CENG 374E - INTRODUCTION TO COMPUTER SECURITY

Prof. Dr. Şeref SAĞIROĞLU
Gazi University
Engineering Faculty
Computer Engineering Department
Maltepe/Ankara

SS@gazi.edu.tr
https://avesis.gazi.edu.tr/ss

RISK OF SECURITY?

Reasons for Cyber Attacks

01 Information Theft and Manipulation

02 Damaging the Reputation

03 Business Disruption

04 Financial Loss

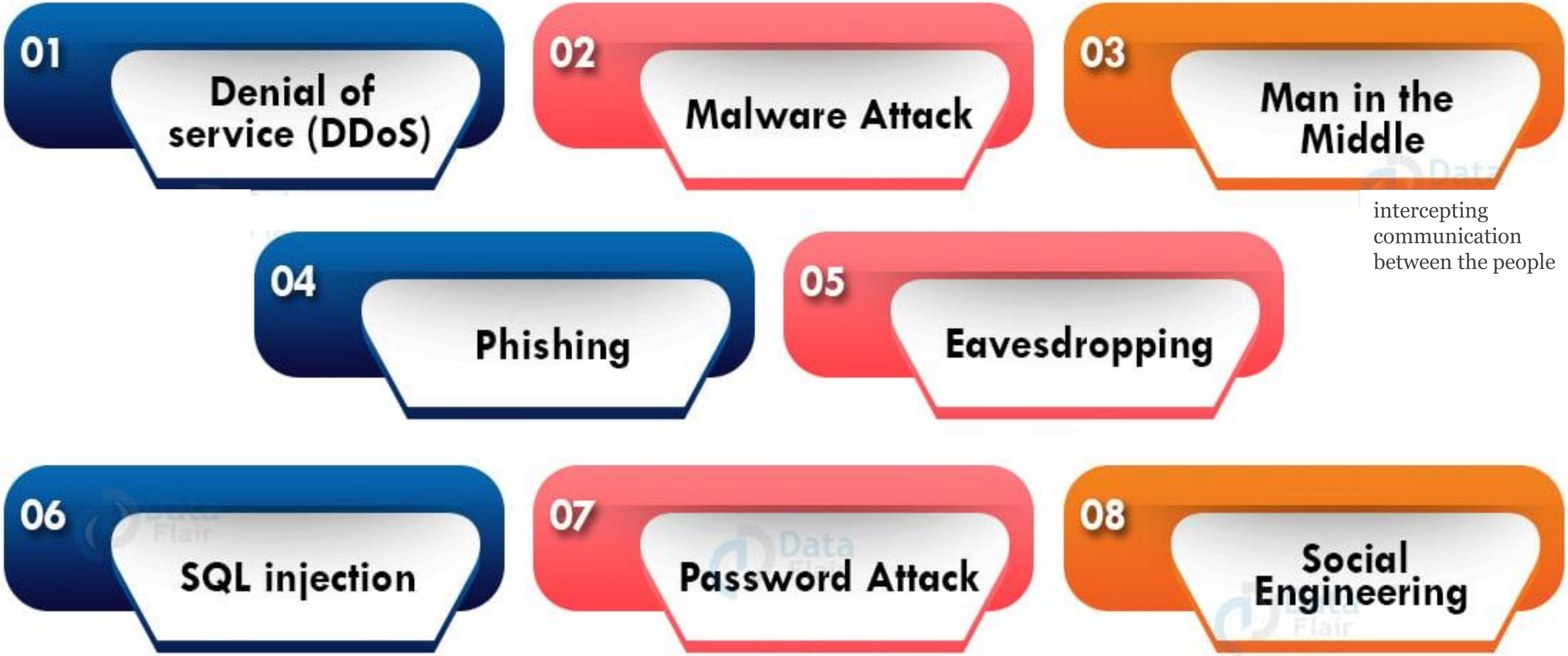
05 Achieving Military Objectives

06 Creating Chaos and Disruption

07 Demanding Ransom

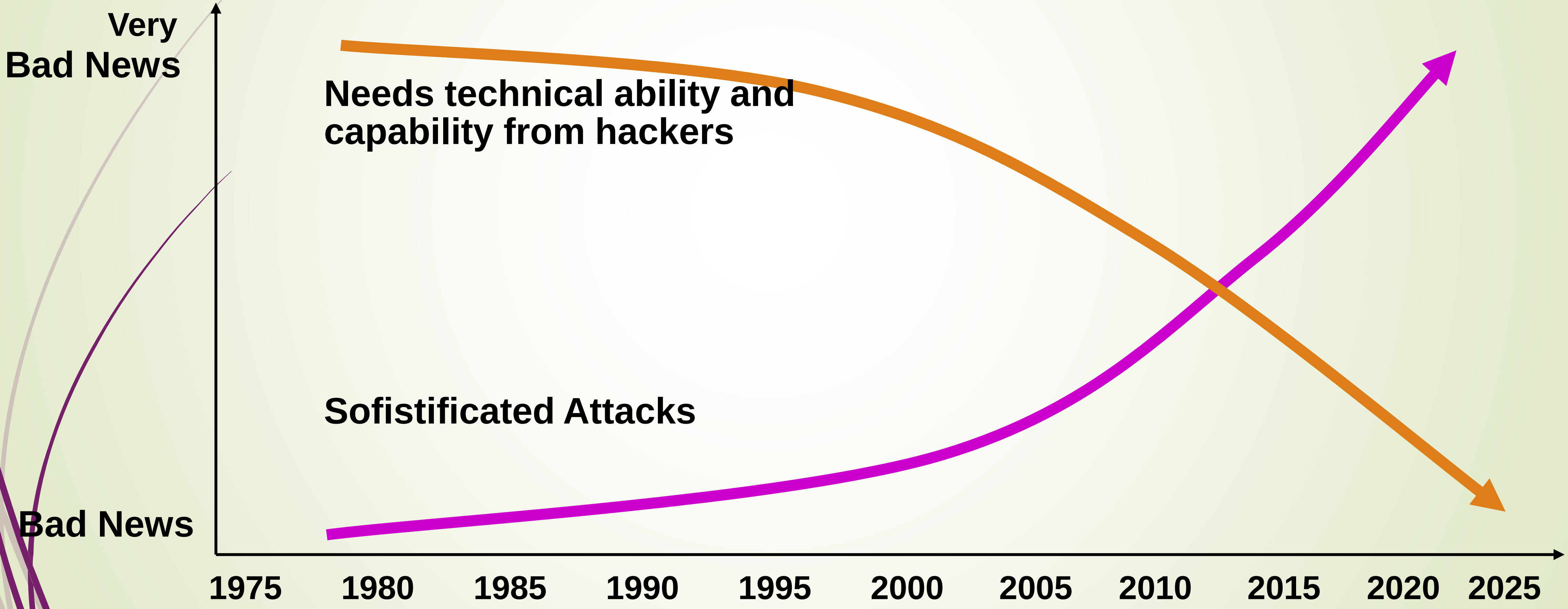
08 Propagating Religious Beliefs

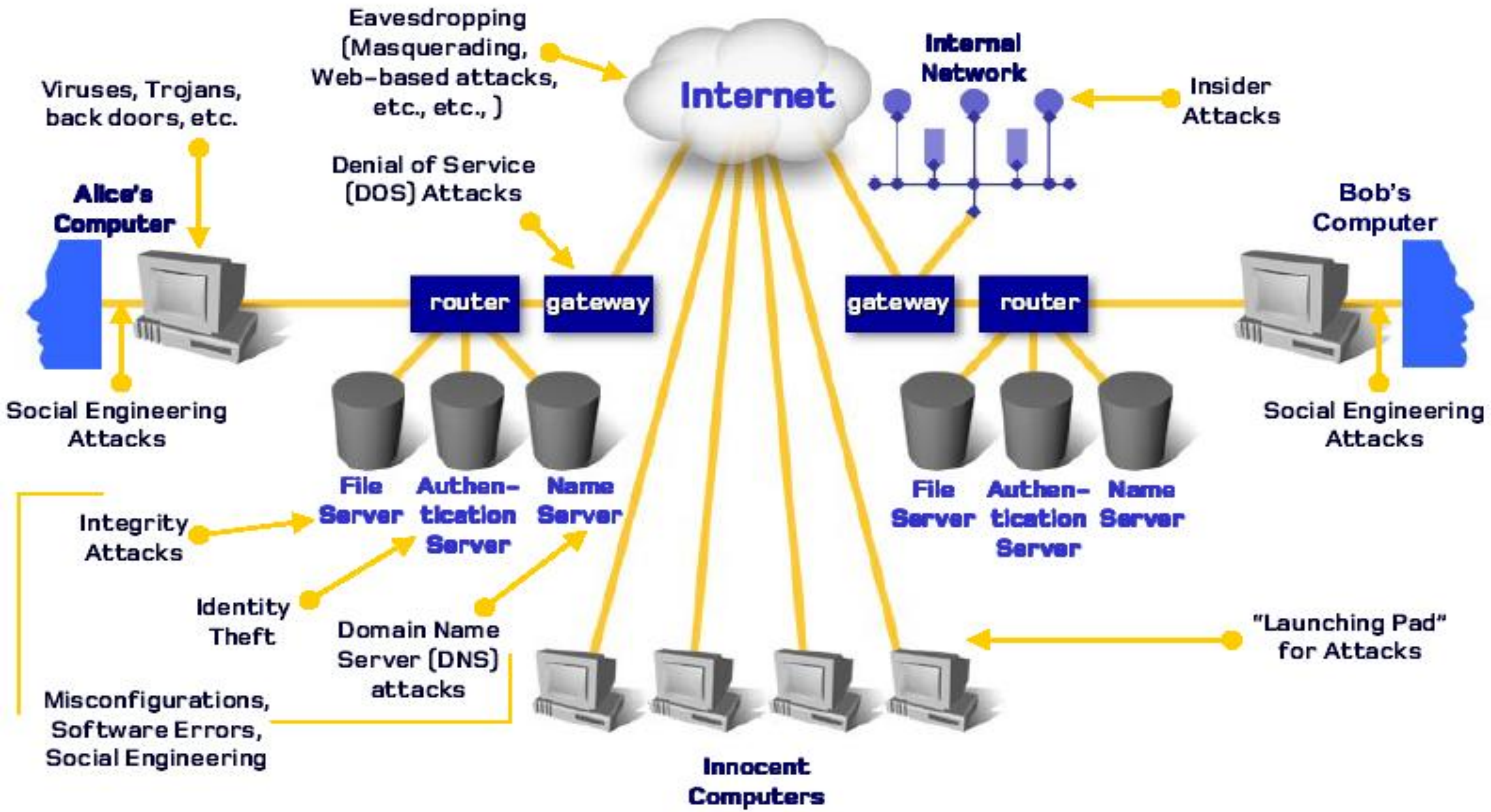
Types of Cyber Attacks



intercepting
communication
between the people

AVAILABLE CONCERNS




Eavesdropping (Masquerading, Web-based attacks, etc., etc.,)
Internet
Internal Network
Insider Attacks
Viruses, Trojans, back doors, etc.
Denial of Service (DOS) Attacks
