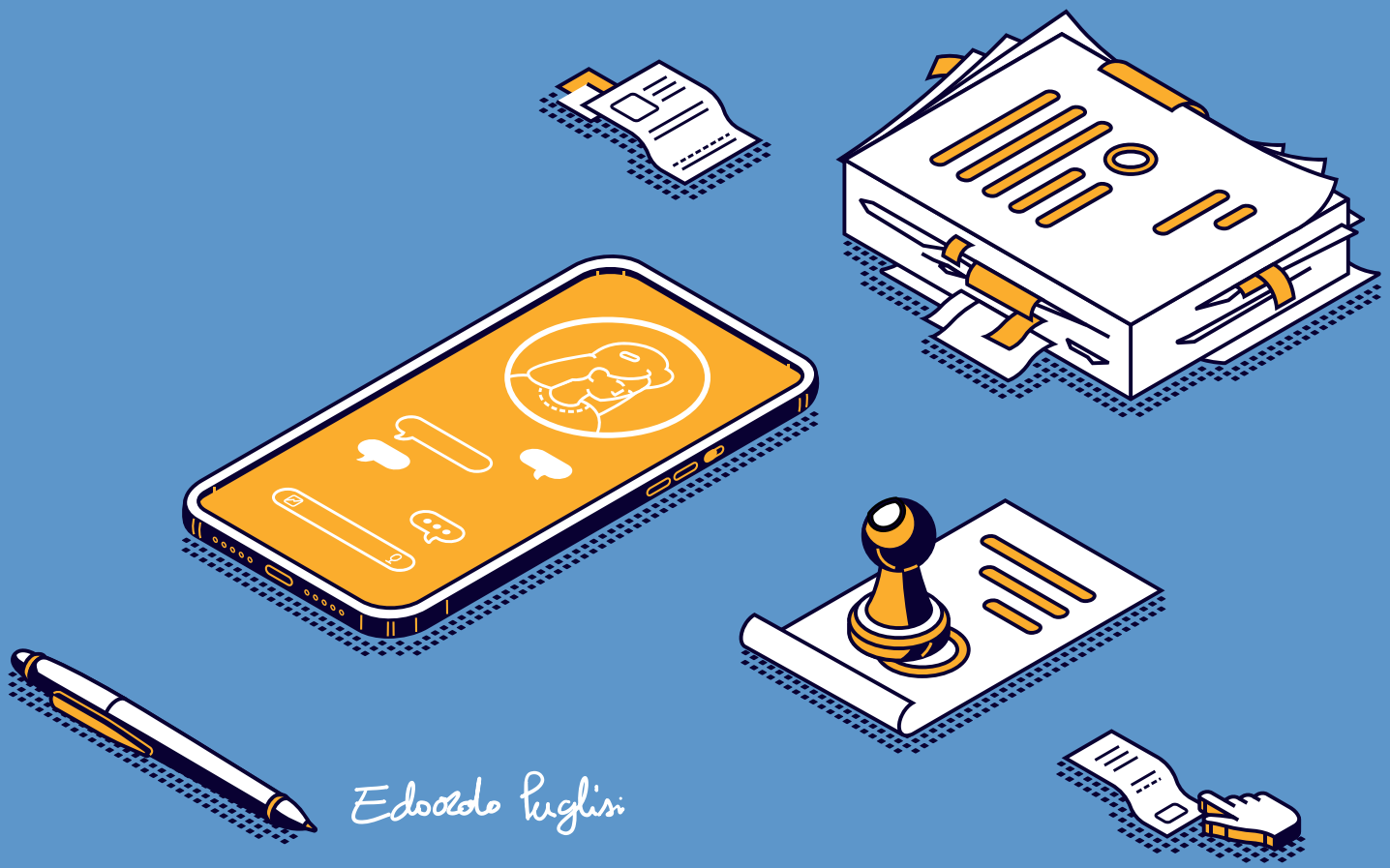
Security Governance

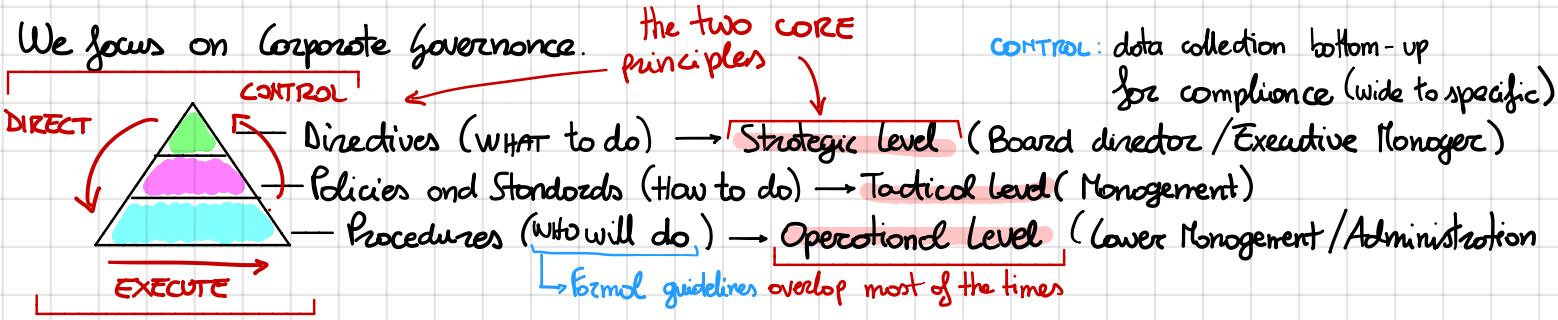


CONTEXT

The context in which we will work is a general enterprise with its own mission.
Enterprises are made by people divided in multiple connected department trough processes and relationships (CEO, manager etc)
We CAN'T focus just on security by technological point of view!

GOVERNANCE: processes + norms.
↳ Enterprice Governance: structure and relationships that control, direct or regulate the performance of an enterprise
↳ ① Business Governance: set of procedures that set how to build organisation's product
② Corporate Governance: set of rule to direct and control the business processes quality according to the rules of the organisation's sector.

We focus on Corporate Governance.



CONTROL: data collection bottom-up for compliance (wide to specific)

Our goal is to put in practice this direct/control loop taking into account

THREATS & VULNERABILITIES

The loop is driven by risks!
Direct = reduce risks
CONTROL = measure risk reduction

IT GOVERNANCE

IT systems causes serious risks to a company in terms of data and information stored and transmitted over the network.
Given a system, computing the risks means to identify electronic assests, their vulnerabilities and make an evaluation.

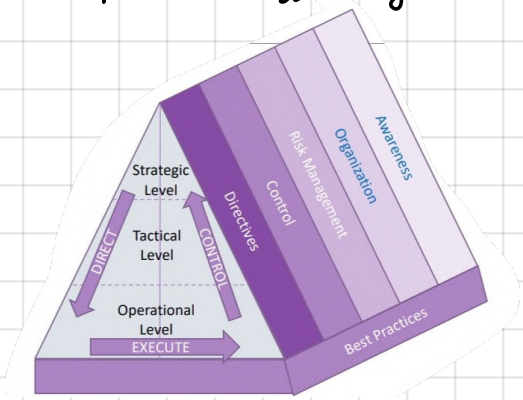
SECURITY GOVERNANCE

Put it simple is direct/control loop according to security. If done well, will effectively coordinate the security activities of the organisation.

Where to put the organisation depends on different factors...

Formalized	Informal
Framework	Approach

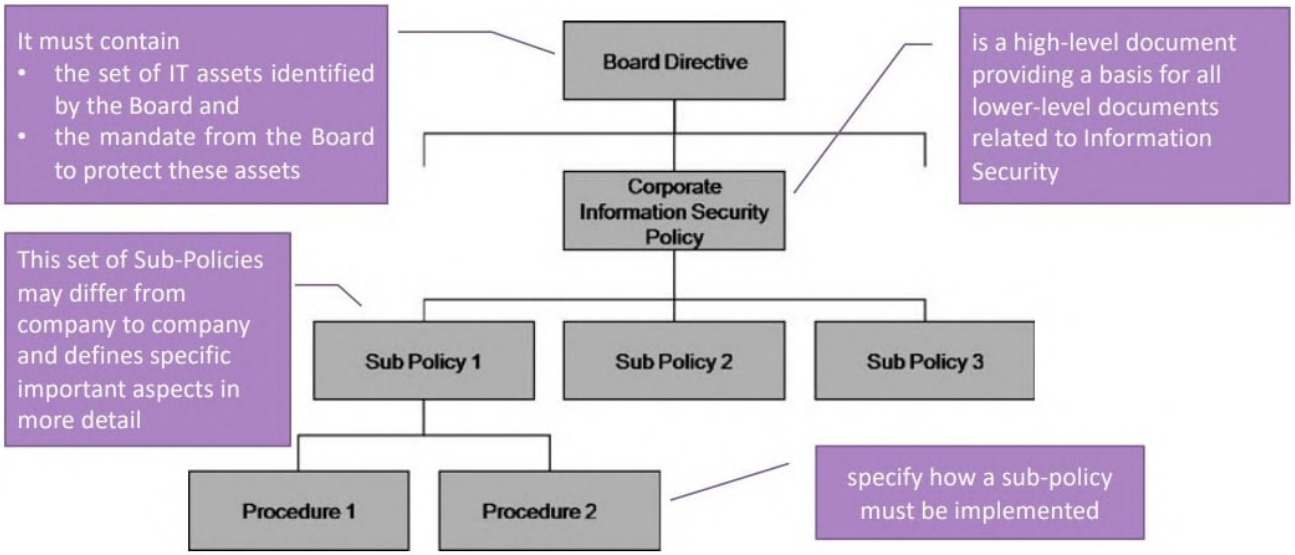
In practical terms we need to:
① Identify security decision needed to be made
② Who will make them
③ Identify information and resources needed



DIRECTIVES

How do we know what are the right things to do? Best Practices (or Standards or Guidelines) are a set of documents reporting experiences and solutions experienced by experts, providing an internationally accepted framework (eg ISO 27002)

Eg ISPA (Information Security Policy Architecture) is the methodology to create, manage and distribute policy related documents.



CONTROL

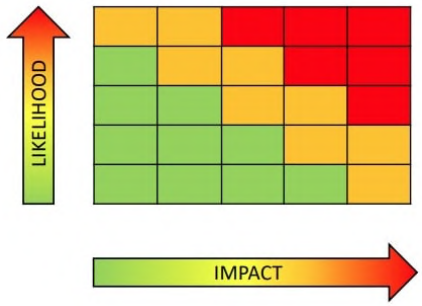
Compliance check is the main scope of the control part but specifying compliance clauses is not an exact science and very few guidelines are available

RISK MANAGEMENT

Is the process to identify and assess all potential risks as well as introducing controls that should mitigate all these risks to acceptable low levels. In most of circumstances risk has two factors associated to it:

① Probability / frequency
② magnitude of gain / loss (impact)

RISK = THREAT x PROBABILITY x IMPACT
= LIKELIHOOD x IMPACT

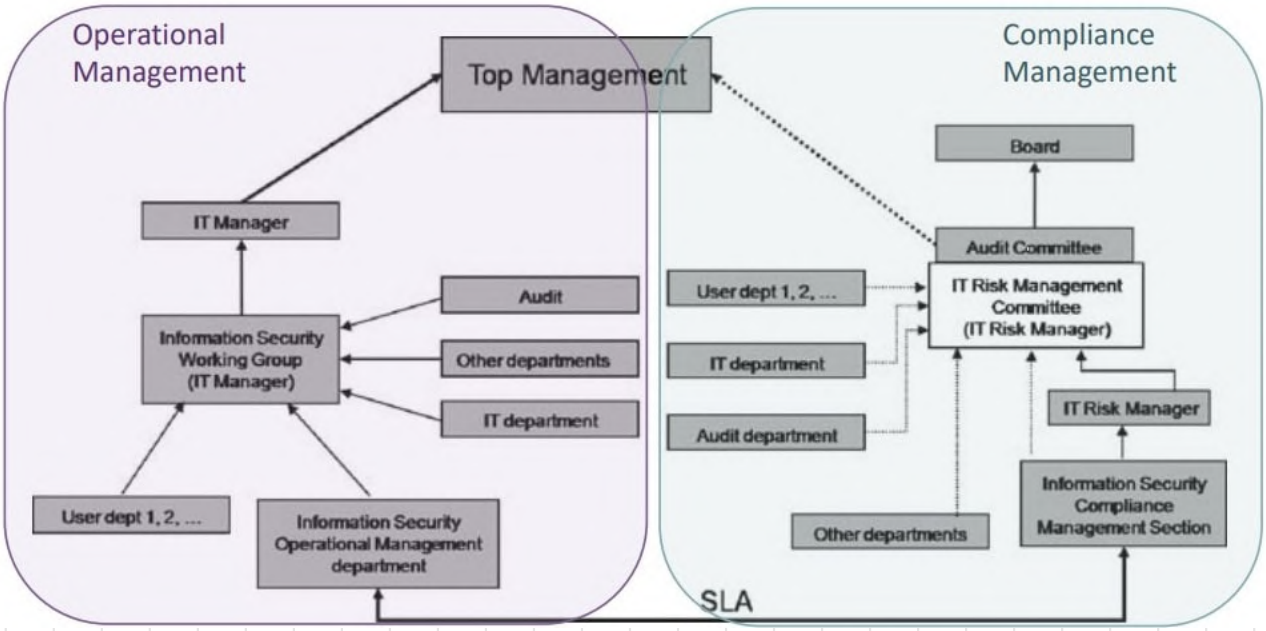


All level of organisational management should be involved in the process of Risk Management. IT-related risks must be managed together with business risks.

ORGANISATION

The way Information Security is organized in any company. At least composed by two components:

① one looking after day-to-day operational aspects
② one responsible for compliance monitoring



AWARENESS

All information workers must be made aware (and trained) of IS policy as well as the associated procedures, guidelines and practices.

FRAMEWORKS AND BEST PRACTICES

Starting from 2014, Obama ("Thanks OBama -.-"), updated the role of National Institute of Standards and Technology (NIST) to include identifying and developing cybersecurity frameworks for voluntary use by institutions and companies.

NIST CSF is composed by Core, Implementation Tiers and Profiles.

Applicability: developed to improve cs risk management in critical infrastructure but can be used in any sector whether the cs focus is primarily on Information Technology (IT), Industrial Control System (ICS) cyber-physical systems (CPS) and connected devices (eg IoT).

It is technology neutral → support technical innovation.

Provides a common taxonomy and mechanism for organisations (eg to describe their current cs position.

⇒ Supports cs assessment, planning and monitoring activities.

CORE

Set of activities to achieve specific cs outcomes and references examples of guidance to achieve them. Not a check list, some practices can be avoided if not needed (eg. small companies)

IDENTIFY: develop an organisational understanding to manage CS risks
PROTECT: develop and implement appropriate safeguards to ensure delivery of critical services
DETECT: prepare possible activities related to CS events.
RESPOND: take action regarding a detected CS incident
RECOVER: practices to recover from a CS incident.

Eg.

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	**CIS CSC** 1 **COBIT 5** BAI09.01, BAI09.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-2: Software platforms and applications within the organization are inventoried	**CIS CSC** 2 **COBIT 5** BAI09.01, BAI09.02, BAI09.05 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2, A.12.5.1 **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-3: Organizational communication and data flows are mapped	**CIS CSC** 12 **COBIT 5** DSS05.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISO/IEC 27001:2013** A.13.2.1, A.13.2.2 **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	**CIS CSC** 12 **COBIT 5** APO02.02, APO10.04, DSS01.02 **ISO/IEC 27001:2013** A.11.2.6 **NIST SP 800-53 Rev. 4** AC-20, SA-9

IMPLEMENTATION TIERS

They gives criteria to evaluate how an organization views cyber risks and the processes to manage them.
Partial (Tier 1), Risk informed (Tier 2), Repeatable (Tier 3) and Adaptive (Tier 4)
Note: Tier 1 doesn't mean less quality that Tier 4.
Progression in Tiers is encouraged if feasible and indicates CS risks reduction. NOT MORE MATURITY!
Eg.

	Risk Management Process	Integrated Risk Management Program	External Participation
TIER 1 Partial	- Lack of formalization - ad hoc and sometimes reactive management - Prioritization of activities may not be directly based on by organizational risk objectives, the threat environment, or business/mission requirements	- limited awareness of cybersecurity risk at the organizational level - irregular, case-by-case basis due to varied experience or information gained from outside sources - The organization may not have in place information sharing processes	No collaboration

	Risk Management Process	Integrated Risk Management Program	External Participation
TIER 2 Risk Informed	- Management approval but possible absence of clear policies - Prioritization of activities may not be directly based on by organizational risk objectives	- awareness of cybersecurity risk at the organizational level but not an organization-wide approach to managing cybersecurity - information sharing within the organization on an informal basis. - not all levels of the organization are involved - Cyber risk assessment of organizational and external assets occurs, but is not typically repeatable or reoccurring.	Low Collaboration

	Risk Management Process	Integrated Risk Management Program	External Participation
TIER 3 Repeatable	- formal approval and definition of policy. - regularly updated	- There is an organization-wide approach to manage cybersecurity risk.	High Collaboration
TIER 4 Adaptive	- Standards and best Practices are applied - Continuous improvement process	- There is an organization-wide approach to managing cybersecurity risk that uses risk-informed policies, processes, and procedures to address potential cybersecurity events	Full Collaboration

PROFILE

Define prototypes of organisation according to functions, categories and subcategories. Usually used to describe current state or desired target.

NATIONAL CS FRAMEWORK

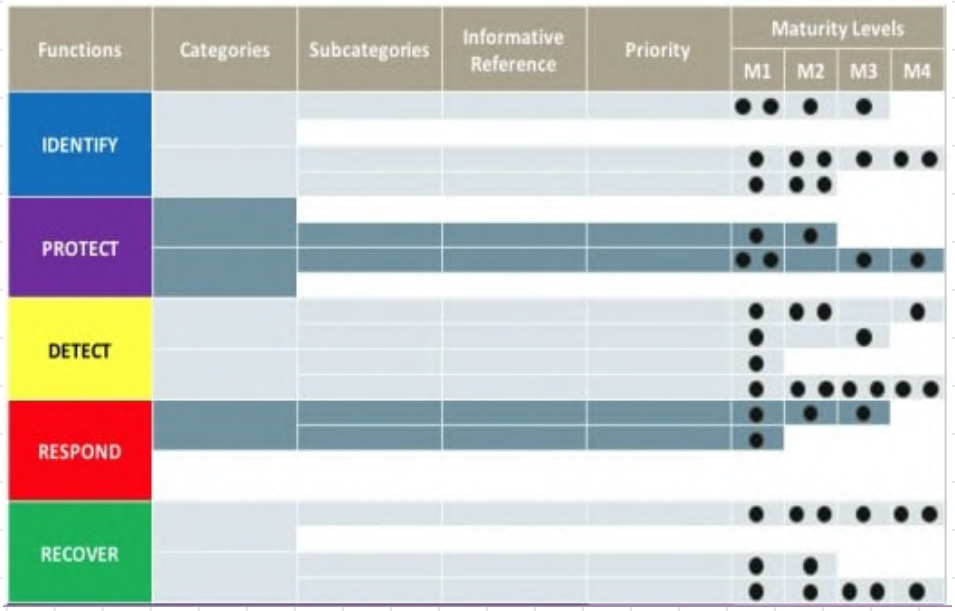
Bring cyber risks awareness to the stupid italian peasants.

The goal was to create something recognized at international level from NIST framework.

Note: National Framework is not a certifiable standard! Is just a tool for self-evaluation.

NF = NIST + Priority Level + Maturity Level

CONTESTUALIZATION: framework can be adopted to a specific scenario changing priority and maturity level for each subcategories



Contestualization can be done for organisation, domain etc.

