irdeto
Building a Secure Future.™

Solution Overview

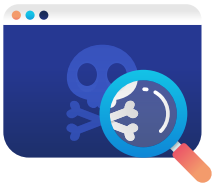
Cyber Services

Cybercrime has become one of the largest threats to the broadcast and live event streaming industries. Cyber criminals use sophisticated technology and techniques to circumvent security measures, steal content and data to generate profit from exploited vulnerabilities in infrastructure and software. Consumers are misled into buying stolen content, accounts or subscription services which are sold on websites, virtual and physical marketplaces, forums and various social media platforms. This negatively affects business models, brand reputation, productivity and profitability.

Businesses must continually invest in cybersecurity expertise to ensure that they have done everything possible to protect their investments and intellectual property. And they need to constantly stay one step ahead of the criminals. Irdeto has developed a suite of Cyber Services that help companies identify, investigate, analyze, shutdown and often prosecute threat actors. With fast moving criminals you need a full 360-degree approach to security.

The Irdeto Cyber Services unit provides this comprehensive protection with:

- Brand Protection
- Investigations & Enforcement
- Threat Risk Assessment & Intelligence
- Advanced Protection Services



KEY BENEFITS

International experts

The Cyber Services team includes investigators, legal specialists, law enforcement specialists, cryptography experts, forensic analysts, security software engineers and content security thought leaders. Their strong technical, network, social media and security skills have successfully identified, investigated and supported clients in civil and criminal prosecutions and even police raids and referrals.

360-degree security

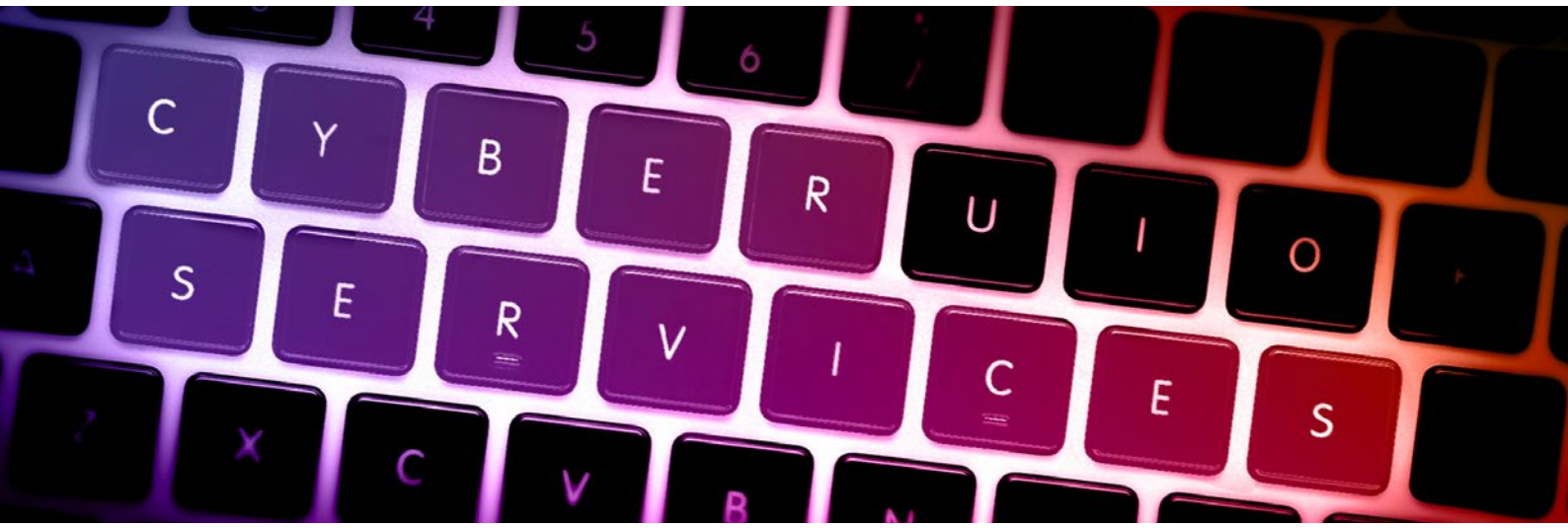
In order to stay ahead of sophisticated criminal networks, you need an end-to-end solution. Our comprehensive 360-degree view of security can be leveraged to solve diverse business threats and predict the challenges on the horizon.

