irdeto

Datasheet

Threat Risk Assesment & 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.

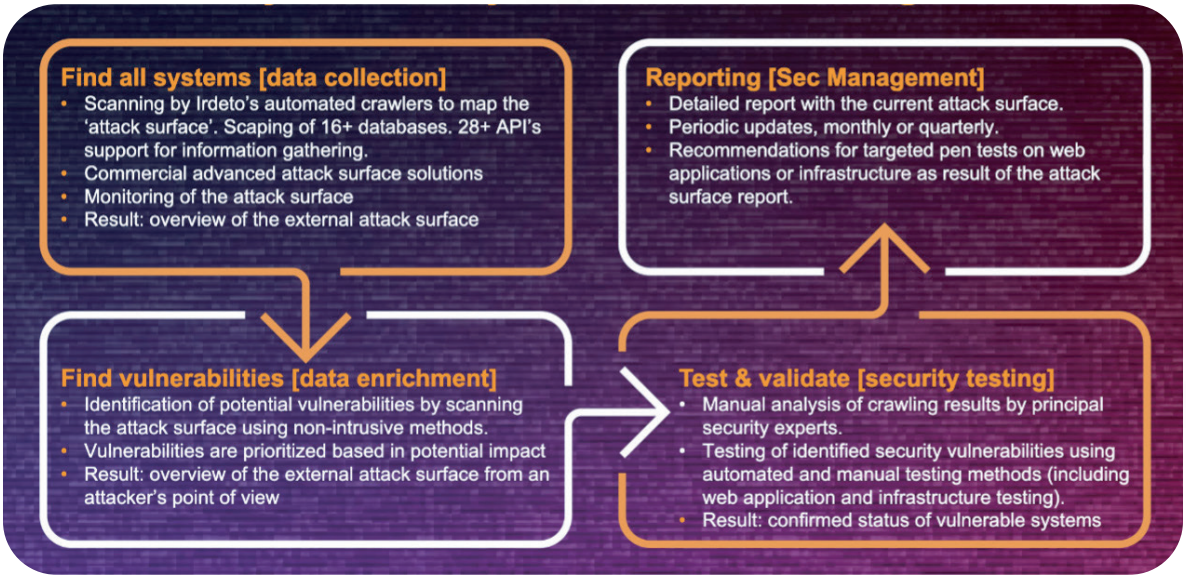

Figure 1. Cyber Security Attack Surface Management

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.

THREAT RISK ASSESSMENT & INTELLIGENCE

GEOGRAPHIC MAPPING OF HIGH-SPEED INTERNET PIRACY

Irdeto was engaged by a tier 1 cable operator to assess the theft of service affecting their highspeed data and video infrastructure. Due to the nature of the infrastructure, it was very important for our team to map out which threats were happening in what location. As a result, the operator was able to better target problematic areas, save on bandwidth and to sign up more customers.

THREAT MITIGATION AND ACTOR'S IDENTIFICATION

Irdeto was engaged by multiple tier 1 videogame publishers to assist them in the identification of actors posing threats to their intellectual property (piracy), user experience (cheats), user security (accounts) and employee security (threats to employees).

In the end, after identifying the main actors involved, Irdeto assisted the legal actions undertaken both in and out of court. Alongside the actor's identification we provided threat mitigation with investigation support, court expert testimonies as well as domestic and international law enforcement relation support resulting in the termination of harmful activities by the actors.

ACQUISITION AND TESTING OF CHEATING SOFTWARE ON A GLOBAL BASIS

Irdeto was approached by a tier 1 video games publisher to help them tackle cheating problems plaguing several of their titles. Irdeto not only acquired and tested the usability of these cheats, but also provided additional intelligence to support further development of their systems and to increase robustness. In the end, Irdeto is happy to report a downward trend in the number of cheats available on the covered titles.

SENTIMENT ANALYSIS

Irdeto was engaged by a tier 1 video games publisher to analyze the negative sentiment plaguing their brand. It was suspected that bad actors had launched an astroturfing campaign against them. In the end, after identifying the main actors involved, Irdeto allayed the fears of the customer and supported them in turning the negative sentiment into a positive one.

CYBERSECURITY SUCCESS STORIES

HARDWARE AND FIRMWARE SECURITY REVIEW

The Irdeto team was requested by a tier 1 cable operator to perform a security review of a set of routers. As result of the security review, Irdeto identified multiple significant security vulnerabilities in the router. These security vulnerabilities included bypassing security measures via physical access, a backdoor used for testing purposes in production and a third-party configuration error causing the device to be susceptible to a man-in-the-middle attack. As a result of Irdeto's review, the customer was able to fix all identified security vulnerabilities.

INCIDENT RESPONSE AND VIDEO PLATFORM SECURITY REVIEW

Irdeto supported a customer during a security incident. A malicious hacker was able to send messages to thousands of set-top-boxes. Support was provided on-site during the incident and it was found that due to a misconfiguration, an internal device was publicly exposed.

As result of the incident, the customer decided to perform a comprehensive (video) platform wide security review. Irdeto supported by a pentest of all internet exposed video systems. As a direct outcome of the security review significant amounts of high-risk vulnerabilities were identified and mitigated. This included detecting a second misconfiguration what caused the initial hack to happen.

CYBER RESILIENCE PROJECT

Irdeto has been supporting a large video operator with a cyber resilience project. This project provides our customer with a monthly attack surface report which includes ongoing consultancy support to improve security related processes and procedures.

As a direct consequence of this project over 1000 servers are now monitored on a daily basis and over 100 high-risk security vulnerabilities have been reported. Furthermore, many procedures and process have been improved and pragmatic incident response plans tailored to the customers situation have been created and implemented.

CYBERSECURITY SUCCESS STORIES

FORENSICS SUPPORT AS PART OF LITIGATION

Irdeto was requested by a video rightsholder to provide support to their lawyer agent as part of a litigation process. The request was to perform a technical analysis of a streaming device, including memory analysis and produce a detailed technical report about the operation of the IPTV streaming device as evidence. To maintain the chain of custody, the IPTV device was collected by Irdeto's Cyber Forensic team and analyzed in a forensic lab.

During the analysis the streaming application was reverse engineered and the memory of the IPTV streaming device was dumped. The video packets in the memory dump were reconstructed to video as part of the forensic procedure. All findings were reported. And the evidence was successfully presented by Irdeto's Cyber Forensics team to the attorney general.

ANTI PIRACY RAID SUPPORT

A rightsholder requested Irdeto to provide technical expertise and forensic support during an IPTV raid operation. Irdeto provided on-site support during the operation by examining the IPTV streaming operation. As a result of Irdeto's support, the suspect was prevented from being able to destroy crucial evidence during the raid such as financial data and passwords to access administrative panels.

FORENSICS SUPPORT

A rightsholder requested that Irdeto provide technical support during a disruption activity of five IPTV streaming applications that provided unauthorized access to their content. Irdeto supported the customer by exploring methods to disrupt the IPTV services and present this to a group of internet service providers and the regulator.

During the operation, Irdeto supported with continued monitoring of 5 IPTV streaming applications and provided multiple daily technical updates on the status of the streaming application as well as the command&control infrastructure. As result of this support, the illicit streaming operations were disrupted.

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.