Development, Implementation and Evaluation of a Security Concept for the Secure Transfer of Sensitive Personal Data Between Different Devices

Oliver Junk
(4568642)

Freie Universität Berlin, Department of Mathematics and Computer Science,
Institute of Computer Science, Databases and Information Systems Group

January 15, 2020

Outline

Motivation

- With advances in information technology more personal data is gathered, stored and shared
- Disclosed sensitive personal data endangers an individuals right to self-determination
- Regulations, such as the General Data Protection Regulation (GDPR), implement law to protect an individuals right to privacy

Outline of Contribution

- Design of a security concept for the transfer of sensitive personal data complying with the GDPR
- Design of the concept as part of the CliniScale project
- Evaluation of the security level of the concept by performing a security risk assessment
- Creation of a guideline for the implementation of identified security measurements

The **Microsoft Threat Modeling Tool (MTMT)** is a core element of the Microsoft Security Development Lifecycle. It allows software architects to identify and mitigate security issues early in the process of designing a software architecture.

Microsoft **STRIDE** is a threat model that supports security analysts in identifying possible threats in six different categories.

The **Yakindu Security Analyst** is a tool created by the Itemis AG to perform risk assessments.

Related Work [1/2]

- **J. Eichler and D. Angermeier.** “Modular Risk Assessment for the Development of Secure Automotive Systems”. In: *31. VDI/VW-Gemeinschaftstagung Automotive Security*, 2015 [1]
- **J. Eichler, D. Angermeier, and A. Nieding.** “Systematic Identification of Security Goals and Threats in Risk Assessment”. In: *Softwaretechnik-Trends 36.3*, 2016 [2]
- **J. Eichler, D. Angermeier, and A. Nieding.** ”Supporting Risk Assessment with the Systematic Identification, Merging and Validation of Security Goals”. In: *Risk Assessment and Risk-Driven Quality Assurance. RISK 2016*, 2017, pp. 82–95 [3]

Related Work [2/2]

- **M. de Gramatica, K. Labunets, F. Massacci, F. Paci, and A. Tedeschi.** "The role of catalogues of threats and security controls in security risk assessment: an empirical study with ATM professionals". In: *International Working Conference on Requirements Engineering: Foundation for Software Quality.* Springer. 2015, pp. 98–114 [4]
- **W. Wilkowska and M. Ziefle.** "Privacy and data security in E-health: Requirements from the user's perspective". In: *Health Informatics Journal 18.3*, 2012, pp. 191–201 [5]

General Data Protection Regulation [1/3]

https://www.zdnet.com/article/gdpr-an-executive-guide-to-what-you-need-to-know/

- Consists of 99 articles, 173 recitals and 14 key issues [6]
- Investigated for regulatory specifications concerning a system collecting and processing sensitive personal data

Article 4: Personal Data Defines personal data as any information relating to an identified or identifiable natural person [7]

Article 9: Sensitive Personal Data Special category of personal data [8]

Article 6: Lawfulness of Processing Defines conditions under which the processing of personal data is lawful [9]

Article 7: Conditions for Consent Defines that consent by the data subject to processing has to be given by a clear affirmative act that is freely given, specific, informed and unambiguous [10]

Article 25: Security of Processing Places the responsibility to implement appropriate technical and organizational measures to secure personal data on the controller [11]

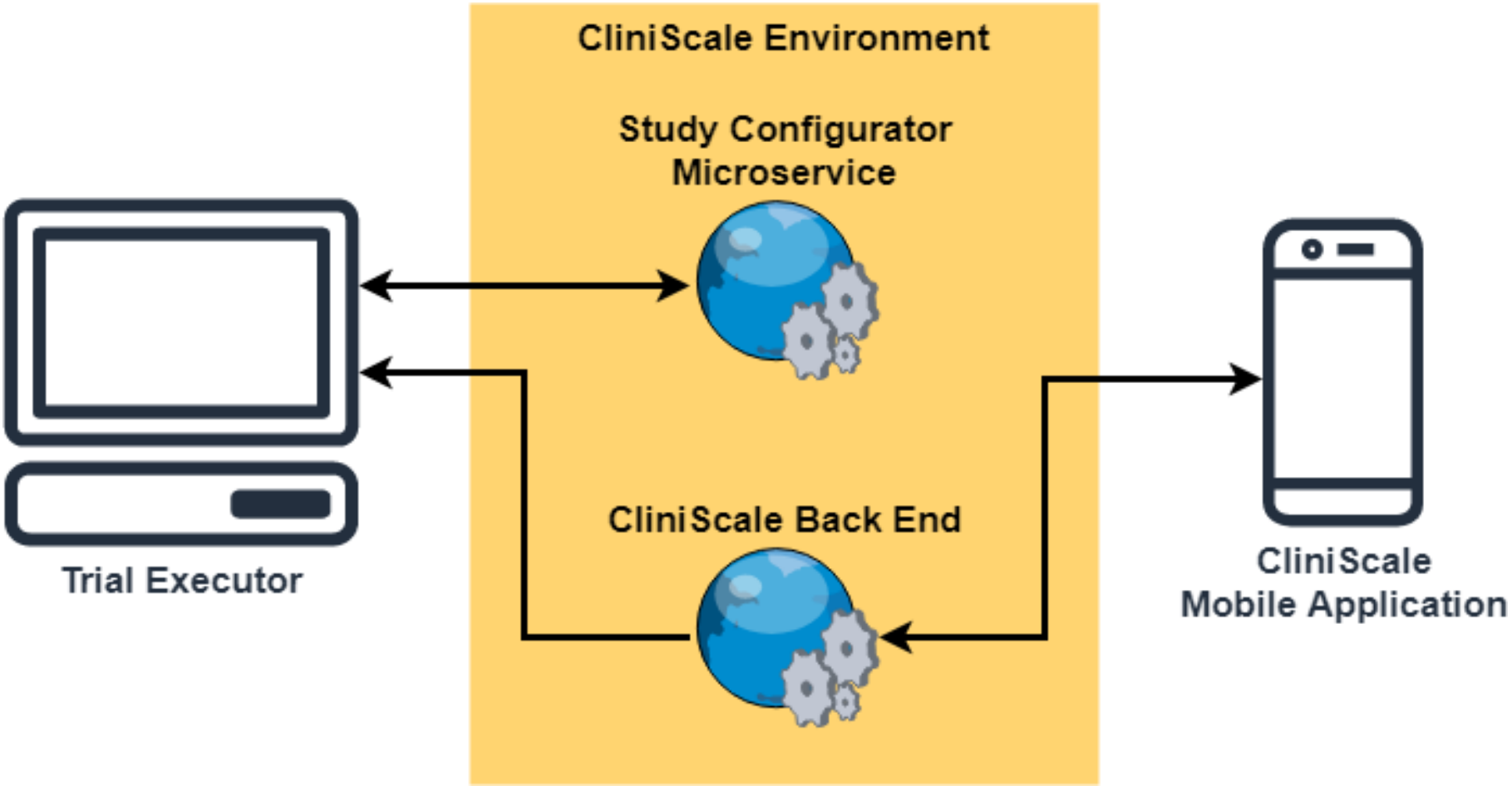
General Data Protection Regulation [3/3]