Alice's Computer
Bob's Computer
router
gateway
gateway
router
Social Engineering Attacks
Social Engineering Attacks
File Server
Authen-tication Server
Name Server
File Server
Authen-tication Server
Name Server
Integrity Attacks
Identity Theft
Domain Name Server (DNS) attacks
"Launching Pad" for Attacks
Misconfigurations, Software Errors, Social Engineering
Innocent Computers

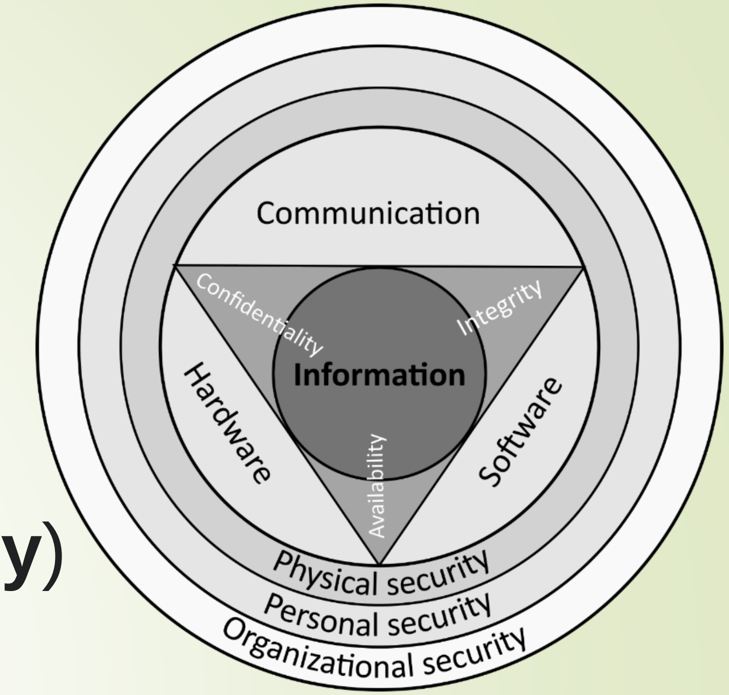
What kind of a SECURITY PERSPECTIVE?

What kind of a security?

Computer security
Cybersecurity (**cyber security**), or
Information technology security (**IT security**)

the protection of computer systems and networks from attack by malicious actors that may result in unauthorized information disclosure, theft of, or damage to hardware, software, or data, as well as from the disruption or misdirection of the services they provide.

