Irdeto End-to-End Piracy

Our 5-step Program for Anti-Piracy and Cybersecurity Management

irdeto

DRM and Conditional Access
Forensic Watermarking
Concurrent Stream Management
Application Code Protection and Obfuscation

Attack Surface Management
Penetration Testing
Platform Security Assessments
STB Policy Management
Anti-Tamper

Threat Intelligence (zero-day vulnerabilities)
Live, VOD and P2P Content Discovery
Brand Protection
Anti-Fraud Management
Anti-Cheat

Threat Investigation
Reverse Engineering
Intelligence Analysis (OSINT & Infiltration)
Technical Investigations
Forensic Evidence Collection

Content Takedown and DMCA Notices
Managed Anti-Piracy Programs
Criminal and Civil Enforcement
Detailed Reports and Dashboards
Anti-Piracy Consultation

© 2022 Irdeto. All Rights Reserved.

PREVENT AND PROTECT

Using DRM and Conditional Access, an industry standard, is the first step in preventing piracy and protecting valuable content. We believe that Forensic Watermarking should be an industry standard as well, and fortunately encoder, packager and CDN standards and integrations have made watermarking content significantly easier. Concurrent Stream Management limits credential sharing and allows operators the ability to upsell additional streams. Finally, the final line of piracy defense involves code protection and obfuscation to protect software from unwanted attacks.

DRM AND CONDITIONAL ACCESS

An effective multi-DRM system provides a frictionless viewing experience, while at the same time protecting and maximizing content revenue. It keeps infrastructure costs in check and helps in untangling and simplifying DRM deployments across a variety of players, streaming formats, devices, and platforms. A multi-DRM system ensures frequent improvements to technologies such as FairPlay Streaming, PlayReady, and Widevine. It also facilitates the management of both business and license rules in a single place; thereby making it operationally easy to use and maintain.

FORENSIC WATERMARKING

Forensic Watermarking identifies the source of pirated content, whether from a specific distributor or an individual account. The extracted forensic watermark then provides irrefutable evidence to support contractual compliance, better manage distribution network/operators, or refine content acquisition/release strategies. Watermarking also allows for the rapid identification and shutdown of unauthorized streams, protecting time-sensitive valuable revenue during live events, Subscription Video on Demand (SVOD), pre-releases, festivals and more.

© 2022 Irdeto. All Rights Reserved.

CONCURRENT STREAM MANAGEMENT

Concurrent Stream Management limits the number of devices that can play content back, at any given time, on a platform. In the process it can also alert viewers if their credentials are being used on another device and possibly compromised. System logs can be continuously monitored using artificial intelligence and machine learning to ensure that new security, piracy, and fraud threats are quickly identified, investigated and addressed.

APPLICATION CODE PROTECTION AND OBFUSCATION

Threats to software security include reverse engineering, software tampering, copying, cloning, and automated attacks. A successful security strategy against these threats requires a multi-dimensional approach including data security, network security, API security as well as code protection and obfuscation. Code protection and obfuscation is often the last and most critical line of defense. Software applications can be protected to conceal proprietary algorithms and secrets, including session keys and tokens. Once protected, these applications can be safely deployed on untrusted hosts and in hostile environments such as mobile and IoT devices.

© 2022 Irdeto. All Rights Reserved.

PLATFORM HARDENING

The second step in fighting piracy involves hardening your platform to minimize the risks from hacking attempts targeting your content or back-end systems. At Irdeto we have seen countless examples where hackers have gained access to a platform and, through that vulnerability, wreaked havoc on other systems.

ATTACK SURFACE MANAGEMENT

Today's digital environments are highly dynamic and complex. Due to the extensive digital footprint, it is challenging to monitor and track all changes to your OTT platform. Systems can be hosted at different locations, various cloud providers and managed by different teams. Systems can become vulnerable.

With our Attack Surface Management (ASM) service, Irdeto's security team will periodically monitor your OTT environment. This includes a monthly attack surface overview and weekly verification service using automated scanning to search for changes, vulnerabilities and detects new security risks. We recommend customers start with a platform security assessment to get a baseline understanding of the security state of the OTT platform and use ASM to continue to monitor and find vulnerabilities before pirates do.

PENETRATION TESTING

Penetration testing is an in-depth security assessment on a specific system or component within your OTT environment, OTT application or even an important server for the OTT platform. During this test Irdeto's security team will simulate an attack by a malicious person on a selected (web) application, infrastructure or device.

Irdeto's security team offers various types of tests such as black, gray or whitebox testing. For example, a pentest on an Android OTT application includes testing the app on a mobile device, but also focuses on the communication with the backend. Furthermore, following industry best practices, static and dynamic analysis of the mobile app is performed. An example might be to test the general ease or difficulty of reverse engineering of the application. We also check the susceptibility of the app to hooking attacks and investigate the handling of key material and other sensitive assets during app execution.

