
jtsec
Applus
Experiences evaluating
cloud services and products
INTERNATIONAL COMMON
CRITERIA CONFERENCE
WASHINGTON DC

JAVIER TALLÓN GUERRI

jtsec Beyond IT Security

jtallon@jtsec.es

- Computer Engineer (University of Granada)
- Co-Director & **Technical Manager at jtsec** Beyond IT Security
- Member of **ENISA ad-hoc Working Group** on SOG-IS successor scheme.
- Co Editor of ISO/IEC TS 9569 **Patch Management** Extension for the ISO/IEC 15408 series and ISO/IEC 18045
- CyberSecurity **Teacher** at UGR (University of Granada)
- **OSCP/OSCE/CISSP**

INDEX

ENS (RD 311/2022)

Artículo 19. Adquisición de productos de seguridad y contratación de servicios de seguridad.

- En la adquisición de productos de seguridad o contratación de servicios de seguridad de las tecnologías de la información y la comunicación que vayan a ser empleados en los sistemas de información del ámbito de aplicación de este real decreto, se utilizarán, de forma proporcionada a la categoría del sistema y el nivel de seguridad determinados, aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición

Article 19. Procurement of security products and contracting of security services.

- In the acquisition of security products or contracting of information and communication technology security services to be used in the information systems within the scope of application of this Royal Decree, those that have certified security functionality related to the object of their acquisition shall be used, in proportion to the category of the system and the determined security level.

CERTIFICACIÓN DE CONFORMIDAD CON EL

ens
Esquema Nacional de Seguridad

Categoría ALTA

RD 3/2010

CPSTIC Catalogue

What is it?

CPSTIC is the reference catalogue for cybersecure ICT products in the Spanish Public Administration. It offers a **list of products with security assurance contrasted by the CCN (the Spanish Certification Body)**.

This catalogue includes **approved products** for handling classified national information qualified products for use in the ENS (a.k.a. the governmental 27001).

Advantages

1. Easy acquisition of cybersecure products.
2. Evaluated by a reliable third party.
3. Available to everyone (not just the administration).

CPSTIC CATALOGUE

Cybersecurity evaluation methodologies

- Fixed-time methodology
- National scope
- Comprehensive standard oriented to vulnerability analysis and penetration testing.
- Limited duration and effort
- Economically feasible
- Accesible to SMEs
- Main use for catalogue inclusion
- Spanish National Standard

Medium-basic ENS category

- Heavy methodology
- International scope, recognized in more than 30 countries
- Different assurance levels
- Versatile, applicable to all types of products
- Technically hard to meet/understand the standard
- Longer time to achieve
- Higher economic cost

