JAYMON SECURITY
Cyberintelligence & Solutions

PRESENTATION

Dear clients,

It is a pleasure to present our service portfolio and to thank you in advance for taking the time to get to know us.

At Jaymon Security, our focus is cybersecurity. Our company was founded by two professionals with extensive experience in business IT and cybersecurity, who decided to offer distinctive solutions based on technical excellence and personalized service.

Our service offering is built on three pillars:

Proprietary methodology focused on quality:

We apply rigorous quality processes at every stage of the project, from the initial analysis to the delivery of reports and follow-up, ensuring reliable, transparent results tailored to your business.

Senior multidisciplinary team:

We have senior specialists in all key areas of cybersecurity (pentesting, audits, hardening, digital forensics, etc.), as well as in regulatory compliance (GDPR, ENS, ISO 27001, etc.) and traditional IT services (development, maintenance, and consulting).

Training and awareness:

We believe the best defense starts with the user. That is why we design customized training programs and awareness campaigns to minimize risks arising from the unsafe use of systems and applications.

Without further ado, we invite you to explore our service portfolio. We are confident that you will find in it the most suitable solution for your present and future needs.

Fernando Romero

Operations Director

INTRODUCTION

To facilitate your review, the services included in this catalog are grouped into the following categories:

- **Cybersecurity:** Cybersecurity audits, Red Team Operations (RTO), consulting services, incident response, and digital forensics.
- **Cyber Intelligence:** Intelligence services based on open sources, including the Deep Web, Dark Web, and Marianas.
- **Information Security and Compliance:** Internal audit and consulting services for regulatory compliance (ENS, GDPR, ISO 27001, etc.).
- **Application development and cloud infrastructures**: Consulting and development services for creating tailored applications and secure cloud infrastructures.
- **On-site and Online Training:** Tailored awareness and practical training services.
- **CISO as a Service:** Coverage of the role of Chief Information Security Officer by a senior multidisciplinary team.
- **SIEM as a Service:** Provides organizations with a fully managed Security Information and Event Management (SIEM) solution, delivered from the cloud or on-premise according to business needs.
- **Consulting, deployment, and integration of cybersecurity tools:** Comprehensive service for the installation, operation, and maintenance of cybersecurity applications.

With this variety of services, we aim to provide comprehensive solutions to any cybersecurity need your organization may have.

CIBERSECURITY

Within the group of cybersecurity services, we have included the following categories:

- Cybersecurity audits.
- Red Team Operations (RTO).
- Consulting and Incident Response Support.
- Digital Forensics (DF).

Each of these categories is described and detailed below.

CYBERSECURITY AUDITS

This category covers all analysis services aimed at identifying vulnerabilities and security weaknesses in **operating systems** (Windows, Linux, macOS, Android), **cloud platforms** (Azure, AWS), and **applications** across different environments (Web, mobile – Android/iOS – and desktop for Windows/Linux).
Depending on the activities carried out and the objectives pursued, we can provide the following types of audit services, which increase progressively in complexity and depth:

- **Vulnerability Assessments:** These services represent the first step toward cybersecurity excellence in your organization. They include scanning and analysis activities to identify potential vulnerabilities in your systems, web or desktop applications, as well as in your cloud infrastructures. To carry them out, we combine the most advanced commercial tools with the expertise of our auditing staff, resulting in comprehensive vulnerability reports.

- **Penetration Testing (Black Box):** These more advanced services consist of performing penetration tests on systems, cloud infrastructure, or applications without any prior information about them, using both manual and automated tools. The objective is to identify and exploit real vulnerabilities, providing your organization with evidence of exploitation along with remediation recommendations.

- **Security Audits (Gray and White Box):** These services build upon the previous ones but cover a broader exposure surface, since their execution relies on internal information about the system being audited (source code, operating manuals, etc.). This allows for much more specific testing, achieving greater depth in both static and dynamic vulnerability detection.

- **Wireless Network Audits:** These services consist of running various detection and exploitation tests on wireless networks with the aim of providing adequate measures to secure them, thus preventing unauthorized access by cybercriminals

seeking to misuse them.

For all the services above, detailed reports are generated containing the vulnerabilities identified, their severity, and the corresponding remediation recommendations. Priority is given to exploitable vulnerabilities, accompanied by exploitation evidence.

As a complement to the previous services, the following offering is presented, which is key to closing the cybersecurity loop:

- **Application Development Lifecycle Evaluation and Enhancement:** A service designed for clients who develop their own software, allowing them to evaluate, from a security standpoint, the entire lifecycle of the products and systems they build (analysis, design, implementation, integration, testing, and maintenance).