© 2022 Irdeto. All Rights Reserved.

PLATFORM SECURITY ASSESSMENTS

While companies are challenged to secure all their IT infrastructure, attackers only need one unidentified vulnerability in a system. If the system is exposed to the internet, it is possible to gain unauthorized access to the internal network, including OTT platforms. A Platform Security Assessment focuses on the OTT platform and includes the security of delivering and providing access to video content. This service is part of our OTT security consulting service suite and is available at two different levels:

- A fundamental security vulnerability assessment of the OTT platform (level 1) and
- A comprehensive security vulnerability assessment (level 2).

The fundamental platform security vulnerability assessment is a time-boxed activity that scans all internet connected OTT systems for security vulnerabilities. The comprehensive platform security test goes beyond the scope of an external vulnerability assessment and identifies security vulnerabilities within the OTT platform. We do this by performing an internal network security test. The goal of this test is to provide insight into the damage an internal threat or malicious hacker can cause once access has been gained to the target network. A platform security assessment provides a comprehensive report on the current state of the platform's security, as well as a set of recommended improvements towards increasing the security status of the platform.

STB POLICY MANAGEMENT

It is vital that the firmware, new software and software upgrades on remote Set Top Boxes (STBs) are up to date. This ensures that the latest functionality is made available to the customer. Both defects from previously released software and security vulnerabilities need to be fixed and addressed as soon as possible. In addition, the application development process is shortened as some features can easily be deployed at a later stage once they have been fully developed and tested. Irdeto provides a cloud hosted over-the-air update service which includes a device and software repository, rollout management, device integration APIs, management UI and management APIs. We assist broadcasters and operators to manage this update process.

ANTI-TAMPER

Anti-Tamper prevents hackers from debugging, reverse engineering and changing the application, or to put it simply: it prevents them from stealing your digital assets. It works on top of any digital distribution platform, allowing developers to deploy the technology seamlessly into their games. By doing so, anti-tamper technology provides a crack-free window during the initial sale of a new game, when the most sales are generated. This protects the significant revenue generated during this key period.

© 2022 Irdeto. All Rights Reserved.

MONITOR AND DETECT

Our third important step in anti-piracy and cybersecurity management involves monitoring and detecting threats. This stage benefits the business strategy by recognizing the type of threats the business may encounter. Online Piracy Detection (OPD) and Brand Protection make it more difficult for pirates to find alternative sources, devices and subscriptions.

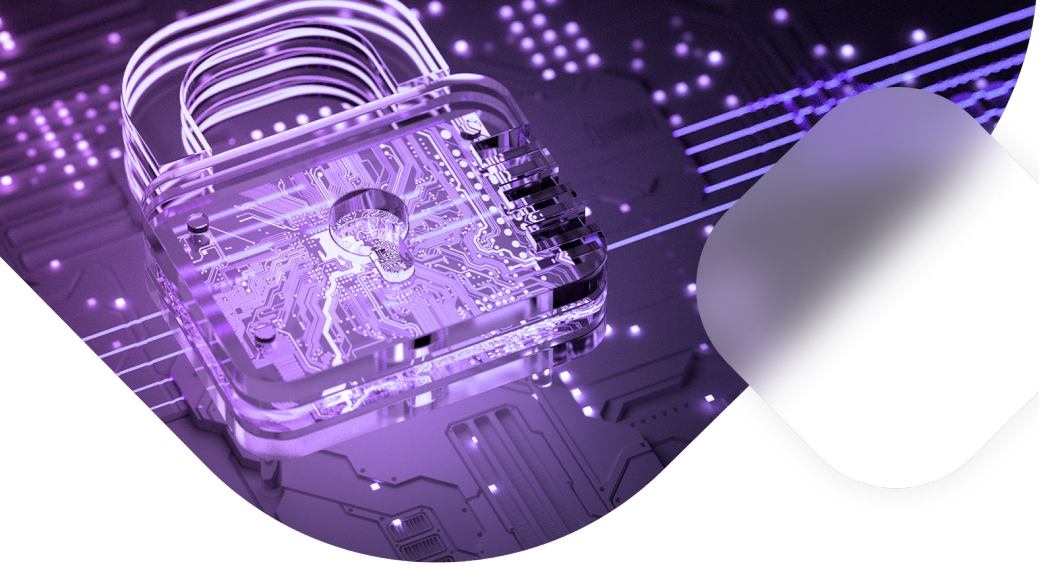
THREAT INTELLIGENCE

With this service our threat intelligence analysts monitor information gathered via proprietary web crawling, deep and dark web mining. By collecting and analyzing this data, specialists are equipped to detect new types of content piracy attacks. Our team uses specialist techniques to monitor themes, threat actors and emerging issues amongst piracy forums and groups.