High ENS category

CPSTIC Catalogue

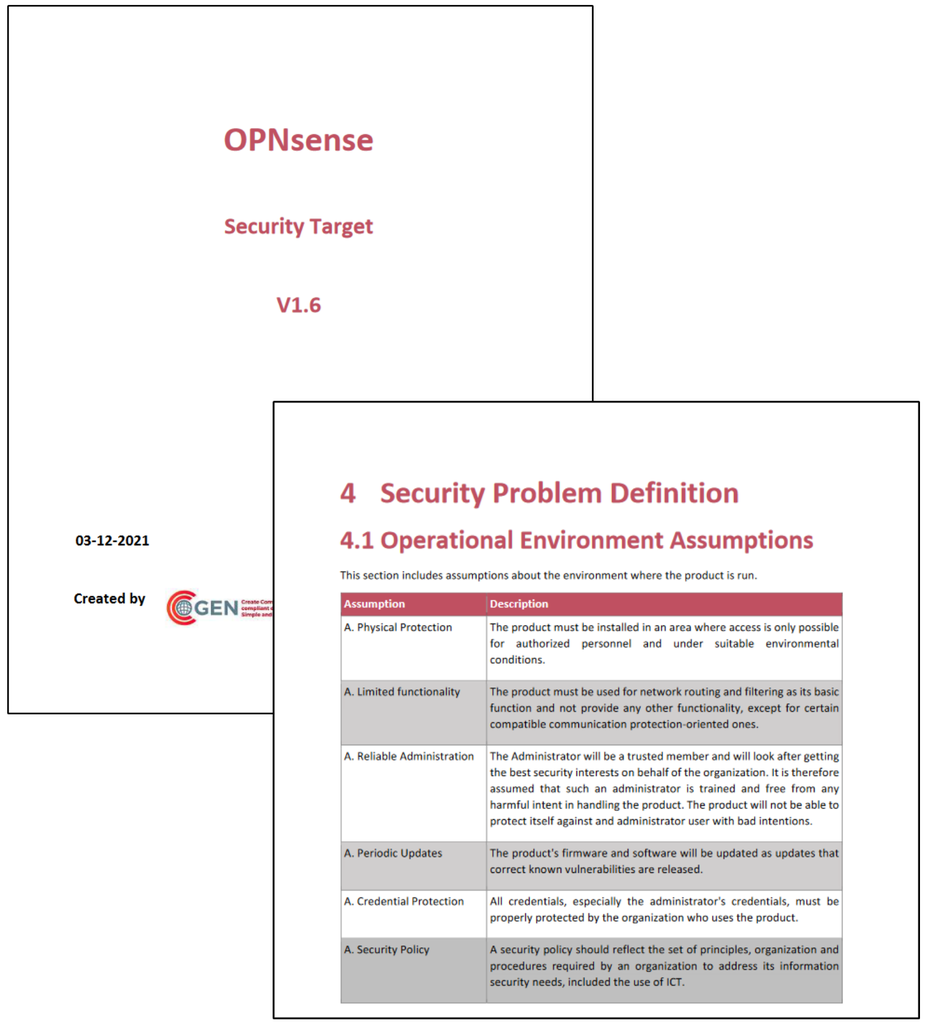
Security Target and taxonomies

- The ST (Security Target) collects the security functional requirements implemented by the TOE, as well as the security problem definition.

The taxonomies define a set of security functional requirements. E.G. The EDR/EPP taxonomy defines the following requirement (one among many) that every TOE that wants to enter the catalog under the EDR/EPP family must fulfill.

Contents of the ST are reviewed by CCN before approval, avoding scoping or TOE vs Product problems.

38. **MAL.1** En caso de que se detecte contenido malicioso en el espacio de memoria de un proceso, se deberá interrumpir la ejecución del mismo.



OPNsense

Security Target

V1.6

03-12-2021

Created by

4 Security Problem Definition

4.1 Operational Environment Assumptions

This section includes assumptions about the environment where the product is run.

Assumption	Description
A. Physical Protection	The product must be installed in an area where access is only possible for authorized personnel and under suitable environmental conditions.
A. Limited functionality	The product must be used for network routing and filtering as its basic function and not provide any other functionality, except for certain compatible communication protection-oriented ones.
A. Reliable Administration	The Administrator will be a trusted member and will look after getting the best security interests on behalf of the organization. It is therefore assumed that such an administrator is trained and free from any harmful intent in handling the product. The product will not be able to protect itself against and administrator user with bad intentions.
A. Periodic Updates	The product's firmware and software will be updated as updates that correct known vulnerabilities are released.
A. Credential Protection	All credentials, especially the administrator's credentials, must be properly protected by the organization who uses the product.
A. Security Policy	A security policy should reflect the set of principles, organization and procedures required by an organization to address its information security needs, included the use of ICT.

CPSTIC Catalogue

Evaluation, certification, qualification

Evaluation

An independent, accredited laboratory verifies whether a product meets its claimed security functionality in a time and effort constrained manner.

Certification

The Certification Body issues a certificate according to the security functionality stated by the manufacturer.

Qualification

A certification has been passed according to the security functionality required by CCN.