- Personal and sensitive personal data has to be secured in a manner appropriate for the risks
- State of the art security measurements
- Consent given by a clear affirmative act that is freely given, specific, informed and unambiguous

https://www.mi.fu-berlin.de/en/inf/groups/ag-db/projects/CliniScale/index.html

- Project by the Databases and Information Systems Group at Freie Universität Berlin
- Run scalable and user-friendly clinical trials in the population
- Mobile devices paired with specific sensors

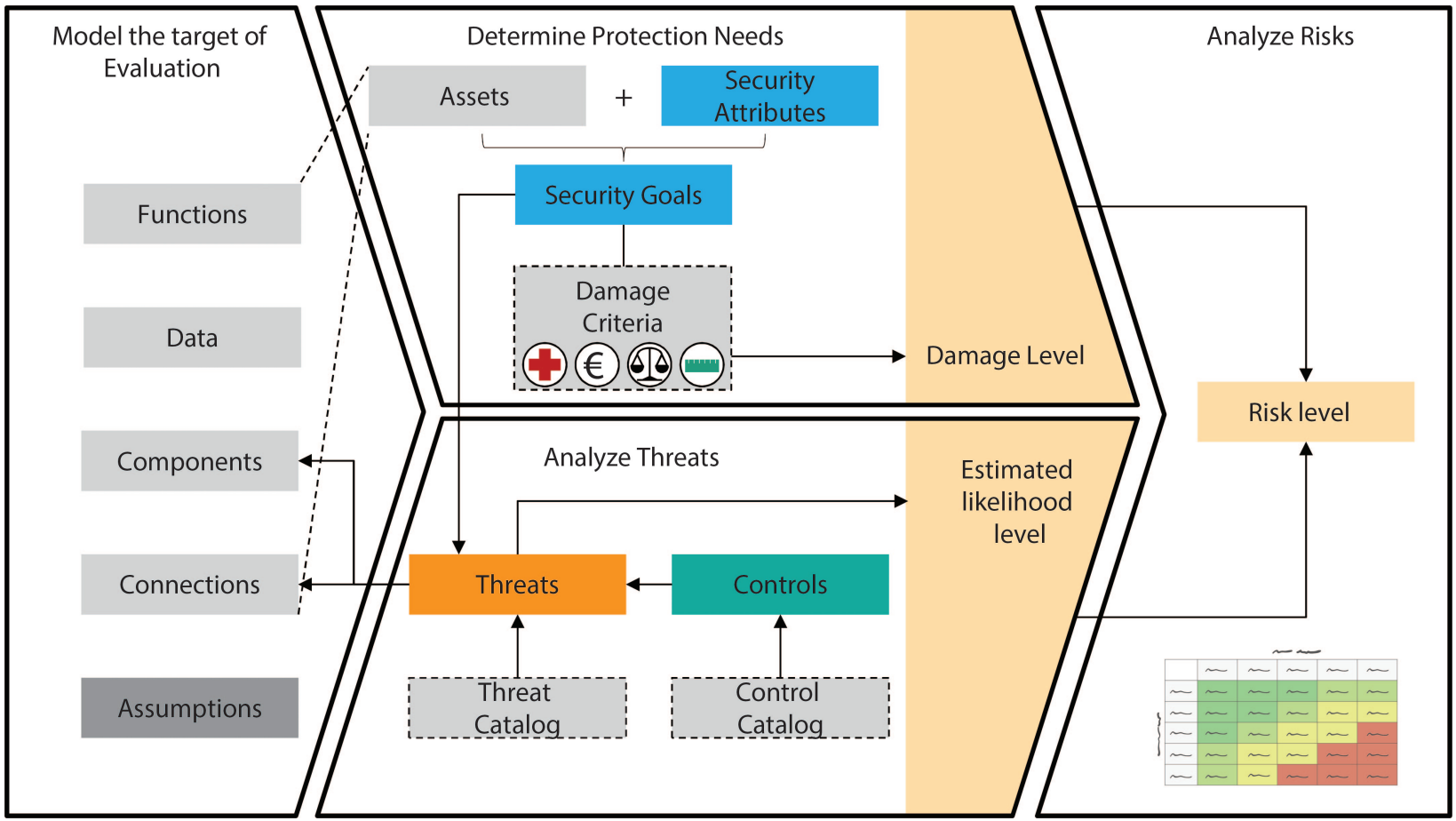
CliniScale Project [2/2]



Modular Risk Assessment (MoRA)