FRAMEWORK 2.0: CS + DATA PROTECTION = Framework nazionale per la cybersecurity e la data protection ⇒ Contestualization ⇒ GDPR

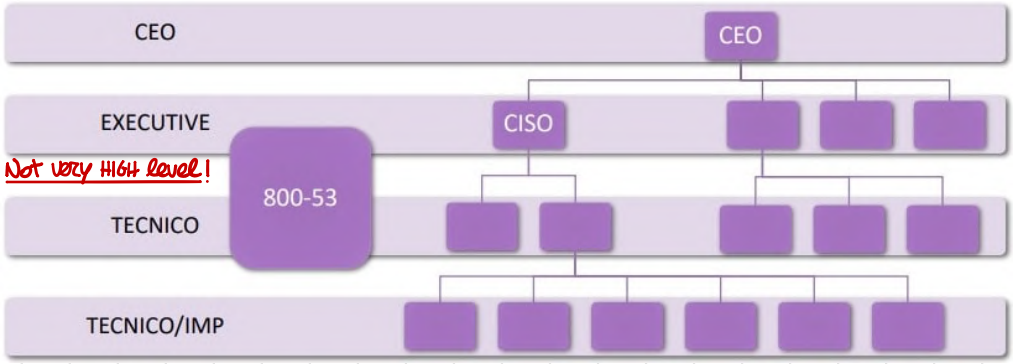
NIST CSF

NIST CSF ← FISMA Ecosystem
NIST CSF ← ISO 27000 Ecosystem
NIST CSF ← SANS 20

FISMA

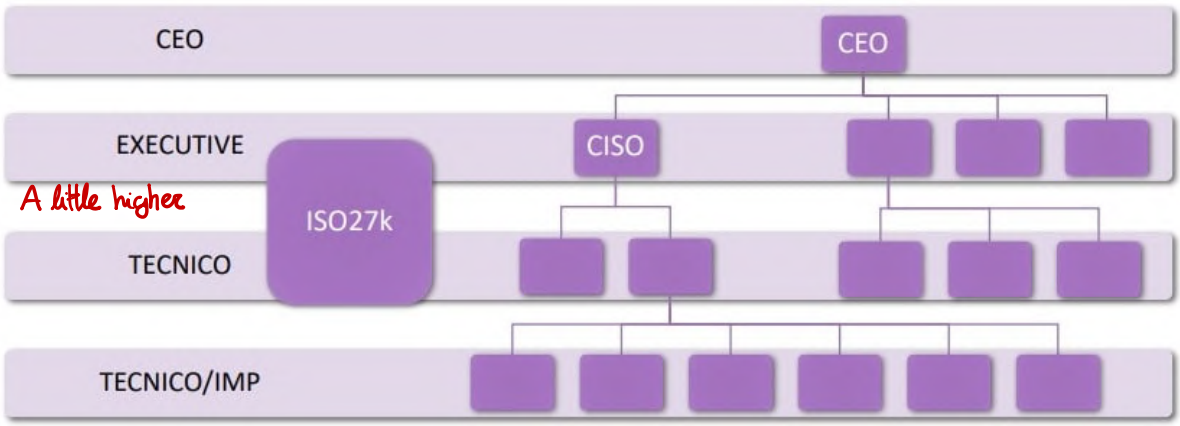
Federal Information System Management Act : each federal agency must provide information security on information and processes (even 3rd parties)
Phase 1 : Standards and Guidelines Development
Phase 2 : Implementation and Assessments Aids

- FIPS 199 & FIPS 200 : "Standards for Security Categorization of Federal Information and Information Systems" and "Minimum Security Requirements for Federal Information and Information Systems".
- SP 800-53 : follow directly FIPS 199/200. Provides a catalogue of controls for federal organizations about CS (accidents/attacks). Controls are divided in 18 families. Each control is characterized by Supplemental Guidance, Control Enhancements, References and Priority and Baseline Allocation.
  - BASELINE
    Starting point for security control selection process. The subset of control implemented (add 1 or more enhancements) depends on impact (LOW, MODERATE, HIGH) the control has on the information systems.
  - CONS: tied to the concept of federal informations systems (US's legislation), very complex, not always make sense to certify outside US.



ISO 27000

Family of huge collection of documents for different kinds of guidance (ISO 27001, ISO27002 etc). The most international framework (over 60 countries).
CONS: expensive to be certified, all requirements are mandatory, no priority on controls.



RISK MANAGEMENT (RM)

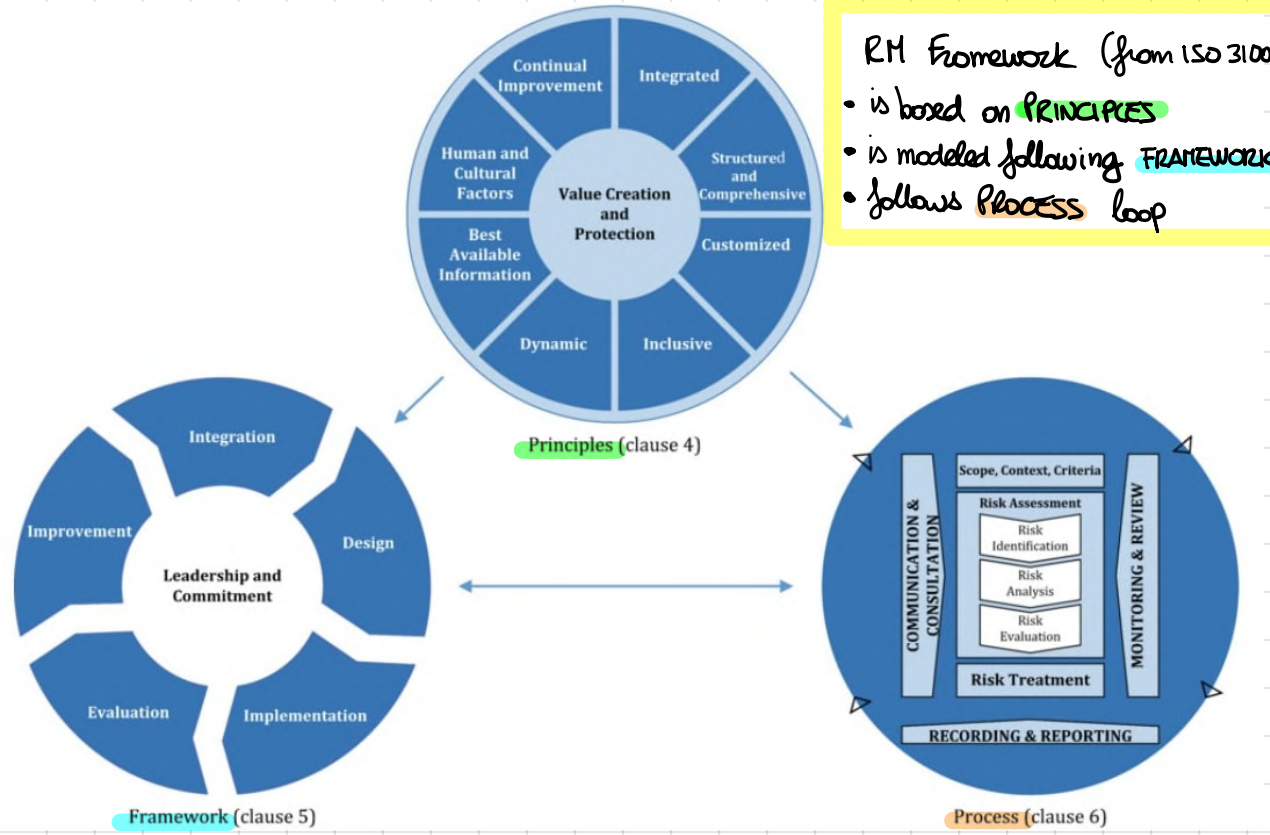
A risk management process must be adequate, efficient and effective.

RM standard ⇒ RM principles —inspiration→ RM framework ⇒ RM process

↓ (RM framework ← experience ← RM process)

ISO 31000

Provides guidelines on RM faced by organisations and can be adopted to any organisation and context



RM Framework (from ISO 31000)

- is based on PRINCIPLES
- is modeled following FRAMEWORK steps
- follows PROCESS loop

Principles set up the basis, framework, in each phase, consider the principle from which is inspired and run all processes needed.

PRINCIPLES

Composed by 8 principles + 1 core element: Value Creation and Protection.

Core element is used to evaluate what can cause loss and how to avoid them (iteratively)

- Integrated: RM is an integral part of all activities. Countermeasures must be applicable in the environment
- Structured and Comprehensive: an approach of this kind contributes to consistent and comparable results
- Customized: framework and process must be adequated to the environment
- Inclusive: involving stakeholders increases awareness
- Dynamic: changes must be taken into account and managed in time.
- Best Available Information: always use informations that suit most the RM activities.
- Human and Cultural Factors: influence all aspect of RM.
- Continual Improvement: learning and experience

FRAMEWORK

→ PURPOSE: integrate risk management into significant activities and functions of organisation

→ EFFECTIVENESS: depends on framework integration in the company

All steps are supervised by some authority (leadership) and there must be Commitment by who put them in place.

Steps are the typical actions made during a project.

PROCESS

Suggests how to structure processes involved in RM activities

- Communication & Consultation : how to acquire and spread informations.
- Monitoring & Review : improve the processes reviewing the past ones
- Risk Assessment : activities aiming to understand and document the risk picture for specific aspects of organisation.

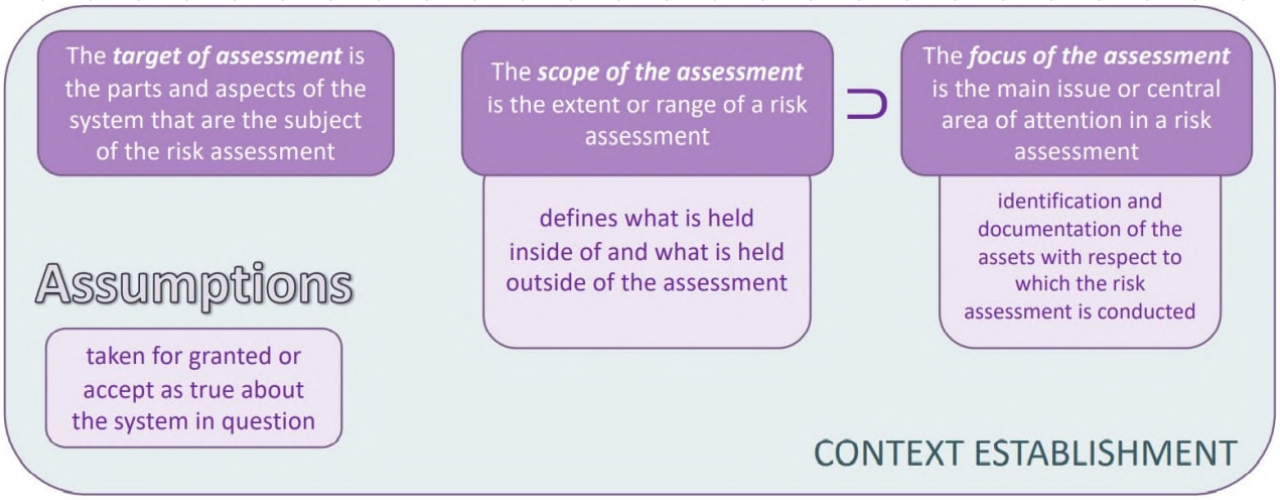
① Context Establishment
② Risk identification
③ Risk analysis
④ Risk evaluation
⑤ Risk treatment

Loop

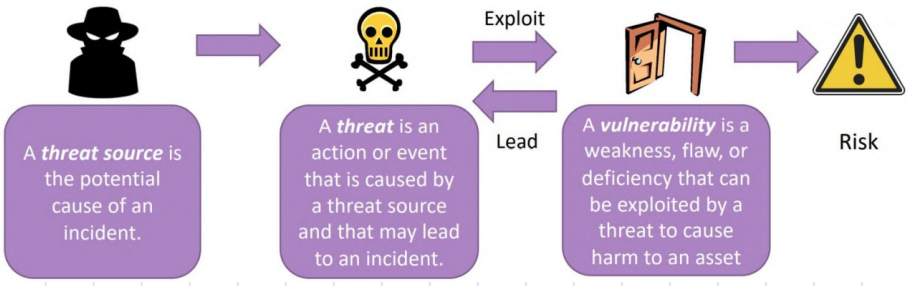
In details :

① Identify and Describe context of Risk Assessment process.
First thing to do is divide the context into :
- External : societal, legal ... environment and relationships with external stakeholders
- Internal : relevant goals, capabilities etc that may determine how risk should be assessed

Then, goals and objectives of risk assessment must be defined.



② Set of activities aiming to identify, describe and document risks and risks sources
- a risk is always associated with an incident
- there are 3 elements without which there can be no risk : Asset (element impacted), Vulnerability (what can be exploited), Threat (how is exploited). → No risk if even 1 is missing !



Goal : identify threats and how they may lead to incidents.

③ Quantify the level of identified risks.
Risk Estimation : likelihoods estimation + Consequences estimation
"frequency/probability" "estimate" for each asset

④ How much severe is the risk for the company?

- Consolidation of risk analysis result
- Evaluation of risk level
- Risk aggregation: investigate to see if certain sets of risk should be aggregated and evaluated as single risk
- Risk grouping: group risks with common elements

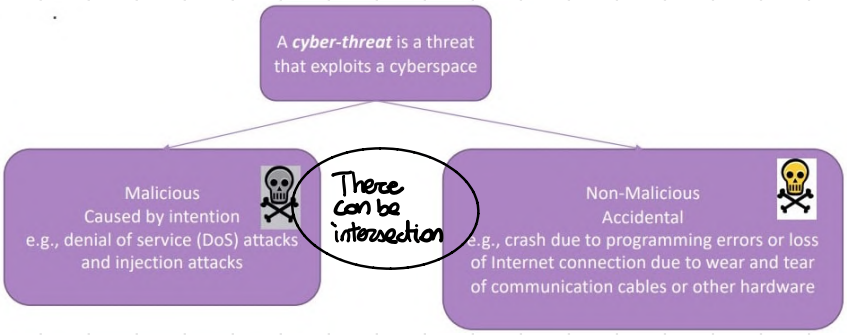
⑤ How to solve the risk.

Risk Reduction	reducing the likelihood and/or consequence of incidents
Risk Retention	accept the risk by informed decision
Risk Avoidance	avoid the activity that gives rise to the risk in question, which sometimes is the only option for unacceptable risks
Risk Sharing	transfer the risk or parts of it to another party, for example, by insurance or sub-contracting

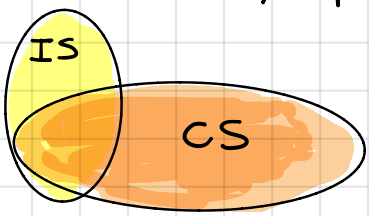
ISO 31000 is a standard USED as inspiration to generate RM frameworks.

CYBER-RISK MANAGEMENT

We focus on risks about cyber security. Note: risk management it self is not only about cyber security!
We define cyberspace as collection of interconnected computerized networks, cyber-system the systems that make use of it and cyber-physical system a cyber-system that controls and responds to physical entities.



Cybersecurity concerns protection from threats that use cyberspace.



Critical Infrastructure Protection (CIP) and Critical Information Infrastructure Protection (CIIP) is concerned with prevention of disruption, disabling, destruction, or malicious control of infrastructure.

COMMUNICATION AND CONSULTATION

More problems:
① cyber-system may potentially have stakeholders everywhere (large boundary)
② potentially adversary everywhere
luckily there is lot of documentation...

ASSESSMENT

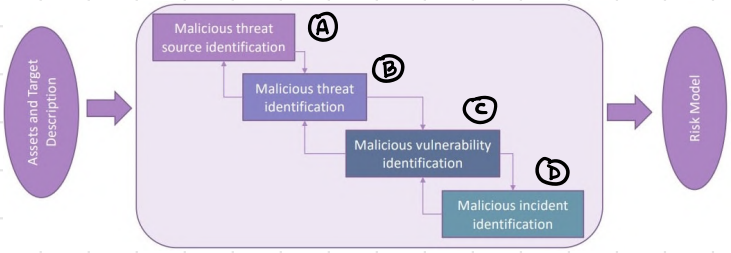
Problem:
① The origins of threats are widespread, possibly global
② Large amount of threat sources and threats.
in addition, Risk identification step is divided in two according to the different types of threats.

Context Estoblishment

The attack surface is all the different points where attacker or any threat source could get into cyber system and where data can get out.
Typical assets of concern are information and information infrastructures.

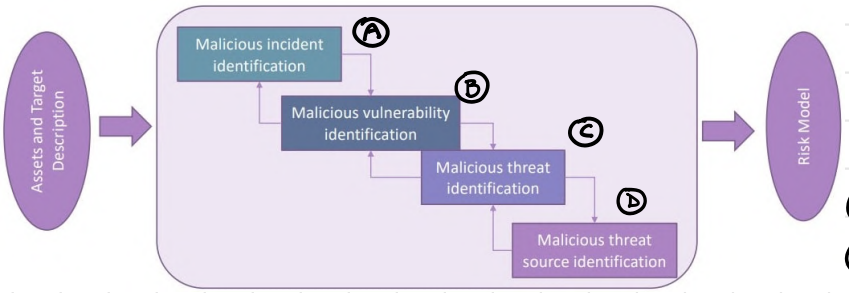
Risk Identification

- Malicious: try to understand what adversary will do. Not easy.



(A) Understand possible attacker and motivation, if is an human or a machine, adversary capabilities and intentions, how attack can be launched (remote or physical) ⇒ Attacker Profile
(B) Pay attention to the interface to cyberspace and the documented attack surface. Lot of catalogues available!
(C) Focus on attack surface and infer the possible weak points of the system, both of human and machines
(D) What are the possible consequences?

- NON Malicious : reverse the procedure



(A) Investigate how assets are represented and how they are related to the target of assessment (logs, external data ...)
(B) Use standards to find out common vulnerabilities
(C) and consequent threats (and how they work)
(D) Who is the user and how can he cause the incident ?

Risk Analysis

Two aspects to keep in mind:
(1) Malicious threats is hard to evaluate the likelihood of occurrence
(2) We have lot of tools to facilitate the analysis due to the nature of cyber-systems

Risk Evaluation

Consolidation of risk analysis results	• Similarly to the general case, focus on the cyber-risks for which the estimates are uncertain • Make the distinction between malicious and non-malicious risks
Evaluation of risk level	for convenience it is possible to evaluate malicious and non-malicious cyber-risks separately
Risk aggregation	As in the general case
Risk grouping	Risks are grouped based on the distinction between malicious and non malicious cyber-risk to improve the selection of the most appropriate treatments

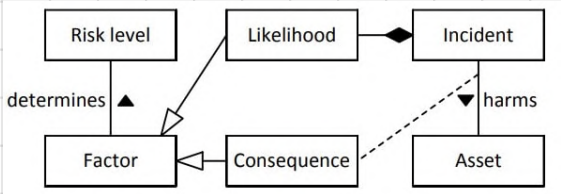
Risk Treatment

Two distinctions from general case:
(1) Most solutions are technical
(2) Distinction between malicious and not risks has implication for the most adequate risk treatment

CHALLENGES IN CYBER RISK MANAGEMENT

Which measure of risk level to use? What scales are best-suited under which conditions? What to do with uncertainty?

MEASURE RISK LEVEL



Up to now we used consequences and likelihood → Likelihood can be estimated "easily" just looking at at past frequency while consequences must be calculated using also a business impact analysis according to the asset.

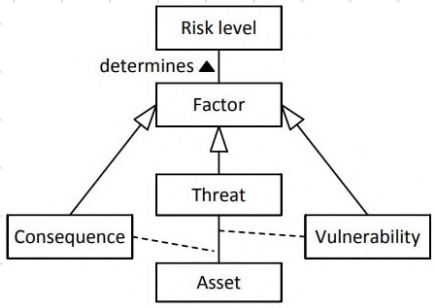
To be more precise we can use a three-factor measure in which we decompose likelihood in:

① likelihood that a threat will occur

② likelihood that a threat occurrence will result in an adverse impact (vulnerability of the target)

eg. Phishing: very frequent, but only very stupid persons can be impacted.

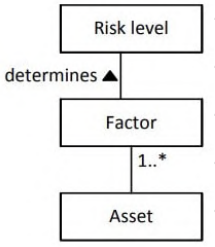
③ the severity of the resulting impact



In many-factor measure we divide risk level in following categories:

① threat agent factors
② vulnerability factors
and consequences in:
③ technical impact factors
④ business impact factors

} eg. OWASP

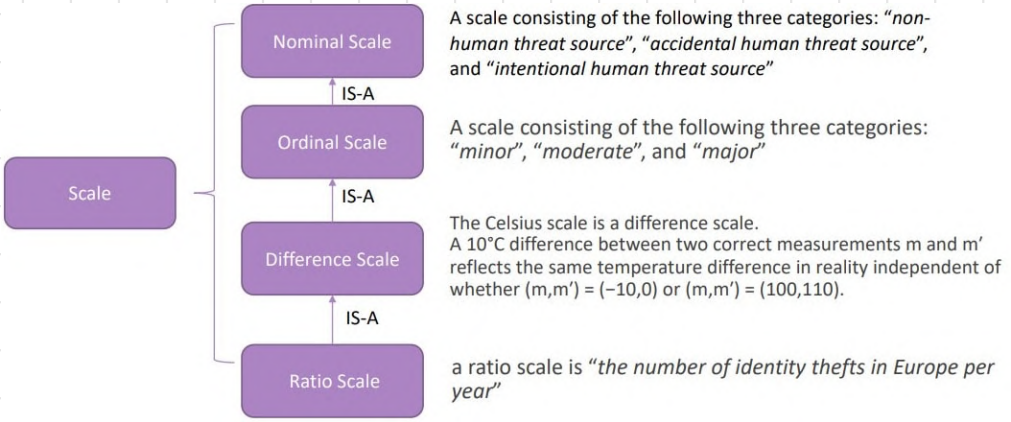


So, which one to use? First of all we have to consider what data we have (eg historical data) and most important the ones we lack respect to the factors we selected.

Be sure that the choice of factors is not influenced by external parts.

Scale choice depends on:

① factors in question
② kind of risk assessment
③ the target of assessment
④ the available data sources.



First two scales are qualitative while the others are quantitative. We focus on Ordinal and Ratio scales.

Quantitative scales tend to work better when the assessment is at a more technical level or requires fine level of granularity, while qualitative scales are used with NOT homogeneous information to be quantified.

Moving from quantitative scale to qualitative is easy, the opposite is hard.

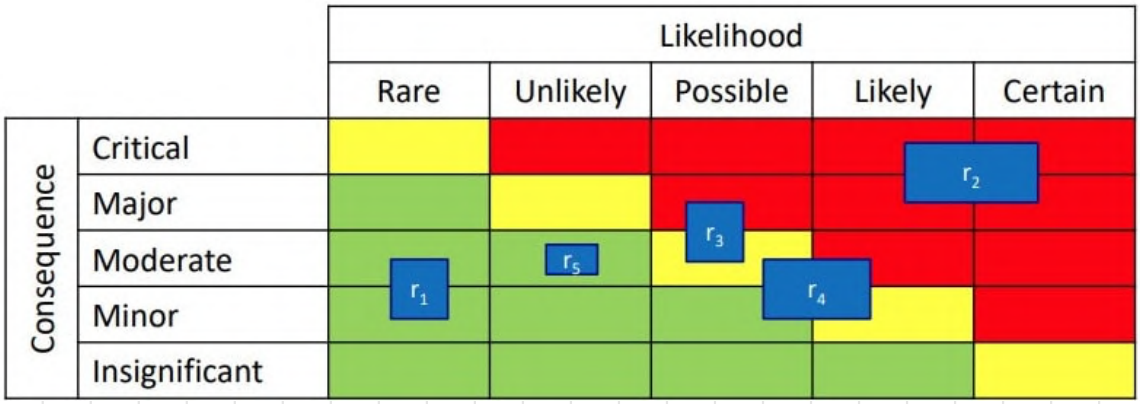
Note: scale of consequences depends on the target asset!