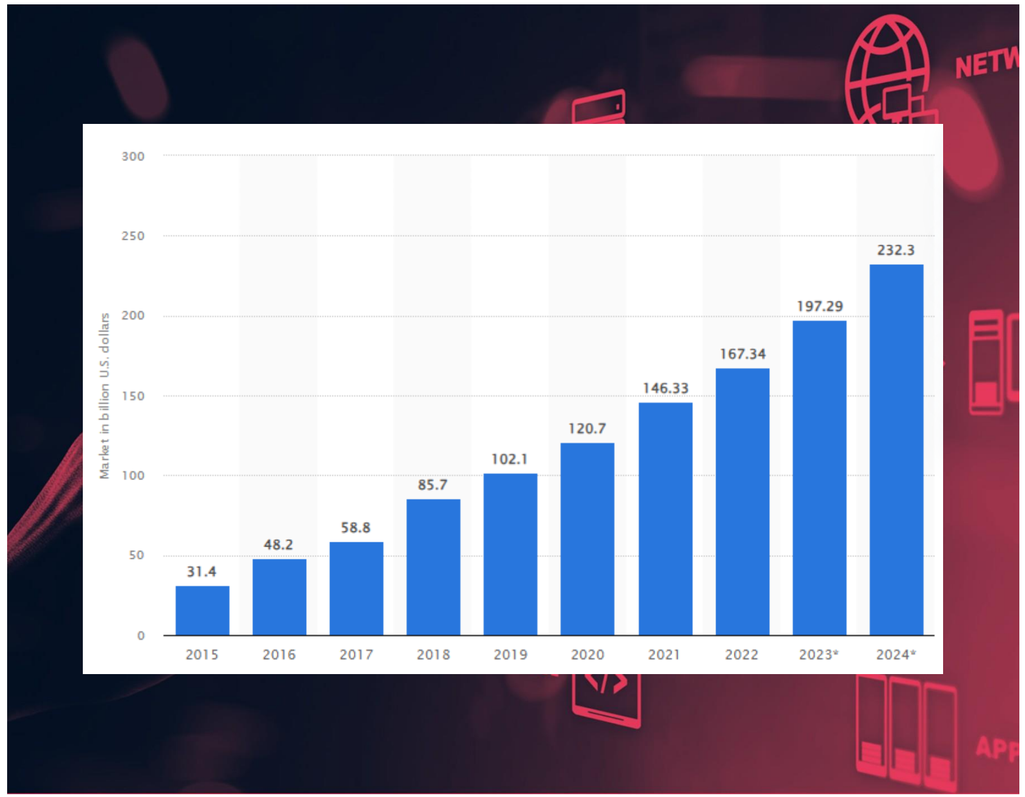
WHAT ABOUT THE CLOUD?

More and more SaaS

- The SaaS market is currently growing by 18% per year.
- Around 85% of small businesses have invested in SaaS options

Existing methodologies are product-based

- Common Criteria
- Spain (LINCE), France (CSPN), Germany (BSZ), The Netherlands (BSPA).



WHAT ABOUT THE CLOUD?

IT-015 Requirements for certification of products deployed in the cloud

REQ-2

Desployed in the lab

REQ-3

Full control of the infrastructure

REQ-5

Functionality provided by the infrastructure is outside the scope

REQ-6

Univocal identification

WHAT ABOUT THE CLOUD?

Common Criteria efforts

The CCUF TC “The CC in the Cloud Technical Work Group (CCitC)" is developing a guide of Essential Security Requirements for Common Criteria in the cloud.

*https://github.com/CC-in-the-Cloud/CC-in-the-Cloud.github.io/blob/main/ESR/CC_in_the_Cloud_ESR.pdf

The National Information Assurance Partnership (NIAP), Canada Common Criteria Scheme (CCCS), and Australian Certification Authority (ACA) agree with the content of the CC in the Cloud Essential Security Requirements (ESR), version 0.3, dated 2 March 2022.

*https://www.niap-ccevs.org/MMO/GD/CC%20in%20the%20Cloud%20Position%20Statement%20v1.0.pdf

WHAT ABOUT THE CLOUD?

