Title: Towards a Mature Cyber Threat Intelligence Practice

Abstract:

Over the past years, the landscape of cyber threats has greatly evolved. To deal with the sophistication and dynamics of present day cyber attacks, many organizations have fundamentally revised their cyber resilience strategies. Among other things, it has become common to complement traditional (preventive) security controls with elaborate provisions for security monitoring and incident response. Arguably, the next step in this evolution is to establish Cyber Threat Intelligence (CTI) capabilities. In essence, such capabilities serve to *anticipate* (imminent or emerging) cyber threats rather than awaiting an actual incident.

Collecting and handling CTI is a relatively new area of work. Correspondingly, practices and solutions in this field are largely in the pioneering stage and there is no commonly acknowledged understanding of what would constitute a “mature” CTI practice. This presentation will introduce the concept of CTI, the typical position of CTI practices in an organizational context and the *CTI Capability Framework* that TNO developed with three major Dutch financials to serve as a foundation for establishing effective CTI provisions.