irdeto

Datasheet

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.

Combining operational best practices, meticulous planning, advances in cybersecurity pioneered by Irdeto, and an extensive network of security experts, Irdeto provides proactive, comprehensive anti-piracy protection. The services include: continuous monitoring for threats; verified breach response using flexible, effective countermeasures; restoration of platform integrity; and rapid disruption of pirates' revenue streams.

MULTI-FACETED APPROACH

Irdeto Advanced Protection Services uses a five- pronged approach to ensure maximum protection from end-to-end: Auditing, Monitoring. Knowledge-Sharing, Planning & Maintenance, and Response & Recovery.

AUDITING

Irdeto Site Security Audit

Irdeto conducts an initial, mandatory security audit of the CAS and its environment. The examination extends to both CAS locations (production and disaster recovery) and to the configuration and management processes— all based on CA Site Security Certification requirements. This security check helps the operator mitigate the risk of piracy and fraud resulting from incorrect and unsafe operation of the CAS, as well as reduce vulnerability to social engineering attacks.

Deliverables

The Irdeto site security audit is guided by a comprehensive list of recommendations and requirements based on ISO 27001 and Irdeto best practices. Completion of the audit provides certification. In the case of non-compliance, Irdeto will provide improvement recommendations to the operator.

The Irdeto Site Security Certification covers:

- Physical security
- Operational security
- System and network security
- CA configuration security, including KMS version & settings

Mandatory re-certification of the CAS site is conducted on a yearly basis.

MONITORING

The true power of Irdeto Advanced Protection Services lies in its ability to detect emerging threats before they can impact the business. Irdeto employs some of the industry's most innovative and sophisticated technologies and capabilities as part of its monitoring service. Working in close conjunction with the operator's security team, Irdeto anti-piracy experts provide comprehensive, proactive, end-to-end protection tailored to the operator's unique risk profile.

Deliverables

Threat monitoring and reporting:

- Monitoring and technical analysis of piracy threats in conjunction with the operator's anti-piracy specialists, a global network of informants, and experts in other IP industries
- Anonymous monitoring of social media and public and private internet forums for credible threats to Irdeto Advanced Protection Services customers
- 24/7 automated, anonymous monitoring of known devices and logging of evidence such as IP addresses, if activity is verified
- Regular reporting on threat monitoring and investigation during the customer's Quarterly Conference Call to evaluate and determine follow up procedures, if any
- Quarterly reports about global and local industry incidents and responses

Piracy analysis and investigation:

- Investigation, analysis and reporting on specific, credible piracy threats to client devices
- Anonymous purchase and investigation of illicit devices, including technical analysis in Irdeto labs
- KMS license for client-side watermarking with detection portal access agreed upon per contract
- 24/7 hotline for piracy incident registration and guaranteed response times

KNOWLEDGE-SHARING

Piracy is continuously evolving. Keeping up with emerging threats requires knowledge of the latest piracy techniques and activities being perpetrated globally across the value chain. Irdeto's network of cybersecurity experts spans the globe investigating breaches and gathering intelligence to ensure Irdeto and its customers have the most up-to-date information available about recent attacks and threats.

Deliverables

Irdeto will conduct knowledge-sharing sessions with its customers throughout the year, including:

Quarterly Conference Call – Customized, one-to-one discussion with Irdeto experts followed by Q&A. Topics include:

- Operator's current piracy threat/risk assessment
- Incidents and issues operator experienced or is experiencing during the current quarter
- Currently known industry vulnerabilities, risk assessments, and countermeasures under development by Irdeto

Call frequency will be increased as needed in the event of a breach.

Quarterly Piracy Update – Published report distributed quarterly to Irdeto Advanced Protection Services customers. Topics include:

- Summary of current piracy activities on a global scale, with particular focus on regions specific to Advanced Protection Services customers
- Forms and methodologies of ongoing and emerging threats and currently rumored compromises within the industry
- Current piracy activities captured by Irdeto which may pose or have posed risks to Irdeto customers
- Potential and confirmed secure chipset vulnerabilities

Annual Security Workshop – This is a one-to-one interactive workshop with Irdeto experts. In addition to the topics covered in the Piracy Update, the Security Workshop will cover:

- Current Irdeto innovations, platform developments and countermeasures
- Best practices for using Irdeto anti-piracy tools to secure operator platform
- The latest piracy and security trends, and Irdeto piracy experiences in the field

This workshop can be combined with the operator's annual audit to take advantage of the most up-to-date information and enhancements.

PLANNING & MAINTENANCE

Being prepared to combat potential threats is key to minimizing the business impact of piracy. With Irdeto Advanced Protection Services, security planning and maintenance is an ongoing effort. Irdeto experts regularly develop and update operator-specific plans for maximizing day-to-day security and ensuring rapid response and recovery in the event of an attack. In accordance with these plans, Irdeto will, in cooperation with the customer, fortify the CAS against new and emerging threats by preparing the platform for countermeasures and security features.

Deliverables

Enhanced Security Plan – Customized, annually reviewed security plan designed, reviewed and adjusted in conjunction with the operator.

- Institutes requirements for CAS configuration, as well as baseline physical, operational, system and network security to ensure safe CAS operation
- Proposes short-, mid-and long-term security goals and establishes the approach and activities required to achieve these goals based on the operator's unique needs and circumstances
- Outlines the basic terms for a proposed course of action in response to specific piracy threats

Remedy Plan – Customized response plan
delivered to the operator within 30 days following a verified breach.

