YOUR ULTIMATE GUIDE TO MONITORING THE WEB FOR STOLEN TEST CONTENT

caveon™

WHY SHOULD I BE "MONITORING THE WEB?"

It's frustrating (and expensive!) for testing organizations to spend the time, creativity, and resources developing great test questions, only to have those items disclosed on the Internet a short time after publication. **The result of such disclosure?** Undeserving test takers pass the exam using pre-knowledge (memorizing the answers they found online). This type of fraudulent activity erodes the validity of your exam and hurts your program's reputation. Worst of all, your investment in developing high-quality assessments goes down the drain. Patrolling the web is a powerful tool that helps to protect your exams from this type of cheating and gives your highly-valued intellectual properties additional validity, lifespan, and security in the current online environment.

What is web monitoring?

Web monitoring is 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 it certainly detects its outcomes and provides the necessary information to take action.

WHERE CAN I FIND EXAM CONTENT ONLINE?

SOCIAL MEDIA

While it may be easy to find public-facing social media posts containing illicit or stolen content, you may not be aware that an entire ecosystem of online forums, chats, and private groups exists for this very purpose. Social media is an excellent place to start your search, but you may be required to dust off your sleuthing skills and assimilate in some corners of the Internet you've never been before.

BRAINDUMPS

Braindump sites, file sharing sites, and affiliated blogs make a practice out of sharing stolen content while dodging requests to take it down. Nevertheless, you must locate and pursue the removal of your content if ever you find it in one of these forums. Make it a practice to regularly crawl the current and most popular sites.

SEARCH ENGINES

You're already familiar with search engines and social media sites in your home country, but are you familiar with those of other countries as well? If your exam is being delivered online, your exam is international. You should familiarize yourself with the most popular tools used to share information in other countries and learn how to use them. Bonus points if you can speak the language!

caveon

THE COST OF EXAM EXPOSURE

1. **LOSS OF INVESTMENT**
2. **INVALIDATED SCORES**
3. **REPUTATION COSTS**
4. **REDEVELOPMENT COSTS**

Exams and tests are not just for organizations dedicated to testing. They're also for training and evaluation purposes within tech companies, medical organizations, and even civil service groups in order to ensure candidates have the skills necessary to do the job well. But what happens when those tests are leaked online? Just one online leak can have the effect of compromising an entire exam—or even the integrity of an entire institution. What else is there to lose from long-term, unchecked exposure?

THE HUMAN ELEMENT

WEB CRAWLING VS WEB PATROLLING

FLEXIBILITY

Human web patrollers (as opposed to automated web crawlers) are capable of adapting seamlessly to the rapid evolution of the online social sphere—and to the specific needs of you, the client.

CRITICAL THINKING

Monitoring the web for stolen test content involves a complicated and nuanced process of piecing together a series of clues that only humans are capable of detecting and connecting. Automated systems can't do that.

INTERACTIVITY

Not only are humans capable of detecting unique vulnerabilities in web security, they are capable of interacting with others as part of their investigation as well. At times, problems only become clear via conversations, private messages, and eliciting tips from those in the know.

CULTURE

Web patrollers with language and cultural skill sets are indispensable aspects of a comprehensive and successful online security plan. Automated bots cannot keep up with the intricacies of the global digital landscape in a way that guarantees security.

PLANNING FOR WEB EXPOSURE

BRING THESE QUESTIONS TO YOUR TEAM AND FIRM UP YOUR PLAN

How much exposure are my exams getting on the Internet?

How is the level of exposure impacting my items' useful lifespan?

Can I rescue the exposed items by restructuring them?

Do items ever appear before the test administration window begins?

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

Do my question types invite exposure?

Are my exams copyrighted?

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

Who decides how to respond to a breach of exam content found online?

What portions of my exams are showing up online?

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 administrators and any third-party or proctoring providers?

Am I doing routine checks of test providers?

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

INTERNATIONAL

WHAT TO CONSIDER WHEN MONITORING ACROSS THE GLOBE

ONLINE = INTERNATIONAL

If your test is administered online, then your web monitoring strategy must be comprehensive and international in scope.

BORDERS AND BARRIERS

Crossing regional boundaries of the Internet, like crossing into foreign territory, will reveal foreign hotspots of online activity, information-sharing models, consumer behavior, and etiquette (all in different languages).

HOT HANGOUTS

Common methods of content sharing and braindumping vary from place to place. Patrolling internationally requires knowledge of each geographic area's popular online hot spots for fraudsters.