Evaluation, certification, qualification

Known evaluation gaps

- Analysis is static
- Use of cryptography
- Platform abstraction
- Environmental evaluation

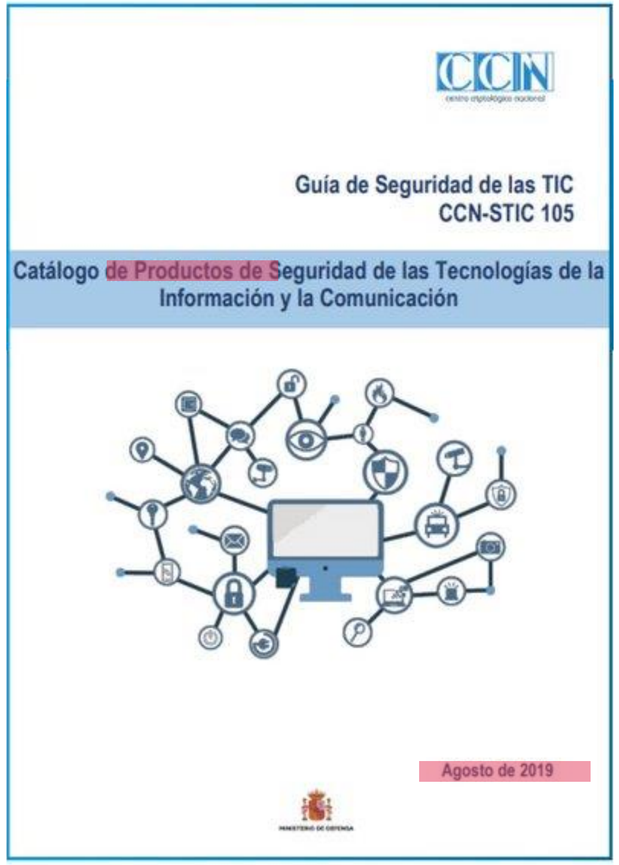
New threat models

- Configuration
- Credentials
- Data sovereignty
- Key management
- Insider threat
- Multi-tenant

The current standard does not allow for service evaluations. We are focused on product evals in a devops deployment

SO, HOW CAN WE QUALIFY SERVICES?

CPSTIC CATALOGUE



Very practical approach: we **need** secure services

QUALIFYING SERVICES

History of the CCN-STIC 106 Guide

Naive approach

1. On-premise certification (including methodology pentesting)
2. Deployment in the cloud
3. Pentesting in the cloud (5 days)
4. + ENS cloud provider

Problem: Most cloud services are cloud-native

Most common approach

1. We use LINCE adapted to the cloud on top of the already deployed service
2. No additional pentesting required as it is already included in the initial LINCE-based assessmentl
3. + ENS cloud provider

Problem: Who qualifies the hyperscaler services?

Connecting all the dots

1. Hyperscaler services also want to be qualified

QUALIFYING SERVICES

Task 1: Requirements Analysis

- The first task consists of defining to which taxonomy the service to be qualified belongs. In addition to the appropriate taxonomy, every cloud service must fit into another taxonomy "Cloud Services" (Annex G).

- The next step is to analyze the service, defining its components and the scope of the TOE. After this, a new document, the SFR Rationale is generated in which all the SFR included in the taxonomy are listed and the following labels are applied to them

APPLICABLE | **NOT APPLICABLE** | **COVERED**

WITNESSING | **VENDOR AFFIRMS**

QUALIFYING SERVICES

Task 2.1 ST Writing

- After finishing the SFR Rationale, the ST is generated. This ST collects the RFS Applicable and those that Cannot be Tested (Witnessing and Vendor Affirms) but are in the scope of the TOE.
- The SFR defined in the ST are subsequently verified in the laboratory through witnessing, functional and penetration tests. For this purpose, use is made of any interface available in the TOE.

QUALIFYING SERVICES

Task 2.2 ST assessment and generation of the ETR

The laboratory is responsible for validating the ST and generating the ETR (Evaluation Technical Report).