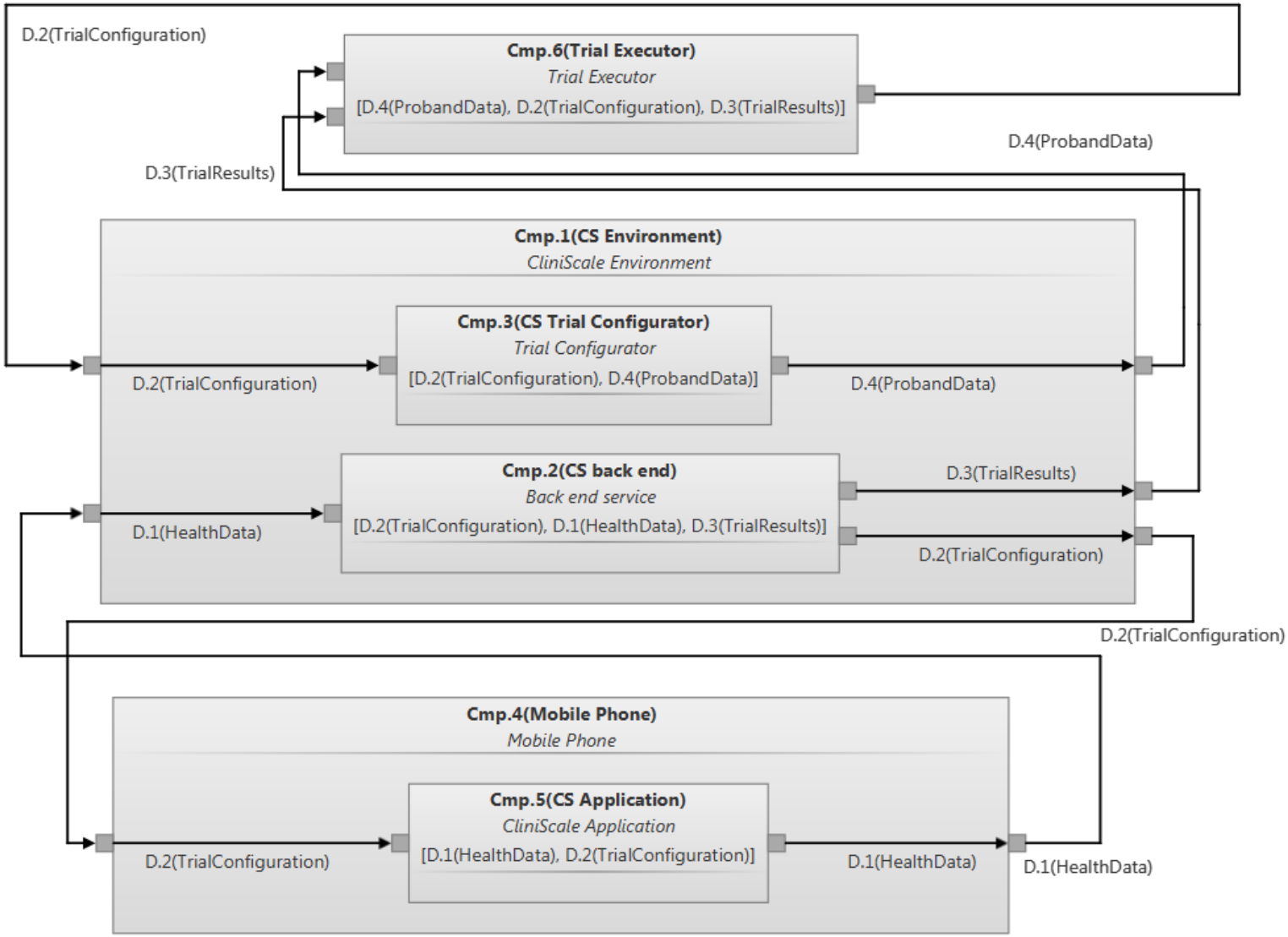
- Method for security risk assessment developed by Jörn Eichler and Daniel Angermeier at Fraunhofer AISEC in 2015
- Flexibility of application in different environments
- Customized in order to integrate the MTMT as threat and control catalogue