UNCERTAINTY

In few words: lack of information / knowledge. It is divided in:

- EPISTEMIC: ignorance or lack of evidence
- ALEATORY: randomness

Quantitative Scale



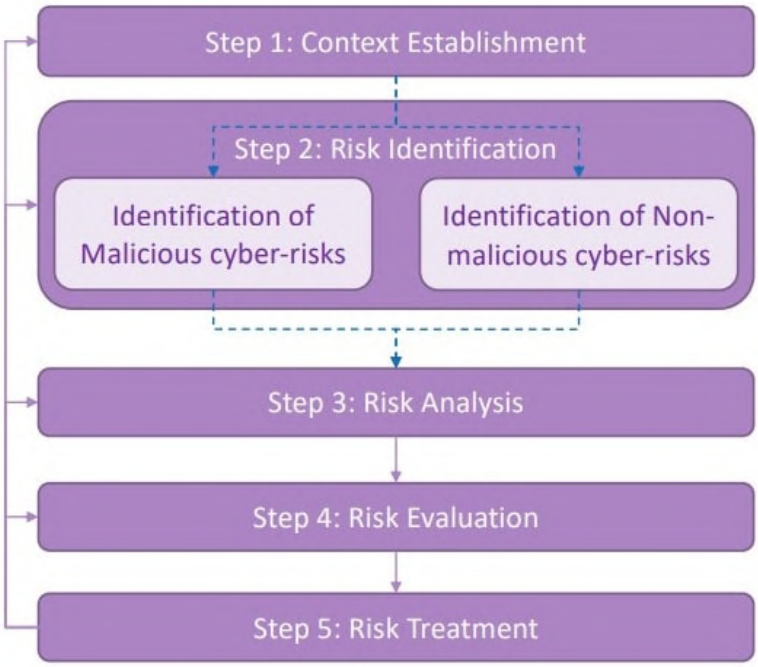
r_4 and r_3 have an high level of uncertainty while the other may change in likelihood but the risk level will still the same. In particular r_4 presents uncertainty in both consequences and likelihood. If we use qualitative scales, uncertainty should be expressed as a separate attribute of the risk.

BLACK SWAN: incident extremely rare and unexpected, but with very significant consequences

GRAY SWAN: incident which has far-reaching consequences, but, unlike a black swan, can be anticipated to a certain degree.

CASE STUDY

Advanced Metering Infrastructure (AMI) in a Smart Grid (electricity distribution network).
AMI = power meters that collect information from customers (power usage) and also provide information to them.
AIM: assess risks for this infrastructure that includes components that turn on/off power to customers or limit it (choking)
PARTY: distribution system operator, who has interest in assessment.



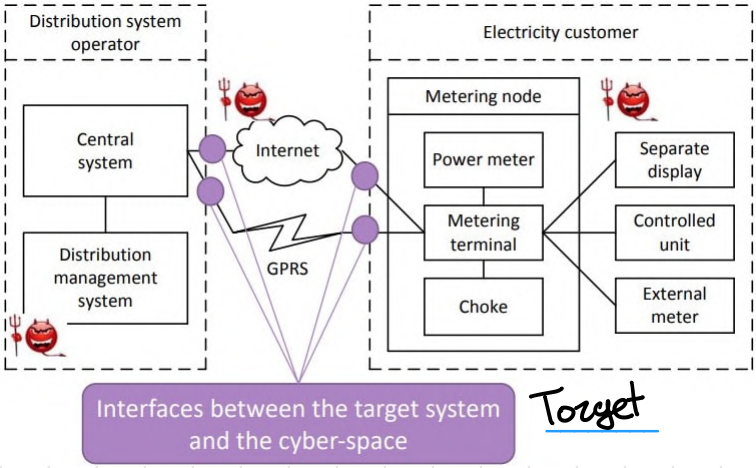
CONTEXT ESTABLISHMENT

1. Context Identification and Description
   - External Context
   - Internal Context
2. Definition of the Assessment Goals and Objectives
3. Target , Scope and Focus of Assessment Definition
4. Assumptions
5. Assets Identification
6. Definition of the Likelihood Scale
7. Definition of the Consequence Scale
8. Definition of the Risk Evaluation Criteria

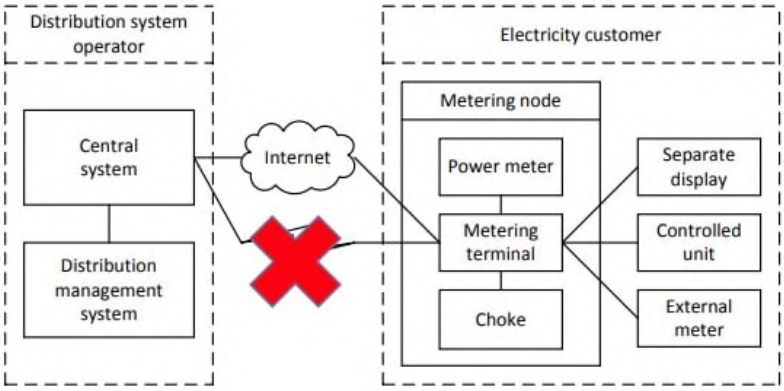
] to be done in exercise

External: description of smart grid that is part of the critical infrastructure. The distribution system operator (our party) is subject to a number of national law and regulations: identify and document them, failing this may put the party out of business.
Power outages or incidents can damage the reputation and public trust.
Internal: goal of the company, policies and capabilities.
In this case: provide power without problems, monitor consumptions and protect customers privacy (+ data integrity - data leaks). Most employees have strong technical competence, few have received special training in risk assessment.
Goals and Objectives: ① Assess risks wrt the business continuity ② law and regulation compliance ③ Improve situation Awareness ("power good, no power no good")

Target, Scope, Focus



Target



Scope: we exclude "power line" from assessment

Focus: ① connection between customers and central unit ② exclude physical attacks ③ Both malicious and non malicious threats ④ Functionalities: register customers data, transfer to party, turn on/off/check power

Assets

Not only physical, what have a value for the party.
① Integrity of meter data ② Availability of meter data ③ Provisioning power to customers.

Likelihood Scale

Likelihood value	Description
Rare	Less than once per ten years
Unlikely	Less than once per two years
Possible	Less than twice per year
Likely	Two to five times per year
Certain	Five times or more per year

A simple way of expressing the uncertainty.
Easy to read.
We used frequencies because we work with historical data.

Consequence Scale

Consequence value	Description
Insignificant	Errors in meter data for up to 100 electricity customers
Minor	Errors in meter data for 101-2,000 electricity customers
Moderate	Errors in meter data for 2,001-20,000 electricity customers
Major	Errors in meter data for 20,001-50,000 electricity customers
Critical	Errors in meter data for more than 50,000 electricity customers

One scale for each asset. Since I'm lazy I copy/paste only one.

Risk Evaluation Criteria

Consequence \ Likelihood	Rare	Unlikely	Possible	Likely	Certain
Critical					
Major					
Moderate					
Minor					
Insignificant					

Possibility to create different matrix for each asset. At least one. This is the default one.

RISK IDENTIFICATION

We plan to create a collection of threats sources, threats, vulnerabilities, incidents and risk. Order depends if looking for malicious or non malicious threats. Basic technique is to start from environment data (logs, monitoring tools etc.) and integrate it with other data eg diagrams, network design, vulnerabilities/threats repositories etc.

Follow the schema we saw some pages ago.

MALICIOUS:

Threat Source Identification

Who and why could bother our family company?

An example on the nigth.

Source	Motivation	Capability
Hacktivist	Similarly to cyber-terrorists, hacktivists are motivated by a political, ideological, or religious agenda and use cyber-attacks to achieve their goals. Although the distinction between cyber-terrorists and hacktivists is fuzzy at best, we assume that hacktivists are less willing to go to extremes and that their aim is to harm selected groups, politicians, or other individuals, rather than society as a whole	Skill level and resources can var lot. Most hacktivists are assumed operate alone or in small or poo organized groups. However, if w organized they can potentially h access to significant computatio resources as well as competence

Threat Identification

Source	Attack Point	Threat
Script kiddie	Internet connection to the central system	DDoS attack on the central system
Cyber-terrorist	Same as the row above	Same as the row above
Cyber-terrorist	Internet connection between the central system and the metering terminal	Tampering with all or most control data in transit from the central system to the choke component
Black hat hacker	Internet connection between the central system and the metering terminal	Tampering with data in transit from the metering terminal to the central system
Black hat hacker	Communication line between the metering terminal and the external meter	Malware to manipulate meter data is installed on the metering terminal through connection to the external meter
Malware	Internet connection to the metering terminal	Metering node infected by malware
Hacktivist	Internet connection between the metering terminal and the central system	Tampering with control data in transit from the central system to the choke components for selected electricity customers
Insider	Central system	Illegitimate control data sent to the choke components from the central system

Attack Point: focus on how the threat source may exploit the attack surface identified during the context establishment

Threat: for each malicious threat source we identify the threats it may initiate.

Vulnerability Identification

For each malicious threat, identify the existing vulnerabilities that threat may exploit. Start looking at Vulnerabilities lists eg ISO27005 or testing activities

Threat	Vulnerability	Description
DDoS attack on the central system	Inadequate attack detection and response on central system	New forms of DDoS attacks are continuously being developed to defeat existing countermeasures. Due to the challenges of keeping the central system running 24/7, combined with the lack of a strong tradition for cybersecurity awareness in the power distribution domain (which has not traditionally operated in cyberspace), countermeasures to various forms of DDoS attacks on the central system are rarely updated and may therefore be out of date

Incident Identification

Same as vulnerability: link threats, incident and target assets.

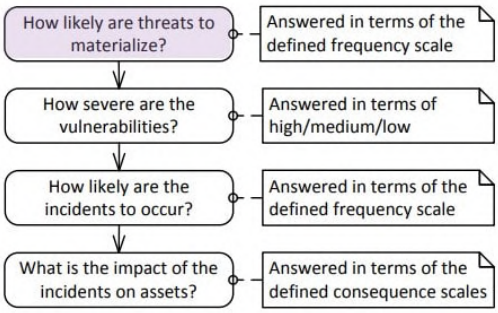
Threat	Incident	Asset
DDoS attack on the central system	Data from metering nodes cannot be received by the central system due to DDoS attack	Availability of meter data
Tampering with all or most control data in transit from the central system to the choke component	False control data received by all or most choke components	Provisioning of power to electricity customers
Tampering with data in transit from the metering terminal to the central system	False meter data for a limited number of electricity customers received by the central system	Integrity of meter data
Malware to manipulate meter data is installed on the metering terminal through connection to the external meter	Same as the row above	Same as the row above

NON MALICIOUS – Incident Identification: link assets, incident and their description

RISK ANALYSIS

Estimate and determine level of identified risk in terms of likelihood and consequences.

We use some information sources of risk identification considering also the severity of vulnerabilities, the likelihood of threats and incidents and consequences of incidents.



Malicious Threats

to evaluate likelihood we can consider event logs (provided by the party) or expert judgements.
We follow an approach inspired by OWASP risk-rating method: factors rated from 0 to 9

Factors	Description
Skill Level	How technically skilled is this group of threat agents? No technical skills (1), some technical skills (3), advanced computer user (5), network and programming skills (6), security penetration skills (9)
Motive	How motivated is this group of threat agents to find and exploit this vulnerability? Low or no reward (1), possible reward (4), high reward (9)
Opportunity	What resources and opportunities are required for this group of threat agents to find and exploit this vulnerability? Full access or expensive resources required (0), special access or resources required (4), some access or resources required (7), no access or resources required (9)
Size	How large is this group of threat agents? Developers (2), system administrators (2), intranet users (4), partners (5), authenticated users (6), anonymous Internet users (9)

→

Threat: DDoS
Source: script kiddie (hackerino stupidino)

Factors	Score [1, 9]	Rationale
Skill Level	3	She/he is relatively unskilled and unable to perform complicated attacks
Motive	1	Motive generally weak
Opportunity	7	She/he has enough resources and opportunities to conduct the attack (low cost)
Size (i.e., it is a measure of how large this group of threat sources is)	7	script kiddies can reside anywhere in the world
AVG	4,5	

Considering multiple source of some threat, we take the worst case AVG value and using our own likelihood scale we estimate the likelihood of the threat. Eg RARE (0 - 1.8), UNLIKELY (1.9 - 3.6) etc.
We do this for all threats. Check the estimate with event logs and confirm with participants, otherwise edit the scale.

NON Malicious: Historical analysis mostly.

How severe are the vulnerabilities?

Vulnerability Analysis

We choose a scale of severity with 3 steps: 0 - 3 = LOW, 3 - 6 = MEDIUM, 6 - 9 = HIGH
As before we evaluate 4 factors for each vulnerability

ease of discovery	How easy is it for this group of threat agents to discover this vulnerability? Practically impossible (1), difficult (3), easy (7), automated tools available (9)
ease of exploit	How easy is it for this group of threat agents to actually exploit this vulnerability? Theoretical (1), difficult (3), easy (5), automated tools available (9)
awareness	How well known is this vulnerability to this group of threat agents? Unknown (1), hidden (4), obvious (6), public knowledge (9)
intrusion detection	How likely is an exploit to be detected? Active detection in application (1), logged and reviewed (3), logged without review (8), not logged (9)

Evaluate AVG and assign severity level (LOW, MEDIUM, HIGH)

For non malicious threats is a bit different since there is no intent to discover exploits → listen to your heart!

Eg

Vulnerability	Severity	Explanation
Single communication channel between central system and metering terminal	High	The Internet connection is the only communication channel to the central system for many electricity customers
Poor testing	Medium	Inspection of maintenance logs revealed a number of instances where bugs have been discovered in the metering terminal software. Previous experience indicates that the testing routines of the external software provider are unsatisfactory, and the central system operator does not test software updates for metering terminals before deployment

How likely are the incidents to occur?

Likelihood of Incidents

combine two previous analysis for both malicious and non malicious

Incident	Data from metering nodes cannot be received by the central system due to DDoS attack	
Threat	DDoS attack on the central system	Likelihood: Likely
Vulnerability	Inadequate attack detection and response on central system	Severity: High

Note: for non malicious threats we also evaluate incident likelihood deriving it from threat and vulnerability.

What is the impact of the incidents on assets?

Consequences: impact of incident on assets.
In order to estimate consequences we need to consider the consequence scale for the identified asset. In our case this require to estimate the expected time to detect and respond to an attack, as well as the number of affected electricity customers.

No.	Incident	Asset	Likelihood	Consequence
1	Data from metering nodes cannot be received by the central system due to DDoS attack	Availability of meter data	Likely	Moderate
2	False control data received by all or most choke components	Provisioning of power to electricity customers	Unlikely	Critical
3	False meter data for a limited number of electricity customers received by the central system	Integrity of meter data	Likely	Minor

RISK EVALUATION

① Consolidation of Risk Analysis

Make sure that the correct risk level is assigned to each risk. Also make sure to check if malicious and non malicious risks that can result on some incident are consistent in term of consequences and likelihood

② Evaluation of Risk Level

Take the risk matrix (likelihood - consequences) and place the incidents on it (malicious and not but on two different matrix)

③ Risk Aggregation

Two cases in which multiple risk can be evaluated as a single one.

Case 1: Some incident that harms multiple asset. The two risk separately may be low but the combined effect warrants higher risk level. Aggregated risk likelihood remains the same while the consequence is the joint consequence of the two risks.

Case 2: multiple incident on some asset that combined yields higher risk. (some nature of incident or the occurrences of the incidents are triggered by some threat.

Eg case 2

Risk	Likelihood	Consequence
(4) Malware compromises meter data	Rare	Moderate
(11) Software bug on the metering terminal compromises meter data	Unlikely	Moderate
(4 + 11) Software on the metering node compromises meter data	Possible	Moderate

After this we modify risk matrix: we merge malicious and non malicious risk matrix and we also add the aggregations (mantaining also the single risk level separated eg #1, #5 and #(1&5))

④ Grouping

Try to group risks that may benefit from some treatment.

Eg

No.	Incident	Asset	Threat	Vulnerability
14	Mistakes during maintenance of the central system disrupt transmission of control data to the choke component	Provisioning of power to electricity customers	Mistakes during update/maintenance of the central system	Poor training and heavy workload
15	Mistakes during maintenance of the central system prevent reception of data from metering nodes	Availability of meter data	Same as the row above	Same as the row above

Consequence \ Likelihood	Rare	Unlikely	Possible	Likely	Certain
Critical		2			
Major	6, 13	(6+13)			
Moderate		8, 11, 12, 14	(4+11), (5+12)	1	
Minor			15	3	9
Insignificant				16, 17	10

Increasing likelihood or consequence of either of them by 1 would rise risk level to medium → Treatments that fix both are worth!

RISK TREATMENT

Final step: find a solution for each risk, assess their effect and evaluate whether the residual risk is acceptable, if not we do on other iteration of treatment identification.
Since is not always posible to treat all threats due to the lack of money we first focus on malicious risks in risk level order (HIGH, MEDIUM, LOW). Usually low ones are skipped totally.
Second criteria of ordering is the type of incident: we try to find a priority according to it and the possibility of aggregation and grouping.
For each of them then we fill the following table

Element	Description
Risk n.	1
Incident	Data from metering nodes cannot be received by the central system due to DDoS attack
Asset	Availability of meter data
Threat Source	Script kiddie; Cyber-terrorist
Threat	DDoS attack on the central system
Attack Point	Internet connection to the central system
Vulnerability	Inadequate attack detection and response on central system
Treatment	Implement state-of-the-art DDoS attack detection and response mechanism on central system

Before applying the treatment we have to evaluate if it's worthy in terms of cost and doing this we can use two kind of approach: quantitative if we merely evaluate it with numbers or qualitative if we want to evaluate it on high level.

Ex.

Q4: Let us consider the XYZ company that is rapidly growing both in terms of market and size. The company passed in one year from 20 to 50 employees and most of them have no technical background, but they have been just trained in order to be able to use the XYZ applications. Given its small size in the past, XYZ has no strict and encoded security process and almost every employee was able to perform all the tasks. As a consequence, there were just two types of credentials used to access systems and applications (one as administrator and one as user) that were shared by every employee.

However, XYZ realized that its growth in the last period requires an investment in order to manage security risks deriving from improper accesses and that can lead to data breaches in terms of confidentiality and integrity.

A.9.4 System and application access control		
Objective: to prevent unauthorized access to systems and applications		
A.9.4.1	Information access restriction	*Control* Access to information and application system functions shall be restricted in accordance with the access control policy
A.9.4.2	Secure log-on procedures	*Control* Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure
A.9.4.3	Password management system	*Control* Password management systems shall be interactive and shall ensure quality passwords.
A.9.4.4	Use of privileged utility programs	*Control* The use of utility programs that might be capable of overriding system and applications controls shall be restricted and tightly controlled
A.9.4.5	Access control to program source code	*Control* Access to program source code shall be restricted

Considering all above:

Select which control should be implemented and why.

- A.9.4.1 → yes, even small companies should have a role system to prevent unauthorized access
- A.9.4.2 → depends. Budget? How much "invasive"?
- A.9.4.3 → yes
- A.9.4.4 → If we are using a role system, ofcourse only admin should be able to override system etc.
- A.9.4.5 → Not necessary since XYZ doesn't look like a software company, it doesn't not have source codes

RISK MANAGEMENT METHODOLOGIES REVIEW

OWASP

Based on two-factor risk model

As we can see there is no context establishment.

① More or less it follow general model: threat (agent), vulnerability, impact identification

② a. Estimate likelihood of the particular group of possible attacker evaluating skill level, motive, opportunity and number (size of group of agents)

b. Estimate the likelihood of the particular vulnerability evaluating ease of discovery, ease of exploit, awareness and intrusion detection.

③ technical impact: on application, data, functions → confidentiality, integrity, availability, accountability

business impact: on business and company → Financial / reputation damage, non-compliance, privacy violation

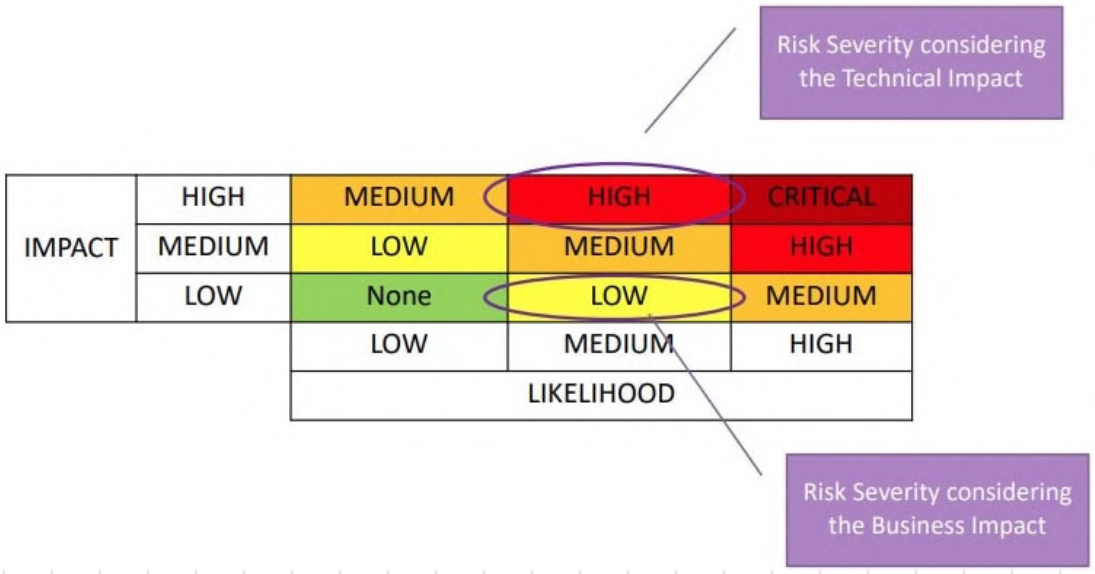
③.5 Put together ② and ③ to create the risk matrix (HIGH, MEDIUM, LOW)

Two approaches:

informal method: easy, one iteration

repeatable method: compare result with other iterations eg some agent - multiple vulnerability

In this step we can combine the two impact estimation: Business impact info are enough? yes → Use business impact, Technical impact otherwise.



