SySS
THE PENTEST EXPERTS.

COMMENTARY

Franz Jahn, Steffen Stepper, Thibaud Kehler, Ludwig Stage

Public Consultation on DORA RTS on TLPT

JC 2023 72

February 26, 2024

Schaffhausenstraße 77, 72072 Tübingen, Germany
+49 (0)7071 - 40 78 56-0
info@syss.de
www.syss.de

1 Commentary on DORA RTS on TLPT

Due to Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (hereinafter "DORA") the three European Supervisory Authorities (ESAs) published a draft JC 2023 72 for regulatory technical standards ("RTS") on threat-led penetration testing ("TLPT").

SySS GmbH is a German midsize IT security consultancy specialized on penetration tests, red team assessments and incident response on the German and European market. Already having experience with the red teaming frameworks TIBER-EU and TIBER-DE, SySS GmbH aims at being an external tester as well as a threat intelligence provider by conducting TLPT according to DORA and its RTS.

1.1 Question 7

Do you consider the proposed additional requirements for external testers and threat intelligence providers are appropriate? If not, please provide detailed justifications and alternative wording or thresholds as needed.

On RTS Section I, Article 5, No 2:

> c. The threat intelligence provider provide at least three references from previous assignments related to intelligence-led red team tests;
>
> d. The external testers provide at least five references from previous assignments related to intelligence-led red team tests;

in accordance wit RTS Section I, Article 4, No 2.d:

> 2. Financial entities shall establish organisational and procedural measures ensuring that:
>
> [...]
>
> d. arrangements relating to the secrecy of the TLPT, applicable to staff of the financial entity, to the staff of relevant ICT third party service providers, to testers and to the threat intelligence provider are in place.

In order to qualify for a TLPT, the external tester and threat intelligence provider have to provide a certain amount of references from previous assignments. The proposed RTS through Section I, Article 4, No 2.d, however, imposes a legitimate obligation of secrecy on the threat intelligence provider and external tester. This limits the possibility of external testers and threat intelligence providers to acquire references in order to participate in a future TLPT. It is to be expected that a TLPT under the presented RTS might become predominant in the financial sector. If providers can no longer refer to these tests, even existing providers could be excluded from the market. Thus, the **requirements** in the current revision **are not appropriate**.

We recommend adding one of the following passages where appropriate, for example to Section I, Article 4 as No 3:

> Financial entities shall allow the threat intelligence provider and external testers to cite the TLPT as reference for future TLPT.

Or alternatively:

> Financial entities should allow the threat intelligence provider and external testers to cite the TLPT as reference for future TLPT. Otherwise, the TCT will issue the reference in pseudonymised form.

This clarification enables threat intelligence providers and external testers to acquire references for TLPT assignments carried out under this regulation and still meet the high requirements for confidentiality.

1.2 Question 8

Do you think that the specified number of years of experience for external testers and threat intelligence providers is an appropriate measure to ensure external testers and threat intelligence providers of highest suitability and reputability and the appropriate knowledge and skills? If not, please provide detailed justifications and alternative wording as needed.

TI providers

With regard to threat intelligence providers, RTS Section I, Article 5, No 2.e.i:

> e. the staff of the threat intelligence provider assigned to the TLPT shall:
>
> i. be composed of at least a manager with at least five years of experience in threat intelligence, including three years of collecting, analysing and producing threat intelligence for the financial sector as well as at least one additional member with at least two years of experience in threat intelligence.

To provide a threat intelligence service, the provider has to collect information of probably illegal origin, for example on the dark web and from data leaks (cf. RTS Annex III, No. 2.a and c). Due to these data sources requiring a lot of memory and usually being unstructured, the only economical approach would be to collect and process the data before and independently of a threat intelligence assignment. It can be assumed that this happens without any authorization of the affected persons and organisations. German national law, however, prohibits obtaining, providing or disseminating data that another person has obtained through an unlawful act.[1] Even now, it remains unclear whether a threat intelligence service would be legal under German law if not conducted in the context of a TLPT according to DORA. Moreover, data leaks usually contain very sensitive personal data. Processing this data without the data subjects' consent is in violation of the GDPR.[2]

The requirement of five years respectively two years of experience can hardly be met by persons under German law, posing a major disadvantage for German companies or any other company following the GDPR.