LIVE, VOD AND P2P CONTENT DISCOVERY

Whether it is movies, high-profile series or live sports events, video content continues to be one of the most valuable intellectual property forms in the world. Increased screen options for consumers (phones, tablets, smart TVs, etc.) have facilitated the growing consumption of video content over the years. It is crucial to ensure that these assets are adequately protected. Irdeto's crawlers are built to discover where infringements happen on the internet. As pirate websites come and go every day, Irdeto's engineers work daily to increase and adapt coverage for as comprehensive an outlook as possible.

© 2022 Irdeto. All Rights Reserved.



BRAND PROTECTION

An effective anti-piracy strategy must include a disruption component. Irdeto's Brand Protection team uses internet crawling capabilities based on keywords and image recognition. This is supported by machine learning to detect (and remove) infringing copyright and trademark content. We have coverage across multiple social media sites, e-commerce platforms on both the open web and dark net.

All potential takedowns are analyst-reviewed and validated for accuracy. As a result of our well-established relationships with social media and e-commerce platforms, we can ensure that content is removed. We then track all reports and follow up all enforcement efforts with responses to counterclaims. This ensures the timely and justified removal of infringing advertisements.

ANTI-FRAUD MANAGEMENT

Vulnerabilities in technologies that support OTT streaming services continue to emerge. Pirates are leveraging these vulnerabilities to steal legitimate streams and sell them as their own. In effect, legitimate broadcasters end up paying for the delivery of these streams to pirate customers, without any recompense. Irdeto's Anti-Fraud Management service combines intelligence gathering, data mining and is supported by machine learning. We can then identify the vulnerabilities and misuse of OTT platforms in order to put a stop to pirates' theft of these assets.

ANTI-CHEAT

Anti-Cheat is a premium cross-platform cheat detection and prevention solution. It prevents the players of online games, playing in multi-gamer mode, from gaining an unfair advantage through the use of third-party tooling. Its binary-level integration means no game source code modification is required, ensuring that gameplay remains unaffected. Denuvo Anti-Cheat has already protected over 1,000 games and reassembled over 2 million builds.

© 2022 Irdeto. All Rights Reserved.

INVESTIGATE AND ANALYSE

Investigation and Analysis is an important fourth step in our anti-piracy program. This is where we operate on the offensive, as opposed to the defensive stance of the previous steps. It is where we find out exactly how pirate applications and devices work.

THREAT INVESTIGATION

Our investigations are structured to respond to your needs and to achieve results. We identify the threat, obtain evidence of infringement, determine the sources and their infrastructure, identify and the humans and businesses behind this threat. We thoroughly corroborate the evidence gathered across open web/dark web/social media platforms to a standard that is admissible to law enforcement. We will support 'on the ground' investigations into human and business targets to provide a clear evidential picture of the entities involved. Our team includes investigators, intelligence analysts, brand protection analysts, financial analysts and former military and law enforcement officers.

REVERSE ENGINEERING

Irdeto has experts who specialize in reverse engineering and hold advanced Offensive Security Certified Professional (OSCP) and Offensive Security Certified Expert (OSCE) credentials. Our reverse engineering service can be applied to customer applications (e.g., OTT apps) to test the robustness of the application against a variety of attack types, For example, when a pirate attempting to reverse engineer the application with the objective of stealing content directly from the OTT platform. This service can also be used to investigate new types of threats.

© 2022 Irdeto. All Rights Reserved.

INTELLIGENCE ANALYSIS (OSINT & INFILTRATION)

The management of information gathered during a covert infiltration is a specialist investigative tool. It can offer significant insights into techniques used by individuals and organizations involved in piracy. It also enables investigators to focus their efforts on those lines of inquiry which are likely to produce the best possible evidence. Our team maximizes opportunities for the extraction of high value information and evidence. We explain what is happening and to whom it may be attributed.

Our team of intelligence analysts are Open Source Intelligence (OSINT) experts that gather, corroborate, and secure important open-source information which is vital in building a solid case against high level targets. These OSINT and infiltration investigations have led to the takedown of major pirate operations in various global regions.

TECHNICAL INVESTIGATIONS

The world is increasingly connected, with billions of nodes coming online every year. As can be expected, investigations evolve with the times. Irdeto's team of investigators perform various types of investigations every day; from pirate network infrastructures, hardware modifications, hacking software, and more. Our investigators gather all necessary evidence and present it to non-technical stakeholders in easy clear, meaningful and actionable reports.