④ Severe risks first, not all are worthy to be fixed (cost-benefit analysis)

⑤ Add factors, customize options, weighting factors.

PRO

- Simple steps
- Easy to apply
- Opensource tools

CONS

- High level analysis
- Not too much support on risk mitigation phase

CRAMM

Qualitative risk analysis and management tool developed by UK government. Makes use of meetings, interviews and structured questionaries

① Three types of assets: data, application software, physical assets.

② Threats and vulnerabilities are investigated against selected asset groups. CRAMM has predefined tables for threat/asset group and threat/impact combinations. Focus on managerial risk assessment

Two way to assess threats and vulnerabilities

Full Risk Assessment
- Analysis with questionaries
- CRAMM tools calculate levels

Rapid Risk Assessment
- threat and vulnerability levels inputted into the system (manually) with a voting guide

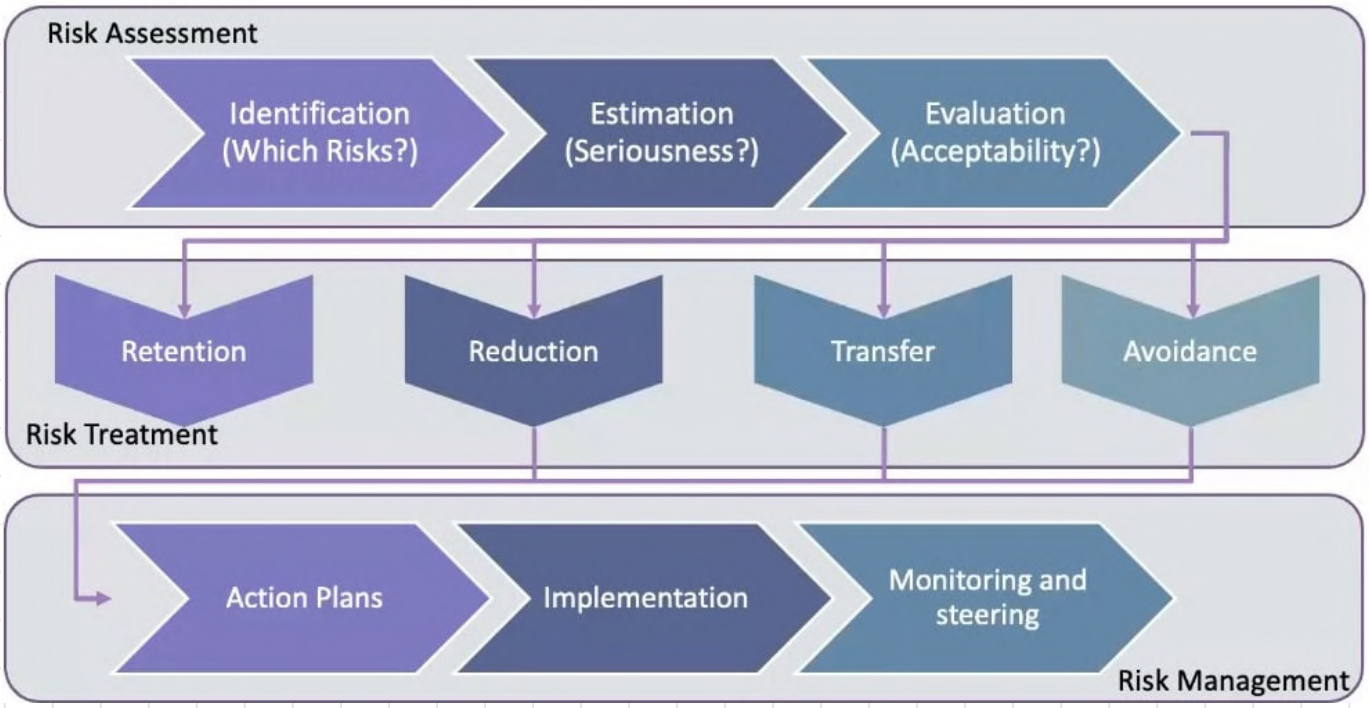
③ The tool generates a set of countermeasures applicable that must be evaluated anyway.
CRAMM is able to automatically give priority to countermeasures eg if prevents multiple threats.

PRO
- Simple steps
- Oriented to management

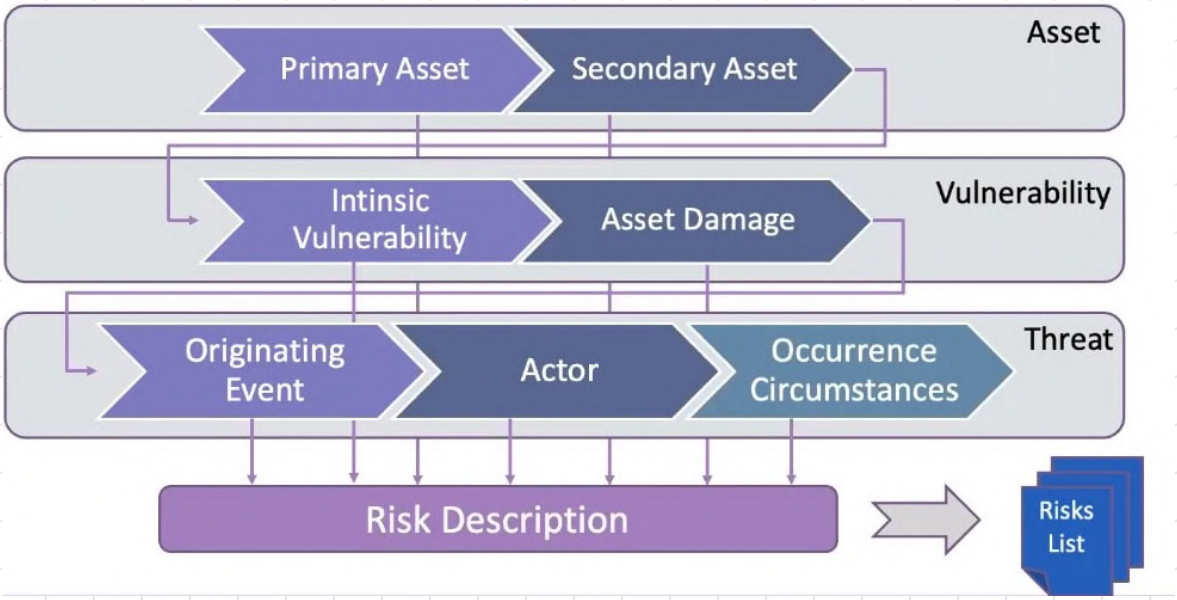
CONS
- Not Open Source

MEHARI

Free, open source information risk analysis assessment and risk management method, for professionals.



① Risk Assessment



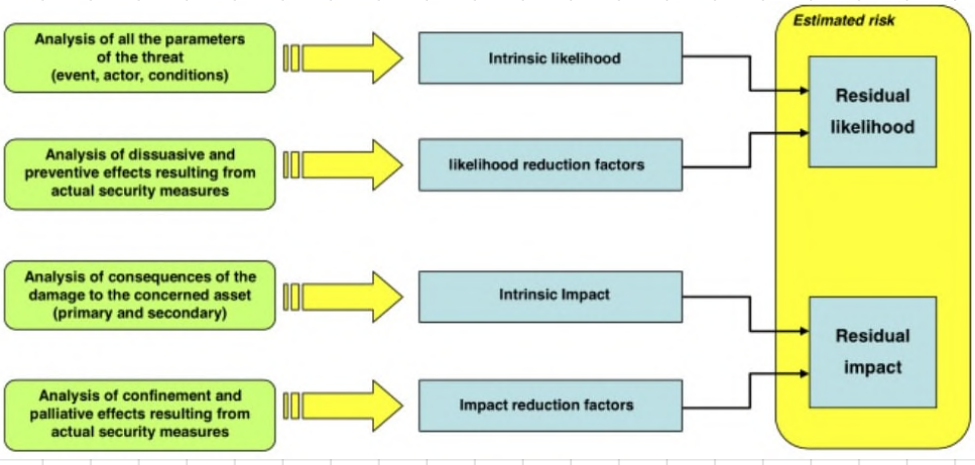
Primary Asset: they are described according 3 categories (Services, Data necessary, management processes) and, for each of them, 5 criteria (type of needs, type of service providers, field of activity/different areas of responsabilities, technology used, users concerned)
Secondary Assets: described by types of means required to meet functional needs described by primary assets. A sort of specification of primary assets.

Intrinsic and Contextual Vulnerability: first one "comes with" the system (eg paper is degradable and this problems comes with documents), the second one instead is a flaw in security system that can be exploited eg no protection against storms.

Events: divided in Accidents, Errors and Voluntary acts. For each of them we ask 3 questions:
- Cause is internal or external?
- Material or immaterial?
- Other relevant factors?

Actors: in case of people is important to distinguish categories of agent according to their rights and privileges.

Now we need to estimate risks and evaluate them
RISK = likelihood · impact
To be more precise we define intrinsic impact and likelihood as impact/likelihood excluding security measures.



Evaluation is done as always (matrix)
MEHARI suggests a decision table using risk acceptability that defines
- intollerable risks (remove ASAP)
- inadmissible risks (remove at some point)
- accepted risks

	L = 1	L = 2	L = 3	L = 4
I = 4	S = 2	S = 3	S = 4	S = 4
I = 3	S = 2	S = 3	S = 3	S = 4
I = 2	S = 1	S = 2	S = 2	S = 3
I = 1	S = 1	S = 1	S = 1	S = 2

② and ③ are as usual (more or less)

THREAT MODELING

Process to identify, quantify and address threats in order to strengthen protection, improve preparedness, increase awareness and support risk management.

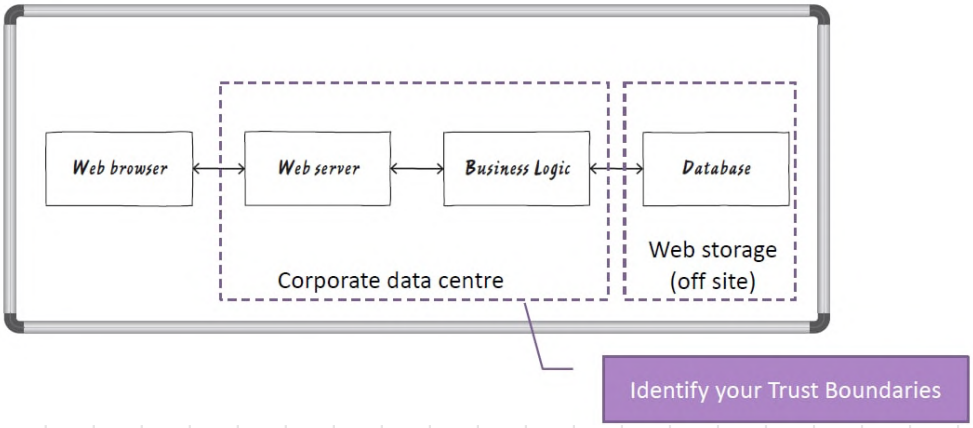
RISK = THREAT x PROBABILITY x IMPACT

Threat Modelling process:

1. What are you building?
2. What can go wrong?
3. What can you do to avoid bad things?
4. Analysis was good?

What are you building?

Diagram with functionalities of the project. Typical brainstorm.

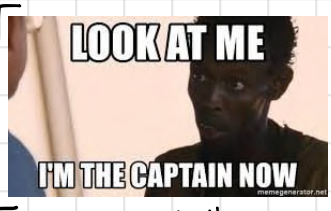


What can go wrong?

Use STRIDE mnemonic to find threats:

- **S**poofing: impersonate someone/something else
- **T**ampering: modify something you shouldn't
- **R**epudiation: claim you didn't do something
- **I**nformation Disclosure: expose information without authorization
- **D**enial of Service: harm system availability
- **E**levation of Privilege: program/user technically able to do something not supposed to do.

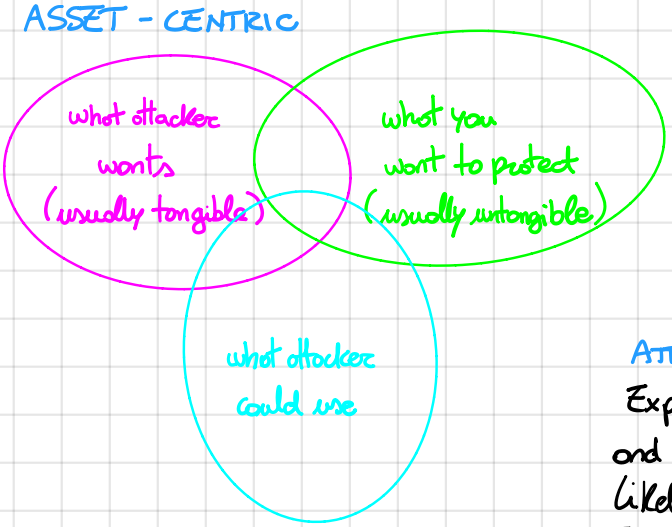
⇒ check them for each "component" of the diagram.



Always start with external entities and never ignore threat because it's not what you are looking for at the moment.

3 model variants: asset-centric, attacker centric, software centric.

ASSET - CENTRIC



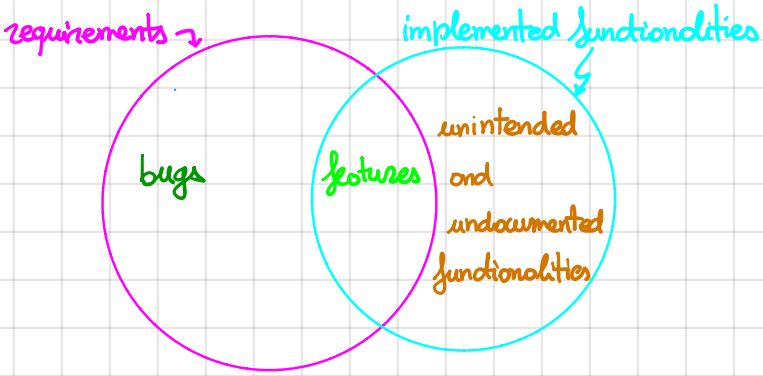
1. List assets and how attacker could use them
2. Connect them to particular (set of) computer system.
3. Redraw the system

Focus on what we want to protect.
This model can be used as attacker - centered brainstorm.

ATTACKER-CENTRIC

Experts can use various attacker lists to find possible threat and provide some structure to a brainstorm approach.
Likely to bring up possibilities that are human - centred
Start from attacker to find threats.

SOFTWARE - CENTRIC



Software is not only the application!
Also focus on HOST and NETWORK.
In practice this kind of approach is used during maintainance process
Focus on potential threats about the architecture (software)

How to model Software?

DATA FLOW DIAGRAM (DFD)

What in input - What in output. Processing steps. Data persistence activities.
DFD is useful to provide high-level view of information system.

Element	Appearance	Meaning	Example
External entity	web client	People, or code outside your control	Your customer, Microsoft.com
Data flow	HTTP →	Communication between processes, or between processes and data stores	Network connections, HTTP, RPC, LPC
Process	DB control	Any running code	Code written in C, C#, Python, or PHP
Data store	Log DB	Things that store data	Files, databases, the Windows Registry, shared memory segments

EXTERNAL ENTITY / TERMINATOR

Can be duplicated and is not part of the system under analysis. No direct control, can (or not) be part of the organization.
MUST receive/send data (why use them otherwise?)
- **Rule 1**: never include in DFD data flow between external entities.

DATA FLOW

Always directed. Represents data moving between elements.

- **Rule 2**: only represent flow of data, not material goods
- **Rule 3**: one type of data per arrow.

Data flow can be forked and joined.

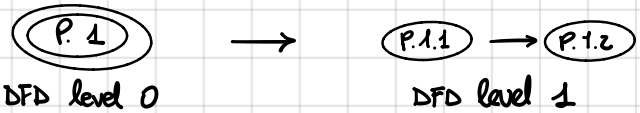
PROCESSES

Represent business logic.

- **Rule 4**: process must have at least one data flow in input and output

When represented as double circle (P) is called composite and can be subdivided in subprocesses.

eg

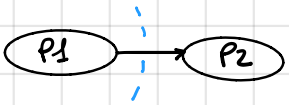


DFD level 0 → DFD level 1

DATA STORE

Where store data (wow!) and can be shared between systems. Data details somewhere else.

TRUST BOUNDARIES



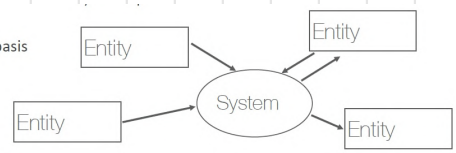
Represent limits in trustability of supports of the system.

So:

1. Identify actions and actor with use cases
2. Build context level DFD: separate external entities from system
3. Build level 0 DFD: identify processes
4. Build level 1 DFD: break down processes, identify inter-process data flow, identify data store
5. Add trust boundaries

eg Context level DFD

- Its a star-like DFD!
- Mainly built on the basis of use-cases



STRIDE, ATTACK TREE AND ATTACK LIBRARY

We now go into the details of "what can go wrong?" question.
STRIDE is a software-centric threat modelling framework (threat elicitation technique)

THREAT	VIOLATED PROPERTY	THREAT DEFINITION	TYPICAL VICTIMS	EXAMPLES
Spoofing	Authentication	Pretending to be something or someone other than yourself	Processes, external entities	Falsely claiming to be Acme.com, winsock .dll, Barack Obama, a police officer, or the Nigerian Anti-Fraud Group

Actors are usually out of the boundaries. The presence of external entities can be used as spoofing threats.
Spoofing can be applied on:
- process on some machine eg creating a trojan "su" and altering the path
- a file eg create an executable or a config file
- an entire machine: IP/DNS spoofing, IP redirection, DNS compromise
- a person: steal account or change display name
- a role: declare to have a specific role eg admin.

THREAT	VIOLATED PROPERTY	THREAT DEFINITION	TYPICAL VICTIMS	EXAMPLES
Tampering	Integrity	Unauthorized modification of data on disk, on a network, or in memory	Data stores, data flows, processes	Changing a spreadsheet, the binary of an important program, or the contents of a database on disk; modifying, adding, or removing packets over a network, either local or far across the Internet, wired or wireless; changing either the data a program is using or the running program itself

Tampering can be done with:
- file: whatever file, yours or of the attacker (on which you rely), also on file server
- memory: edit code or data supplied via API
- network: modify dataflow or redirect them.

THREAT	VIOLATED PROPERTY	THREAT DEFINITION	TYPICAL VICTIMS	EXAMPLES
Repudiation	Non-Repudiation	• Claiming that you didn't do something, or were not responsible. • It can be honest or false • Often apperars at the business level • The key question for system designers is, what evidence do you have?	Processes	Process or system: "I didn't hit the big red button" or "I didn't order that Ferrari." Note that repudiation is somewhat the odd-threat-out here; it transcends the technical nature of the other threats to the business layer.

Typical cases are repudiation of an action eg claim to have not received something or not have done something else.
Also importants are attacks on logs: edit or deletion of logs.

THREAT	VIOLATED PROPERTY	THREAT DEFINITION	TYPICAL VICTIMS	EXAMPLES
Information Disclosure	Confidentiality	Providing information to someone not authorized to see it	Processes, data stores, data flows	The most obvious example is allowing access to files, email, or databases, but information disclosure can also involve file-names, packets on a network, or the contents of program memory.

No need to explain, whatever action in which attacker can read what it shouldn't.

THREAT	VIOLATED PROPERTY	THREAT DEFINITION	TYPICAL VICTIMS	EXAMPLES
Denial of Service	Availability	Absorbing resources needed to provide service	Processes, data stores, data flows	A program that can be tricked into using up all its memory, a file that fills up the disk, or so many network connections that real traffic can't get through

DoS attack: absorb memory/CPU, fill data store or consume network resource

THREAT	VIOLATED PROPERTY	THREAT DEFINITION	TYPICAL VICTIMS	EXAMPLES
Elevation of Privilege	Authorization	Allowing someone to do something they're not authorized to do	Processes	Allowing a normal user to execute code as admin; allowing a remote person without any privileges to run code.

EoP can be against a process by corrupting it eg gain access to RW memory inappropriately or generally by missing authorization checks, buggy ones or through tampering data eg modify bits on disk to gain privileges.

STRIDE - per - Element

A variant of STRIDE consists of focusing only on specific classification depending on the element we are studying eg a data store is unlikely to spoof another data store

		S	T	R	I	D	E
VICTIM	External Entity	X		X			
	Process	X	X	X	X	X	X
	Data Flow		X		X	X	
	Data Store		X	?	X	X	

STRIDE - per - Interaction

In this variant is also important the way an element interact with another.