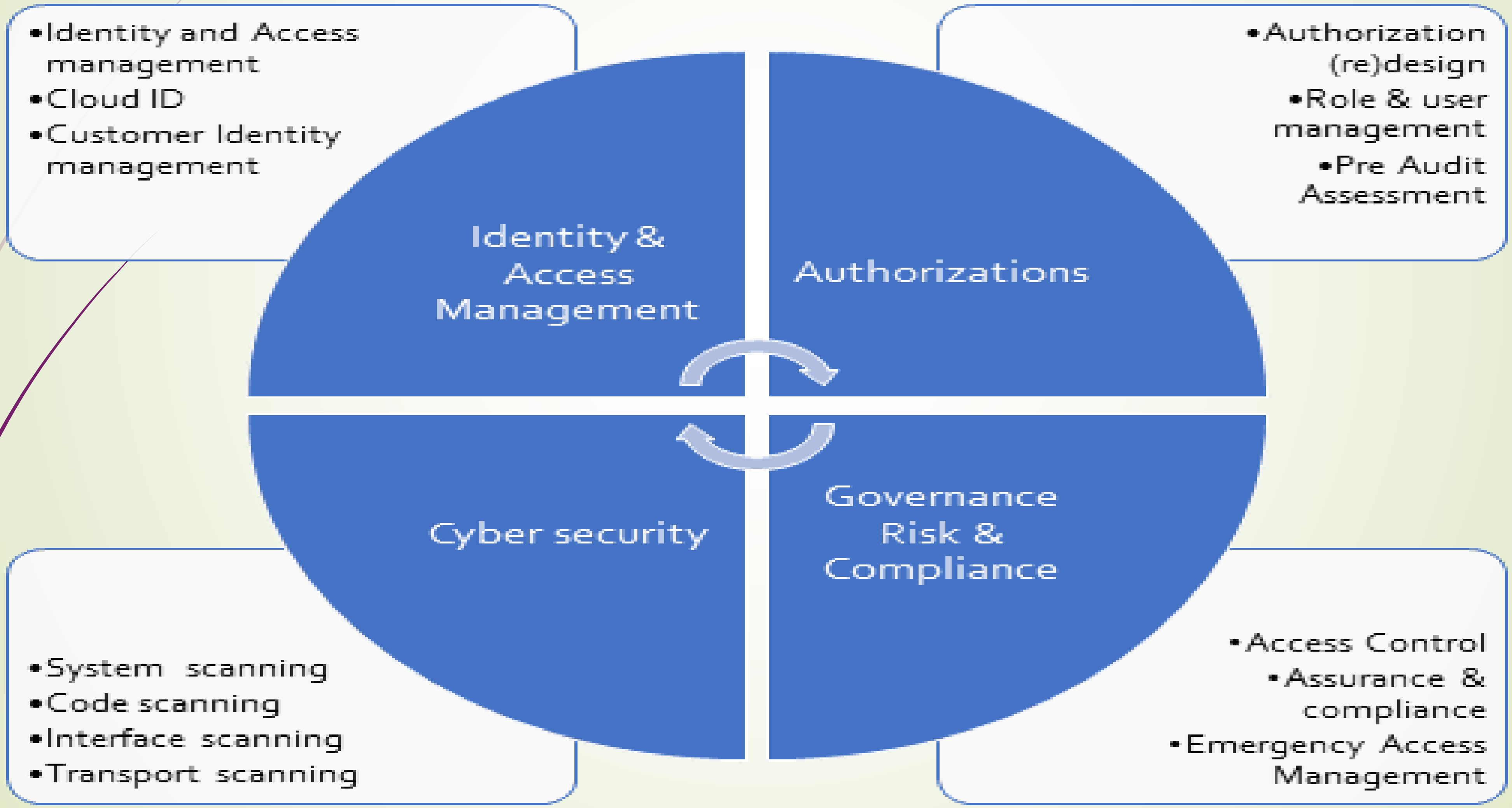
What kind of a security?



Computer security
Cybersecurity (cyber security), or
Information technology security (IT security)

the protection of computer systems and networks from attack by malicious actors that may result in unauthorized information disclosure, theft of, or damage to hardware, software, or data, as well as from the disruption or misdirection of the services they provide.

What kind of a security?



- Identity and Access management
- Cloud ID
- Customer Identity management

Identity & Access Management

Authorizations

- Authorization (re)design
- Role & user management
- Pre Audit Assessment

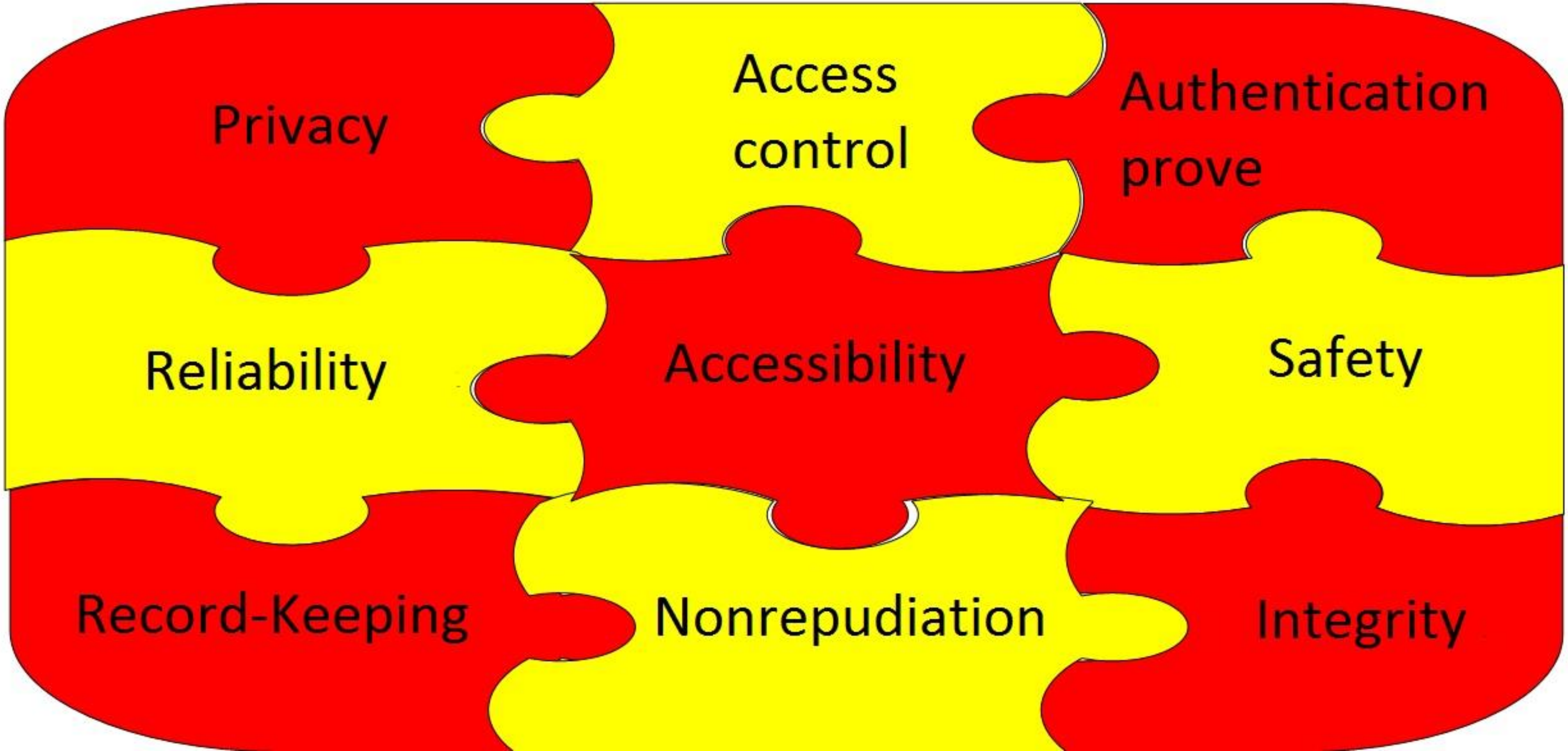
Cyber security

- System scanning
- Code scanning
- Interface scanning
- Transport scanning

Governance Risk & Compliance

- Access Control
- Assurance & compliance
- Emergency Access Management

What kind of a security?



