MISP
Threat Sharing

Grumpy Legal Section
(Uh oh…)

Dr. Matthieu Farcot

matthieu.farcot@securitymadein.lu

CIRCL.LU c/o SECURITYMADEIN.LU

MISP
Threat Sharing

Malware and Threat Information Sharing & EU Personal Data Regulation

Dr. Matthieu Farcot
matthieu.farcot@securitymadein.lu
CIRCL.LU c/o SECURITYMADEIN.LU

MISP
Threat Sharing

EU REGULATION OF DATA ABOUT IDENTIFIABLE LIVING INDIVIDUALS

Current situation and difficulties

- Personal data consists in **data about identifiable living individuals**
- Current regulation at EU level is **Data Protection Directive 95/46/EC**
  - Directive had to be **implemented in each EU Member State**
  - Drawback : heterogeneity has arisen across Member States in many areas due to **differences in implementation**
    - No harmonized sanctions for breaching the legislation
    - No harmonized need to notify the local data protection authority
- **Issues** for companies - across the EU:
  - **How to adopt a common compliance framework**?
  - **What is the digital single market**?

MISP
Threat Sharing

Welcome to the GDPR

- **GDPR clarifies the shape of the future data protection framework within the EU**
- **Core novelties**
  - **Accountability obligations**
    - keep records of processing
    - conduct impact assessments
  - **Much higher fines for breach** of obligations
  - **Data breach reporting obligations** for all companies
- **A major step towards a digital single market**

Welcome to the GDPR

- Obligations at EU levels?
  - **Micro-level**
    - Organizations dealing with data about identifiable living individuals
  - **Mezzo-level**
    - National authorities devoted to personal data protection
  - **Macro-level**
    - Data protection board, replacing Article 29 Working Party

Micro-level

- *Clarified roles, new obligations*
  - **Data Controllers**
    - Must comply with the Regulation (and be able to demonstrate the compliance)
      - Formalize processes and related documentation
      - Do data protection impact assessment (article 35)
      - Implement data protection by design
  - **Data Protection Officers** (in certain situations)
    - Ensures Data Controllers follow their due obligations
  - **Data Processors**
    - Strongly impacted by Regulation
      - Must notify Data Controller in case of Data or Information Security Breach

MISP
Threat Sharing

Mezzo-level

- **National Data Protection Authorities**
  - (e.g. CNPD in Luxembourg)
- **One-stop-shop**
  - Lead Authority works together with Concerned local Authorities
- **No more Notifications requirements for organizations**
  - Counterpart: **More obligations at Micro-level**

Macro-level

- **European Data Protection Board**
  - Issues **opinions** and **Guidance**
  - **Reports** to the Commission
- Clarifies **cross border** (outside EU) **data transfer**

Information security and Personal Data

- **Pro-active obligations at micro-level**
  - Taking into account the **state of the art**, the **costs** of implementation and the **nature**, **scope**, **context** and **purposes** of **processing** (…), the **controller** and the **processor *shall implement*** appropriate technical and organisational measures to ensure a level of security appropriate to the risk (…)
  - *(Including a)* process for regularly **testing**, **assessing** and **evaluating** the effectiveness of **technical** (…) measures for ensuring the security of the processing
    - *GDPR - Section 2 - Security of personal data - Article 32 (Security of processing)*

Information security and Personal Data

- **Promotion at Mezzo and Macro level**
  - The (…) **supervisory authorities**, the **Board** and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the **proper application** of this Regulation…
    - Section 5 - Codes of conduct and certification - Article 40

MISP
Threat Sharing

MISP AND THE GDPR

Reminder - goal of MISP

- **Malware Information Sharing and Threat Sharing Platform** (MISP) is a **software dedicated to sharing, storing and correlating**
  - **Indicators of Compromises of targeted attacks** (example: MD5 Hashes)
  - **Cyber-security threats** (example: threat actor names)
  - **Financial fraud indicators** (example: Bitcoins address)
- **Data feeds might include Personal Data**
  - Issue under GDPR: Legitimate interest?

MISP
Threat Sharing

Warning

< Next slide *might* hurt >

MISP and the GDPR

« The processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data, and the security of the related services offered by, or accessible via, those networks and systems, by public authorities, by computer emergency response teams (**CERTs**), computer security incident response teams (**CSIRTs**), by providers of electronic communications networks and services and ***by providers of security technologies and services***, **constitutes a legitimate interest of the data controller concerned. »**

GDPR – Introduction – [49]

MISP
Threat Sharing

Warning

< You were warned >

Reminder - goal of MISP

- **Core issue**
  - MISP Feeds include personal data
    - Legitimate interest?
    - **YES…**
  - It should be ascertained whether **all appropriate technological protection and organisational measures** have been implemented **to establish immediately whether a personal data breach has taken place** (…)
    - GDPR – Introduction – [87]

MISP
Threat Sharing

Conclusion

- **How to comply with obligations of identification of data Breach and information security requirements**?
  - ***Pro-active surveillance*** *of technical infrastructure*
  - ***Permanent monitoring*** *of compromized data diffusion*

- **Information sharing is therefore a tool needed in order to implement the obligations related to the GDPR at all levels (Micro, Mezzo & Macro)**

Conclusion

- **Future work:**
  - **Create a Personal Data dedicated Taxonomy in MISP**
    - Facilitate demonstration of legitimate interest
    - Usefullness of information classification