For this we will use the LINCE methodology adapted to the cloud.

- The limit of effort and duration of the methodology is eliminated, adapting it to the scope of the TOE.
- Certain tasks are not applicable, e.g. installation phase.
- More flexibility is allowed in certain aspects, e.g. product versions

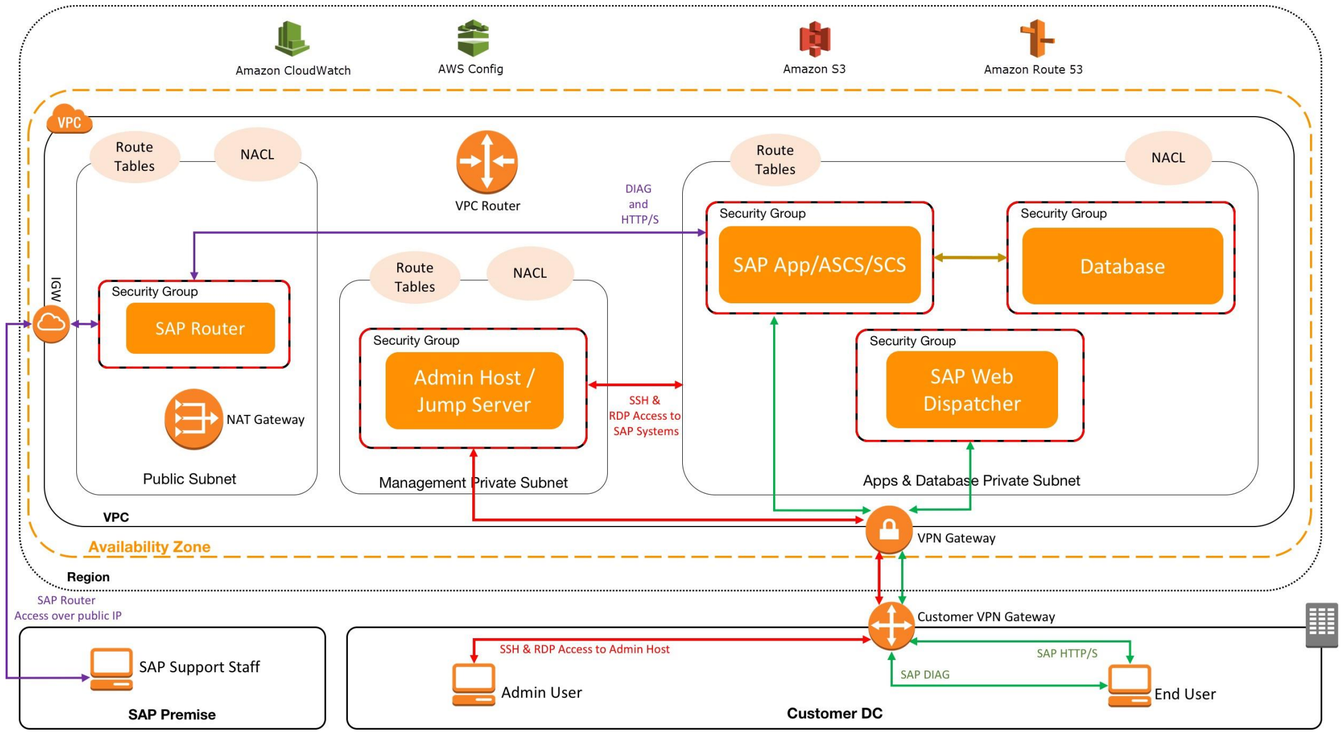
QUALIFYING SERVICES

Task 3. Security architecture

The manufacturer must provide some assurance on the security of the cloud architecture. For this purpose, the manufacturer shall define in the document “Cloud Security Architecture":

a) The separation in blocks of the solution.
b) The connection between blocks.
c) Which third-party services used by the solution are qualified (e.g. AWS S3)
d) What sensitive data is handled by the solution and how the flow of this data is handled

The cloud where the service is hosted must be ENS certified and GDPR compliant.