Customized services

One-size does not fit all. Our tailored solutions empower our customers to continually adapt, grow and prepare for the diversity of threats that may affect them. As our customer's needs grow, we continuously advise them on best practices.

Global network of partners

Our global network of partners includes law enforcement, industry bodies, government agencies as well as consumer and technology partners. Our worldwide presence allows us to track and expose highly complex and globally operating cybercriminal networks.



BRAND PROTECTION

The sale of pirated and counterfeit products through e-commerce websites and social media are a growing challenge. Criminals utilize these websites (and other tools) to take advantage of unsuspecting consumers to buy pirated or counterfeit products on a global scale. To minimize business risk, it is essential to rapidly block the online sale and distribution of pirated and counterfeit products.

Brand Protection disrupts the online sale and distribution of illegal products and services. This is performed through a comprehensive process of identification, analyses, verification and removal of illegitimate advertisements and websites.

Our Brand Protection services:

- use automated crawlers to monitor e-commerce, social media and websites to detect infringing advertisements using keywords and logo recognition searching.
- allow IP owners and broadcasters to identify and eliminate piracy and counterfeit risks that jeopardize their revenues.
- confront unlawful resellers of illegal products and services with clear and enforceable messages that their illegal activities will not be tolerated.

KEY BENEFITS

Swiftly remove infringing content

We quickly identify pirated and counterfeit products that infringe intellectual property rights on the major global online marketplaces, social media platforms and website. Working in line with the policies set by our customer, we are able to swiftly enforce and remove the infringing advertisements. With extensive web crawling, human analysis, effective compliance and professional reporting, we provide a unique and comprehensive level of service.

Global online partners

Irdeto collaborates with major global online marketplaces and social media platforms to ensure that advertisements for pirate and counterfeit products are effectively taken down on a global scale.

Frequent collaboration with global e-commerce sites

As a key measurement to this service is to analyze the takedown rates on each online marketplace involved. Irdeto conducts a detailed analysis to identify the top infringing wholesalers and retailers. A strong working relationship with the world's largest e-commerce sites facilitates the quick and effective removal of infringing advertisements.

Tracking new threats and trends

Irdeto provides detailed threat intelligence on the most prolific advertisers of pirate and counterfeit products so our customers can focus on the delivery of their (legitimate) products and services. We also identify new piracy activities, counterfeit products, and report on emerging market trends.

AREAS OF EXPERTISE

- Copyright & trademark infringement detections (including illicit streaming devices, pirate subscription services, pirate apps & addons, stolen/compromised customer credentials, unauthorized reproductions of trademarked hard goods)
- Coverage across social media sites, e-commerce platforms, open web and dark net
- Internet crawling based on keywords and image recognition, supported by machine learning
- Analyst review and validation of all results
- Enforcement and responses to counter claims to effect timely removal of advertisements
- Online dashboard reporting via the Irdeto real-time intelligence system (IRIS)

