Panel Discussion on CTI Trends and Developments

Notes form the Panel Discussion on CTI Trends and Developments during the ENISA 2018 CTI-EU Event.

1 Threat intelligence community and practices

- Threat intelligence is not a feed or a threat list you can import, but it is an organizational function that deserves full attention. CTI depends on the organization and its structure.
- ENISA is good positioned to build a community around CTI: it is not a political entity, it has a brand and is trusted.
- Community building and collaboration should come from the government, but often there is a lack of expertise to do this. The request to provide these needs to first come from the people.
- There is a big shortcoming in the ingestion of threat intelligence, even if companies have security-related functions such as a SOC/CERT.

2 Training

- There is a significant shortage in work force. There are a number of commercial trainings for CTI available, but it is not clear whether these are enough and of high enough quality.
- Companies do not want to invest in training, they rather buy appliances.
- To solve the staffing problem, we should also look to automation and develop guidelines to apply machine learning to cyber security.
- Retention of talent is a problem in the public sector.
- Funding (e.g. from the EU) should not only be money, but also in-kind contributions for training such as a high-quality CTI syllabus.

3 CTI and SBM

- How SMBs can adopt CTI is a main concern, thus the benefits of CTI may not be applied to the majority of European companies
- For companies that don't have resources to build up a CTI capability, a managed CTI product would be a solution.

- But it is impossible for an external provider to deliver 'tailored' CTI to a company, you need in-house staff for this, - they can create -actionable- intelligence. It is however possible to create by-sector tailored CTI.

- Especially for SMEs, for example a bakery, it would be interesting to develop (thus fund) a small and low-maintenance CTI appliance that acts as a sensor device.

4 Changing threat landscape

- We see an increasing volume in malware, and the trend is accelerating. We should look for new opportunities for defense.

- In major recent incidents, we saw APTs did not actually rely on 0-days but completed the compromise with basic tools. This is indicative of the low level of cyber preparedness.

- In the cyber crime sphere, we have seen a push for professionalization and division of labor over the past decades. It has become almost trivial to conduct cyber criminal activities given these readily available services.

- The bulk of adversaries hasn't become more advanced, it is rather that we as a society are getting more vulnerable, for example with the introduction of low cost devices such as IoT.

5 Threat intelligence sharing

- It is very difficult to share information within and between communities, we need to establish common practices first.

- We need a common language when discussing cybersecurity issues / CTI with management, the NIST cybersecurity framework could be such a language.

- We probably need more regulation to legally require companies to share intelligence and information about possible vulnerabilities.

ENISA 2018 CTI-EU Event, Brussels 5th and 6th November 2018.