Privacy

Access control

Authentication prove

Reliability

Accessibility

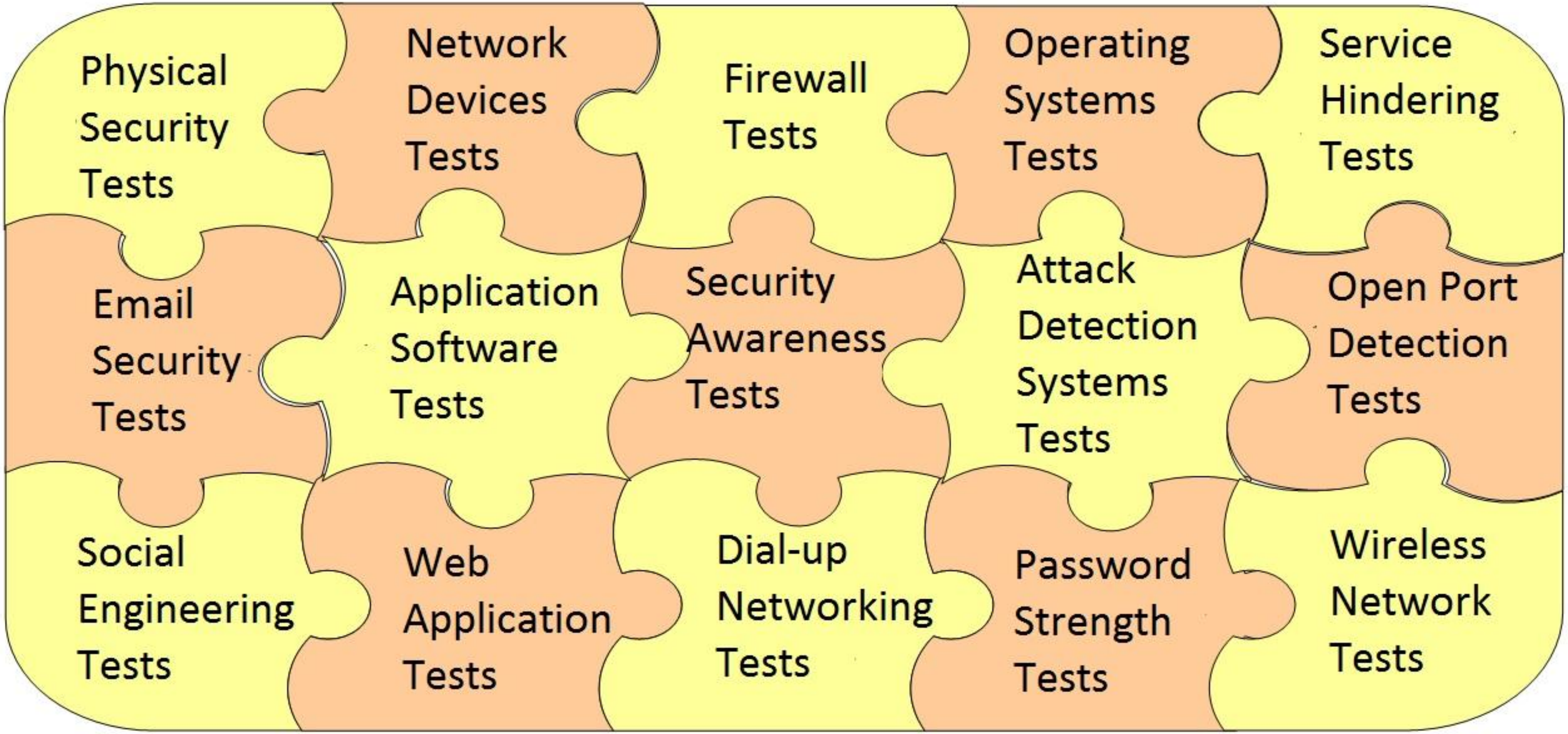
Safety

Record-Keeping

Nonrepudiation

Integrity

What kind of a security?



Physical Security Tests

Network Devices Tests

Firewall Tests

Operating Systems Tests

Service Hindering Tests

Email Security Tests

Application Software Tests

Security Awareness Tests

Attack Detection Systems Tests

Open Port Detection Tests

Social Engineering Tests

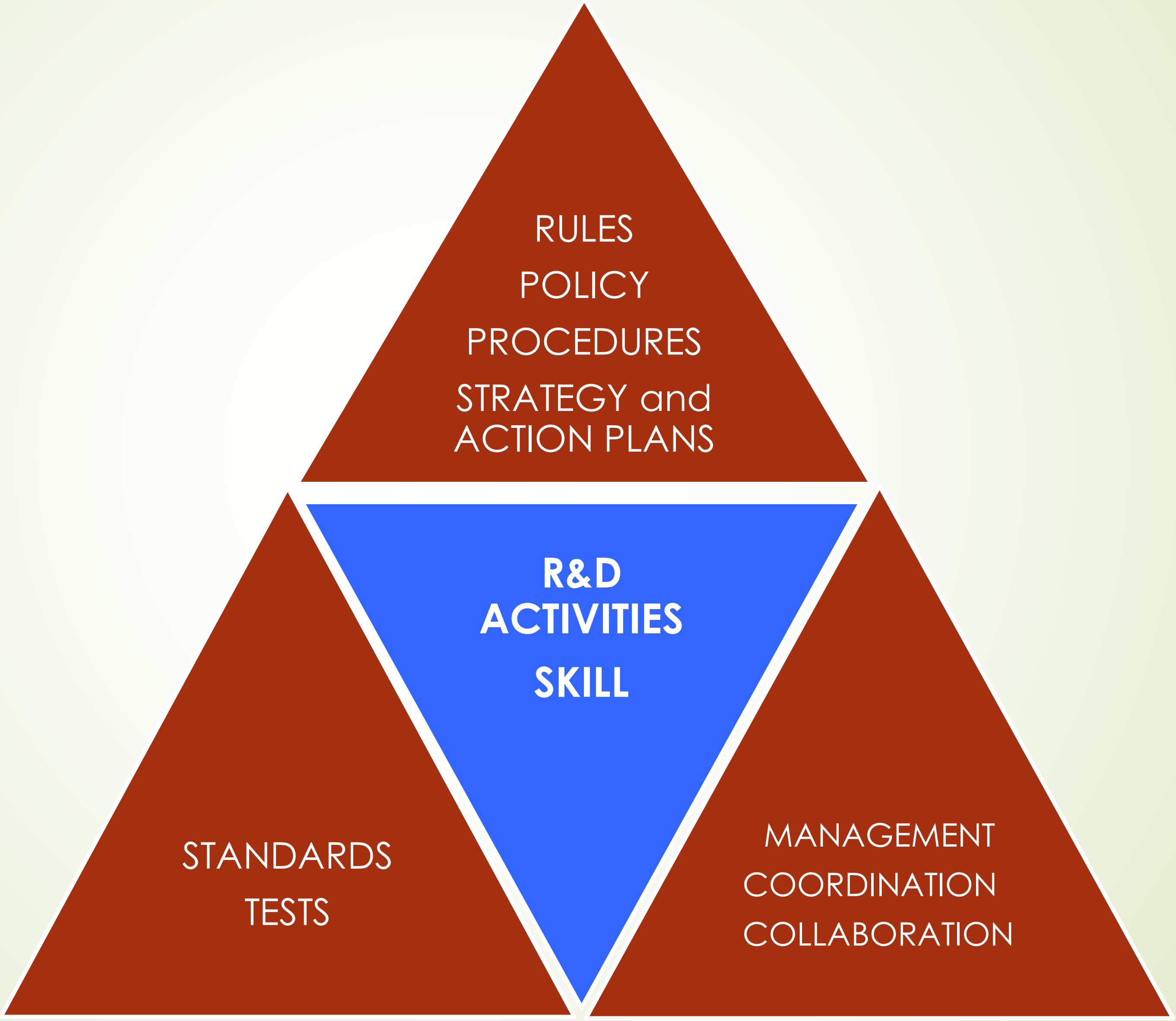
Web Application Tests

Dial-up Networking Tests

Password Strength Tests

Wireless Network Tests

What kind of a security?