Methodology Overview

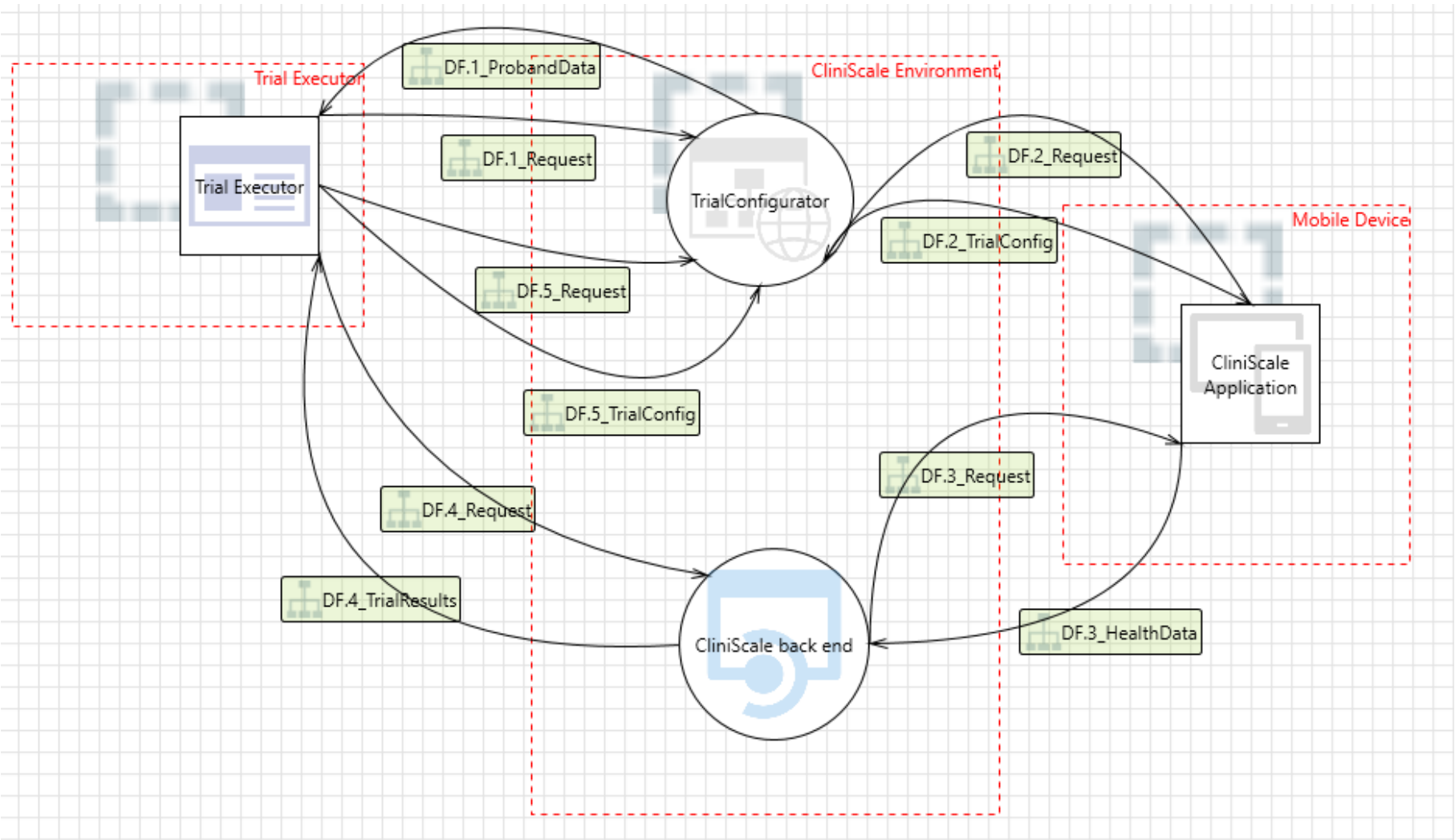


https://www.aisec.fraunhofer.de/de/presse-und-veranstaltungen/presse/pressemitteilungen/2018/it-sa2018.html

System Under Development [1/2]



System Under Development [2/2]



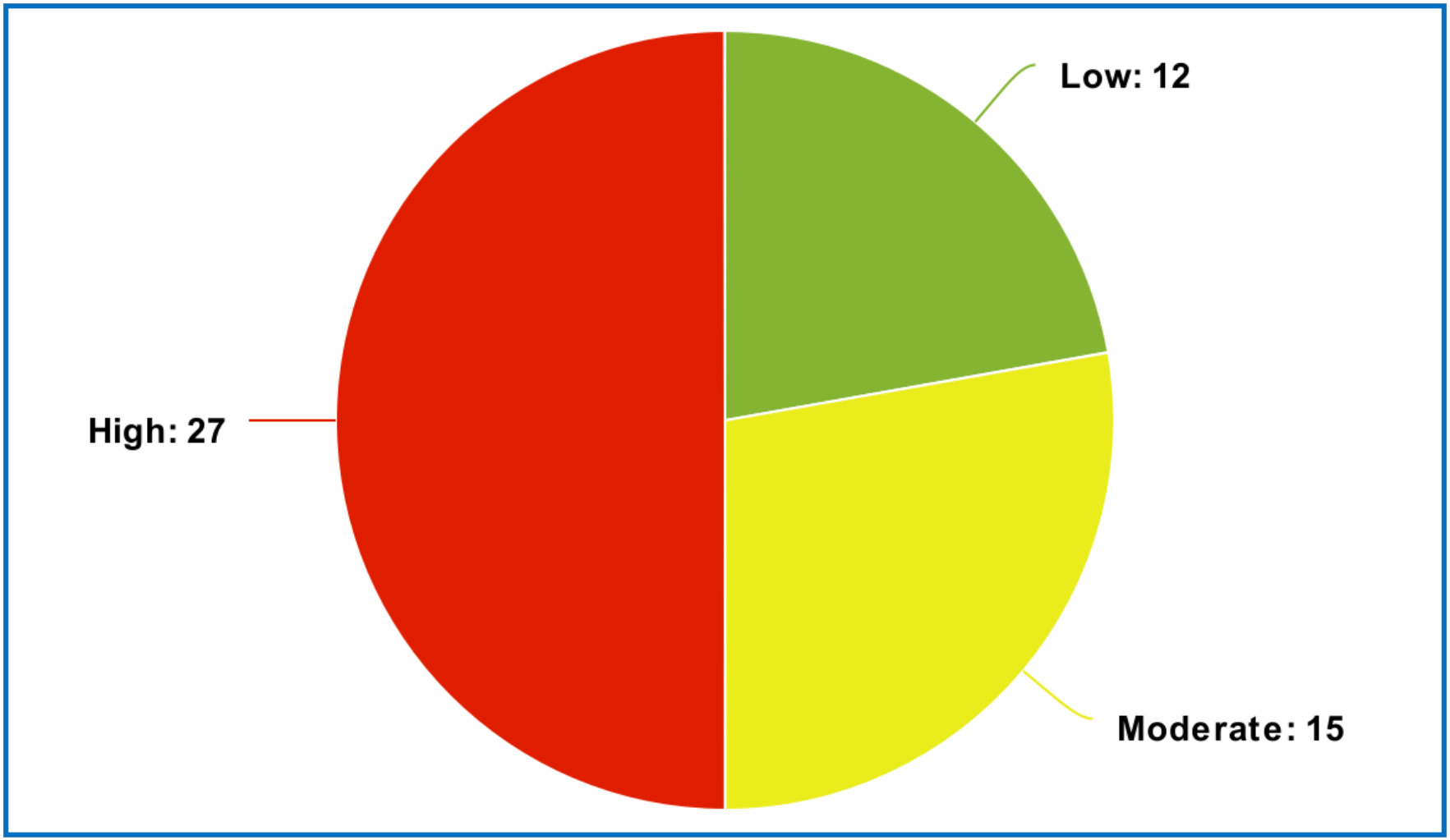
Determine Protection Needs [1/2]