#	ELEMENT	INTERACTION	S	T	R	I	D	E
1	Process 1	Process 1 – Data Store 1	X			X		
2	Process 1	Data Store 1 - Process 1	X	X			X	X
	Data Store 1	...			X			
	Data Flow k							
n	External Entity							

For each Interaction, list all the possible threats in the identified category

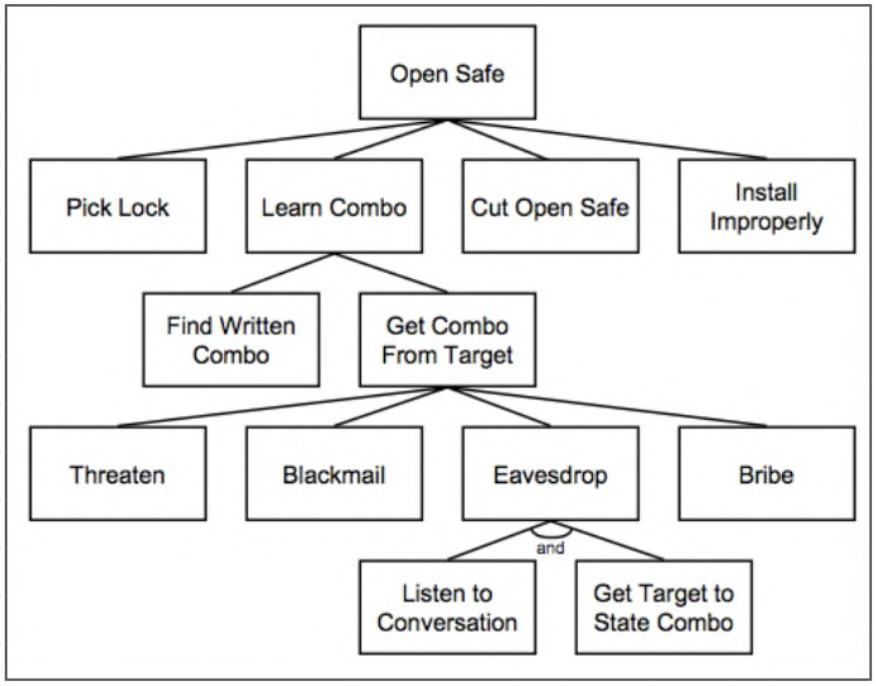
DESIST

- Dispute (= repudiation)
- Elevation of Privilege
- Spoofing
- Information Disclosure
- Service Denial (= replace Denial of Service)
- Tampering

After the model is done we must check it. Easiest way is to check if there is a possible attack for each category. A bit harder is ensuring we have one threat per element. Most complete model is STRIDE per element. Anyway doing this does not mean the model is complete.
Note: STRIDE is just an enumeration of threats that may happen, not how!

ATTACK TREE

A way of describing security of the system graphically. Focuse on one aspect we want to secure and decompose it in details. It represents attacks and countermeasures as a tree structure. Root node is the goal of attacker, leaf nodes are specific attacks used to reach the goal.



Three way to use it:
① Use tree already created to find a threat
② Create by yourself to help you find threats in your project
③ Create for the others.

CREATE A TREE

① Decide a Representation
- AND tree: state of node depends on all its child being true. Represent different steps in achieving a goal
- OR tree: a node is true if any of its child is true. Represent different ways to achieve a goal

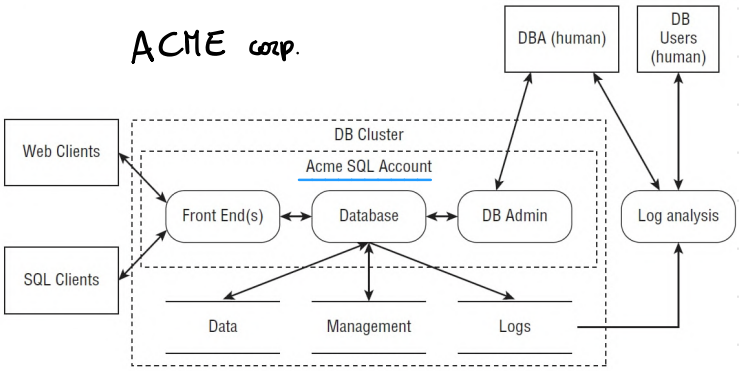
② Create Root Node: it can be the component that prompts the analysis, an adversary goal or a problematic state.
We can assign values to nodes to characterize potential attack eg Boolean: possible or impossible
Node's value is a function of its child's values eg $P \wedge I \rightarrow I$

③ Contextualize countermeasures: specify countermeasure (and cost) for the nodes.

④ Make structure clear and information rich.

THREAT MODELLING EXAMPLE

ACME corp.



ACME sell databases currently at version 3.1. Unfortunately there was not too much attention to security in the past and now they want to improve this aspect

The system is composed by 3 processes (Front End, Database and DB Admin) and 3 datastores (Data, Management on Logs).
Log Analysis is a process but not inside trust boundaries.
External entities are: Web client and SQL clients that work as interface and 2 HUMAN entities (DBA and DB users. Is important to specify human entities!

At this point we need to study the interplay between Requirements, Threats and Mitigation (solve threats):
- Threats help identify req. but at some time they violate them
- Impossibility to mitigate a threat implies Non-requirement.

SECURITY REQUIREMENTS

First type is Business Requirements. They are divided in:
- Competition-Driven: customer requirement or competitive differentiator
- Industry Requirements: specific of the domain in which the product will be used.

Then we have many way to come up with security requirements:
① Prevent/Detect/Respond: try to prevent threats you know. Then detect new ones and solve them.
② People/Process/Technology: study who use the product, how and with which technology.
③ STRIDE
④ ... etc

ACME formalized this list of security requirement at first:

Req Id	Requirement Description	Req Type
1	The product is no less secure than the typical competitor (Acme's software is currently very insecure, and as such, stronger goals are deferred to a later release)	BR
2	The product can be certified for sales to the U.S. government	IR
3	The product will ship with a security operations manual. A security configuration analysis tool is planned but will ship after the next revision	PPT
4	Non-requirement: protect against the DBA	NR
5	As the product will hold arbitrary data, the team will not be actively looking for privacy issues but nor will they be wilfully blind	PR
6	Additional requirements will be applied to specific components	

Will use STRIDE-per-element to compute security requirements.

		DFD APPLICABILITY			
	THREAT TYPE	External Entity	Process	Data Flow	Data Store
S	Spoofing	X	X	X	
T	Tampering		X	X	X
R	Repudiation	X	X		X
I	Information Disclosure		X	X	X
D	Denial of Service		X	X	X
E	Elevation of Privilege		X		

① Front End(s)

#	Front end Requirement Description
1	It should support authentication
2	It should support load balancing and related functions so that the core database can be as fast as possible
3	Only authenticated users will have create/read/update/delete permissions on DB
4	Single-factor authentication will be sufficient for front-end users
5	Accounts will be created by processes designed by customers deploying the Acme DB software
6	Data will be subject to modification only by enumerated authorized users, and actions will be logged according to customer configuration

⇓

#	Description
Spoofing	Authentication from both web and SQL clients is weaker than the team would like. Requirement to support web browsers and third-party SQL clients imposes limits on what can be required.
Tampering	A number of modules included for authentication were poorly vetted for security properties. Auto-updates can be exploited for tampering purposes
Repudiation	Logging at the front end is nearly non-existent
Information disclosure	There are both debugging interfaces and error messages, which reveal information about the database connection parameters
Denial of Service	Reliability engineering has already removed most of the problems for this process
Elevation of privileges	A separate security engineering pass will perform a variety of testing on input validation. The front-end team will document the limited validation it performs on data, and review that against backend assumptions

	S	T	R	I	D	E
Front End(s)	X	X	X	X	X	X
Web Client DF	X	X		X	X	
SQL Client DF	X	X		X	X	

+ Connections use SSL protocol ⇓

	S	T	R	I	D	E
Front End(s)	X	X	X	X	X	X
Web Client DF	X					
SQL Client DF	X					

② Database

#	Database Requirement Description
1	All database permissions rules will be centralized into a single authorization engine to enforce confidentiality, integrity, and authorization policies

⇓

#	Description
Spoofing	The front end has the ability to impersonate and perform actions as any user account; this needs further investigation
Tampering	Input validation raises questions of SQL injection, and those lead to questions about what assumptions are being made about the front ends
Repudiation	Reviews found that the database logs nearly everything originating from the front end, except several key session establishment APIs fail to log how the session was authenticated
Information disclosure	SQL injection attacks against the database can lead to information disclosure in all sorts of ways
Denial of Service	Various complex cross-table requests may have a performance impact
Elevation of privileges	A code review found two routines that by design allow any caller to run arbitrary code on the system

	S	T	R	I	D	E
Front End(s)	X		X			X
Web Client DF	X					
SQL Client DF	X					
Database	X	X	X	X	X	X

Data and Management can be analyzed together with Database ⇓

	S	T	R	I	D	E
Front End(s)	X		X			X
Database	X	X	X	X	X	X
Data (Data Store)		X		X	X	
Management (Data Store)		X		X	X	

③ DB Admin

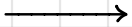
#	Database Requirement Description
1	Authentication Strength: Required authentication strength is debated, and a bug is opened to ensure that the agreed upon requirement is crisp
2	Account creation: Creating new DBA accounts will require two administrators, and all administrators will be notified
3	Sensitive Data: There can be requirements to protect information from DBAs (create a deny ACL for an object or encrypt data with a key that's passed in)

#	Description
Spoofing	The DBA can connect in two ways: (i) via a web portal and (ii) via SSH. The web portal uses SSL, which incorporates by reference all several hundred SSL CAs in a browser, and as such the portal may be "spoofable". Furthermore the module only support single-factor authentication
Tampering	The DBA can tamper, and in some sense that's their job
Repudiation	Logs can be changed by the DBA
Information disclosure	The DBA login page provides a great deal of "dashboard" and overview information pre-login as a convenience feature
Denial of Service	The DBA module can turn off the database, re-allocate storage space, and prioritize or de-prioritize jobs
Elevation of privileges	There is a single type of DBA. Does not apply

	S	T	R	I	D	E
Front End(s)	X		X			X
Database	X	X	X	X	X	X
Data (Data Store)		X		X	X	
Management (Data Store)		X		X	X	
DB Admin	X	X	X	X	X	

④ Logs Data Store

#	Description
Spoofing	NA
Tampering	Logs are read only
Repudiation	Some Logs are stored in different location
Information Disclosure	Because the log analysis code is outside the trust boundary, the logs must not contain information that should not be disclosed, and a review of logging will be required, especially focused on personal information
Denial of Service	The log analysis code has the capability to make numerous requests.
Elevation of Privileges	NA



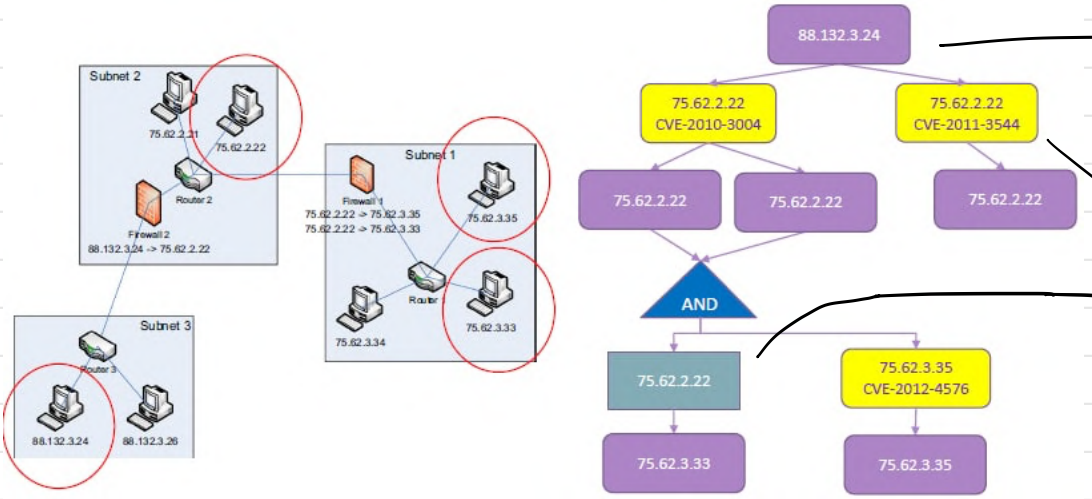
	S	T	R	I	D	E
Front End(s)	X		X			X
Web Client DF	X					
SQL Client DF	X					
Database	X	X	X	X	X	X
Data (Data Store)		X		X	X	
Management (Data Store)		X		X	X	
DB Admin	X	X	X	X	X	
Logs (Data Store)			X	X	X	

⑤ Log Analysis (even if not in trust boundaries)

- Spoofing - All the typical spoofing threats are present.
- Tampering - The log analysis module has several plugins to connect to popular account management tools, each of which presents a tampering threat. Keeping the logs read only mitigates these risks.
- Repudiation - The log analysis tools may help an attacker figure out how to engage in a repudiation that is hard to dispute
- Information disclosure - The log analysis tools, by design, expose a great deal of information.
- Denial of Service - Complex queries from log analysis can absorb a lot of processing time and I/O bandwidth
- Elevation of privileges - There are probably a number of elevation paths based on calls from the log analysis module to other parts of the system, designed in before trust boundaries were made explicit.

ATTACK GRAPH

Graphical representation of possible way of attacks. Typically nodes are privileges gained by attacker on the network hosts/devices while edges are software vulnerabilities that can be exploited. Computation of an attack graph requires computation of reachability conditions among network hosts. Not Easy!



Privileges node indicating attacke privileges that can be obtained on a particular IP

Vulnerability exploit that can be used by attacker

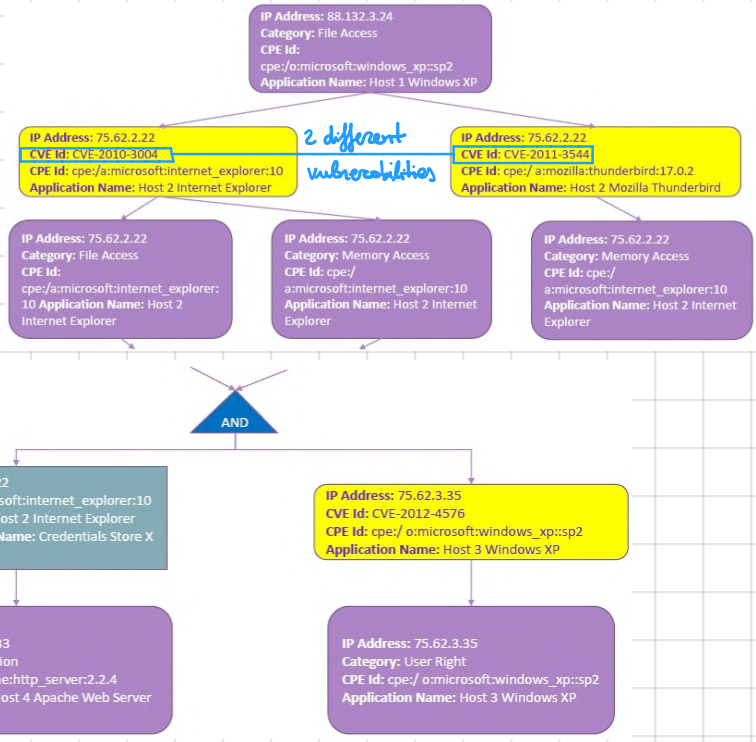
Information Source usage that can be used by attacker

All nodes (except conjunction) contains:

- IP
- CPE id: product identifier of software
- Application name

Additionally:

- Category
- CVE id: vulnerability id
- Information Source Name



General Problems

- Reachability Analysis
- Attack template determination
- Attack graph structure determination
- Attack graph core building mechanism

REACHABILITY ANALYSIS

Typically makes use of matrix. Column and rows are hosts and each cell provides information about reachability between the two corresponding column/row hosts.

Eg (Boolean) reachability matrix

		88.132.3.x		75.62.2.x		75.62.3.x		
		24	26	21	22	33	34	35
88.132.3.x	24	1	1		1			
	26	1	1					
75.62.2.x	21			1	1			
	22			1	1	1		1
75.62.3.x	33					1	1	1
	34					1	1	1
	35					1	1	1

More informations can be included in the reachability matrix eg protocols, topology of network, prevention systems etc.
The more info are obtained the more accurate the attack graph will be

ATTACK TEMPLATE DETERMINATION

Describes the conditions required by an attacker to perform a set of specific attack successfully. It also describes the conditions gained by him after the attack. Generally collectively form the attack model.
The detail level of the determined privileges gives us the precision of the resulting chains of vulnerability exploits in the generated attack graph, but the more precise it is, the more time and space is required in the attack graph core building process

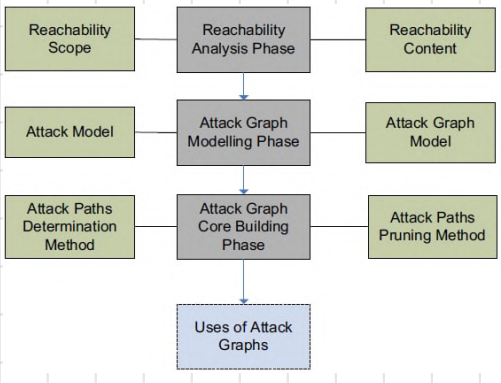
ATTAC GRAPH STRUCTURE DETERMINATION

Decide the structure of the attack graph depending on its complexity. As said more details require more space/time ⟶ find a trade off

ATTACK GRAPH CORE BUILDING MECHANISM

Initial attacker privileges are given as input for attack paths determination.
Full attack graph generation list each possible attack path from the initial to the target privileges.
Most of the attack graph generation algorithms use some form of searching algorithm to find the corresponding nodes in the resulting attack graph

Main Issue: Scalability.
Countermeasures:
① Monotonicity assumption: an attack can't negate any privileges obtained by attacker so far
② Pruning attack paths based on depth and/or likelihood of success of traversed attack path
③ Compute just the shortest attack path (or fixed length)
④ Cycle-free attack graph



TAXONOMY

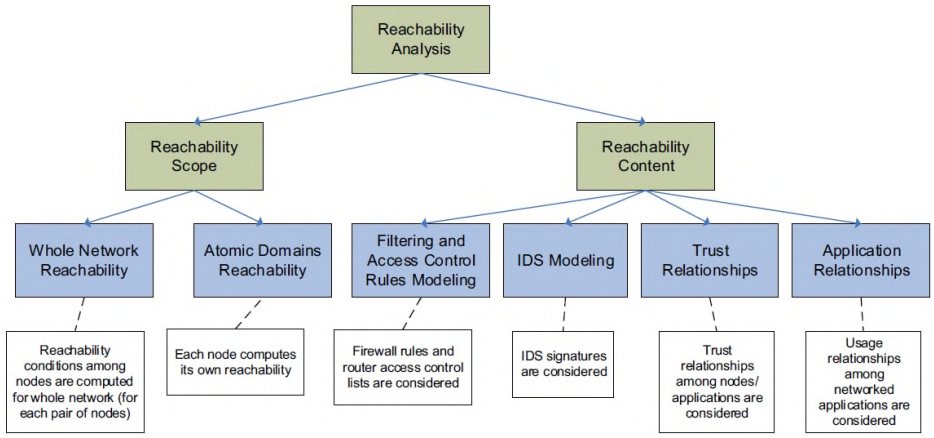
Activities can be divided into 3 main high-level phases

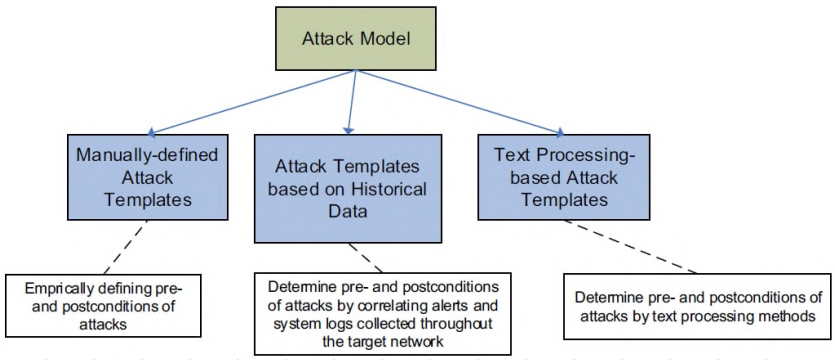
Reachability analysis phase

Making it simple: determine if two given hosts can access each other.

SCOPE: determines the scope of the network hosts among which the reachability conditions are computed before core building process

CONTENT: determines network security entities that are in the computation of reachability information



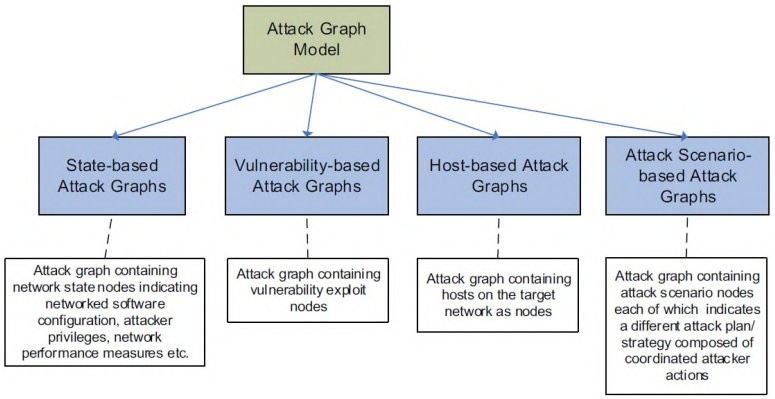


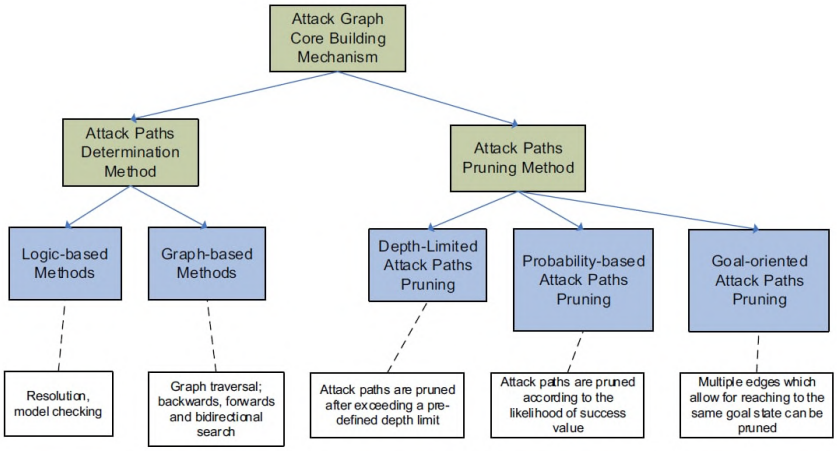
Attack Model

① Pre/post conditions of possible attacks eg in terms of privileges
② Information extracted from logs.
③ Infer pre/post by analyzing description of exploit itself.