RULES

POLICY

PROCEDURES

STRATEGY and ACTION PLANS

R&D ACTIVITIES

SKILL

STANDARDS

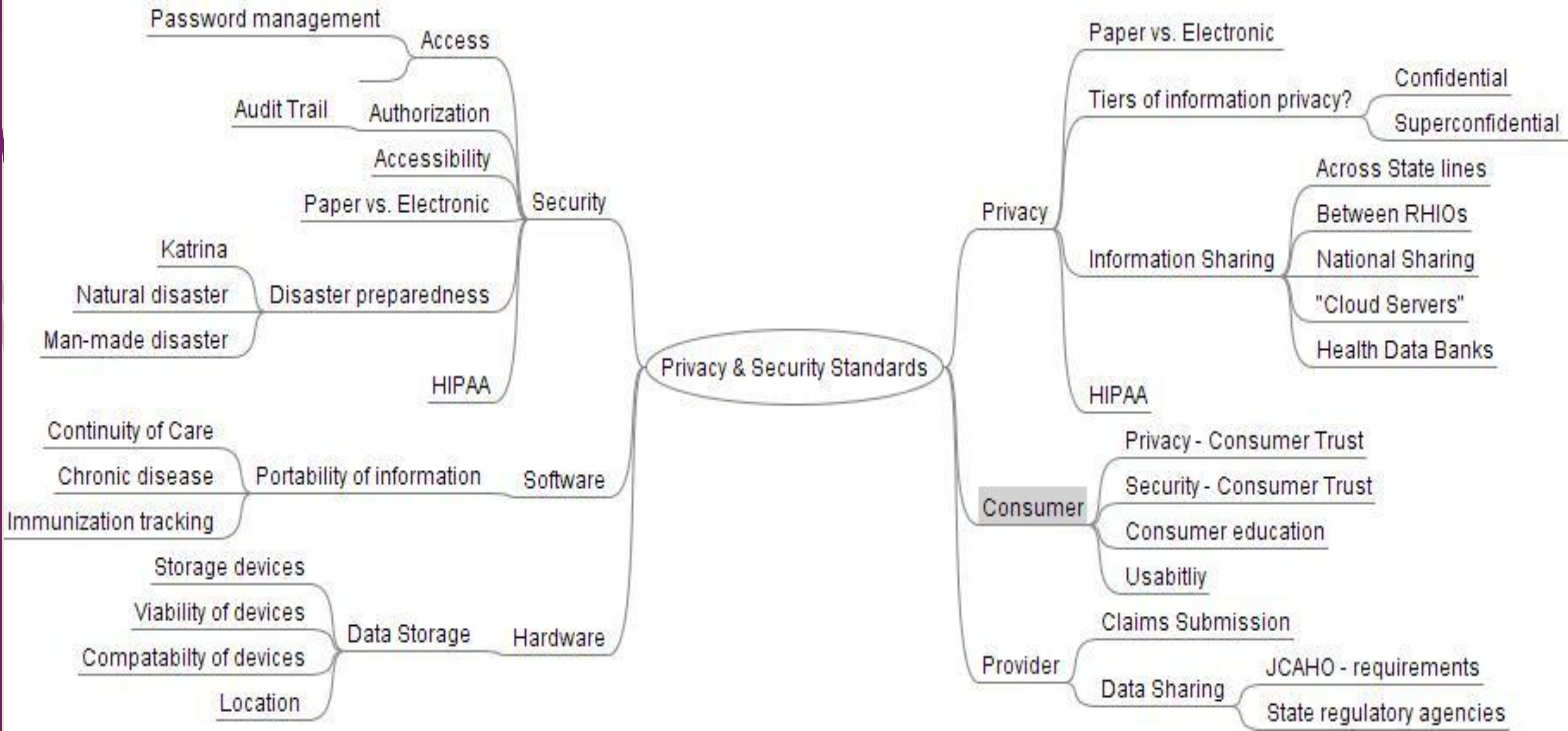
TESTS

MANAGEMENT

COORDINATION

COLLABORATION

What kind of a security?



Information Security Standards

ISO 27000 series defines InfoSec standards.

- ISO 27001: Information Security Management System (ISMS) Requirements
- ISO 27002: ISM Code of Practice
- ISO 27003: ISMS Implementation
- ISO 27004: ISM Measurement
- ISO 27005: Information Security Risk Management
- ISO 27006: Audit and Certification of ISMS

…

Information Security Standards

ISO 27000 series defines InfoSec standards.

- ISO 27011: ISM Guidelines for Telecommunication Organizations
- ISO 27014: Information Security Governance
- ISO 27015: ISM Guidelines for Financial Services
- ISO 27033: Network Security
- ISO 27034: Application Security

…

What kind of security?

- Cyber security is very good research area
  - Technical
  - Social
  - Economical
  - Policy
- It contains many threats and opportunities.
  - To establish cyber security ecosystem
  - A good management, collaboration,
  - To find the common sense
- To Know, Implement, Monitor and Control the Standards
- Human-Education-Technology

What to do?