- Process of identifying and defining security goals
- Assessment Model: Security Goal Classes, Damage Criteria

```
security goal G.31: Confidentiality HealthData instantiates CON: Confidentiality damage potential: High
  concerns         D.1(HealthData): HealthData
  damage criteria  SelfDet: Right to self-determination:
                     SensDat: Leak of sensitive personal data (High) rationale: <no rationale>
                   FinCon: Financial consequences:
                     ExcFine: Existence-threatening fine               (High) rationale: <no rationale>
                     ExcRep: Existence-threatening reputational damage (High) rationale: <no rationale>
  depends on       G.13 || G.34 || G.36
  threatened by    <no expr>
```

Determine Protection Needs [2/2]

- 54 security goals



Analyze Threats [1/2]

- Process of identifying and defining threats
- Import threats generated by MTMT

1	An adversary may jail break into a mobile device and gain elevated privileges	Elevation of Privileges	DF.3_HealthData
2	An adversary may gain unauthorized access to Web API due to poor access control checks	Elevation of Privileges	DF.3_HealthData
3	An adversary can gain access to sensitive information from an API through error messages	Information Disclosure	DF.3_HealthData
4	An adversary can gain access to sensitive data by sniffing traffic from Mobile client	Information Disclosure	DF.3_HealthData
5	An adversary can gain access to sensitive data by sniffing traffic to Web API	Information Disclosure	DF.3_HealthData
6	An adversary can gain sensitive data from mobile device	Information Disclosure	DF.3_HealthData

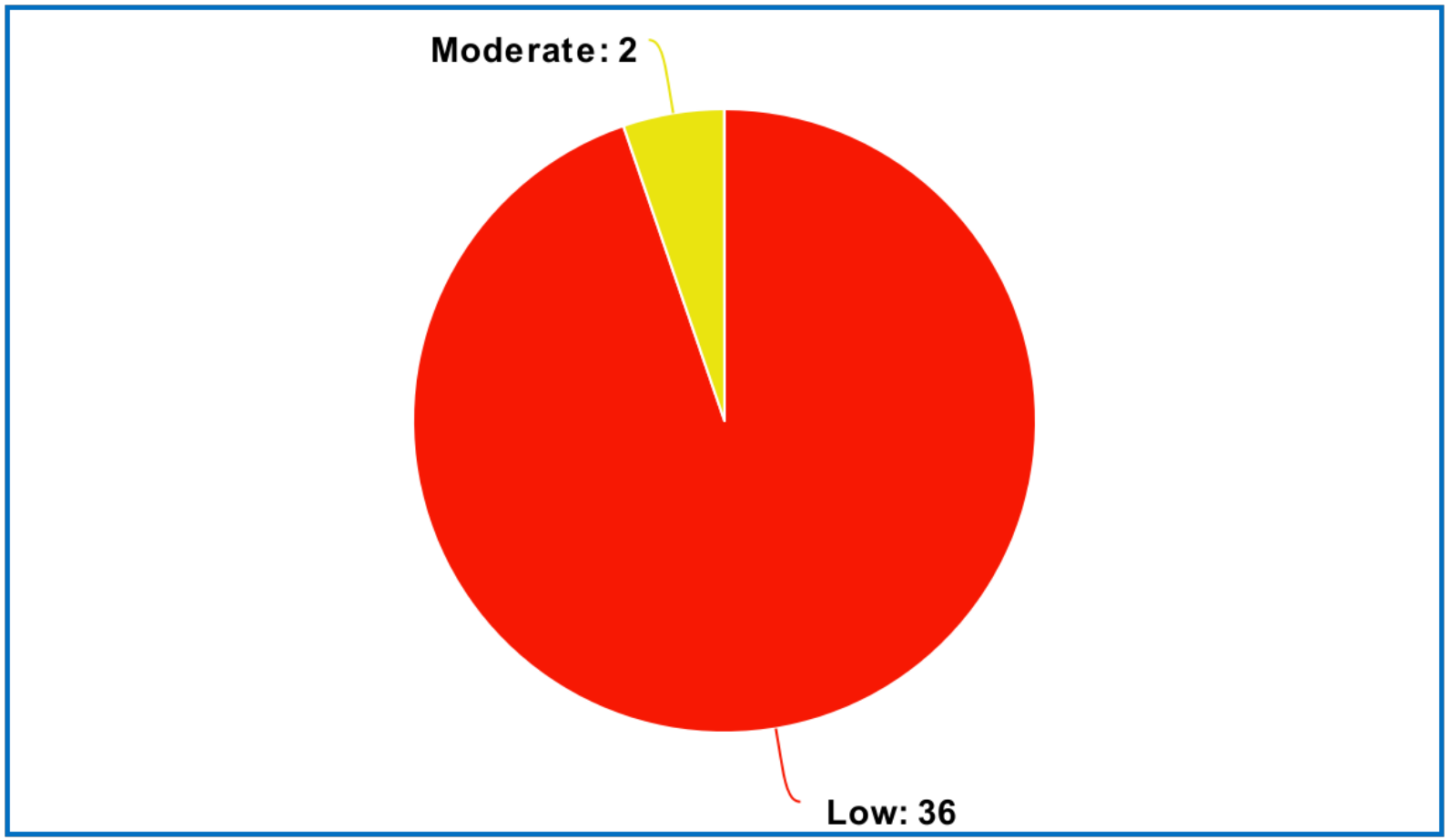
threat T.2: Gain access to API end points due to unrestricted cross domain requests instantiates
TC.1.2: An adversary can gain unauthorized access to API end points due to unrestricted cross domain requests
required attack potential: High

threatens + G.22
acts on << ... >>
mitigated by C.29 || C.70
risk factors

	Risk factors					Required attack potential	-> explicit
	SPEX	ACCS	TIME	EQUIP	KNOW		
Initial						none	<no attack effort>