- Includes workarounds and countermeasures from Irdeto's proven portfolio of anti-piracy tools
- Provides for customized countermeasures and over-the-air updates for smart cards or Cloaked CA
- Other activities deemed necessary within the guidelines set forth in the Enhanced Security Plan

RESPONSE & RECOVERY

In the event of an attack, Irdeto Advanced Protection Services is ready to root out the cause, quickly recover and block the pirate's revenue stream, while ensuring customers never experience disruption or other inconvenience.

Once a breach is verified, Irdeto performs the following activities in close conjunction with the operator:

- Assembly of a task force consisting of Irdeto technical and customer care engineers, architects and anti-piracy experts
- Before a root cause is identified, Irdeto may roll out disruptive countermeasures to block the pirate's revenue stream
- Rapid deployment of effective countermeasures, which are optimized based on results and redeployed
  if necessary
- Investigation and technical analysis to discover the root cause
- Rapid development, delivery and execution of the Remedy Plan
- STB security evaluation at a 10% reduced cost

HOW WE'VE HELPED OUR CUSTOMERS

COMMON SCRAMBLING ALGORITHM UPGRADES

Common Scrambling Algorithm (CSA) is an encryption algorithm used in digital television broadcasting for encrypting video streams. Over the years, most customers have upgraded from CSA1 to CSA2. This was highly recommended due to CSA1 being insecure. Some smaller operations did not have the knowledge or manpower to do this and eventually their services appeared on pirate services; including customers from Turkey and the UK. We helped both customers to upgrade to CSA2 in less than a month. The developments of piracy at the British service were monitored by many sports customers as they carry premium content. Not only was this success story good for our reputation but also for other customers with premium sports content.

OTT LOG FILE ANALYSIS

Irdeto was requested by a customer to investigate potential content theft of their OTT platform. Pirate services were streaming high-quality content of the customer and intelligence collected on the illicit streaming service indicated that the content was indeed sourced directly from the OTT platform by abusing legitimate user accounts.

The Irdeto team investigated the piracy threat by collecting further intelligence on the pirate operation and by analyzing multiple datasets of the OTT platform. Due to the extensive OTT security expertise of our technical analysts, they were able to quickly identify anomalies in the customers OTT data, which showed abuse of the OTT system. With ongoing support from the Irdeto team, new anomalies were detected and attempts by the pirates to bypass newly implemented security measures could be blocked.

As a result of on-going technical OTT investigations, analysis of multiple OTT datasets and innovative blocking methods, the activities resulted in the unavailability of the customers content on the illicit streaming service.

HOW WE'VE HELPED OUR CUSTOMERS

COMPLEX INVESTIGATION OF A PIRATE STREAMING OPERATION

A valued Irdeto customer requested investigative support into an active piracy threat. Intelligence about the pirate operation was identified which indicated that this operation was specifically targeting the customers' content. The content was offered in many different ways and channels and was even wholesale (i.e. selling streaming devices in bulk to resellers), making this streaming pirate a significant streaming threat.

The Irdeto anti-piracy team supported the customer with a covert investigation, which included making test purchases directly from the pirate and technical investigations into the provided devices and service. As result of an ongoing investigation, persistence and expertise combining OSINT with data acquired during the technical and covert investigation, the Irdeto team was able to identify an identity behind the streaming pirate operation.

As result of this investigation, the team was able to create a comprehensive case file including evidence about the streaming operation which helped tremendously with forwarding the casework to law enforcement in the Netherlands.

BROADCAST WATERMARKING HARDENING

Irdeto's watermarking solution TraceMark – along with the acclaimed Online Piracy Detection solution – enables content owners, broadcasters and OTT providers to efficiently protect content at all stages of the value chain. Back in May 2020 we hardened our broadcast watermarking product. During a watermarking deployment at a customer we found that pirates had countered our standard watermarking, i.e. the way watermarking was operating. We came up with two new innovative solutions which were subsequently implemented. At the end of the year, we were able to test these new features which successfully improved detection with multiple cards (collusion) and detection speed.

HOW WE'VE HELPED OUR CUSTOMERS

REVERSING A PIRACY SECURITY EXPLOIT

As part of Irdeto's ongoing intelligence gathering into pirate activities, an anomaly was identified with a streaming pirate service. It appeared that the pirate service had found a method that bypassed an anti-piracy measure known as "fingerprinting" on set-top-boxes (STB's) that were used by the customer. This is cause for concern, as STB's are typically well protected against modifications to protect video content against streaming piracy.

The information was shared with the customer and a collaborative investigation was started into the pirate service with the objective to find out how the pirate was able to modify the STB. The customer was able to obtain a STB which was sold by the streaming pirate. After an initial investigation by Irdeto's team it was confirmed that the pirate service was indeed able to block fingerprints that were sent to the device. We initiated an in-depth technical investigation focusing on the possibility of a hardware or software vulnerability that was exploited by the streaming pirate. This process of reverse engineering the STB to identify the security vulnerability that was abused, resulted into a technical report that revealed that the streaming pirate had indeed modified the software on the STB. The exploit could be linked to the STB manufacturers code.

As result of Irdeto's in-depth technical analysis of the STB security exploit, the vulnerability was resolved via a close collaboration between the customer, STB manufacturer and Irdeto. Furthermore a plan was provided for new firmware developments to improve the STB's security level in the future.