Recorded test sessions • Basic security strength	
What behaviors are not permitted for test takers?	• Using a cell phone during a test • Speaking to another person during a test • Navigating to external applications during a test	
What behaviors are expected of proctors during a test?	• Authenticate each test taker's identity • Warn test takers of certain information • Pause or abort an exam under specific circumstances	
What is your ideal flow of the test-taker's experience, from registration to score reporting?	• Will you include elements like authentication and proctoring? • Can the candidate move easily through the workflow?	

QUESTION	EXAMPLES	IMPLEMENTATION
Who will we use as monitors/auditors?	• Outside professionals • Trained staff • Yourself • Volunteers	
How many instances of monitoring will we commit to?	• 5% of exam administrations • 10% of exam administrations	
Does my type of testing impact my need for monitoring/spot checking sessions?	• Record and review will need more instances of monitoring. • How often do we want to QA our proctoring vendor?	
How will you train and manage your team of auditors/monitors?	• Are there experts who should contribute to training? • How often should training be conducted?	

What is your plan if/when you discover any untoward behavior—from test takers, administrators, proctors, etc.—during quality assurance?

How will you capture and report data?

What are the primary goals of this quality assurance plan? Do you hope to identify test taker misconduct? Are you evaluating your proctoring solution?

How can you standardize data collection, analysis, and reporting? Do you need a checklist, auditor protocols, or monitoring technology?

MODULE 6 · PART 5

MONITOR RESPONSIBILITIES

Use this checklist to develop training materials for your remote monitors.

□ Observe the testing environment

- Test administration procedures
- Staff/proctor roles
- Student behaviors
- The physical environment

□ Mimic the test taker experience

□ Attempt to stress test any security weaknesses

□ Capture standardized observations for later review

- Use a standardized, binary checklist
- Require explicit narrative descriptions
- Provide clear procedures for managing data
- Use qualitative analytics to pinpoint quality assurance concerns
- Use supplied tools to communicate with stakeholders
- Escalate serious issues to the predetermined appropriate individuals

MODULE 7

SEARCH THE WEB FOR STOLEN CONTENT

QUESTIONS YOU MAY HAVE

- What is web patrol? (Page 20)
- Where can I find my stolen test content online? (Pages 22, 27)
- How can I make someone remove my stolen intellectual property from the internet? (Pages 22, 27)

CONTENT TERMS AND CONCEPTS

Web Monitoring

The practice of monitoring common places on the internet for stolen or otherwise exposed test content. Web monitoring may not detect the theft in action, but certainly detects its outcomes and provides enough information to take action.

Intellectual Properties

A work or invention that is the result of creativity, such as a manuscript or a design, to which one has rights and for which one may apply for a patent, copyright, trademark, etc. In testing, this includes all test content, providing the legal grounds for removal from infringing parties.

Braindump Sites

A website, group chat, or other digital forum in which an organization shares, offers for sale, or disseminates copyrighted test content that is not theirs.

DMCA Letter

A letter that conforms to the provisions of the Digital Millennium Copyright Act (DMCA), designed as a legal remedy to have content removed from the internet.

Pre-knowledge

In testing, a candidate who benefits and gains an unfair advantage from having been given prior knowledge of content or from seeing the exam before.

Validity

In testing, validity is the trustworthiness of the test results. Validity can be undermined by a number of factors, including exposure and test fraud.

PATROLLING THE INTERNET

CARY STRAW

Cary Straw is an Executive Web Patrol Manager at Caveon with more than thirty years of experience in online computing, design, and test security. These varied strengths enable him to understand and know where the bad guys hide online and how to find them.

"Well, I've never seen that before."

After fifteen years scouring the online world exposed exam content, I've learned to expect the unexpected. I am constantly surprised by how, when, or where exam content will be discovered online. The internet is constantly evolving, and so too must our focus and goals for finding and addressing these exposures.

In the beginning, most testing companies weren't aware of the security vulnerabilities introduced by the internet. Back then, the online ecosystem was not nearly as robust as it is today, and social media was not the star of the show. During these simpler times, infringing exam content typically came from individuals or small companies with no nefarious intent—they were mostly looking to either help out a friend, or in some cases, sell a few questions and gain some small advantage for customers taking the exam.

The processes and goals for web patrol were simple: Search online in forums, discussion groups, and websites for infringing content; report that content; have the client verify it; and send a letter asking to have the content removed. Clean, simple, and it worked a large percentage of the time.