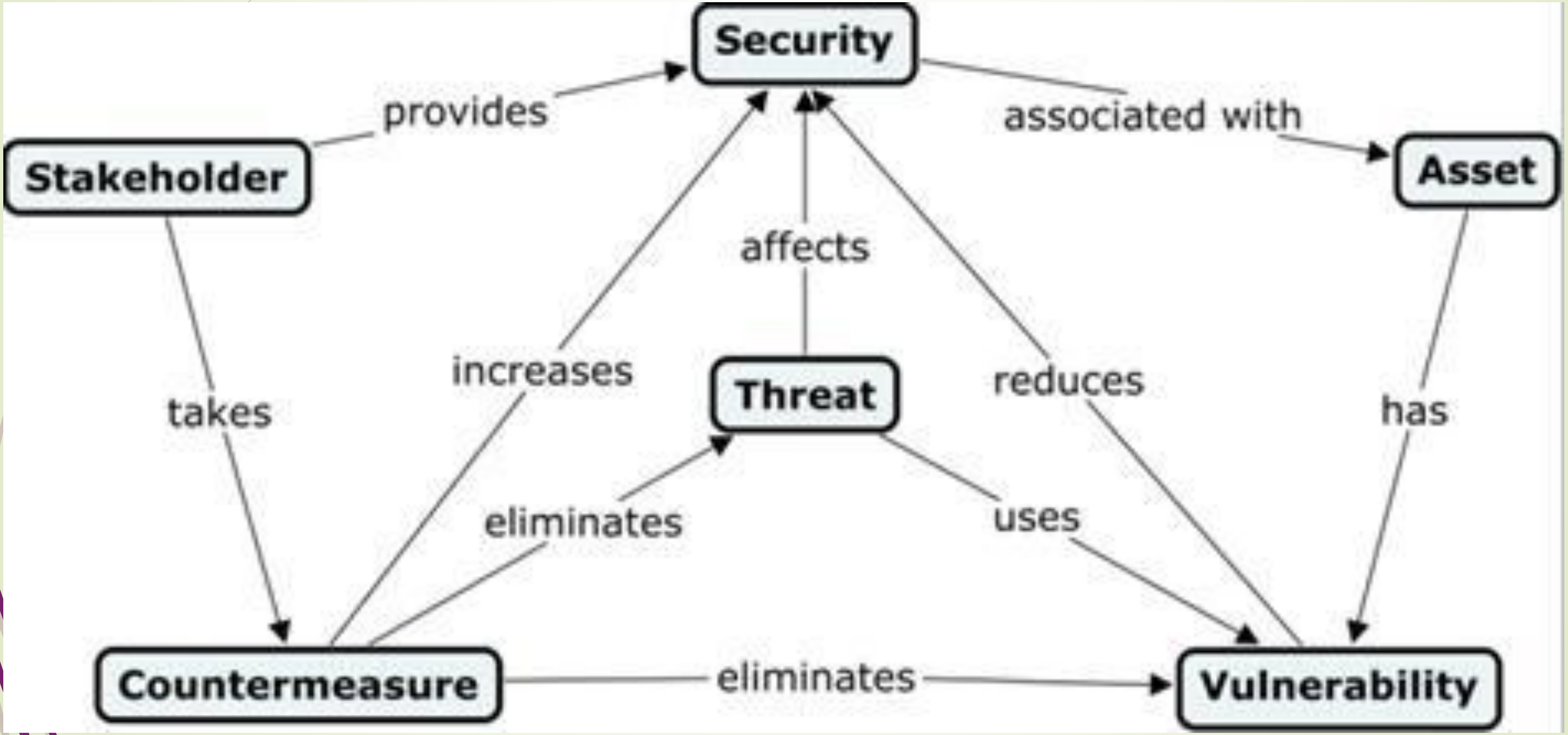
- To invest in cyber security,
- To create eco-system,
- To produce more, to improve the terms of protection,
- To increase the skilled manpower,
- To increase the number of organizations implementing the standards,
- To increase audits and publish the results,
- To increase the number of programs,
- To increase cooperation,
- To strengthen the weak links,
- ..

Ontologies?

- a structure consisting of a set of concepts and categories related to a certain area of knowledge, as well as information about their properties and the links between them.
- Ontologies are distinct from **knowledge bases** or **taxonomies**.
- The ontology of a particular area of knowledge must include comprehensive general information about it, whereas a knowledge base may contain incomplete data and information about particular cases.
- Data scientists use a variety of **ontology languages** to work with ontologies. OWL (Web Ontology Language) is the most common ontology language.

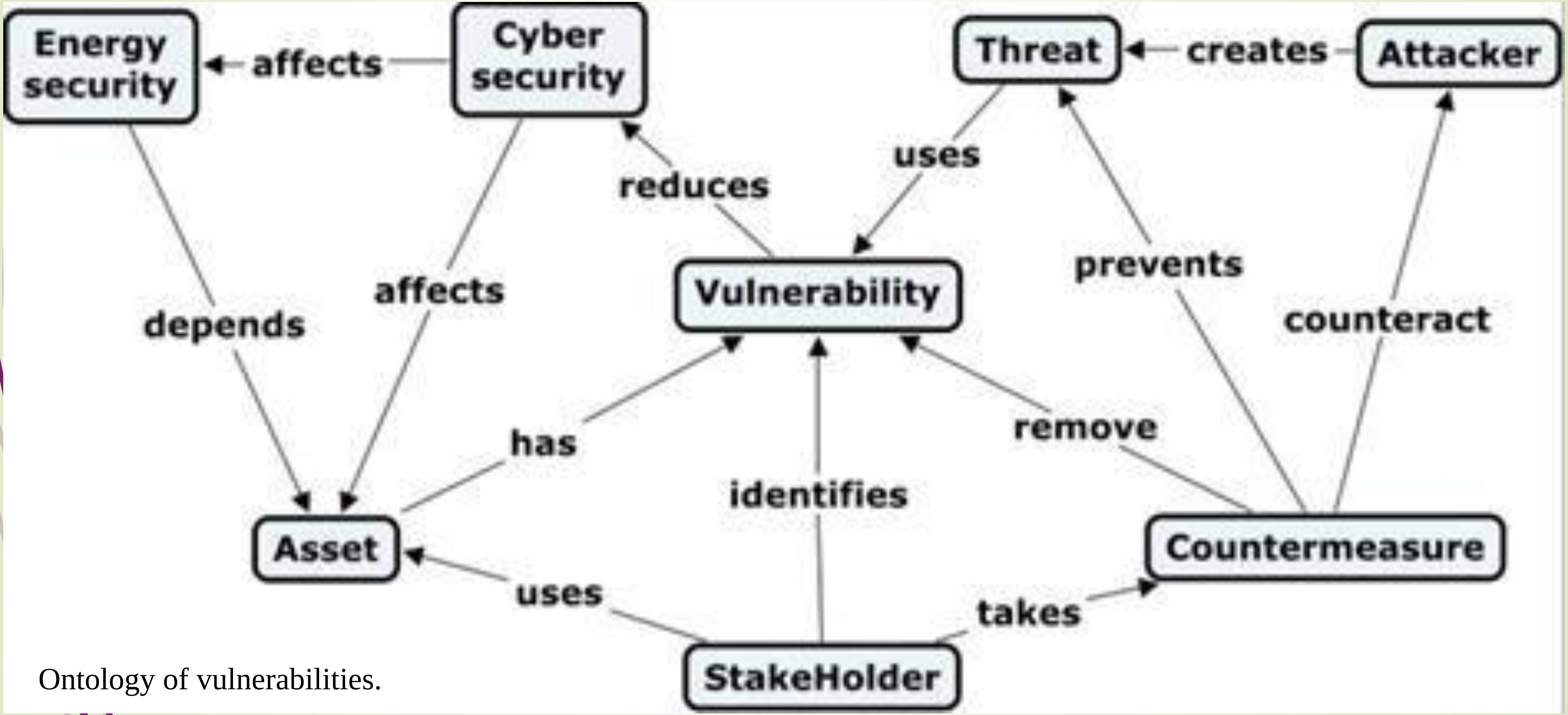
What kind of a security?