Attack Graph Model

① Represent the state of whole system and how attacker may evolve within it. Low scalability.
② Relation between vulnerabilities
③ Focus on network topology.
④ Build graph taking into account different attack plans. Not so used.



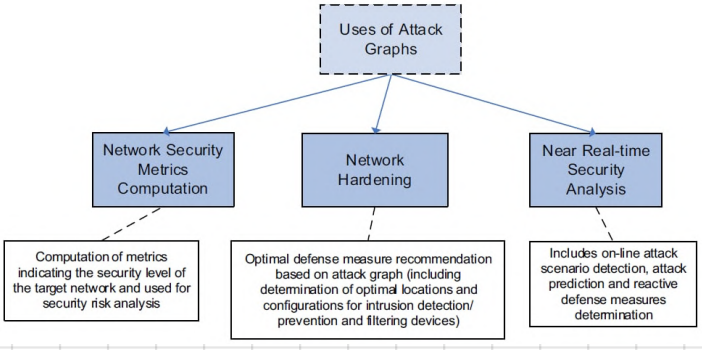


Attack Graph Core Building Mechanism

① Identify the way we want to compute the graph
1.1 Reasoning based
1.2 Run algorithms on graph to find a path.
② How we want to prune it ?
2.1 Apply the determination method until specified length
2.2 Contextualy compute likelihood of path and expand only path with high level of success
2.3 Start from the target to the source

Uses of Attack Graphs

Attack graphs can be used for these 3 uses categories. →

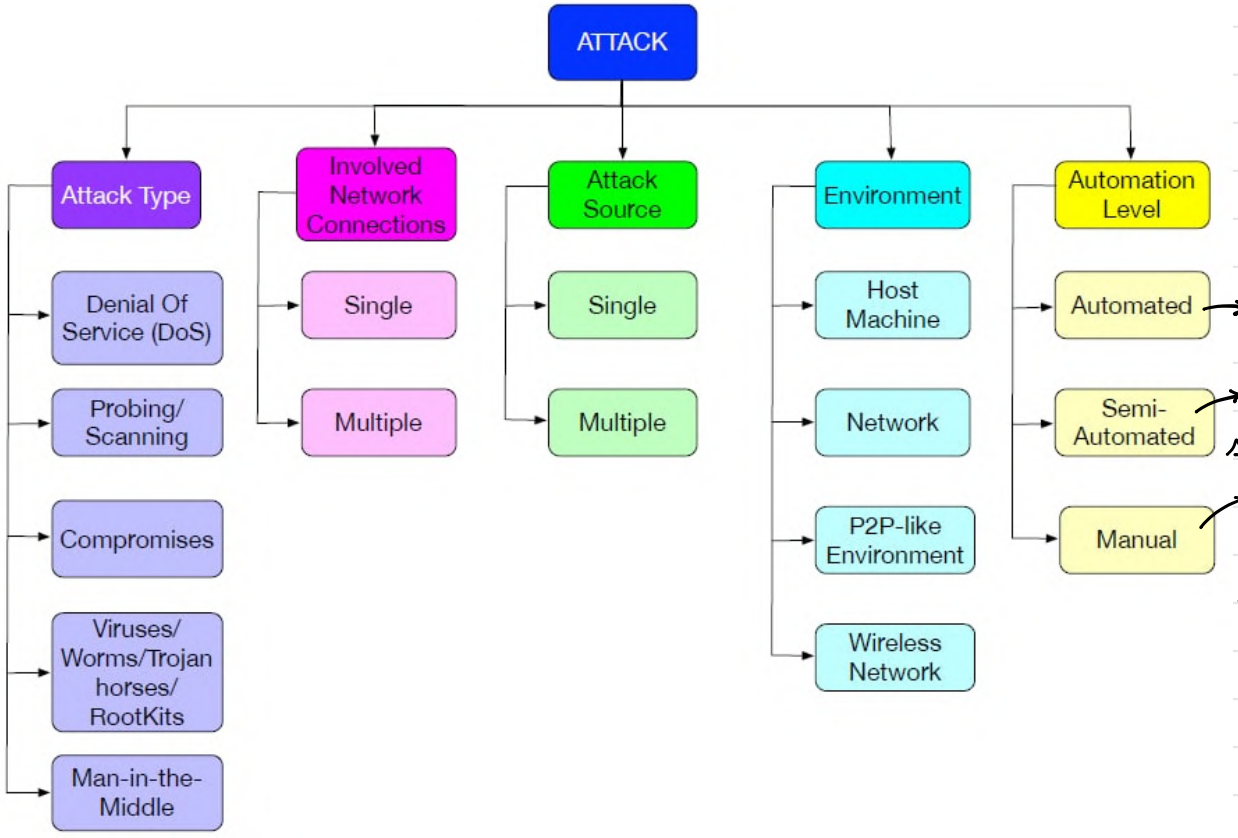


INTRUSION DETECTION SYSTEM (IDS)

Nothing is 100% intrusion proof eg firewall / VPN etc. → Continuously monitor the systems and detect attacks (both from outside and inside)

ID = monitor events occurring in system / network and analyze them to prevent intrusions
defined as attempts to compromise confidentiality, integrity, availability or bypass security mechanisms

ATTACK TAXONOMY



→ automated tools

→ deploy virus and start them from master

→ requires lot of knowledge, not frequent

(D)DOS: typical goal is compromise availability usually shutting down (part of) the network (also physically). Consumption of resources or alteration of configuration information (reducing privileges).

Eg. Teardrop: attacker overlaps TCP/IP packets to original ones avoiding their re-assembly at destination

Eg SYN flood: attacker send multiple SYN packets (create connection messages) leaving pending the ACK responses → too many "half connections" block new ones

PROBING/SCANNING: attacker want to find critical information about the system that can be exploited eg open ports. Generally use specific tools such IPsweep, nmap that are also used by the defender → hard to identify.

Analyze frequency of scans to prevent scanning attack, stealthy one are more challenging.

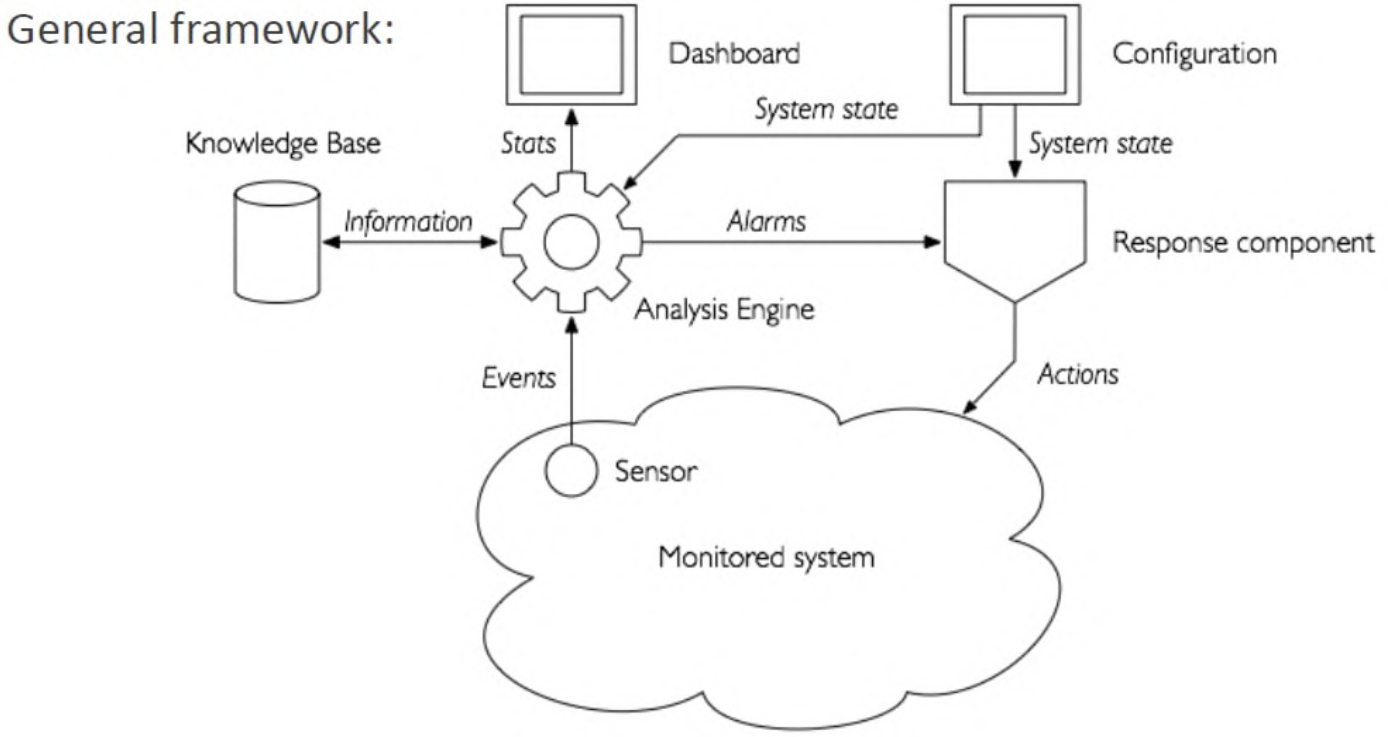
COMPROMISES: break the system to perform privilege escalation using bugs and vulnerabilities.

Eg Remote to Local attack: attacker who has the ability to send packets to a machine over a network (in which he has no account) gaining access → password guessing / known vulnerabilities

Eg User to Root: attacker has an account on machine (no root) but gains root privileges.

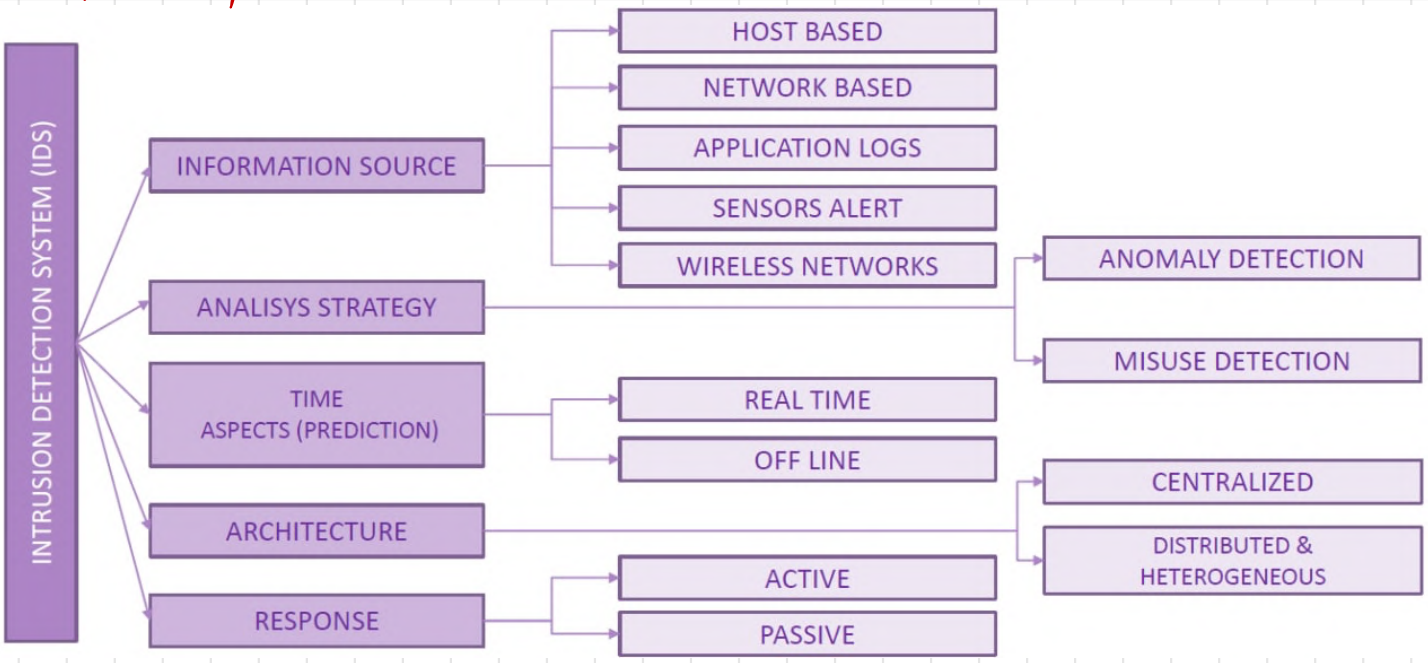
VIRUS / TROJAN HORSE etc: software agents running directly on machine. Goals are a lot depending on threat category eg Rootkit: open a port used by attacker to access the machine and gain privileges.

MAN-IN-THE-MIDDLE: attacker gain confidential data / inject false information intercepting the communication.



IDS is characterized by its detection precision (detection rate, false alarm rate), timeliness (processing / propagation time) and fault tolerance (IDS are not invincible!).
⇒ Find tradeoff between precision and time.

IDS TAXONOMY



INFORMATION SOURCE

HOST BASED: monitor events occurring within a single host (internally and along interfaces). Network traffic, logs, running processes, file access and configuration changes. Possibility to monitor a single application. Generally used for sensitive hosts (eg. servers). Combined with other IDS for monitoring encrypted channels.
Typical usage: code analysis (infer normal behaviour of system from code and check error while running), sandbox-based execution (stress host in protected environment), network traffic analysis, filesystem monitoring and log analysis.
Note: lack of context make attack detection hard (+ complex configuration and tuning)

NETWORK BASED: monitor traffic within specific network segments. Deployed at boundary between separated network. Perform analysis at application/transport/network/lower layer.
Sensors are deployed in line (in the channel where the traffic is moving eg in firewall) or passive (make copy of traffic flow and analyse it)
Typically works stealth (no IP address) but requires high level of resource usage. Good aspect is that it can be deployed without interfering on existing computer systems. Bad point: can't scan encrypted communication.

APPLICATION LOGS: monitor ONLY specific application using information not available to previous type of IDS. Can keep track of session information but requires complex tuning.

WIRELESS NETWORKS: new possibilities but new risks too. Communicate using what can be considered a broadcast medium is much less secure than wired networks. Lot of confusion no router, separation between normal and anomalous traffic hard to do and hard to deploy.
"Very shitty! 1/5"

SENSOR ALERT: information provided by sensors (wow!). Simpler management, improves detection rate.

ANALYSIS STRATEGY

MISUSE DETECTION: based on knowledge about attack. Try to identify what is considered not normal behaviour. Match attack behaviour? → Alarm

Signature based: knowledge base of IDS contains all signatures of attacks and perform checks on entities (like antivirus). Unable to identify new attacks/variants. Must keep updated the fingerprint DB.
Rule based: "if ... then ..." to identify attacks.
State transition analysis: build a finite state machine of IDS. When the automaton reach an "attacked" state → alarm.
Machine learning based: train classifier over historical data about events (normal or malicious). High level of accuracy in detecting know attacks and their variants. Cons: can't find new attacks

ANOMALY DETECTION: based on knowledge about WORKING system (contrary of misuse detection)
Programmed Systems: system configured with fixed behavioral models.
- Default Deny: behavior model accurately modeled. Only modeled states are allowed
- Descriptive Statistics: system described by statistical model.

Self learning Systems: system itself build the model.
- Non time series: stochastic model not considering time
- Time series: model considers time correlation of events.

Rule based: same as misuse detection (but inverse)
Statistical methods: monitor user/system behaviour by measuring variables over time

Distance based methods: how far we are from normal behaviour?
Profiling methods: create a profile of correct behaviour and use it to find suspicious actions.

TIME ASPECTS

ONLINE: check streams of data in real time. React quickly but requires high level of technology.
OFFLINE: check stored data and can perform more complex analysis. Used mostly for forensic purpose

ARCHITECTURE

CENTRALIZED: computation executed in a single point of system, not easily scalable
DISTRIBUTED: multiple points for execution, scalable but more complex.

RESPONSE

PASSIVE: only alarms to human admin
ACTIVE: performs automated actions (typically only increases sensitivity of sensors to gather more informations)

PORT SCAN DETECTION

Port scanning is very important couse is used by attackers to infer information about the system.
Not easy to detect. Attackers try to interact with ports for gathering info about reachability and status and this is a common action that not necessarily is malicious.

SCAN FOOTPRINT: set of port/IP combinations which the attacker is interested in characterizing. The target of attackers.
- Horizontal Scan: most common case, attacker is looking for a specific port to exploit a specific vulnerability within a range of IP addresses
- Vertical Scan: rare case, attacker focus on a particular host and start scanning all its port to find an unfixed vulnerability. Mostly used by administrator to secure a specific machine
- Block Scan: a set of ports is scanned within a set of IP addresses.

SCAN SCRIPT: the way how the attacker succeed (techniques/operations/time sequence)

SCAN PROBES

Different way to scan a connection:
- Full TCP connection: just try to connect to a specific port. Cons: every connection is wrote in log → easy to be detected
- Half connection (SYN scan): send SYN packet and wait ACK but then stop connection to infer if port is open or there is a firewall / port is closed depending on response
- Dirty bit scan: generate packets with invalid flags inside to observe how the receiver will answer inferring port status. Also detect protocol if port is open. Easy to detect → check packets validity
- ACK scan: check which port is protected by firewall → no answer = firewall

These scan can be combined in multiple way.

SCAN CHARACTERIZATION

We need a way to measure possible impact of scan because scanning is also a normal operation. Need to fine alarm only when needed!
Simplest way is by size of footprint, most useful way is to count total amount of information (not just open/close bit).

Some info are easier to detect. Closed size = number of IP/port combinations that are closed at the time of scan. Administrator already know closed port, no need to scan them!

Anomaly Score: $A(x) = -\log(P(x))$ = prob. $P(x)$ for normal packet to target x
Total anomaly score $A(x) = \sum A(x_i)$

DETECTION AVOIDANCE

- Change Scan order: don't use sequential order to create "noise" at defender's side
- Slow Down: most IDS work on time windows → slow scan may avoid alerts. Enlarging time window is is difficult because increase size of internal state.

- Randomize inter-probe timing: scan few ports using random interleaving between scans. Same concept of previous one.
- Randomize non essential fields: random fields such as source port, sequence number etc to generate noise
- Change Source Address: change IP address between scan making difficult to identify an attack
- Distributed port scanning: similar to DDoS but for scan.

DETECTION TECHNIQUES

GRAPH BASED INTRUSION DETECTION SYSTEM (GRIDS)

Vertex = host and edges = traffic between them. Scan probe can be represented as edge. High degree of a node → suspicious. Hierarchy of graph can be built to represent multiple levels.

SNORT portscan preprocessor

Flexible rule language to identify anomalies. Monitor frequency of packet flow. Unable to detect scans from multiple sources. Easy to avoid by decrease probe frequency

EMERALD

Create profiles for each IP addresses. Check if there is a match to a normal behaviour or not.
Unable to detect slow scans since they don't create a "solid" profile.

THE SPICE system

IDEA: keep track of anomalous packets for longer time periods. eg scan on private ports

ARCHITECTURE

- Sensor: monitor network and assign anomaly score to events
- Correlator: analyze high anomaly score events and try to correlate them.

How to compute this score?
It depends on combination of P(DestPort, DestIP, SourcePort, SourceIP) pairs but maintain this probability is costly in size/time
→ build estimation on probability of limited features
$P(DestPort)$, $P(SourcePort \mid DestPort)$, $P(DestIP \mid SourceIP, SourcePort)$

Once computed the anomaly score, we set a threshold and group packets.
Metaphor: events are atoms and correlation between them is the energy bonds. → Bond graph
All related events are connected by weighted edges above threshold. All heuristic functions produce results in $[0, 1]$ range: 0 = no connection between events.

In presence of a new event simulated annealing is used to find its right position by finding local maximum

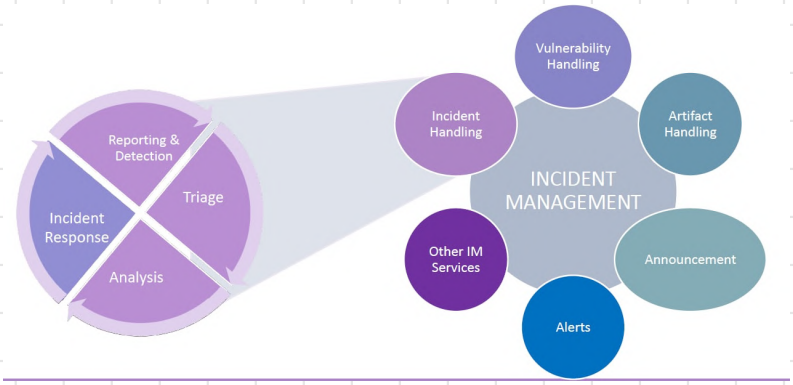
INCIDENT MANAGEMENT

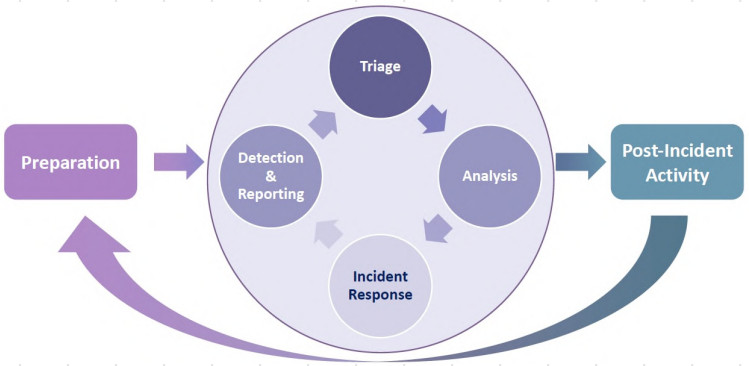
The process aimed at identifying, analysing and correcting hazards to prevent a future re-occurrence

A cyber security incident is any malicious act (or suspicious event) that:
- compromises the electronic security perimeter or physical security perimeter of a critical cyber asset
- disrupts the operation of a critical cyber asset

An incident is the act/attempt of violating an explicit or implicit security policy.