Fifteen years later, the online ecosystem has drastically changed. The testing industry now faces large conglomerates of braindump sites numbering in the thousands, each one owning hundreds (if not thousands) of individual URLs that routinely steal content from a vast number of private, public, and governmental industries. We must now deal with groups that recruit test-takers to travel the world to steal, remember, and record as much exam content as possible, and then turn around and sell and distribute that content at a global level.

Most often, owners of these infringing sites are inundated from all sides with takedown requests from companies looking to protect their materials (and in some cases, substantial monetary investments) by leveraging the Digital Millennium Copyright Act (DMCA). But with DMCA letters becoming such a popular (and often misused) tool, it has become exceedingly difficult to have content removed with a letter… or three.

But these braindump sites aren't the only threat our exams must overcome—Social media, a practice so prolific and entrenched in our online discourse that even the greatest of online search companies have a hard time keeping up. Faced with a beast of this power and magnitude, we recommend that clients not only institute routine web patrol into their test security strategies and remove content where possible, but create an environment of both diligence and innovation that extends the usable life of their exam, both online and in the real world.

In an ideal testing environment, these security threats would not exist. If the online environment was the utopian ideal envisioned by many people during its infancy, web patrollers would not have to continually update and modify their approaches to online exam security. However, until we reach those pinnacles, a comprehensive and broad scope system that incorporates security measures that prevent, deter, and detect test fraud is necessary. Web patrol is just one of the powerful tools at your disposal to give your highly-valued intellectual properties additional validity, lifespan, and security in the current online environment.

MODULE 7 · PART 1

WHAT SHOULD YOU BE ASKING YOURSELF ABOUT YOUR WEB EXPOSURE

BIG PICTURE

- □ How much exposure are my exams getting on the internet?
- □ When in my testing cycle do exposed items begin to show up?
- □ Do items ever appear before the test administration window begins?
- □ What is currently being said about my exams on the internet?

TEST DEVELOPMENT

- □ What forms are most often exposed? Why?
- □ Do my question types invite exposure?
- □ Are my development and security teams working together?
- □ Can I rescue the exposed items by restructuring them?
- □ How is the level of exposure impacting my items' useful lifespan?
- □ How does the level of compromise compare over time?
- □ How does the level of compromise compare between forms?

TEST SECURITY

- □ What portions of my exams are showing up online?
- □ How quickly do items spread across the internet?

□ Who is posting the exams online?

□ If a site is claiming to have "real" items, what items do they typically have?

□ Am I doing routine checks of test providers?

□ Am I doing routine checks of test administrators and any third-party or proctoring providers?

LEGAL QUESTIONS

□ Is my legal team involved with test security planning?

□ How do I address privacy issues?

□ Are my exams copyrighted?

□ Do I have boilerplate letters/procedures to quickly address exposures?

□ Is my legal team well versed in proper procedures for protecting our intellectual property?

THE REALLY, REALLY IMPORTANT QUESTIONS

□ Do I have a plan in place before content is found online?

□ Over time, have I observed the exposure situation getting worse or better?

□ Who makes the ultimate decision on how to respond to a breach of exam content found on the internet?

WORKSHEET:DEVELOP A WEB EXPOSURE STRATEGY

What steps need to be taken in order to implement the below components into your web exposure strategy?

QUESTION	EXAMPLES	IMPLEMENTATION
Who in your organization should be involved with web monitoring?	• Senior management • Test development team • Test security manager • Legal counsel	
What actions could you take to decrease the chance of your content being exposed online?	• Use secure item types • Have a strong presence in test takers' online environments • Provide large quantities of free test materials, limit the re-use of exams, forms, & items • Create and enforce non-disclosure agreements	
What is your typical test-taker profile? Knowing this, where can you most effectively use your web monitoring resources?	• K-12 students are typically very active on social media • Professionals may congregate in industry-specific chat rooms	
What benefits (in addition to finding and removing test content) might you receive by monitoring the web?	• Increased lifespan for exams and questions • Increased perception of exam quality • Decreased resources spent rewriting and republishing content	

QUESTION	EXAMPLES	IMPLEMENTATION
Why should you continue to monitor after you have found and removed content online?	• The content could be re-posted in the same place or spread to other places • Other content could appear in unexpected places	
What are the potential consequences of having your exam exposed online?	• Financial loss to rewrite and republish exams • Reputational damage • Loss of trust in the validity of your exam scores • Media involvement	
Who can you recruit to help monitor the web for your exams?	• Test security and web patrol professionals and consultants • Forum moderators • Peer ambassadors • Media contacts	
Why should you continually explore cutting-edge technologies and processes for monitoring the web?	• The internet changes quickly, with new platforms popping up every day • Thieves are creative, programs need to stay ahead • Exam validity is the #1 priority, one cannot let any online threats go untraced.	