The relationship of the basic concepts



Source: Advances in Intelligent Systems Research, volume 158

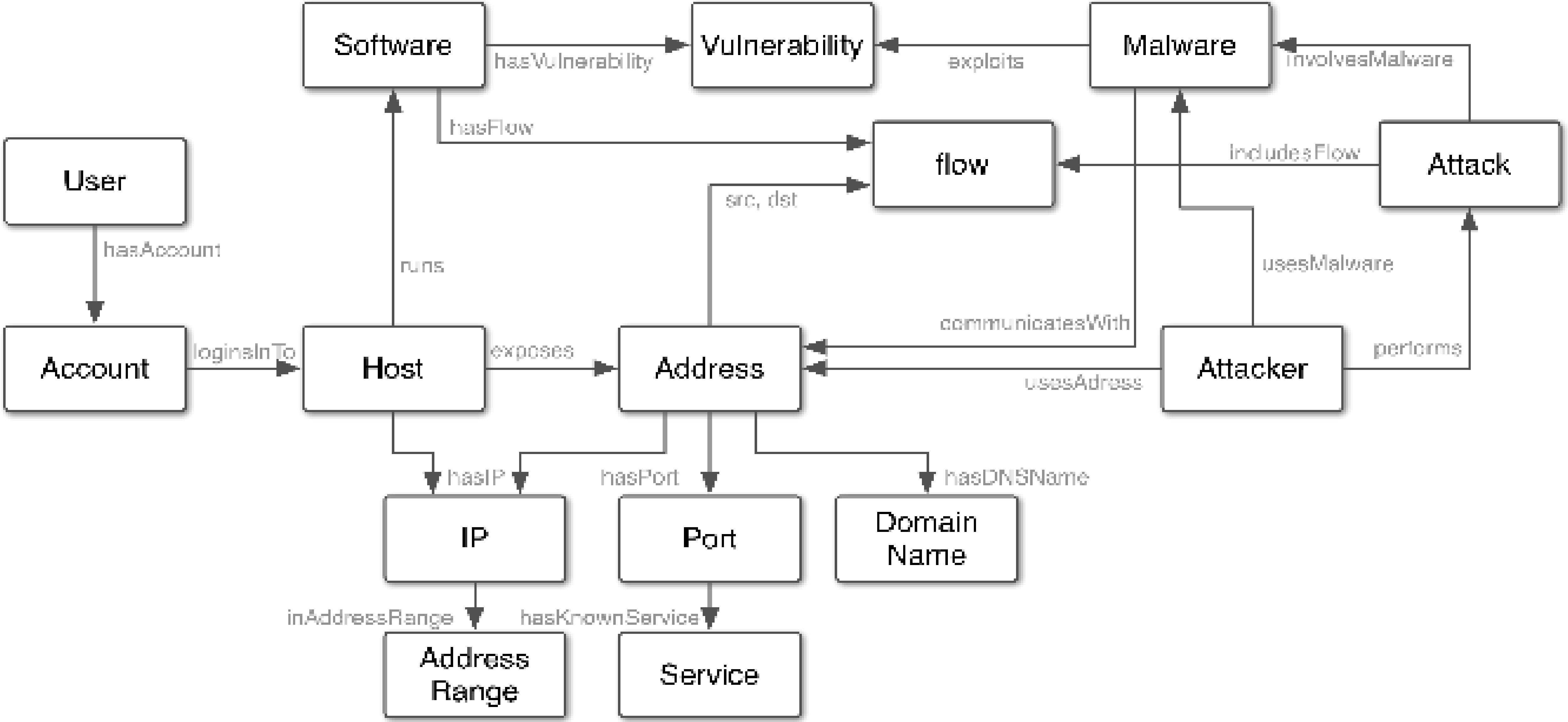
What kind of a security?



Ontology of vulnerabilities.

Source: Advances in Intelligent Systems Research, volume 158

What kind of a security?



https://www.semanticscholar.org/paper/Cybersecurity-Vulnerability-Management%3A-An-Model-Syed-Zhong/b90bfd42b74622cc5afc77d59e613f6113f05e26

What kind of a security?

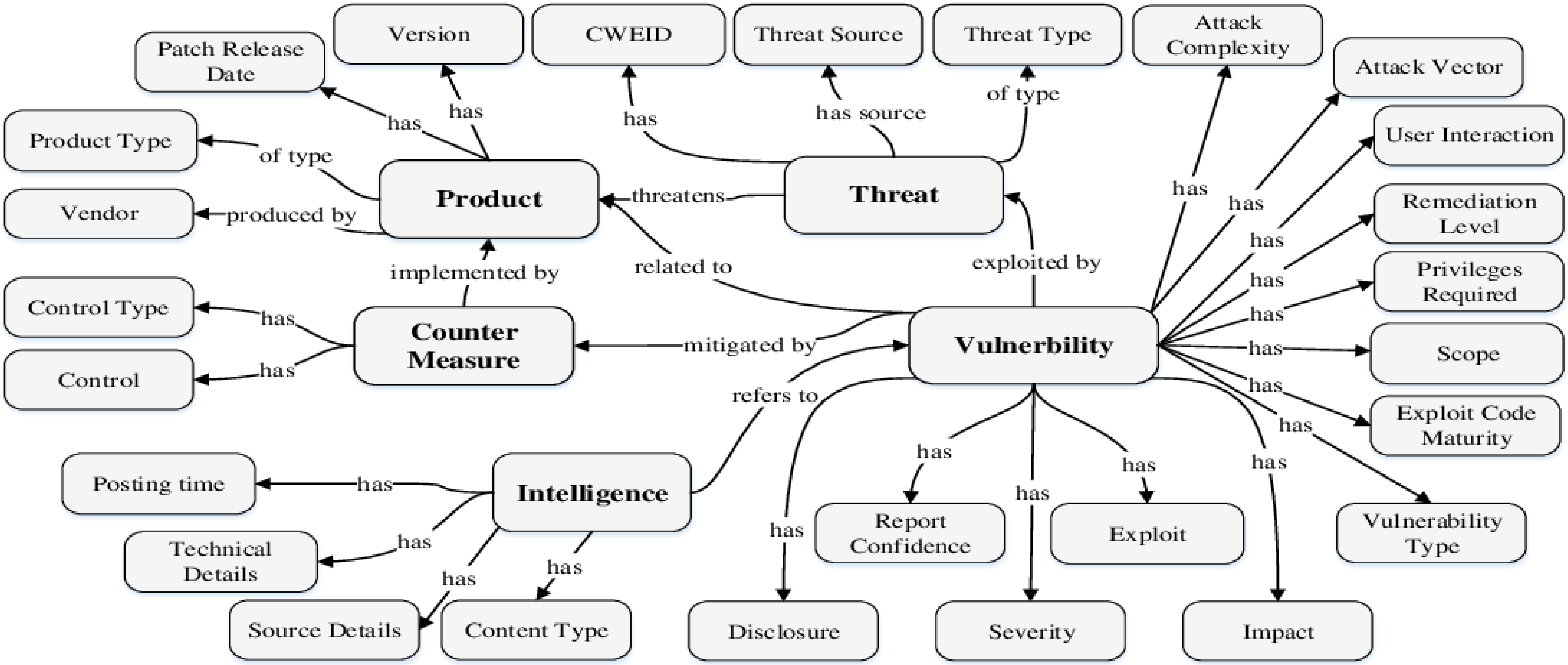
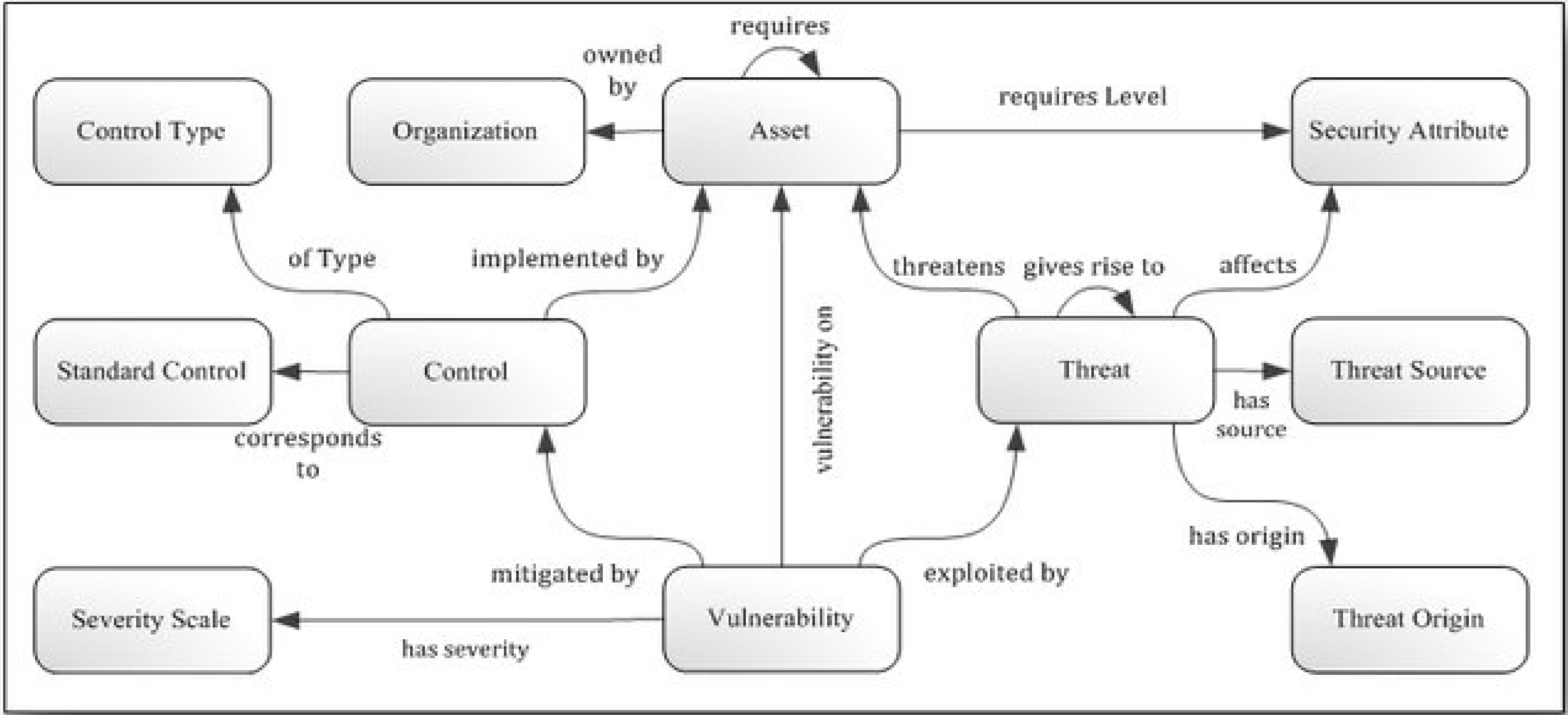