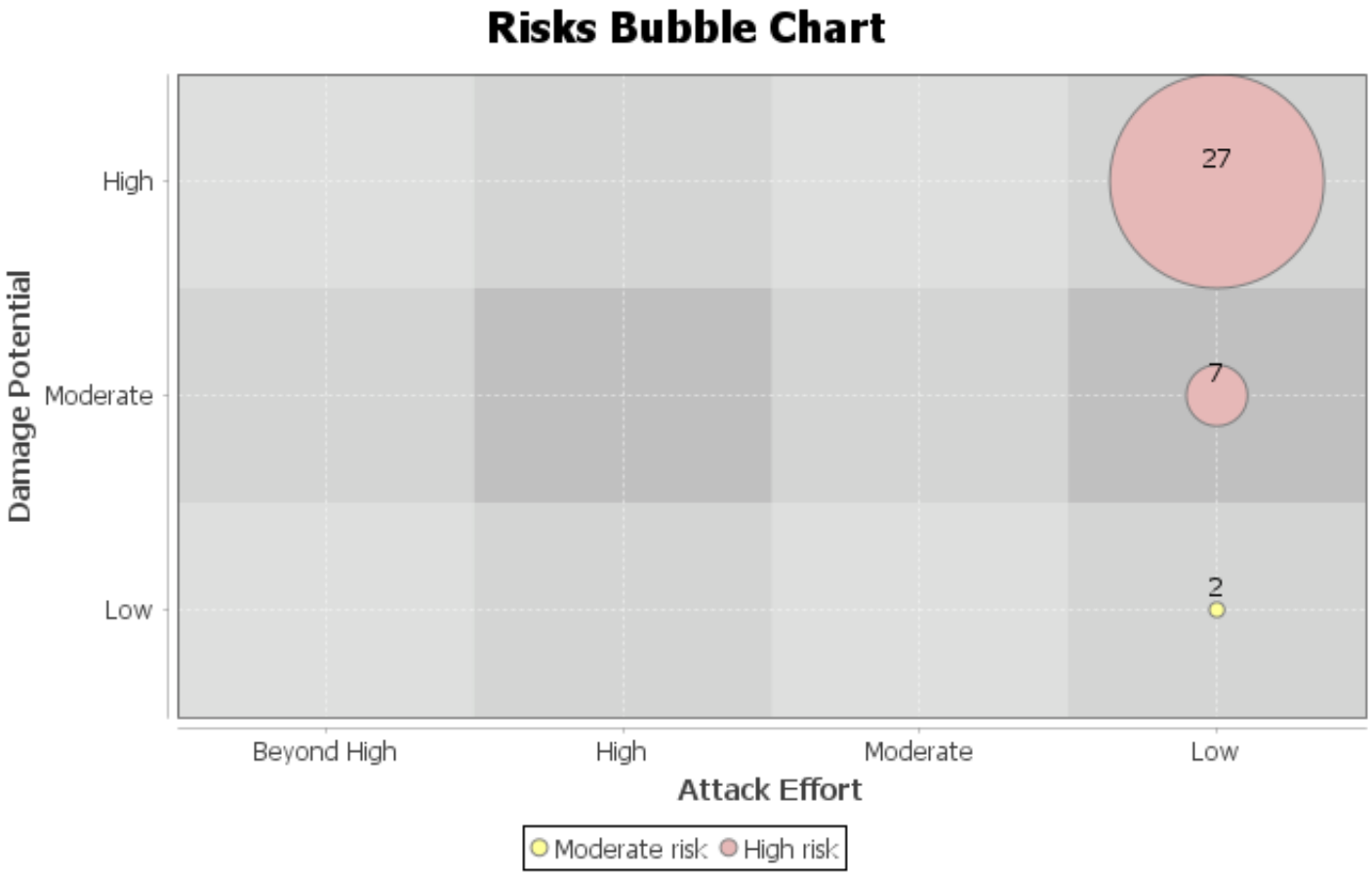
Analyze Threats [2/2]

- 100 threats generated by MTMT
- 38 aggregated threats imported



Analyze Risks

- Process of identifying and defining risk elements
- Risk elements provide a summary of the overall risk level



Establish controls [1/2]