FORENSIC EVIDENCE COLLECTION

Irdeto's Cyber Forensics team has the capability to perform extensive digital forensic investigations around the world. Our experts perform on-site evidence gathering according to forensic industry standards. Follow-up analysis can be performed in one of our five secure forensic laboratories. Irdeto is also experienced in preparing detailed briefs of evidence and expert witness testimony to support both criminal and civil proceedings.

© 2022 Irdeto. All Rights Reserved.

REPORT AND ENFORCE

During this step we report and enforce, in collaboration with international partners. We work on the offensive. This can involve payment disruption, IP blocking, and takedowns, but also insights, managed services, consultations and training others in the anti-piracy/content protection community.

CONTENT TAKEDOWN AND DMCA NOTICES

A Digital Millennium Copyright Act (DMCA) notice advises a company, web host, search engine, or internet service provider that they are hosting or linking to copyrighted material. The party that receives the notice is required to immediately take down the material. Our investigators are highly experienced in this process. We know what evidence to use, when best to use it, and how to get optimal and immediate results in this busy ecosystem.

Our evidence and recommended takedown strategies have empowered our clients to tackle pirates in person and legally instruct them to stop. It has been used to negotiate the withdrawal of payment services with payment processors and disrupting pirates' business models. Using our evidence and associated takedown strategies, we collaborate with hosting companies to ensure that infringing content is promptly removed from websites. One client reported a 'career result' when a takedown strategy resulted in the removal of their content from global illicit streaming devices and services.

MANAGED ANTI-PIRACY PROGRAMS

In order to comprehensively tackle piracy, problems must be confronted with several approaches. But these can cost time and money. Irdeto's Managed Anti-Piracy Programs take out the guesswork. They provide a rich suite of products and expert services to help customers achieve the results they require and demand when faced with the significant cost of piracy threats.

© 2022 Irdeto. All Rights Reserved.

CRIMINAL AND CIVIL ENFORCEMENT

A successful investigation needs a tangible outcome, which has a meaningfully disruptive impact on the threat actor. Irdeto investigation reports are available for onward dissemination to civil or law enforcement agencies around the world. And to support you in taking civil enforcement action or making a criminal complaint. Any physical evidence gathered in our investigations will be lawfully provided, and the important chain of evidence maintained to ensure that evidence safely reaches the court room. Our investigators have successfully given evidence in both civil and criminal court rooms. Irdeto has a large network of law enforcement contacts at regional, national and international levels. We will leverage this support to ensure that legislation is upheld and intellectual property owners are protected.

DETAILED REPORTS AND DASHBOARDS

Detailed reports and digital dashboards provide our customers with actionable information at their fingertips. From impactive executive summaries to detailed operational reports, they help communicate the issue and visualize results. These products also show value to your stakeholders, at all levels of the process.

Our comprehensive target investigation reports – modelled on law enforcement intelligence products for professionalism and comprehension amongst subsequent recipients - will provide you with a clear summary of the issue and suspects. This allows decision makers to quickly understand the landscape and decide on a course of subsequent action. The investigative report will then outline in detail evidence collected as a result of technical, OSINT, community infiltration, and other evidence collection efforts. This material can be provided to your legal advisors and/or law enforcement partners for use in subsequent investigations.

ANTI-PIRACY CONSULTATION

Our internationally operating Anti-Piracy and Cyber Security team liaises with platform owners, anti-piracy bodies and law enforcement agencies around the world. We have a proven track record in identifying and disrupting cybercrime and piracy, leveraging established relationships and networks, and tracking down cybercriminals and illicit supply chains.

Our teams' diverse skill set ranges from infiltration of pirate rings, evidence collection in support of prosecution, technical analysis of platforms and breach responses. We also have in-depth expertise gained through years in law enforcement, the military and covert surveillance. Through these extensive skills, knowledge and experience we advise our customers on their anti-piracy strategy and provide recommendations on the implementation of solutions and technology to best protect their content.

© 2022 Irdeto. All Rights Reserved.

As video entertainment and videogame delivery and consumption evolve, pirates find new ways to circumvent security technologies and steal valuable assets.

Protect your content, brand, and investments while meeting premium content security requirements.

Contact Irdeto

Irdeto is the world leader in digital platform cybersecurity, empowering businesses to innovate for a secure, connected future. Building on over 50 years of expertise in security, Irdeto's services and solutions protect revenue, enable growth and fight cybercrime in video entertainment, video games, and connected industries including transport, health and infrastructure. With teams around the world, Irdeto's greatest asset is its people and diversity is celebrated through an inclusive workplace, where everyone has an equal opportunity to drive innovation and support Irdeto's success. Irdeto is the preferred security partner to empower a secure world where people can connect with confidence.

Last modification: 26-09-2022 / 02:05 pm GMT+01:00

© 2022 Irdeto. All Rights Reserved.