INCIDENT MANAGEMENT DECOMPOSITION





Incident Handling is the core part of incident management.

PREPARATION

Subset of activities that are proactive, needed to prevent incident and to establish an incident response capability to timely respond to them.
- Preparing to handle incident: define the plan to put in place in case of emergency, hardware and software available, who we should call (IT management? Police? Ghostbusters?), recovery procedure and any kind of resource needed to prevent a disaster.

  Many incident response team create a jump kit: portable case always-ready that works as first aid kit for investigation (laptop, backup devices, blank media, networking equipment etc)
- Preventing incidents: keeping number of incidents as low as possible. High numbers of incidents may overwhelm the incident response team.
  Typical activities: risk assessment, host security, network security, malware prevention, user awareness and training.

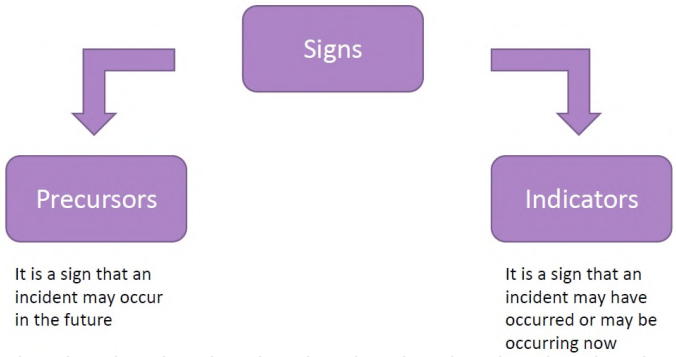
DETECTION AND ANALYSIS

Is impossible to develop a step-by-step guide for each incident so the organization should be ready to handle incidents that use common attack vector. Most common are: removable media, attrition (eg brute force), web, email, impersonation, improper usage, loss/theft of equipment ...

SIGNS OF AN INCIDENTS

To respond to an incident it is fundamental to detect and classify it. This is hard cause:

1. there are different kind of means
2. volume of potential signs is usually high
3. high specialized training is needed.



INCIDENT ANALYSIS

Detection and analysis is deeply impacted by several factors:

- Accuracy: trade off between false positive and time
- huge amount of events
- Indicators not necessarily related to incident
- Many incident dont have clear syntoms.

INCIDENT DOCUMENTATION

Is important to record facts related to possible incident in case of suspect. Note timeline and possible tools to be used keeping these data safe (integrity and confidentiality)

INCIDENT PRIORITIZATION

Label each incident with a priority level. Take into account:

- functional impact } business impact
- information impact
- recoverability

INCIDENT NOTIFICATION

Different incidents require different response team. In security policy should be specified a notification list and procedures. Very important is also to make communication strategies fault tolerant eg. SMS + email etc. (add redundancy)

CONTAINMENT STRATEGY

Important to avoid incident to overwhelm resources or increase damage. This grants time for developing a tailored remediation strategy. Decision making is fundamental (easier with predetermined strategies) → define acceptable risks that may occur while dealing with incidents.

EVIDENCE GATHERING AND HANDLING

Post incident procedure. Collect evidence of the incident for two reasons:

1. resolve future incidents
2. legal proceedings

In both case everything must be kept safe and preserved.

IDENTIFYING ATTACKING HOSTS

May be useless and time consuming for a response team.

Common procedures:

- validate attacking host's IP
- research attacking host on search engines
- incident DB
- monitor possible attacker communication channels

ERADICATION AND RECOVERY

Eradication may be necessary: eliminate components of incidents, disable breached accounts, identify and mitigate vulnerabilities.

Recovery instead consists in restoring system status to normal and fix vulnerabilities to prevent similar incident.

Clean backups, patches, change password, remove compromised files etc.

LESSON LEARNED

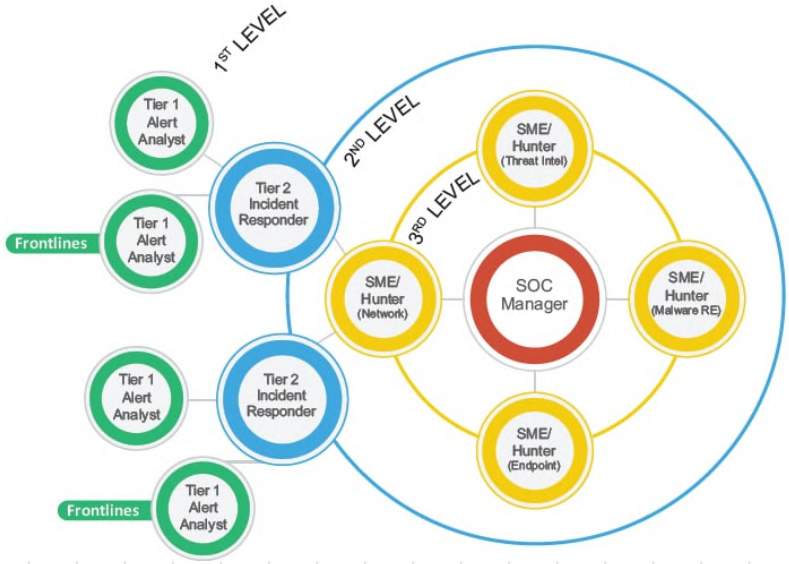
Analyse whole previous process and evaluate it. Check what could be improved and what instead was not effective at all. Learn by mistakes.

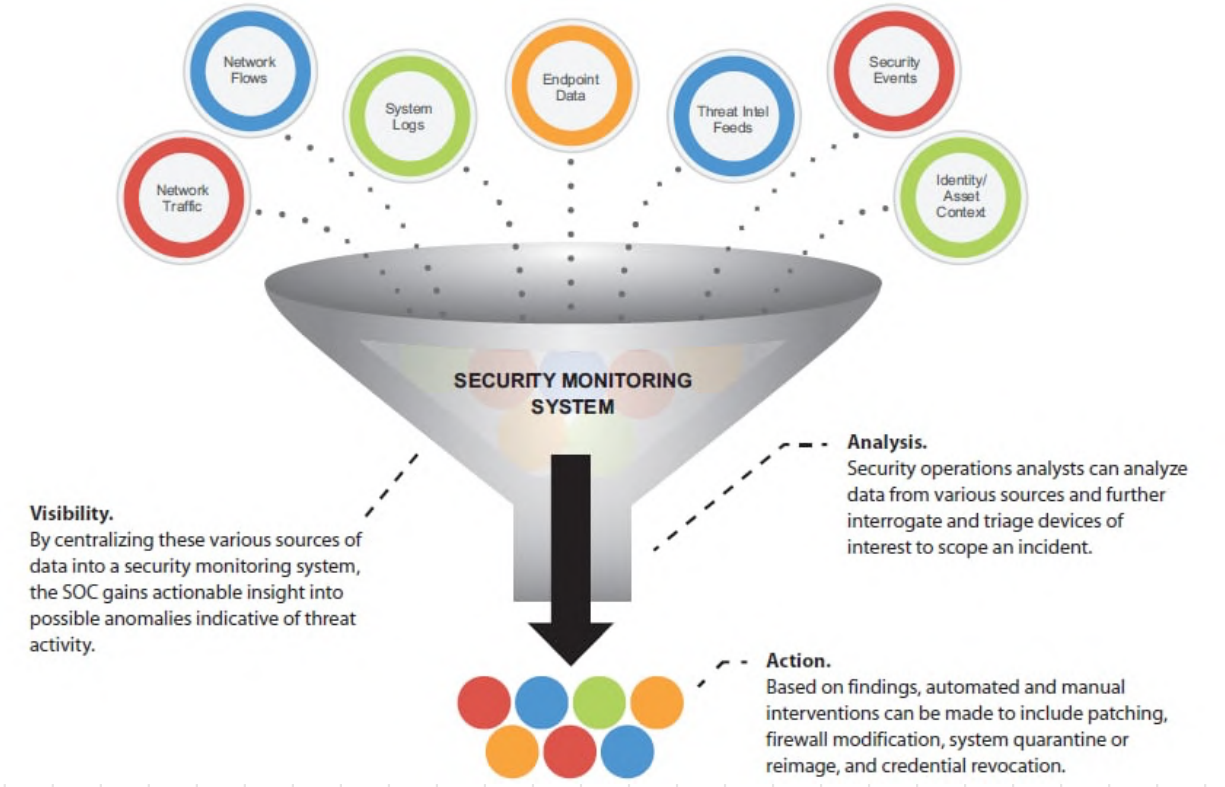
ORGANIZING INFORMATION SECURITY

SECURITY OPERATION CENTRE (SOC)

A centralized security organization that assists companies with security functions. It can be internal or external to the companies. End goal of SOC is to improve security posture by detecting and responding to threats / attack before it is too late.

Features: from "basic" Log management, Monitor and Alert, Incident Management to more complex like Service Security assessment, threat intelligence and security analytics.





When should we adopt a SOC?

- in presence of critical or "sensitive" data or process
- the company is growing and internal information security function is not enough anymore
- there is the need of higher level of security due to infosec events.

COMPUTER EMERGENCY RESPONSE TEAM (CERT)

In few words: the SWAT team of cybersecurity. Focus on response to cyber incidents.
Main functions are providing preventive service (such as alerts), security bulletins, training and management of security services (overlap with SOC). It shifted from pure reaction team to security providers. From Navy Seal to NSA.
Also known as CSIRT, Computer Security Incident Response Team.

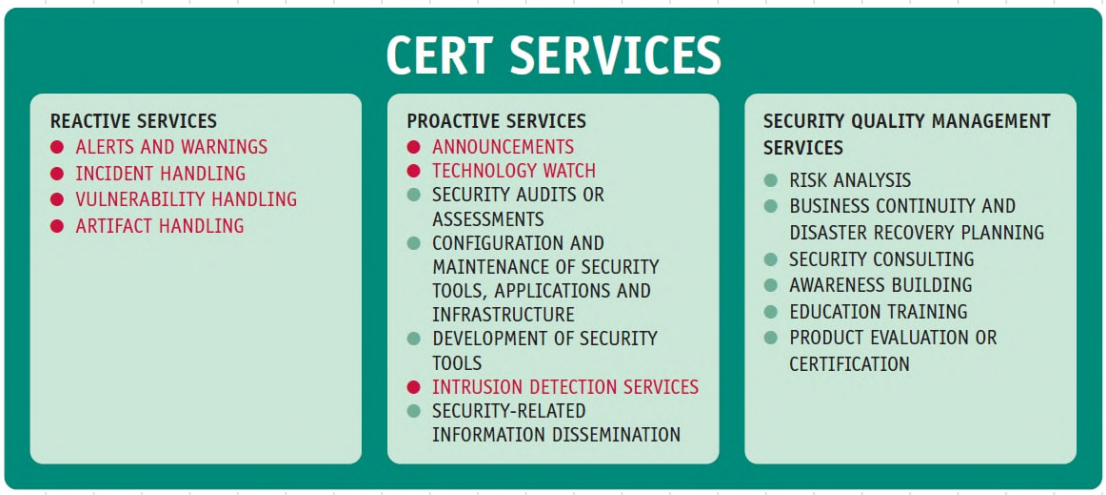
Basis of CERT:
- Mission: the goal and its activities. Aligned to the one of the company it is protecting.
- Costituency: who CERT is protecting (organization and/or people)
- Responsibility: what CERT is expected to do according to its mission
- Mandate: the "power" to do what should be done
- Organizational framework: which process CERT will apply
- (Possible) Available Services

RESPONSIBILITY

Answer following questions:
- What types of incidents must be handled and with what priorities?
- Is duty of CERT to track incident resolution and close it or it just need to notify the company?
- Is CERT obliged to solve incidents or should just notify and give advises about the solution?
- What (and who) to do if costituent (company) is not fast enough to solve the problem?
- Must CERT contact specific entities in presence of specific incidents?
- Are responsibility limits clear enough or should be improved?

MANDATE

Again questions:
- CERT only give advices or can obligate costituents to react and solve issue and keep it informed?
- Deadlines to costituents are allowed? If so which are the sanctions? What is the power of CERT?
- Can CERT collect data in costituents network for analysis?
- Again, is mandate well defined?



ROLES

Mandatory:

- Duty officer: takes care of all in-coming requests + periodic /ad hoc activities
- Triage officer: deals with all incidents reported. Decides priority, who will deal with the incident and when. Must be updated with latest trends about attack vectors etc
- Incident handler: manage the team who handle the incident
- Incident manager: responsible for the coordination of all incident handling activities.

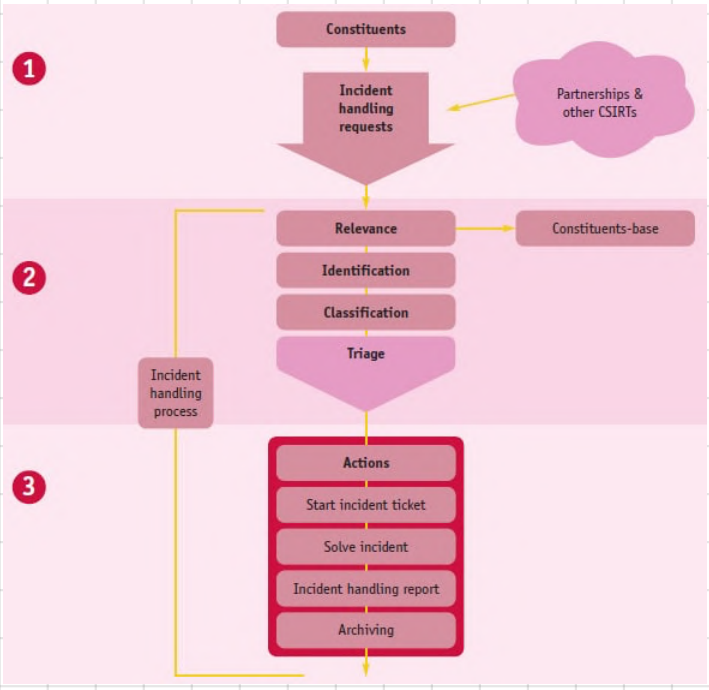
Optional:

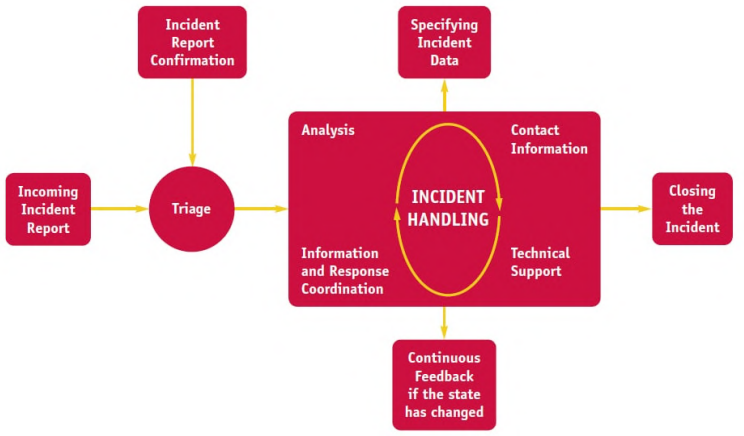
- PR officer
- Legal officer
- Team manager
- Hotline operator

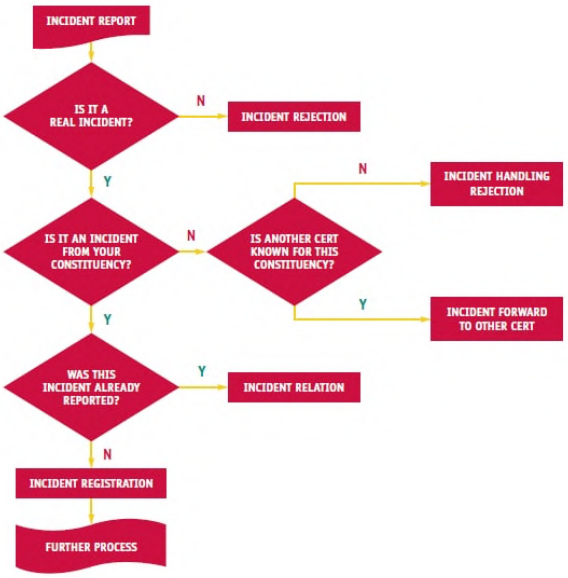
} Usually the same person

WORKFLOWS

Workflows can be different depending on CERT specifications







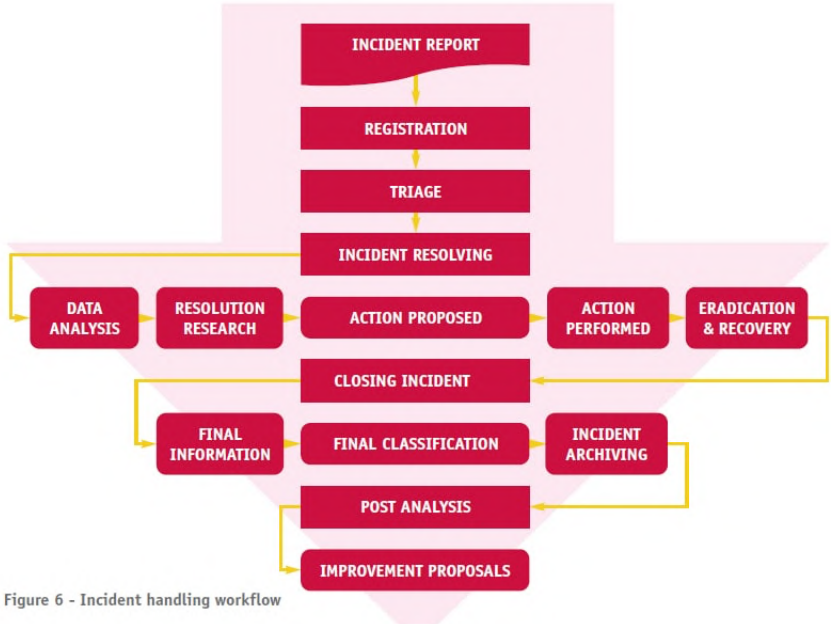
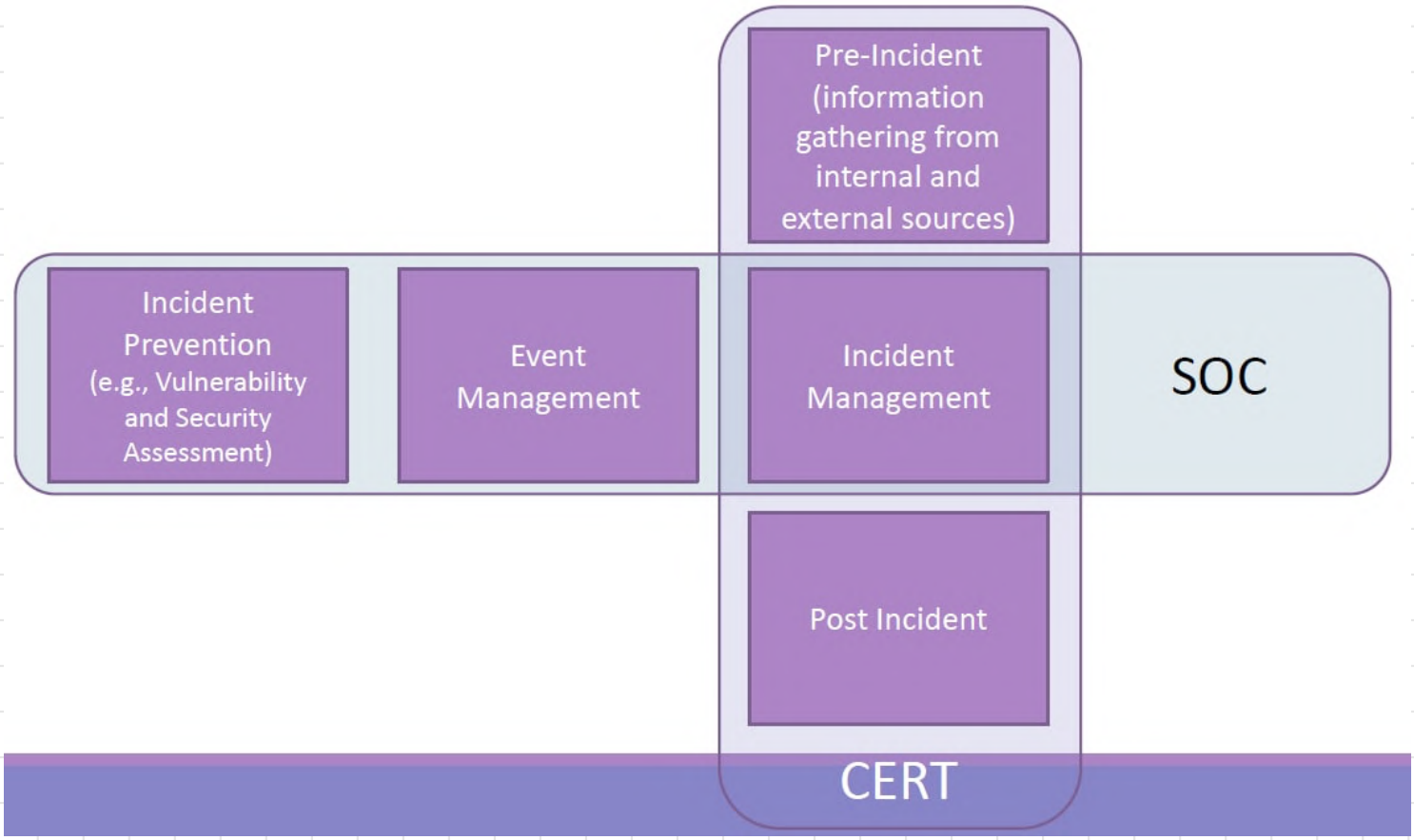


Figure 6 - Incident handling workflow

POLICIES

Basic policies :

- information classification policy : how to rigth classify information
- information disclosure policy : which info could be disclosured and how
- media policy : how to manage media
- privacy policy : how to handle data according to privacy
- security policy : define security policy inside organization



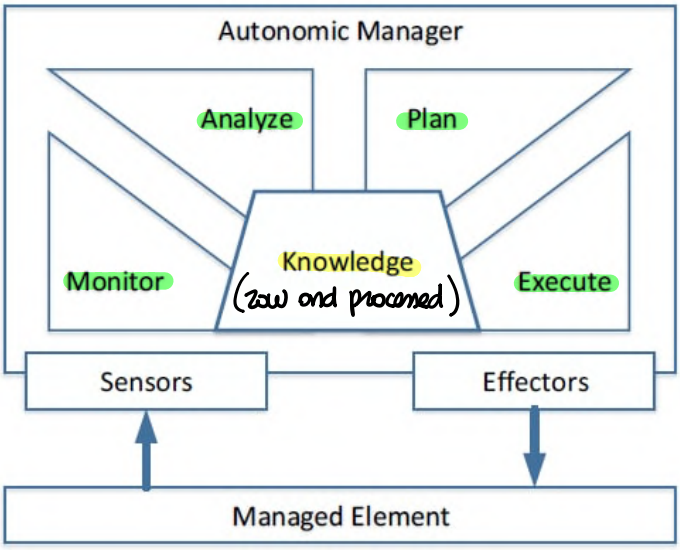
A SOC centralizes the roles responsible for protecting information security in the organization and includes prevention, detection, incident management, response and anything to do with managing and defending infosec within organization.
CERT/CSIRT/CIRT may, instead, work under a SOC and includes not only the roles dedicated to information security (pre / post incident) but also roles dedicated to public relations, communication, marketing, customer support and management.