- Process of identifying and defining security control elements

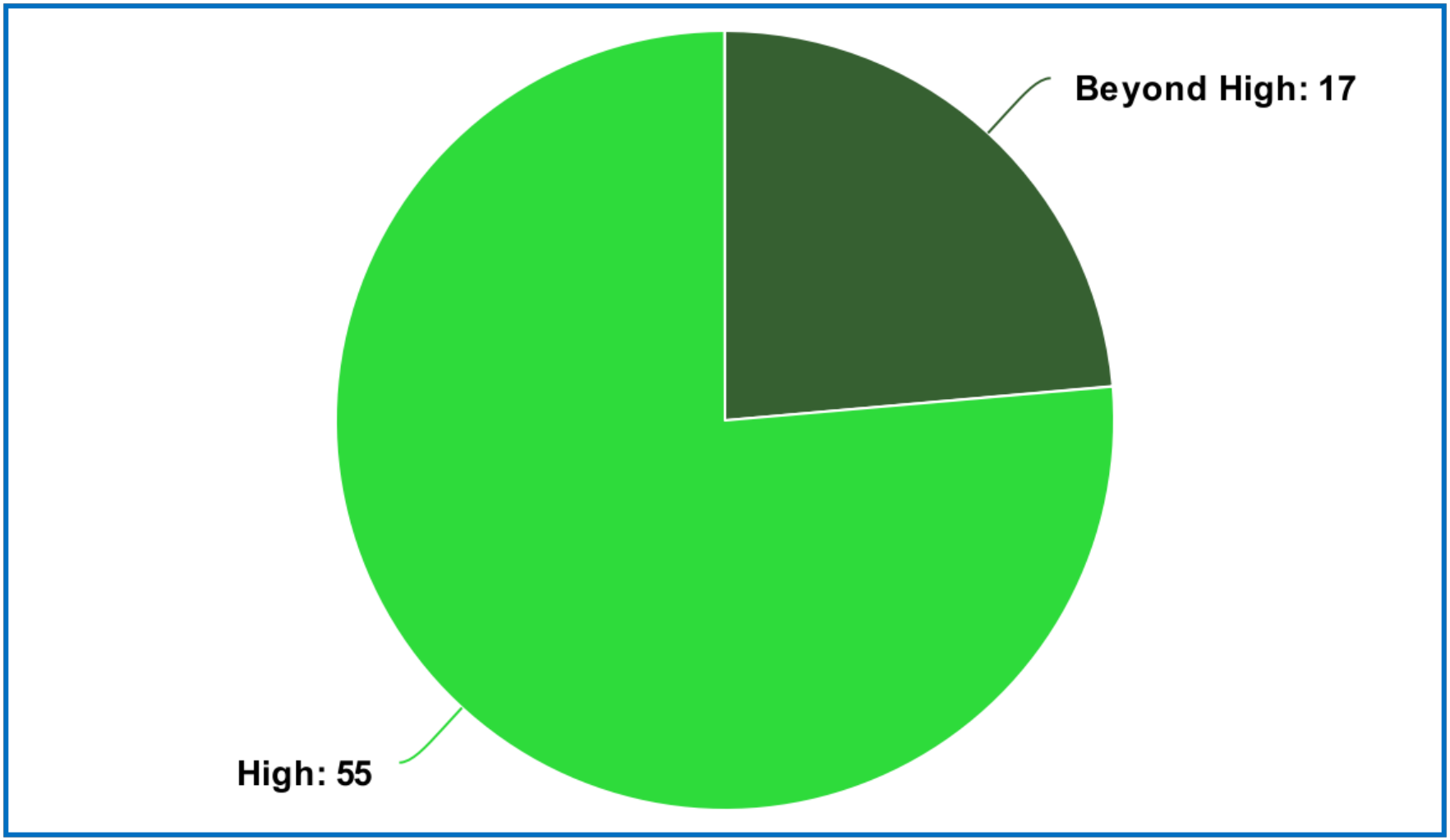
1	Elevation of Privileges	DF.3_HealthData	Implement implicit jailbreak or rooting detection. Refer: <a href="https://aka.ms/tmtauthz#rootin...
2	Elevation of Privileges	DF.3_HealthData	Implement proper authorization mechanism in ASP.NET Web API. Refer: <a href="https://aka.ms/t...
3	Information Disclosure	DF.3_HealthData	Ensure that proper exception handling is done in ASP.NET Web API. Refer: <a href="https://aka.ms/...
4	Information Disclosure	DF.3_HealthData	Implement Certificate Pinning. Refer: <a href="https://aka.ms/tmtcommsec#cert-pinning">https:...
5	Information Disclosure	DF.3_HealthData	Force all traffic to Web APIs over HTTPS connection. Refer: <a href="https://aka.ms/tmtcommsec...
6	Information Disclosure	DF.3_HealthData	Encrypt sensitive or PII data written to phones local storage. Refer: <a href="https://aka.ms/tmtda...

```
control C.68: Applications available over HTTPS must use secure cookies instantiates
    CC.10.1: Applications available over HTTPS must use secure cookies required attack potential: High
  depends on    <no expr>
  mitigates     + T.33, T.8
  risk factors
```