RED TEAM OPERATIONS (RTO)

These services consist of replicating the tactics, techniques, and procedures of a cybercriminal group targeting an organization. Such engagements are highly complex, both in preparation and execution, but they deliver unmatched value since the results are 100% realistic and test all your organization's security controls — including staff awareness and preparedness.

In these operations, the scope is agreed upon in advance with the client, defining the success criteria and the extent of the exercise. Tests may include physical intrusion into client facilities, social engineering (targeted phishing campaigns), creation of custom malware designed to connect with external Command & Control (C2) systems, evasion of perimeter security controls and antivirus solutions, among others.

Through these exercises, organizations obtain a clear and realistic assessment of their security posture, gaining highly specific and practical insight into both the strengths and weaknesses of their infrastructure, personnel, and procedures.

CONSULTING, INCIDENT RESPONSE & DIGITAL FORENSICS

This group includes the remaining cybersecurity-related services we can provide, ensuring full coverage of your organization's needs.

- **Consulting:** General cybersecurity consulting: best practices, procedures, common attack vectors, etc. We can also identify, assess, and recommend commercial products tailored to your requirements, compatible with your existing enterprise infrastructure, and aligned with your budget.

- **Incident Response Support:** When needed, we provide guidance on the most effective ways to respond to specific security incidents. This also includes consulting services for incident management in relation to the General Data Protection Regulation (GDPR) and the Spanish Data Protection Agency (AEPD). Our consultants assist with incident handling, documentation, and reporting to the AEPD when the severity of the incident requires it.

- **Digital Forensics (DF):** This analysis service focuses on identifying the root cause of an incident, determining its scope, and recommending mitigation measures to prevent recurrence. The types of digital forensic analysis we offer include:

    - **System Forensics:** Analysis of physical hard drives, virtualized images, RAM, live systems, and devices.

    - **Mobile Forensics**: Examination of evidence collected from mobile devices.

    - **File Forensics:** Primarily the analysis of office documents (Word, PowerPoint, etc.).

    - **Malware Analysis:** Examination of binaries and scripts posing security threats (e.g., trojans, ransomware).

    - **Email Forensics:** Analysis of different types of emails (e.g., phishing).

    - **Network Forensics:** Examination of inbound and outbound network traffic to identify potential cyberattacks (malware downloads, phishing, sensitive data exfiltration, etc.).

The methodology applied in these services guarantees that the generated reports can serve as admissible evidence in court, fully respecting protocols for data extraction, chain of custody, and forensic soundness.

CLIENT DOSSIERS (OSINT)

This service consists of obtaining actionable intelligence through the collection, filtering, and analysis of all publicly available information on the Internet about a natural person or legal entity.

It involves in-depth research of information offered through “open sources” — all origins of data openly available on the Internet — as well as the “Deep Web,” the “Dark Web,” and the “Marianas.”

The usual result of this type of investigative service is delivered in a report containing all relevant information for the client.

What does this information provide to the client?

- It enables the client to understand their level of exposure on the Internet and take steps to reduce it according to their interests.

- It also allows the client to identify, first-hand, whether information about leaks, attack results, etc. exists in major cybercrime forums that was previously unknown.

Why is this information relevant?

- Because it can be used in future attacks by cybercriminals. Knowing first-hand what information about a person exists in such forums helps prevent potential attacks and supports threat modeling.

- Because it can alert the client to attacks they may have already suffered but were not yet aware of.

COMPLIANCE

This group of services includes all consulting activities aimed at internally assessing the degree of compliance with different regulations. It also covers the preparation of audit reports and the recommendation of remediation measures to ensure conformity with the audited standard.

This type of service is particularly valuable when preparing for an official compliance audit or certification, as in some cases a prior internal audit is mandatory, and in all cases it allows the organization to face the process with greater confidence, knowing that requirements are already being met.

Below are the standards we are currently auditing:

- **GDPR Assessment and Implementation**: Internal audit and evaluation of the organization's current level of compliance with GDPR. Includes auditing of data processing activities, purposes of data use, etc., identification of gaps, and recommendations for full implementation.

- **ISO 27001 Assessment and Implementation:** Internal audit and evaluation of compliance with the ISO 27001 standard. Includes identification of requirements to be met and recommendations for implementation.

- **ENS (National Security Framework) Assessment and Implementation:** Internal audit and evaluation of your organization's compliance with the Spanish National Security Framework. Includes identification of requirements to be met and recommendations for implementation.

JAYMON SECURITY
Cyberintelligence & Solutions

ON-SITE AND ONLINE TRAINING

We currently offer the following types of training. In addition, we are available to organize training sessions on these or other topics tailored to your specific needs.