THE THREAT REMOVAL PROCESS

1 IDENTIFY TEAM ROLES

Determine who in your organization will be responsible for online threat removal. At a minimum, they should be directly involved and familiar with your exam security efforts. Also consider to whom that person should report their findings—a single individual at the top, multiple team members in different departments, or a representative on your legal team? We recommend a combination of these. Evaluate over time to see which processes provide the quickest pipeline to threat removal. Time is of the essence!

2 SEND DMCA LETTER

Prepare, approve with your legal team, and send a takedown letter to any offending site owner and affiliated web hosting company. Make sure your letter conforms to the Digital Millennium Copyright Act (DCMA) guidelines, found at www.copyright.gov. Please note that these laws apply only to domestic sites. International sites may require different methods and procedures, based on the copyright protection in their country.

3 TRACK REMOVAL

Depending on the offending site, threats may be removed within hours of your first DMCA letter. It may also take weeks and multiple letters before you are successful in removing the content from the site. Strong determination and follow-up with each and every site are key to getting content removed.

4 ESCALATE TO LEGAL

Even after several attempts, some sites and individuals will refuse to remove your content, at which point you'll want to involve your legal team. Sometimes this can be as simple as a strongly-worded letter implying forthcoming legal action. In the worst case, a lawsuit will have to be filed to protect your intellectual property. This worst-case scenario is rare when steps 1-3 are followed.

5 CLEAR THREAT

Congratulations! Your efforts have paid off and the offending sites have taken down your content. Now that the present threat is cleared, it's important to follow through with the final step in the process.

6 ONGOING MONITORING

Continual monitoring is the most important step in the process. It is your assurance that if a threat appears again, it will be found and dealt with before it impacts the integrity of your exams.

NOTES / BRAINSTORMING PAGE

TO-DO LIST

TASKS	PRIORITY	DUE DATE	
			□
			□
			□
			□
			□

MODULE 8

REVIEW YOUR TESTING DATA

QUESTIONS YOU MAY HAVE

- What is data forensics? (Pages 30, 32)
- What does my testing data say about the health of my test program? (Pages 33-34)
- What kinds of data should I be collecting? (Pages 34-35)

DATA TERMS AND CONCEPTS

Data Forensics™ (DF)
A set of security methods dedicated to detection. Data Forensics analyzes examinee responses in a set of test results, looking for unusual patterns that may be indicative of various types of test fraud.

Testing Data
The data collected before, during, and after testing that can provide insight into results, patterns, or trends. Testing data may include response data, time signatures, wrong-to-right answer changes, and more.

Statistical Anomaly
Unusual patterns in the data that may or may not reflect violations or fraud. Example: An examinee demonstrating two different levels of proficiency.

Testing Irregularity
Out-of-the-ordinary events occurring during testing, not always violations. Example: A fire alarm disrupts test takers during the testing window.

Test Fraud
An intentional act that reduces the integrity of an exam. Example: An administrator intentionally discloses answers to examinees.

DATA FORENSICS: WE'RE SAYING THERE'S A CHANCE

JENNIFER PALMER

Jennifer Palmer is a Certified Exam Security Professional and Data Forensics Coordinator. She works with clients to plan and execute forensic analysis of their test response data, interpret their analysis results, and strategically plan to improve their overall program security. With more than fifteen years of experience in managing technical and scientific projects, Jennifer has a valuable and unique perspective on test security processes.

At the end of the movie *Dumb and Dumber*, Lloyd (the doofus-turned-hero who saves the day for the beautiful damsel in distress) asks Mary Swanson a question in the hopes of sparking a romantic relationship:

“What are my chances?”

Mary quickly replies, “Not good.”

Lloyd pauses, then says, “You mean ‘not good’ like, one out of a hundred?”

“More like, one out of a million,” she says.

Lloyd, with a gleam in his eye exclaims, “So...you’re saying there’s a chance!”

Data forensics uses statistics to analyze test response data looking for anomalies (or testing irregularities) that may be indicative of cheating. When testing irregularities are found, testing program managers typically review and may ultimately invalidate scores based on evidence that the scores are not representative of the examinees’ knowledge. Like with Lloyd, the statistical results are often presented in the form of probabilities. For example: The probability of two examinees having selected the same answers on the test form by chance alone is 1×10^{-12}, or one in one trillion.

