Contribution ID : **34** Type : **not specified**

Cybersecurity as a service: the POC tool/platform for design and implementation.

The overwhelming increase of cyberattacks in all fields of Internet interactions points out, among other domains, a growth of 138% in the domain of online research and education in the first semester 2017.
The presentation will draw a framework for the interpretation of the global cybersecurity challenges dealing with vulnerabilities and threats, on one side.
On the other, it will face the definition of proper tools for prevention, detection and resiliation of cyberattacks by defining a new approach to cybersecurity.
Cybersecurity as a service is here intended as a multifaceted design in the technological approach and development of online services. Cybersecurity as a service asks for a brand new design and implementation of Internet infrastructures and services to be required of vendors on one side for asset technologies supplied to clients. On the other, cybersecurity as a service implies the capability of companies and institutions to manage cyber risks and perform assessment and evaluation according to structured analytics parameters that can manage conspicuous amounts of data.
The integration of the two approaches requires a cybersecurity analytics tool such as an ontological and pragmatic platform capable of control of technological assets, vulnerabilities, threats, events, incidents, etc.
In this perspective, the ability to prevent and detect cyberattacks, the definition of methods and technologies for risk assessment and the application of remedial, technological and behavioral systems, the standardization of safety automation, etc. ask for the knowledge, definition and representation of the constituent elements of potentially or factually recorded cyber events and incidents, the typological variables that define events and incidents, data representation models, and so on. "The domain of information risk can be visually represented as four intersecting landscapes of Threat, Asset, Impact, and Control. The organization's ability to understand and manage the risk requires information from each landscape. Security metrics, then, should create knowledge that improves management's ability to make decisions and execute on them "(Veriscommunity.net).

The over-all effort requires therefore the availability of knowledge repositories to be structured into ontological systems where operations security management processes may allow for systems
and software assessment and turn into operational enterprise networks where specific check points activities may be regularly conducted.
In the POC platform I shall briefly illustrate the operational tool that offers the cybersecurity domain ontology/knowledge representation as well as the pragmatic operational tools for distinct cybersecurity activities.
The pragmatic cybersecurity ontology allows several interconnected applications: operational grids/forms, ontology metalanguages, cyber-security remedial software, industry specifics.
The cybersecurity domain ontology is a system of linked relations standing for the knowledge representation. It comprises seven fields and more than 600 entities. It is open to eventual integrations as needed by the evolution of the system.
The cybersecurity pragmatic ontology is based on the domain ontology and displays a suite of seven digital services: the semantic vocabulary, the risk assessment and the risk evauation areas, the mitigation and the remediation tools, the standards references and the application tools.
The application tools include virtual forms to be filled in and archived in customizable data bases that may be connected with legacy systems.
Services accessed in POC allow for:
• the back up and archive data bases related to trends of assessment, evaluation and incident reporting such as statistics, metrics, standards;
• the comparison of data referring to events and incidents;
• big data analytics with preventive and predictive actions.
Multiple implementation of categories and insertion of new entities are envisaged in POC and the application of machine learning and complete automated acquisition of data are the final expected results.
POC is realized on Liferay, a horizontal portal written in Java; Post-gres, relational database and Elastic search engine written in Java.

Primary author(s) : Prof. ZUANELLI, elisabetta (university of rome "tor vergata")

Presenter(s) : Prof. ZUANELLI, elisabetta (university of rome ”tor vergata”)

Track Classification : Advanced Network Technologies and Services