BLIND SPOTS

In Korea and China, people are familiar with the national web platform Naver; it is an integral aspect of their online experience. But how familiar are *you* with Naver? This is just one example among thousands of potential international blind spots.

BEING MULTILINGUAL

Who takes your tests? In what languages? Be sure to monitor for your content in multiple different languages across the internet.

THE THREAT REMOVAL PROCESS

A PROCESS FOR MONITORING, REMOVING, AND MITIGATING ONLINE WEB EXPOSURE

1

IDENTIFY TEAM ROLES

Determine who in your organization will be responsible for online threat removal. 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. Over time, evaluate which processes are 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 (DMCA) 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

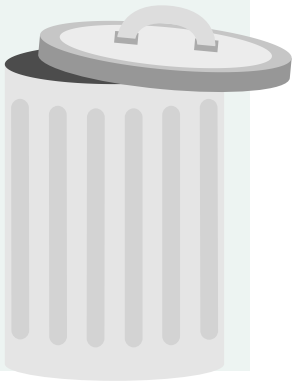
ESCALATE TO LEGAL

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.

DMCA

THEN AND NOW

There are **hundreds of braindump sites** disclosing actual exam content, with new sites **being created daily**—including thousands of affiliated blogs, filesharing sites, social media posts, and more.

While takedown notifications leveraging the Digital Millennium Copyright Act (**DMCA**) **have been effective in the past**, the sheer volume of potential sites today makes it difficult to address all of them with your limited time and resources.

Today, many braindumps never even respond to a takedown request (even after several attempts). Fraudsters often use privacy protection services, making it nearly impossible to find an address for sending a complaint. If you do make contact, a braindump owner may make claims of "fair use," knowing that the likelihood of your starting legal proceedings against them is slim. **Or they remove the material from one of their URLs, only to post it minutes later on several new sites.**

BUT BEFORE YOU GET DISCOURAGED...

DMCA IS STILL A VALUABLE TOOL!

What can your ongoing DMCA activity tell you about your program? You'll glean trends on the amount and type of braindumps that share your content, the types of platforms they target, and the number of your exams they have for sale. In conjunction with other online data you've gathered about your exams, **this information can help you identify trends and provide critical insight into the useful lifespan** of your exam items and forms.

SO HOW SHOULD YOU LEVERAGE THE DMCA?

1. **Obtain registered copyrights** to your items and tests.
2. In consultation with legal counsel, **draft appropriate DMCA language** to be sent to offending websites.
3. After finding a braindump site with stolen test content, immediately **send a DMCA notification** to the contact email on its webpage, the registered owner of the website, *and* the host of the website.
4. If no response is received within 72 hours, send the DMCA notification **again, and again**... and perhaps one more time. The fourth time may be the charm.
5. **Track and revisit** this data to plan security proactively.

NOW WHAT?

Now that you know how to find content that has been exposed online, what can you do to decrease the damages and reduce your chances of future tests getting stolen and shared in the first place?

1

Analyze Your Testing Data

Cross-examine the results of your web monitoring efforts with other data from your test takers, comparing known "Test Killers" with response data to see who may have used illicit study material.

2

Evaluate Your Online Testing Solution

Ask your online testing provider to show you the security features of your online tests that will help reduce and track content exposure—like watermarking, secure item types, and more.

3

Convert Your Item Types with DOMC™ and SmartItem™ Technology

It is now possible to build tests that self-protect from content theft, either by reducing overall exposure of your pool or by rendering braindump content unnecessary and ineffective.

4

Publicize Your Security Measures

While you're engaging in security-enhancing efforts, be sure to allude to them (or describe them) to your test takers. Send the message: "If you attempt to cheat, you will be caught."

5

AIG

It can be hard to stay ahead of exposure, so reduce the consequences! Use AIG to easily and inexpensively create a huge item bank, allowing you to republish your exam quickly whenever the need arises.

LEARN WITH US

This learning resource was created by Caveon.

At Caveon, we recognize that validity, reliability, and fairness can only be achieved when exams are secure. Quality exams that are secure benefit assessment programs, test takers, and society alike. That's why, for more than 15 years, Caveon has driven the discussion and practice of exam security in the testing industry.

Today, as the recognized leader in the field, Caveon's offerings have expanded to encompass innovative solutions and technologies that provide comprehensive protection: Solutions designed to detect, deter, and even prevent test fraud. We are committed to integrity in testing. Period.

caveon™

801-208-0103
alison.foster@caveon.com
www.caveon.com