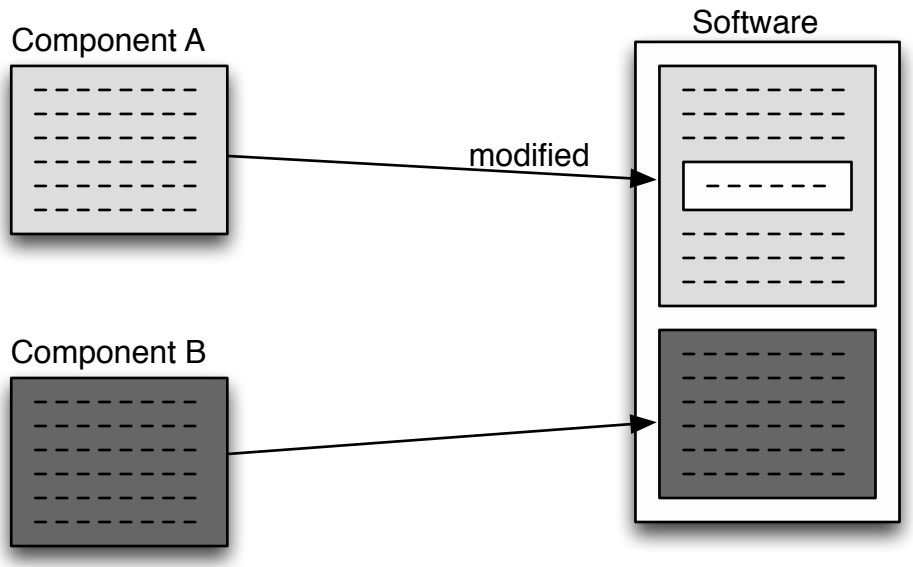
MISP Licensing Reminder

Dr. Matthieu Farcot
matthieu.farcot@securitymadein.lu
CIRCL.LU c/o SECURITYMADEIN.LU

MISP
Threat Sharing

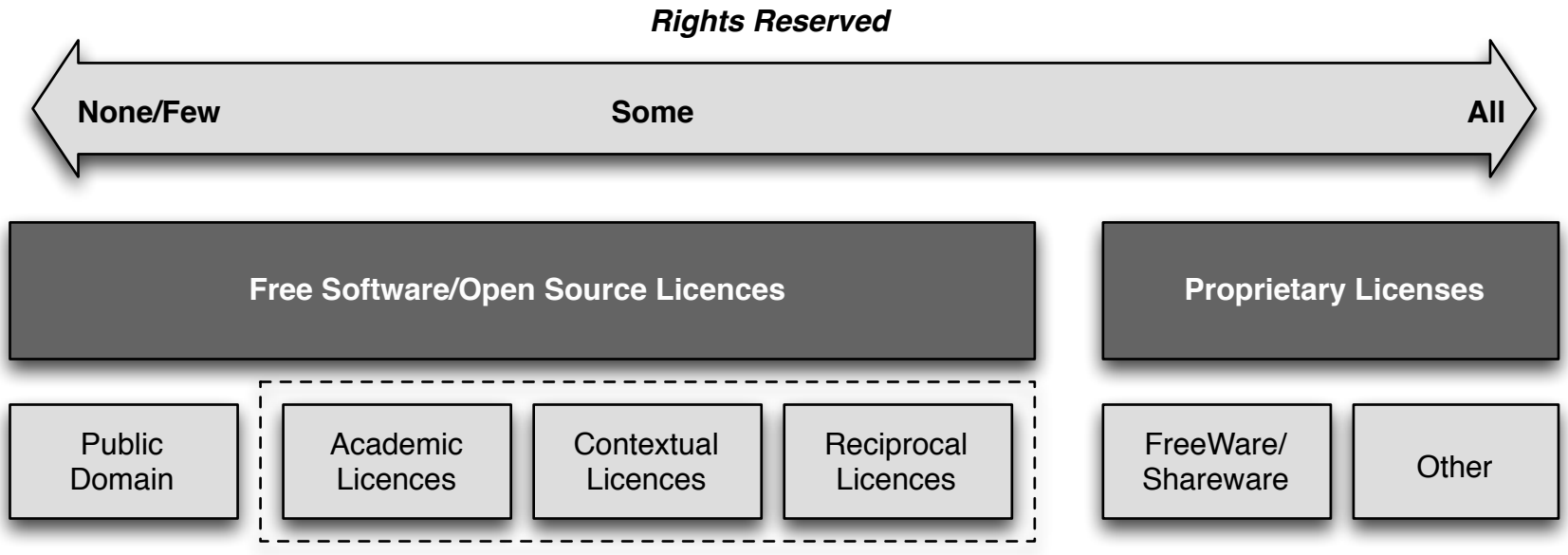
INITIAL SITUATION

License?



- Software is
  - A derivative work of component A
  - A larger work of component B

License?


Rights Reserved
None/Few
Some
All
Free Software/Open Source Licences
Proprietary Licenses
Public Domain
Academic Licences
Contextual Licences
Reciprocal Licences
FreeWare/ Shareware
Other

MISP LICENSE

MISP
Threat Sharing

License?

- MISP License
  - Affero GPL v3

  The GNU Affero General Public License is a modified version of the ordinary GNU GPL version 3. It has one added requirement: **if you run a modified program on a server and let other users communicate with it there, your server must also allow them to download the source code corresponding to the modified version running there** (Source: FSF.org)