QUALIFYING SERVICES

Task 4. Cloud form Responsible statement

1

The veracity of the “Vendor affirmed” SFRs and the information provided in the Cloud Security Architecture is guaranteed.

2

The data handled by the solution complies with the stipulated geographical limits.

3

Future users of the solution will be able to request and receive audit logs related to the use of the service. Furthermore, these logs will not contain information from other users.

4

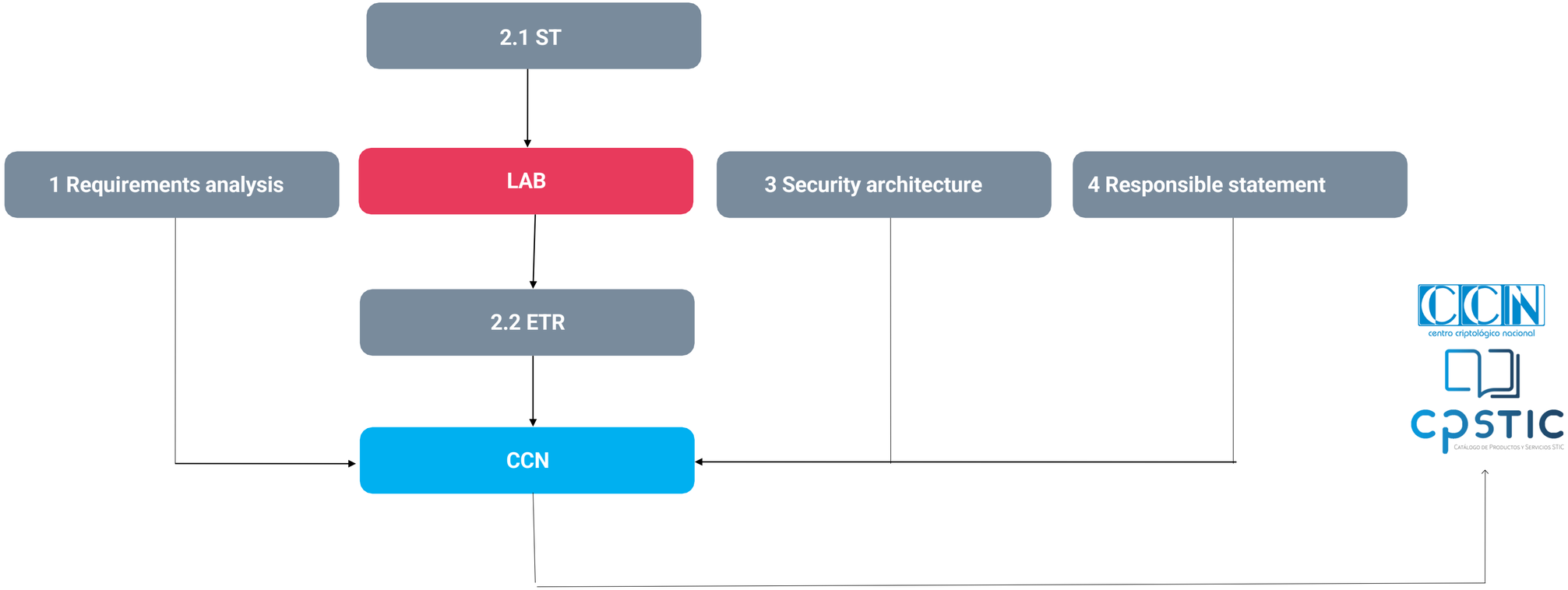
Incident response capabilities and corresponding description.

5

Cryptographic capabilities and key management details.

