Understanding Threat Intelligence

What is "threat intelligence"? A term overused and ill-defined! What is required to create a true threat intelligence capability, and how does this relate to the nirvana of cyber situational awareness? During this talk, we will: Define "threat intelligence", distinguishing between threat data and how this can be processed into "intelligence". Discuss some of the data sources (open and closed networks), how organizations are beginning to share more data, and the benefits of incorporating threat data into correlation systems. Explain why data must first be contextualized and ranked before it becomes "intelligence". Argue why this is difficult to automate effectively, and the role your security staff have in operationalizing the output.

Continue to describe the term "cyber situational awareness", referencing literature and movies in a fun way to explain how this is achieved and why it is important. Show how this enables organizations to achieve an almost unconscious heightened level of security preparedness.

Prof. Claudio Cilli,
CGEIT, CRISC, CISA, CISM

Prof. Claudio Cilli is a recognized world leading authority in the areas of National Security and Intelligence, company protection, information systems security and compliance, with over 25 years of experience. He currently advises governments and international companies in the cyber-security and critical infrastructure protection areas.

University professor and researcher. Lesson arguments include: computer science, software compilers, lexical and semantic analyzers, information systems analysis and development. Prof Cilli is a member of the scientific and advisory boards and teacher post-graduate master's in computer security and IT Governance.

He is a consultant to the U.S. Government and companies who supply the Department of Defense as well as to the United Nations. With many big firms, he is responsible of IS Audit and security projects, which include civil and military sectors, software quality and code security, security of the information systems and installations. Prof Cilli has designed and implemented systems based on mainframes and distributed architecture, including Disaster Recovery and both data and physical security, information and site protection.