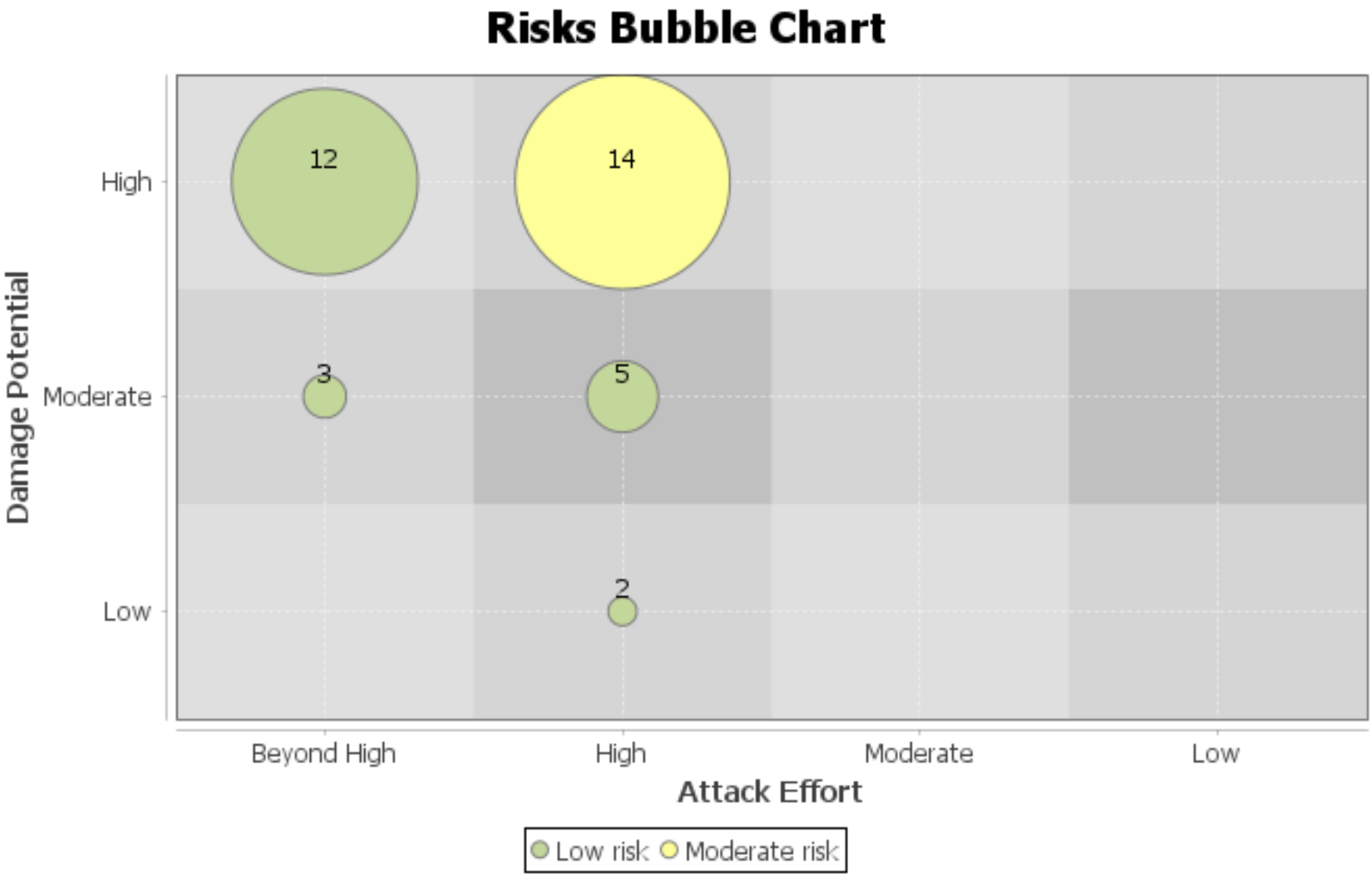
	Risk factors					Required attack potential	-> explicit
	SPEX	ACCS	TIME	EQUIP	KNOW		
Initial						none	<no attack effort>

Establish controls [2/2]

- 72 security controls



Analyze Need for Further Iterations [1/2]



- Mitigations recommended by the MTMT
- Ten categories of mitigations: **Auditing and Logging**, **Authentication**, **Authorization**, **Communication Security**, **Configuration Management**, **Cryptography**, **Exception Management**, **Input Validation**, **Sensitive Data**, **Session Management**
- Recommendations on implementation for every control

CC.4.4: Force all traffic to Web APIs over HTTPS connection

- Hypertext Transfer Protocol Secure
- BSI Technical Guidelines [12]
- Implementation supported by the Spring Security Framework

Conclusion

- Compliance with the GDPR
- Successful integration of the MTMT as threat and control catalogue into the MoRA methodology
- Implementation guideline applicable to any client-server infrastructure gathering, storing and processing sensitive personal data

Limitations

- GDPR investigated for regulations concerning this thesis
- Missing information on the required attack potential

Future Work

- Domain specific threat and control catalogues
- Complete security risk assessment of the CliniScale system

Questions?

References I

[1] **J. Eichler and D. Angermeier**. “Modular Risk Assessment for the Development of Secure Automotive Systems”. In: *31. VDI/VW-Gemeinschaftstagung Automotive Security* (2015).

[2] **D. Angermeier, A. Nieding, and J. Eichler**. *Supporting Risk Assessment with the Systematic Identification, Merging, and Validation of Security Goals*. Ed. by J. Großmann, M. Felderer, and F. Seehusen. Cham: Springer International Publishing, 2017, pp. 82–95.

[3] **D. Angermeier, A. Nieding, and J. Eichler**. “Systematic Identification of Security Goals and Threats in Risk Assessment”. In: *Softwaretechnik-Trends* 36.3 (2016).

References II

[4] **M. de Gramatica, K. Labunets, F. Massacci, F. Paci, and A. Tedeschi**. "The role of catalogues of threats and security controls in security risk assessment: an empirical study with ATM professionals". In: *International Working Conference on Requirements Engineering: Foundation for Software Quality*. Springer. 2015, pp. 98–114.

[5] **W. Wilkowska and M. Ziefle**. "Privacy and data security in E-health: Requirements from the user's perspective". In: *Health informatics journal* 18.3 (2012), pp. 191–201.

[6] **General Data Protection Regulation**. *(Online; Last accessed January 15, 2020)*. URL: https://eugdpr.org/.

References III

[7] **General Data Protection Regulation Article 4**. *(Online; Last accessed January 15, 2020)*. URL: https://gdpr-info.eu/art-4-gdpr/.

[8] **General Data Protection Regulation Article 9**. *(Online; Last accessed January 15, 2020)*. URL: https://gdpr-info.eu/art-9-gdpr/.

[9] **General Data Protection Regulation Article 6**. *(Online; Last accessed January 15, 2020)*. URL: https://gdpr-info.eu/art-6-gdpr/.

[10] **General Data Protection Regulation Article 7**. *(Online; Last accessed January 15, 2020)*. URL: https://gdpr-info.eu/art-7-gdpr/.

References IV

[11] **General Data Protection Regulation Article 25**. *(Online; Last accessed January 15, 2020)*. URL: https://gdpr-info.eu/art-25-gdpr/.

[12] **BSI TR-02102-2**. *(Online; Last accessed January 15, 2020)*. URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-2.pdf.

[13] **General Data Protection Regulation Article 32**. *(Online; Last accessed January 15, 2020)*. URL: https://gdpr-info.eu/art-32-gdpr/.