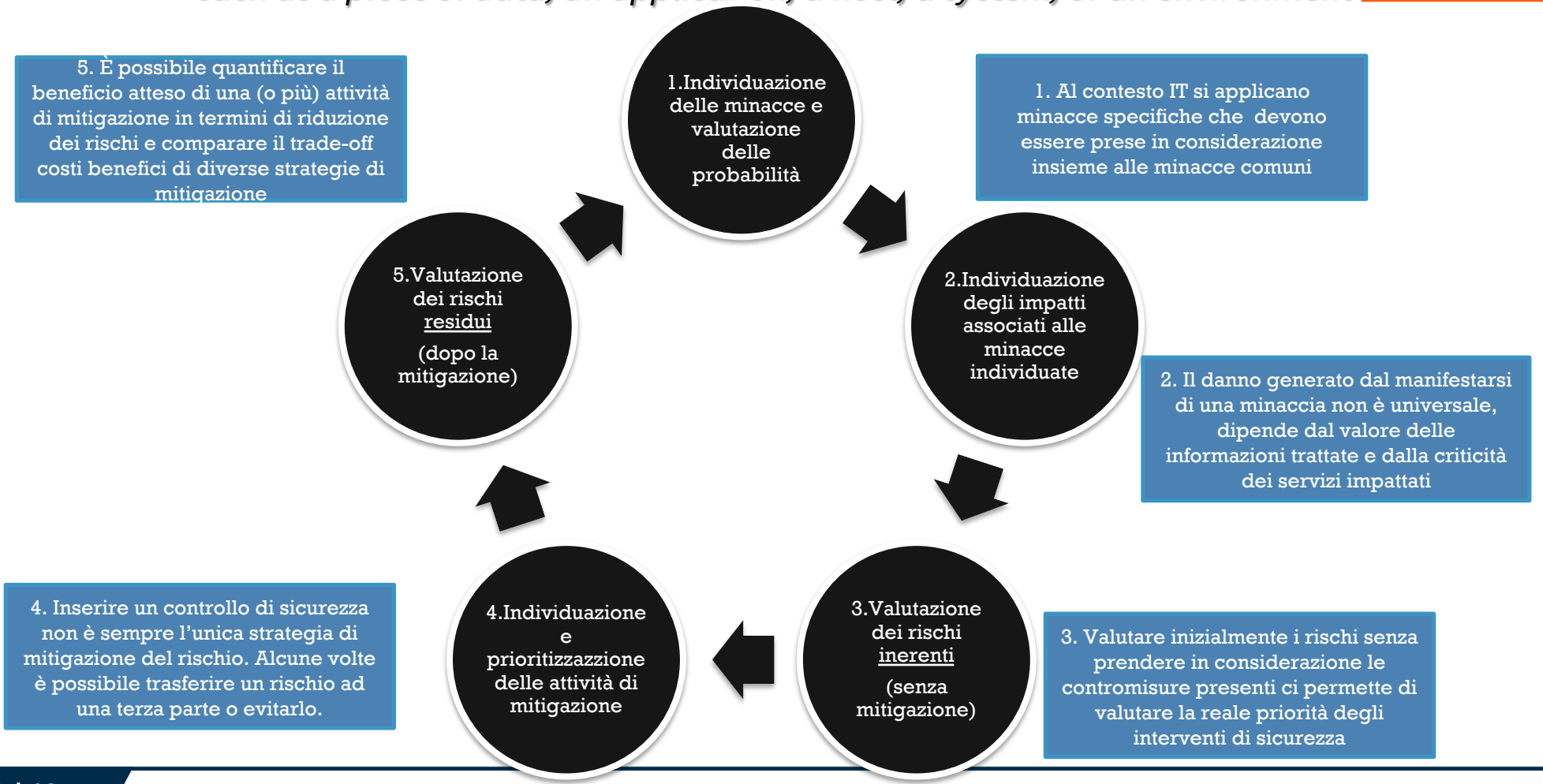
CYBER THREAT MODELLING

TAVOLO 2 – 21 Novembre 23

Marco Lombardozzi
Pre Sales Leader

BeDisruptive™

A form of risk assessment that models aspects of the attack and defense sides of a logical entity, such as a piece of data, an application, a host, a system, or an environment NIST SP 800-53 Rev. 5



Una classificazione delle tattiche associate agli attacchi informatici e relative tecniche viene fornita dal MITRE Att&ck per tre tipologie di contesto: Enterprise; Mobile e Industrial Control Systems (ICS).

ATT&CK®

Reconnaissance	Exfiltration	Discovery	Lateral Movement
Resource Development	Persistence	Collection	Credential Access
Initial Access	Privilege Escalation	Command and Control	Defense Evasion
	Impact		

Definizione Glossario CSRC del NIST (SP 800-53): Vulnerability

Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.

Nell'ambito della sicurezza informatica possiamo definire due macro-categorie di vulnerabilità:

- Vulnerabilità non note (0 day): Vulnerabilità non espressamente note al proprietario del software (e.g. vendor, sviluppatore) e di conseguenza non rese pubbliche;

- Vulnerabilità note: Vulnerabilità pubblicamente documentate per cui il proprietario del software ha (o sta sviluppando) una patch correttiva da mettere a disposizione degli utilizzatori del software (e.g tramite aggiornamento).

Esempio: Probabilità Exploitation di una vulnerabilità