# CTI and Automation

## Supporting CSIRT capabilities and reduce manual operations

Panel Session 3 - Automation of CTI *TLP:WHITE*

ENISA - CTI - Rome

# Background

- Security team often rely on **small teams** and especially with **tight resources**.
- Retaining staff within the security field can be challenging especially for highly skilled and curious people.
- Diversity and versality are significant in incident response tasks.
- **Automation** can support security team to reduce workload or **improve quality of the tasks to be performed**.
- Sharing and ratio of capability for processing at receiving CSIRT/PoC.

# Common tasks where automation can help

- **Gathering intelligence** and information to discover vulnerable systems, compromised devices, active attacks or leaked information.
- **Notification** towards constituents and outside constituency about compromised or vulnerable infrastructures (e.g. **take-down**).
- Notification towards constituents about current threats, associated risks and potential remediations.
- Provide **situational awareness** including statistics (KPI) or the trend about specific threats.

# Benefit of automation - human aspects

- **Context** coming from real analysts is critical in automation (e.g. false-positives, ensuring quality).
- Silo is still a practice in information sharing and it doesn't support automation:
  - but we need to promote the bridging information and sectors.
- Confrontation (competitive analysis) is important to **improve standards, tools and processes**.
- Fun is a critical aspect to keep your staff, partners or colleagues happy.

*The* **nice thing** *about standards is that you have so many to choose from.*

Andrew S. Tanenbaum

# Automation - formats

- Non-contextualized format are still actively used for automation (e.g. **CSV is still the King**).
- Formats strongly depends of the **tools or devices** ingesting the information shared.
- Automation and format are strongly bound to the **team capabilities** handling the information.

# What's next?

- Automation and CTI (feeds versus contextualised information) are critical for security operations but we need more practical exchanges to learn from the failures and successes of others.
- Organising at **EU-level hackathons targeting tooling and standards on real datasets** (e.g. boosting ENISA IHAP initiative).
- **Sharing use-cases** and practices with the community especially to improve tooling and standards (e.g. describing common models of automation and sharing to improve tooling and standards).
- Provide positive incentives to increase willingness to share more information (sighting, reporting) to improve automation within other organisations.