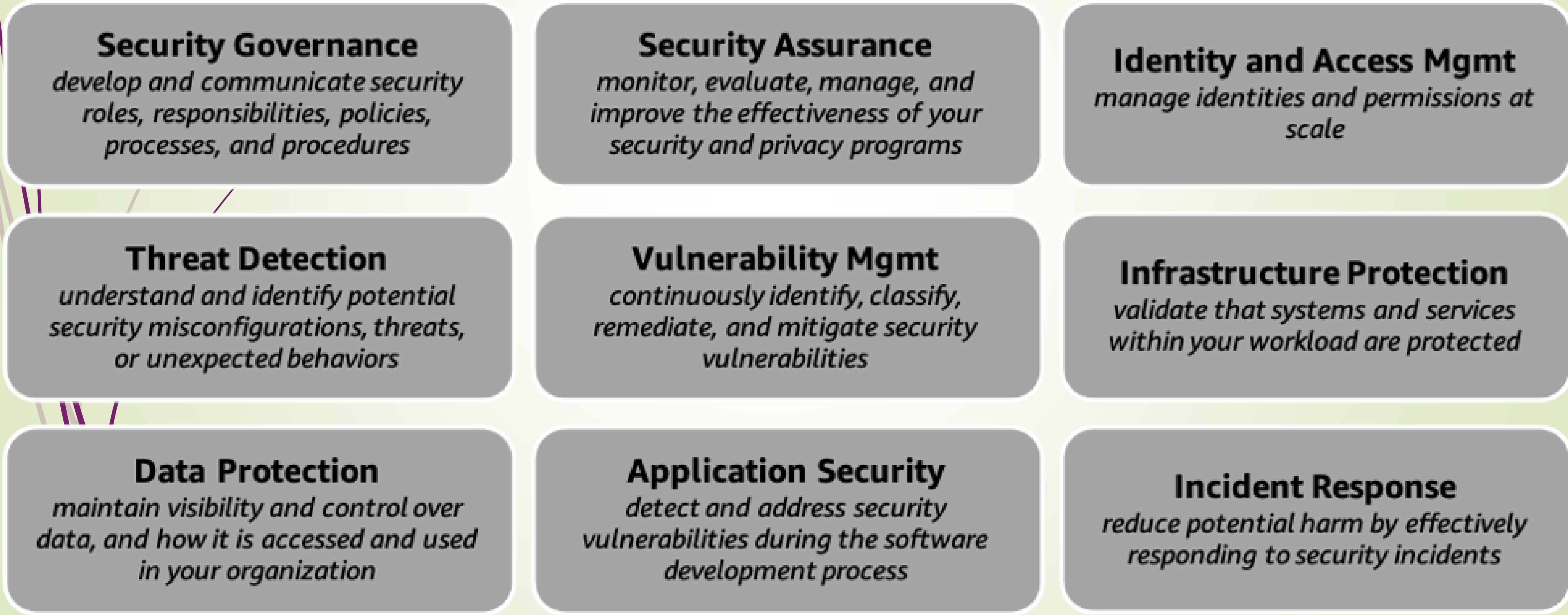
Figure 1: Conceptual Vulnerability Management Ontology

What kind of a security?



Security perspective: compliance and assurance

The *security* perspective helps to achieve the confidentiality, integrity, and availability of the data and cloud workloads. It comprises nine capabilities.



Security Governance
develop and communicate security roles, responsibilities, policies, processes, and procedures

Security Assurance
monitor, evaluate, manage, and improve the effectiveness of your security and privacy programs

Identity and Access Mgmt
manage identities and permissions at scale

Threat Detection
understand and identify potential security misconfigurations, threats, or unexpected behaviors

Vulnerability Mgmt
continuously identify, classify, remediate, and mitigate security vulnerabilities

Infrastructure Protection
validate that systems and services within your workload are protected

Data Protection
maintain visibility and control over data, and how it is accessed and used in your organization

Application Security
detect and address security vulnerabilities during the software development process

Incident Response
reduce potential harm by effectively responding to security incidents

Q&A