While such statements are often confusing, they are undeniably valuable. So, what is data forensics, and why is it so important?

Data forensics is the practice of diving into your testing data and looking for inaccuracies, inconsistencies, potential incidents, and (in some cases) fraud. Data forensics analyses utilize a wide variety of statistics designed to identify whether various test security breaches may have occurred. It can be helpful to think of data forensics being similar to an MRI or X-Ray machine that is used when a medical professional suspects a particular illness or ailment. The machine is focused in on a specific area to help identify whether a condition exists. The goal is to determine the scope of a problem's impact upon the individual's health so that a trained professional may prescribe an appropriate remedy. It's the same thing with the data forensics analysis of test data.

There are a wide variety of data forensics analyses that can be used (Caveon has a suite of more than 25 powerful statistical analyses). As such, it is important that you carefully consider the intended focus of the data forensics analyses. Every testing program is different, as are their risks. K-12 education professionals are concerned with what is happening in classrooms and schools; many international testing programs want to flag test centers with concentrations of unusual results; and others like to spot trends in groups with similar "demographics"—that is, test takers that studied in the same school, attended the same training program, work for the same company, etc.

Data forensics is vital for understanding the health of your program. The practice of diving into your testing should be habitual for every single exam. You've been trusted with the responsibility to make sound decisions for your testing program, and data forensics will arm you with the strength you need.

USE YOUR DF RESULTS TO...

Detect which test scores might not be valid and why

Decide security strengths and vulnerabilities

Determine where test security resources should be allocated

Track test security threats over time (within windows or across years)

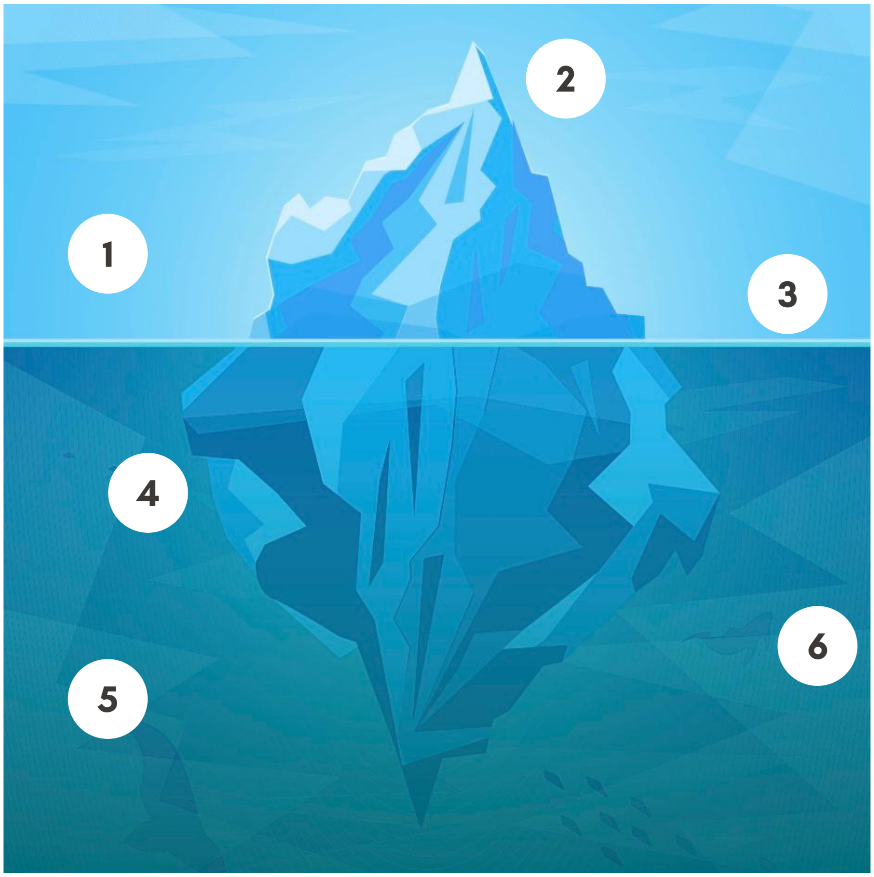
Identify areas where further investigation is necessary

Find evidence to support inquiries into disclosed and shared content

Deter test fraud before it happens by publicizing your use of DF

Maintain the value of your certification

Recalibrate security policies and procedures



BELOW THE SURFACE

What test security threats can be detected by Data Forensics? Hint: They're not all easy to spot with the naked eye.

