Standarts for sharing cyber security incidents and threats

Ivana Budinská[1]

[1] Institute of Informatics, Slovak Academy of Sciences, Dubravska cesta 9, 845 07 Bratislava, Slovakia

budinska@savba.sk

Internet is recognized as a global critical infrastructure. Since first internet worms have appeared, the need for sharing information about incidents and threats has been constantly increasing. Sharing information about cyber security incidents helps professionals and users of the internet to cope with attacks, and to prepare and protect their systems against known attacks. FIRST, the Forum of Incidents Response and Security Teams has been established in 1990 with the aim to bring together experts from cyber security response teams to cooperate on handling security incidents, to share information about vulnerabilities and threats. FIRST is also very active in publishing standards related to the cyber security. Among the most commonly used systems operated by FIRST belongs CVSS: Commmon Vulnerability Scoring System that provides standards on the characteristics and severity of softeare vulnerabilities. Another broadly used system MISP (malwareinformation sharing platform). Besides of a sw platform for collecting, storing, distributing and sharing malware information, it provides also a great number of standards that help sharing info with humans and automated systems. The MISP core format is based on JSON. The other standards address various template that are used to construct MISP objects, taxonomy format for description of machine (triple) tag vocabularies, galaxy format for attaching additional information such as MISP events or attributes, and a SightingDB format that helps to give automated context to attributes (e.g. by counting occurrences and tracking times of observability). A new standard is being prepared – MISP warning list format.

The presentation will provide a brief introduction to MISP standards.

References

1. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) https://eur-lex.europa.eu/eli/reg/2019/881/oj.
2. MISP – A threat sharing platform, User Guide, https://www.circl.lu/doc/misp/book.pdf