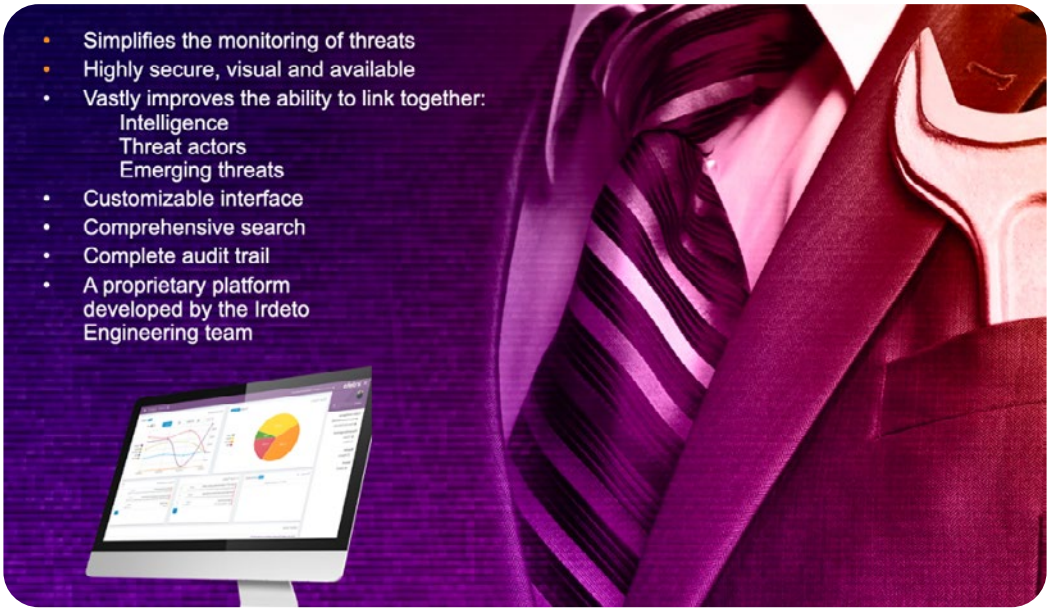


Figure 1. IRIS - Irdeto Real Time Intelligence System

INVESTIGATIONS AND ENFORCEMENT

Cybercrime and IP infringement are global, and while consumers can select from an ever-growing variety of legal services, illegal streaming services have emerged in their shadow, leveraging stolen content and off-the-shelf streaming technologies to deliver entertainment at a fraction of the cost of legitimate content providers. Here at Irdeto our investigations and enforcement team recognize the importance in identifying, preventing and defending against such cybercrime and understand how best to support our clients and take appropriate action against these threat actors.

Investigations & Enforcement provide these services:

- covert infiltration and investigations of high-profile targets
- covert infiltration and investigation of networks active in virtual currency, accounts and black markets
- test purchase and technical investigation of illicit streaming devices and services, apps, addons and websites
- acquisition and reverse engineering of tools altering gameplay, virtual economies and legitimate licensing processes
- intelligence collection and analysis
- production and management of evidence
- coordination with law enforcement bodies
- search & seizure support for raids of pirate operations
- expert witness testimony to support prosecutions
- support customer enforcement activities through civil litigation and criminal prosecution

Our team has broad legal, security consulting and law enforcement expertise and a wealth of experience in preparing casework and liaising with lawyers and prosecutors on a global scale. This ultimately reduces the risk and protects the bottom line.

Figure 2. Key Relationships & Partnerships

KEY BENEFITS

Multi-disciplinary expertise

Customers have a single partner who has a proven track record in each stage of the investigation and enforcement lifecycle; from performing technical and forensic device analysis, open-source intelligence research which is supported by a global network of information sources, to conducting people investigations, and providing expert witness testimony. We conduct covert and overt investigations and operate in both the digital and physical world.

Diverse network of partners

Our global network of partners includes law enforcement, industry bodies, and agencies as well as consumer and technology partners.

Control risks and costs with a tailored service

Cybercrime prevention needs differ for per customer. One size does not fit all. Our suite of services and best practices ensures that the customer is able to minimize risks while maintaining cost predictability.

THREAT RISK ASSESSMENT & INTELLIGENCE

Cybercrime is often performed by highly skilled and internationally distributed organizations who continuously search for business and consumer vulnerabilities.

The Threat Risk Assessment & Intelligence unit will:

- provide comprehensive security assessments (including open- source intelligence from multiple sources)
- ensure threats or vulnerabilities are swiftly detected and addressed
- minimize the threat of cybercriminals gaining access to business-critical systems and data
- protect the investments and rights of digital platform owners
- identify, prioritize and provide recommendations to mitigate future threats
- provide feedback from the hacker themselves about security countermeasures customers deploy

KEY BENEFITS

Comprehensive security assessments

Highly trained security consultants perform security assessments in our forensic laboratory including software application and infrastructure vulnerability scanning, wireless security testing, system configuration reviews and remote access vulnerability testing.

Intelligence, data, insights and reporting

Combining expert analyst interaction with automated tools ensures we detect and gather data on a wide range of threats from the open, deep and dark web. This data is then analyzed, categorized and assessed in-line with the specific requirements for each customer. Each threat to the customer's business is assigned a threat severity rating and one or more recommended mitigation actions. This results in tailored insights and actionable reports.