As discussed in the draft impact assessment (No 36), the European market is already small. This applies especially to the pool of qualified German threat intelligence providers. Rising German threat intelligence providers would be excluded from the market until 2030. Therefore, the **requirements** of the proposed RTS for the staff of threat intelligence providers **are not appropriate**.

We suggest reducing the requirements for threat intelligence providers to one year, increasing them yearly up to a maximum of three years. As an alternative, experience in reconnaissance during classic penetration testing,

[1] Crime of data theft ("Datenhehlerei"), § 202d, Strafgesetzbuch (StGB), Bundesgesetzblatt 2015 Teil I Nr. 51, p. 2218, 17 December 2015

[2] Article 5 GDPR, Regulation (EU) 2016/679, 27 April 2016

certifications and other comparable experience should be taken into account. For example, the TLPT authority (TCT) could be granted a certain amount of judgment.

External testers

With regard to external testers, RTS Section I, Article 5, No 2.f.i:

> f. for external testers, the staff of the red team assigned to the TLPT shall:
>
> i. be composed of at least the a manager, with at least five years of experience in threat intelligence-led red team testing as well as at least two additional testers, each with red teaming experience of at least two years;

Having a broad knowledge and understanding within different domains of IT security is more crucial than having a set amount of years of experience in TI-based red team tests. General experience in IT security also results in a better understanding of the bigger picture, communication skills to present findings and experience in supporting risk management from the attacker's point of view. Therefore, we consider this **specified number of years to be not appropriate**.

We advise – for the test manager – a combination of five years of experience in the field of general red teaming within different sectors and industries and of only three years of experience in threat intelligence-led red team tests. This change allows different red team providers to compete with each other which will also increase the overall quality of the tests within the sector. In addition, a bigger market and more competitors increase the diversity within each red team, allowing for a more holistic approach and better simulation of real advanced threat actors.

This results in the following alternative wording for RTS Section I, Article 5, No 2.f:

> f. For external testers, the staff of the red team assigned to the TLPT shall:
>
> i. be composed of at least a manager, with at least five years of experience in red team testing as well as three years of experience in threat intelligence-led red team testing as well as at least two additional testers, each with red teaming experience of at least two years;
>
> ii. display a broad range and appropriate level of professional knowledge and skills, including, knowledge about the business of the financial entity, reconnaissance, risk management, exploit development, physical penetration, social engineering, vulnerability analysis, as well as adequate communication skills to clearly present and report on the result of the engagement;
>
> iii. have a combined participation in at least five previous assignments related to threat intelligence-led red team tests;

1.3 Question 11

Do you agree with the proposed requirements on the use of internal testers? If not, please provide detailed justifications and alternative wording as needed.

The requirements on internal testers being employed for at least two years and having passed through a training is not sufficient to guarantee successful and proper threat intelligence-led penetration tests. Overall, the requirements appear to be very lax in comparison to the strong requirements on external testers and threat intelligence providers.

Thus, being too involved with the assessed financial entity and lacking experience in red team tests – especially TLPT – internal testers can be expected to fall far too short of the quality of external testers. From this, it follows that the **requirements in the current revision are not appropriate**.

Internal testers and testers of ICT service providers (therefore also classified as internal testers) should meet at least the same requirements as external testers, as implied in Article 27, No 2 of DORA: "When using internal testers, financial entities shall ensure that, *in addition* to the requirements in paragraph 1, the following conditions are met".

We propose that internal testers should also have an experience similar to RTS Section I, Article 5, No 2.f., which is five years of experience in red team exercises as well as three years of experience in threat intelligence-led red team tests for the managers and at least two years of red team test experience for the testers.

THE PENTEST EXPERTS

SySS GmbH Tübingen Germany +49 (0)7071 - 40 78 56-0 info@syss.de

www.syss.de