1 **Administrator Collusion**

Wrong-to-right answer-changes and similarity analyses can help detect those who may be committing test fraud.

2 **Examinee Collusion**

Similarity statistics and source-copier statistics can sniff out examinees who peek at others' exams or share test content.

3 **Test Killers**

Similarity statistics and flawed-key analyses detect use of stolen exam content contained in distributed "Test Killers."

4 **Proxy Test Takers**

Uncover the illicit activity of professional proxies who take tests for others, and of the candidates who employ them.

5 **Fraudulent Test Sites**

Data Forensics can detect test sites operated by pirates and can provide the necessary evidence for taking legal action.

6 **Large-Scale Collusion**

Data Forensics can detect large-scale collusion, supporting disciplinary actions against fraudulent individuals.

6 STEPS TO BUILDING A STRONG DATA FORENSICS PROGRAM

□ **01. Identify your greatest test security risks.**
How much damage results when someone undermines the integrity of test scores? What motivates them to violate your security? Understanding your risks will help you decide which analyses will be most informative as you manage them.

□ **02. Develop plans for handling identified incidents.**
How will you respond if you find evidence of fraud? Decide what you will do when the data forensics evidence meets your threshold and standard for taking action.

□ **03. Find out what data you have access to.**
Determine what types of data you can obtain. These can include test center identifiers, response times, answer-change data, or timestamps that track when each item is viewed. What you have access to will determine the types of data forensics analyses that can be performed.

□ **04. Determine which statistics you can compute.**
These should mirror the primary security concerns you determined in Step 1. How well do your selected statistics detect and measure the threats and risks you identified? Ensure that you capture critical information and evidence to support your test security initiatives.

□ **05. Figure out what layers you can analyze.**
Will you analyze individuals, test sites, test forms, or items? Perhaps some combination of these? Often, detection in data forensics is a multi-layer issue. The deeper you dive into the layers of data, the more information you'll have about what is actually going on.

□ **06. Decide what type of information you want.**
How should the results be presented, summarized, and formatted so they are most helpful for your team and stakeholders? What resources are available to help you understand the results? You want the ability to digest your results and take action quickly, if necessary.

MODULE 8 · PART 4

WORKSHEET: DIVING INTO YOUR DATA

What steps need to be taken in order to implement the below components into your Data Forensics Strategy?

QUESTION	EXAMPLES	IMPLEMENTATION
What is your program's mission statement with respect to assessment?	Do you provide the most secure tests? The most accurate?	
How are the scores from your program used? Who uses them?	• Assess job candidates • Assess scholastic ability	
What are you most concerned about discovering for your testing program? What legal agreements or legal foundation should be in place in order for you to consider invalidating scores based on data forensics results?	• Statistical anomalies • Testing irregularities • Security violations or breaches • Candidate agreements and ethics policies • A comprehensive security plan	
Who are your stakeholders? What do those stakeholders need and want?	Students, parents, review boards, job candidates, etc.	

QUESTION	EXAMPLES	IMPLEMENTATION
How do you intend to use the data forensics results?	• Build and create exams • Ensure quality • Interpret scores	
What actions is your organization willing to take based on your data forensics results?	• Replace test questions and forms • Invalidate test scores • Pursue legal action	
What policies relevant to taking action are currently in place within your program?	• Replace test questions and forms • Invalidate test scores • Pursue legal action	
What data will provide the most relevant information for your specific testing program?	• Response-time data • Wrong-to-right answer change data • Etc.	
When implementing a data forensics plan, what will be your biggest challenges and concerns?	• Political • Legal • Operational	

QUESTION	EXAMPLES	IMPLEMENTATION
Rank the following from most important (1) to least important (3).	□ Protecting the integrity of my items/forms by detecting which may be compromised. □ Identifying groups that may not be following secure administration procedures. □ Certifying that each and every individual score accurately represents the examinee's knowledge and ability.	
Given your program's current policies, consider how you would use your data forensics results. What actions are supported? Do these actions align with the priorities you identified above?	• Retire and redevelop items • Invalidate individual scores • Revisit training and administration materials	

NOTES / BRAINSTORMING PAGE

TO-DO LIST

TASKS	PRIORITY	DUE DATE	
			□
			□
			□
			□
			□

YOU DID IT!

CONGRATS! YOU FINISHED THE TEST SECURITY BOOT CAMP SERIES.

Want exclusive access to more testing resources, workbooks, or other helpful industry content?

SUBSCRIBE TO OUR EMAIL LIST

Learn more over at
caveon.com