To deliver these courses and awareness programs, we provide labs and tools that allow participants to put into practice what they have learned:

- **Secure Development Training:** Training for developers to integrate cybersecurity throughout the entire lifecycle of their projects. This course includes hands-on exercises.

- **Cybersecurity Training – Ethical Hacking:** Training for professionals to get started and deepen their knowledge in cybersecurity through one of its most engaging areas: ethical hacking. This training complements the secure development course and includes also hands-on exercises.

- **Security Awareness:** Training for organizational staff aimed at raising awareness of the critical importance of cybersecurity in all areas. The training covers employee activity both inside and outside the company and includes practical workshops and collaborative activities.

- **Phishing Campaigns:** As a complement to awareness and training actions, we conduct targeted malicious email campaigns to:
    - Evaluate the level of awareness and alertness among employees.
    - Assess the effectiveness of previous training sessions.

APPLICATION DEVELOPMENT AND CLOUD INFRASTRUCTURES

This group of services includes both pure software development projects and secure cloud infrastructure projects (mainly on Microsoft Azure), as well as the combination of both.

The advantage of our projects over the competition is that **security is built in from the start**, ensuring that best practices and methodologies are considered from the initial stages through to project completion. Our applications are internally audited at each iteration of the development process so that, if any security-related corrections are required, they can be implemented as early as possible — saving both time and money.

To further secure systems, we also offer the option of deploying developed applications in Microsoft Azure on infrastructures designed and implemented by our team, once again placing security as a primary objective. The infrastructures we design and implement in Azure leverage the components available within the Azure ecosystem (WAF, DDoS protection, secure key vaults, etc.).

JAYMON SECURITY
Cyberintelligence & Solutions

CISO AS A SERVICE

The role of **Chief Information Security Officer (CISO)** is highly specialized and in high demand. The investment of time and money required to bring a reliable CISO on staff often exceeds both the timelines and budgets available. A true CISO profile combines knowledge and experience in areas such as cybersecurity, information security, compliance, and software engineering. As we have mentioned, this makes finding the right candidates extremely challenging.

To address this need, we have designed our **"CISO as a Service"** offering, which provides rapid and much more cost-effective coverage compared to the traditional hiring process. Under this service, a dedicated professional assumes the responsibilities of CISO on-site and serves as the main point of contact with your organization. Supporting this role is our **CISO Office**, a team of senior professionals with expertise in different areas. This way, we consolidate the combined experience of all our experts into a single service.

This service can also support newly appointed CISOs, providing assistance during their initial period in the role. The CISO Office offers strategic and tactical support, covering both general security strategy and specific issues that may arise.

JAYMON SECURITY
Cyberintelligence & Solutions

CONSULTING, DEPLOYMENT AND INTEGRATION OF CYBERSECURITY TOOLS

At Jaymon Security, we aim to be your trusted partner in the field of cybersecurity. To this end, we have developed this service for the consulting, deployment, and integration of cybersecurity tools for Security Operations Centers (SOC).

This comprehensive service covers all the necessary steps — from identifying the need to delivering the final solution. In this way, we simplify the process of incorporating and operating new elements into your organization's security architecture.

We can provide either full or partial coverage, advising or intervening at any stage of the process as required.

Special attention is given to small and medium-sized enterprises seeking compliance and certification under frameworks such as the **Spanish National Security Framework (ENS)**. We deliver fast-to-integrate, cost-effective solutions that facilitate consistent compliance within record timeframes.

JAYMON SECURITY
Cyberintelligence & Solutions

SIEM AS A SERVICE

Our SIEM as a Service offering provides organizations with a fully managed Security Information and Event Management (SIEM) solution, delivered from the cloud or on-premise according to business needs.

We take care of the deployment, configuration, integration, and continuous operation of the SIEM platform, ensuring that security logs from servers, applications, endpoints, and network devices are collected, correlated, and analyzed in real time.

Key benefits include:

- **24/7 monitoring and alerting** on potential threats and anomalous behaviors.
- **Expert analysis** by our security team to reduce false positives and highlight critical incidents.
- **Regulatory compliance support** (ENS, GDPR, ISO 27001, etc.) through comprehensive reporting and evidence retention.
- **Scalability and flexibility**, adapting to the growth of your infrastructure without additional complexity.

By outsourcing SIEM management, your organization gains advanced detection and response capabilities while reducing the operational burden on internal teams, allowing them to focus on strategic security initiatives.

We hope the services presented meet your needs, and that we will be able to work together soon.

If there is any other service you require that is not included in this presentation, please contact us at info@jaymonsecurity.com — we will be glad to assist you.