Rapidly scalable services

The Irdeto Threat Risk Assessment & Intelligence service ensures that customers are well equipped to fight the different and emerging threats by identifying, analyzing threats and ensuring enforcement. We can quickly scale up for our customers when needed.

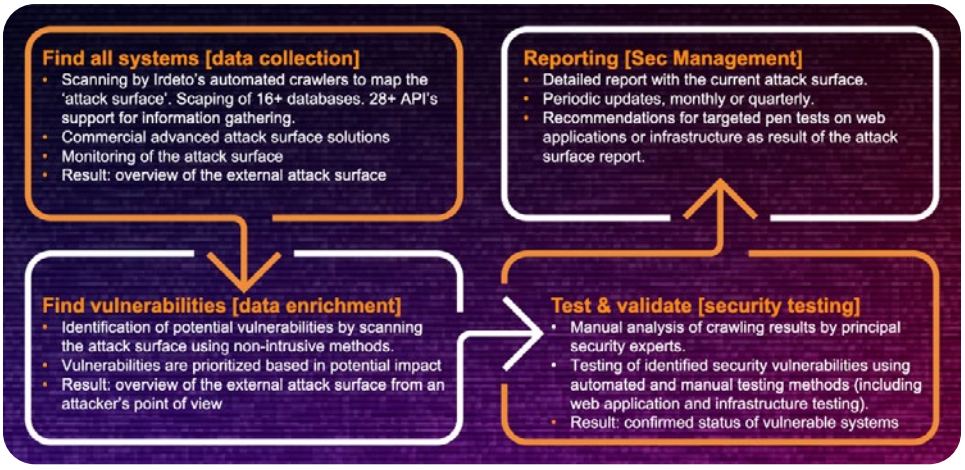


Figure 3. Cyber Security Attack Surface Management

AREAS OF EXPERTISE

Our Threat Risk Assessment & Intelligence has two primary streams of work. Firstly:

- Threat identification through infiltration & interactive monitoring of hacking and piracy communities
- Threat intelligence gathering via proprietary web crawling, deep and dark web mining
- Intelligence analysis, threat landscape reports and other visualizations
- Sentiment analysis

Secondly, you will want to improve your organizations cyber resilience by assessing your digital footprint. Do you want to know what's at risk when a malicious hacker targets your company? Our Cybersecurity experts, pen-testers and reverse engineers can help with

- Cybersecurity Resilience Programs
- Security management (e.g. advisory)
- Penetration testing (IT infrastructure, apps)
- Attack surface management (on-going security testing of all internet connected devices)
- Hardware hacking (IoT devices, routers etc.)
- Code reviews (Whitebox code review of applications)
- Reverse Engineering (apps)

Irdeto performs targeted security assessments on network (cloud) infrastructure, web and mobile applications or hardware and provides actionable recommendation to improve your security. With our Irdeto attack surface management service, your security organization will get a monthly update on your threat exposure level.

ADVANCED PROTECTION SERVICES

Advanced Protection Services is an operator's eyes and ears at every point along the digital content value chain. Minimizing risk requires more than just securing the CAS (conditional access system). These services include continuous monitoring for threats; verified breach response using flexible, effective countermeasures; restoration of platform integrity; and rapid disruption of pirates' revenue streams.

There are thousands of ways pirates can steal digital content. A vulnerability can be found and exploited anywhere along the value chain. An operator's business model relies on maintaining the integrity of their content and platform. This means an operator needs the ability to root out and resolve vulnerabilities and data leakage anywhere they occur.

AREAS OF EXPERTISE

Auditing
Physical building, operational, system, network security and CA security requirements.

Monitoring & Reporting
Threat, device, forum, and social media monitoring, anonymous monitoring and reporting (incl. illicit device analysis, watermarking and 24/7 hotline).

Planning, Response & Recovery
Enhanced security plan (with a focus on global piracy trends and anticipating on them, planning ahead of piracy), remedy plans, task force assembly with key people from different disciplines and piracy counter measure deployment planning.

Collaboration
Quarterly reports (piracy activities of clients), quarterly conference calls, with increased frequency in the event of incidents and annual security/piracy workshops.

Certification
Secure chipset certification (including liabilities and insurance) for 6 years.