QUALIFYING SERVICES

Documentation validation



EXPERIENCES

1

Lack of control over TOE and its versions

2

Interoperability vs. security (cloud services have to be compatible with obsolete software) (e.g. old versions of SSL/TSL)

3

Need to ask for permission to test (risk of DoS)

4

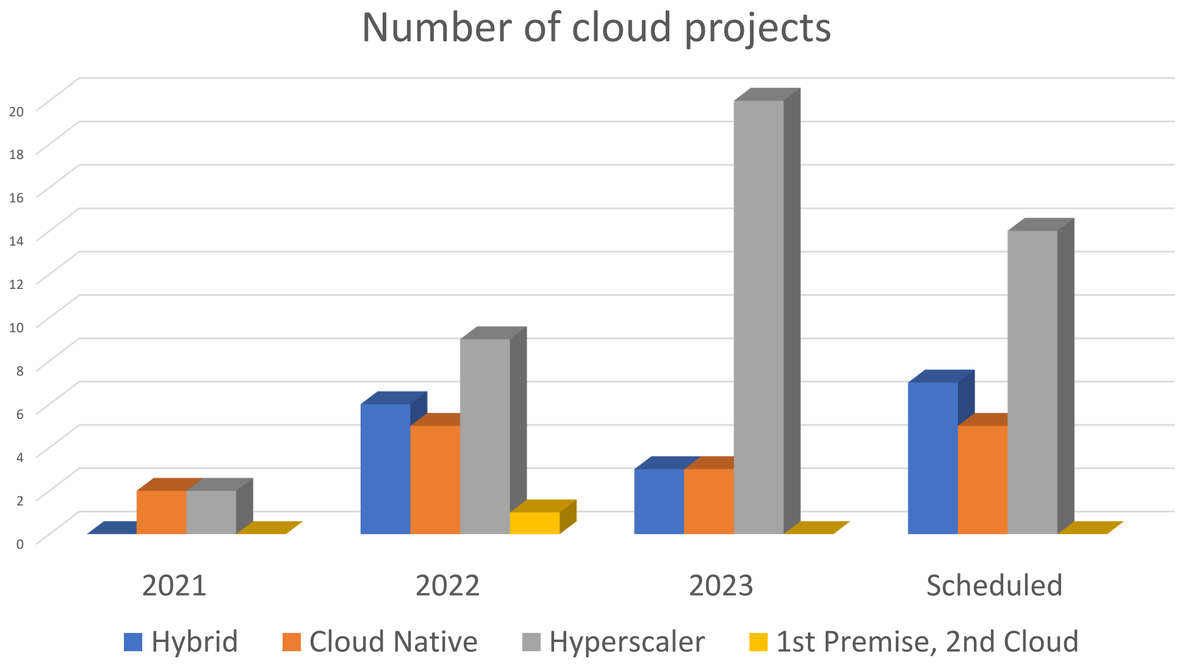
Mixed agent + server products (e.g. AV/EDR taxonomy requires both sides to be qualified)

5

We need to gain assurance from new sources (Cloud security architecture) and to increase trust in the vendor

EXPERIENCES

- Average number of tests: 30
  - Average failed tests: 5
- Average number of pentests: 24
  - Average failed pentests: 4



CONCLUSIONS

- All existing methodologies are for evaluating on premise products.
- No methodology for evaluating cloud products is expected at European level.
- It will probably take years for standardize how to deal with this…
- CCitC TC is focused in evaluating DevOps while we are dealing with evaluating SaaS using a CC based approach.
- Spain is a pioneer country in qualifying (not certifying) cloud services

CONCLUSIONS

CRA (9) “This Regulation ensures a high level of cybersecurity of products with digital elements. **It does not regulate services, such as Software-as-a-Service (SaaS)**, except for remote data processing solutions relating to a product with digital elements understood as any data processing at a distance for which the software is designed and developed by the manufacturer of the product concerned or under the responsibility of that manufacturer, and the absence of which would prevent such a product with digital elements from performing one of its functions” […] **[Directive XXX/XXXX (NIS2)] applies to cloud computing services and cloud service models, such as SaaS**. All entities providing cloud computing services in the Union that meet or exceed the threshold for medium-sized enterprises fall in the scope of that Directive.


jtsec
Applus
Thank you