CASE STUDY : THE PANOPTESEC SYSTEM

Basically how to translate in practical what we discussed until now.
Focused on detection and prioritization and mitigation actions.

The consortium behind panoptesec system wants to deliver a risk-based approach to automate cyber defence.
Proactive side : mitigation actions based on current level of risk of the system
Reactive side : improve detection and find best mitigation action for specific incidents.

MAPE-K CYCLE



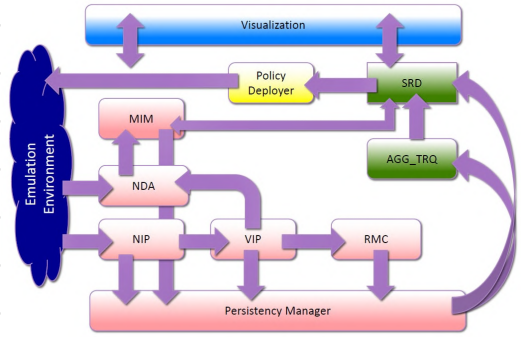
Decision support for cyber vulnerability, incident detection and response management
Monitor vulnerabilities
Analyze risks and impact
Plan mitigation responses
Execute actions

Even though the aim of the tool is to automate risk evaluation/mitigation, it still has a visualization system to increase risk awareness of security teams.

GENERAL APPROACH

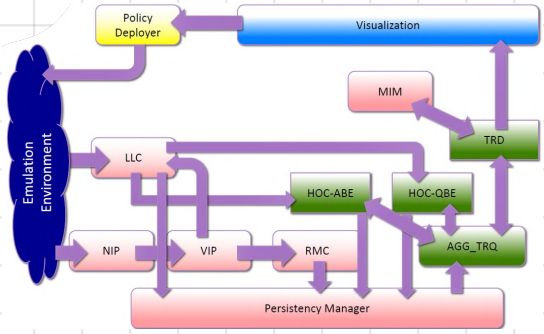
In PROACTIVE RESPONSE SYSTEM the idea is to provide a strategic response (also in long term). Identify attack path and evaluate best mitigation actions. In REACTIVE RESPONSE SYSTEM we still use an attack graph to identify attack path but instead of considering most dangerous one in terms of impact we try to identify attacks path that are most likely to be followed by an attack
In few words: reactive strategy focus on bulking up your defense against common attacks, proactive strategy aims to prevent these attacks from happening.
Difference between IDS and proactive system is that both analyze network/host information and provide notification about particular behaviour they are observing but second one then correlates IDS alerts to provide increased information (attack pattern taking into account business perspective)

All system is maintained efficient by its modularized architecture.

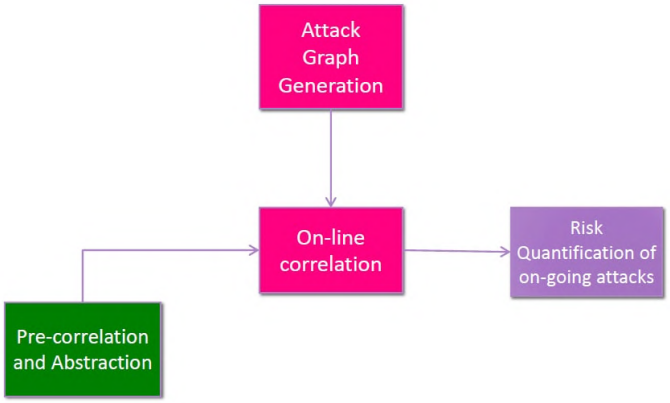


Proactive

Reactive



ON-LINE MULTI STEP ATTACK DETECTOR



Attack graph + low level alerts (IDS) aggregated and preprocessed = possible attack patterns and their level of advancement.

Attack graph translation into Correlation Queries

From attack graph generates an Enriched Attack Graph JSON file.

QBE - QUERY BASED ENGINE

Detect the multi-step attack early enough to react and take proper countermeasures
⇒ use Complex Event Processing (CEP) techniques to detect temporal and spatial correlation among events happening at different hosts.
It is based on alerts correlation in addition with attack graph to realize on-line attack detector.
Possible problems: potential big data (handle Volume, Variety, Velocity) or incomplete/inaccurate information (eg wrong event order)

When receiving an alert, it will be matched with the queries built from possible paths.
If no edge of queries/path matches the alert it will put aside for further analysis.

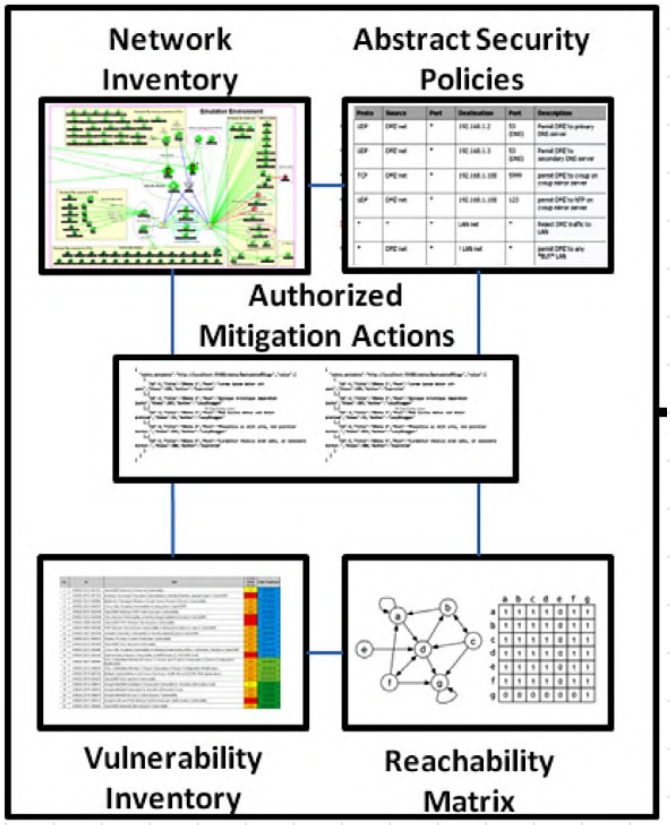
Attack matching is done using text matching techniques such as Jaccard Similarity that also take into account possible errors in order or notifications inaccuracy.

ABE - AUTOMATION BASED ENGINE

Takes as input automatically generation rules to predict incoming multi-step attacks.
The difference from QBE is that correlation rules (tree) are translated into automatons
Rise alert when reach final state. To "fix" missing alerts is possible to use "fictional" states.

PROACTIVE CHAIN

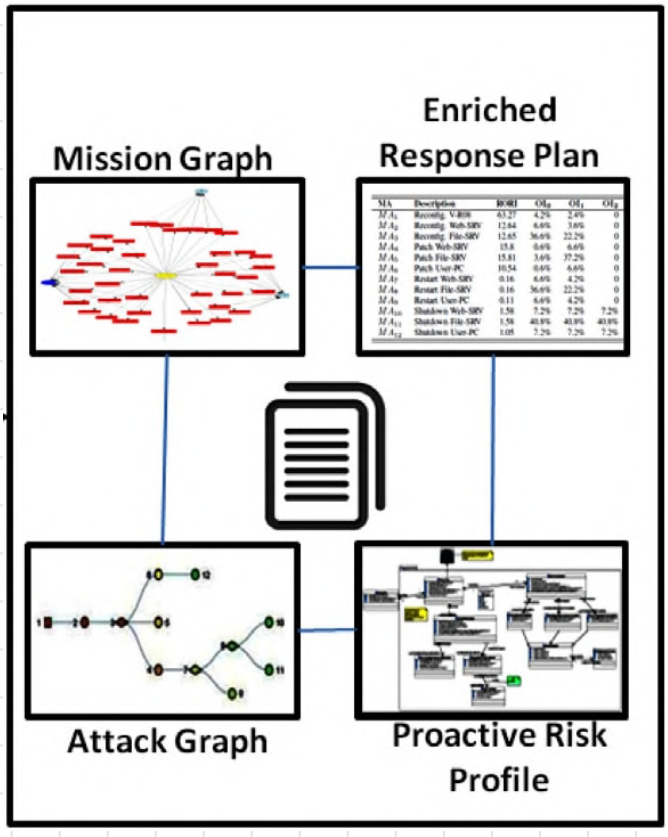
INPUT DATA



- **NETWORK INVENTORY**
  Contains info about devices currently active inside monitored system. Including deactivated devices would increase input size for nothing (+ cant be added automatically). Each device has specific information such as ID, PEP_TYPE, vulnerabilities (CVEs). and annual cost (AEC). The sum of all AEC gives the annual infrastructure value (AIV) used to compute RORI index
- **ABSTRACT SECURITY POLICIES**
  Tables of information needed for instantiation of security policies: threats, policy enforcement points (PEP) and mitigation actions.
  Each threat is described using threatID + its severity, frequency and likelihood threshold

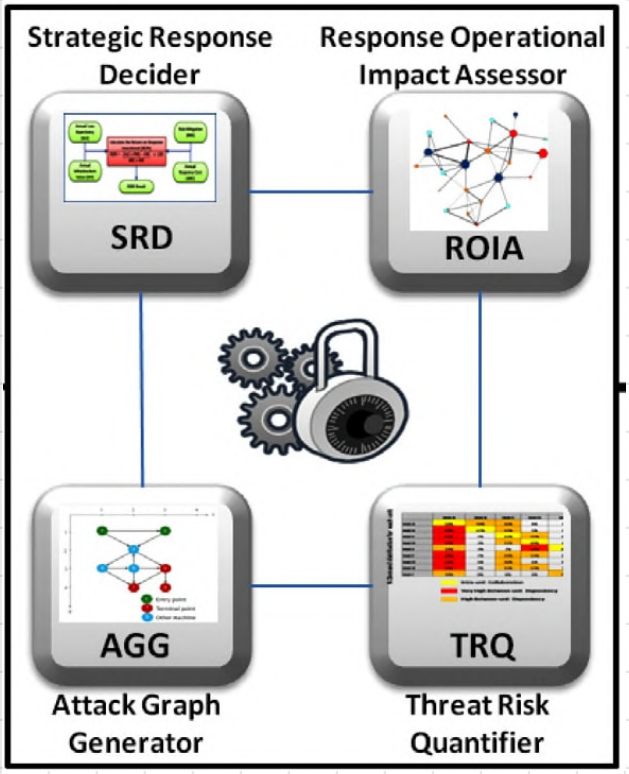
- **AUTHORIZED MITIGATION ACTIONS**
  List of authorized actions used as response to threats.
  Each action has: ID, scope of enforcement (tactical or strategic), enforcement point (where can be applied), annual equipment value associated to PEP and its annual response cost

OUTPUT DATA



- **MISSION GRAPH**
  Describe business model of organization in term of process and functions.
- **PROACTIVE RISK PROFILE**
  Contains structured information about risks in mid-long term and allows to analyse all elements that contribute to risk analysis (impact and likelihood)
  To be noted also the presence of detrimental events, events that could harm the accomplishment of an organization's mission.
- **ENRICHED RESPONSE PLAN**
  Detailed info about mitigation actions.

FUNCTIONAL PROCESSING MODULES



Placed, of course, between previous sections.

- **ATTACK GRAPH GENERATOR**

Based on pre/post conditions concept of attacks try to match attacks with system using First Order Logic.

precondition → postcondition ...

This approach has been transpose on graph theory for which there exists lot of optimum algorithms.

Thanks to this has been possible to implement Backtracking and improve path searching algorithms

Problems occur with fully meshed networks → exponential growth of attack path number.

- **THREAT RISK QUANTIFIER**

Analyze Elementary Risks composed by technical attack path, linked business proces and relative detrimental event, aggregate them w.r.t detrimental events and calculate organizational risks and risks contributions.

Likelihood is the metric used to evaluate risks and increases as the attacker progresses on the attack path. For two paths with same length the one with easiest vulnerability exploitation will have the lowest likelihood. Impact of ER is evaluated analyzing the violation (or not) of specific vulnerabilities multiplied by a qualitative/quantitative variable that indicates the impact magnitude on the organization. Each possible attack path may lead to [0, x] detrimental events (DE) which can be seen as relationship (a path) between a business proces and a network device.

- **RESPONSE OPERATIONAL IMPACT ASSESSOR (ROIA)**

Evaluate posible mitigation actions and their impact on organization's mission.

Every mitigation is a posible threat to the operational capability and any local impact may spread throughout the network (eg patch with new bugs). To do this, a Resource Dependency Model is built. RDM is a probabilistic graphical model representing dependencies of involved resources.

An other data structure used is the Mission Dependency Model that captures the dependencies of company/mission on its business processes.

- **STRATEGIC RESPONSE DECIDER (SRD)**

Asses and combine mitigation actions from the set of authorized mitigation actions. Select best one using RORI INDEX measuring the benefits of each one.

NETSPA ATTACK GRAPH

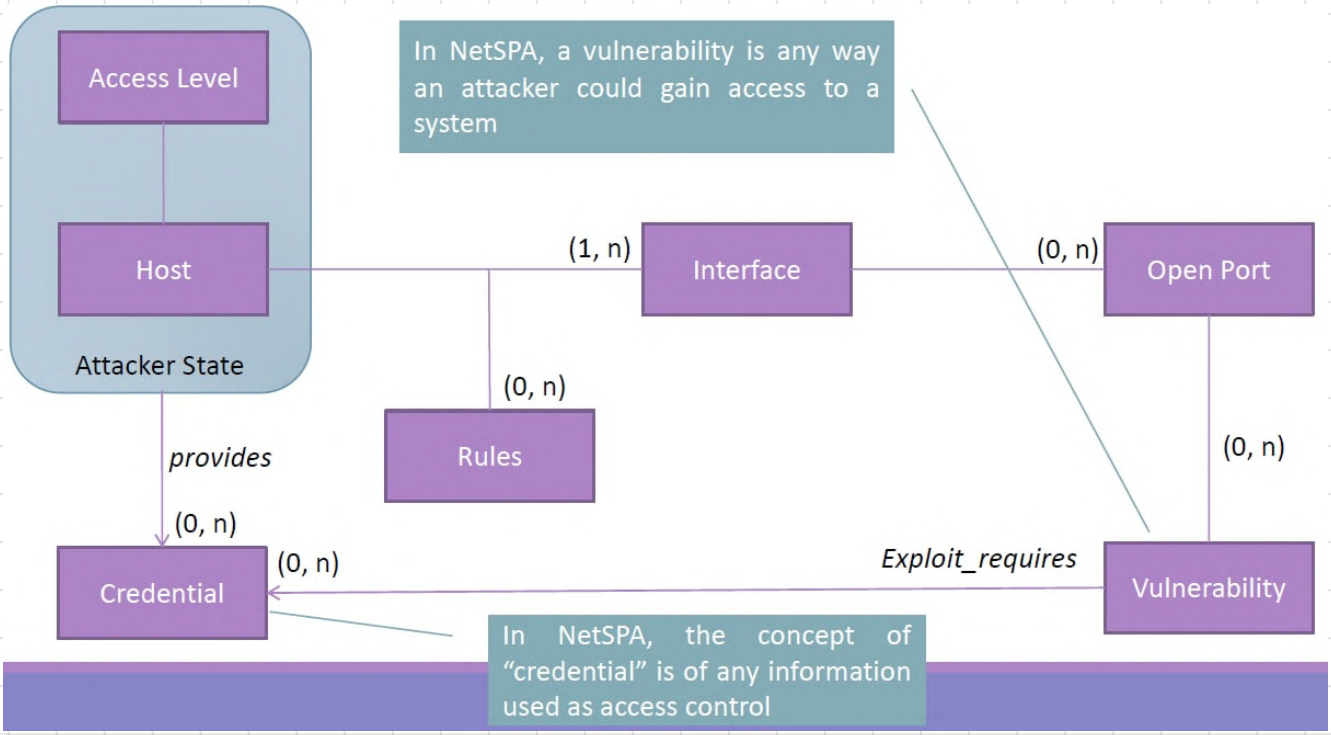
Recap.

In a typical attack graph: nodes are privileges and edges vulnerabilities exploited to gain them.
Computation of attack graph requires the computation of reachability of network's hosts.
NetSPA is an attack graph system with following features:

- Multiple-prerequisite (MP) graph: combines multiple privileges.
- Interface with common data sources
- Automatic reachability computation

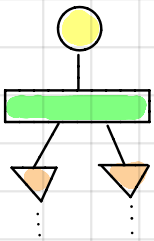
Main data types:

- Hosts = machines in the system
- Interface = of each host, how hosts communicate
- Rules = the way hosts communicate via interfaces (eg routing, for reachability)
- Open Ports = ports allowing communications associated to interfaces
- Vulnerabilities = associated directly to open ports (and indirectly to the host)
- Access level = possible privileges that can be obtained on an host.
- Credential = gained after exploitation of vulnerabilities.



MP graph use 3 node types:

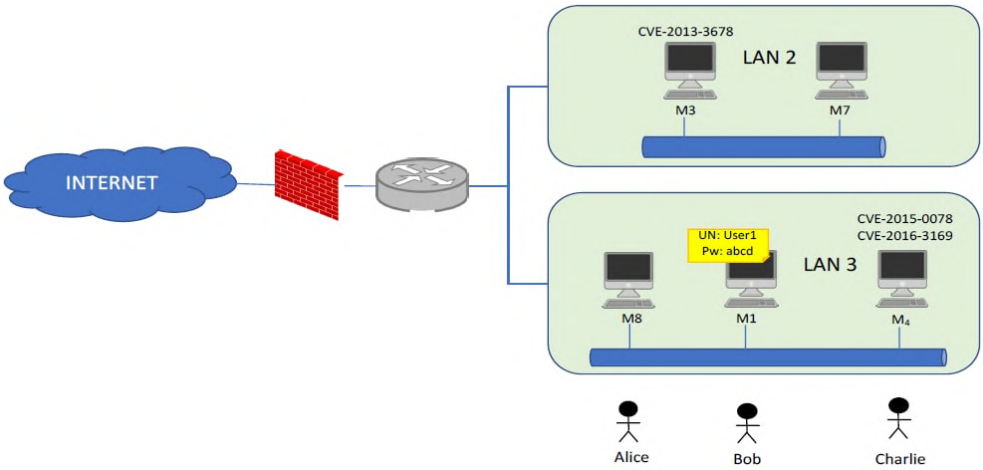
- STATE NODE: attacker's level of access on a particular host. Circular nodes.
- PREREQUISITE NODE: either a reachability group or a credential. Rectangular nodes
- VULNERABILITY INSTANCE NODE: a particular vulnerability on a specific port. Triangular nodes



Ex.

Assess the risk that an attacker is able to compromise availability of M3 by assuming that:

- M3 reachable only from LAN2 and M4
- Alice has user access to M8 and she shares credential with her colleagues
- BOB has access to M1 and poor memory so he writes password on postit
- Charlie can access M4 but tends to leave the machine logged during the break



① Context Establishment

We need to identify at least the likelihood and consequence scale

For example: LOW, MEDIUM, HIGH, CRITICAL mapping to NIAO (?)

Likelihood	Normalized NIAO
Low	[0; 0,25]
Medium	[0,26; 0,5]
High	[0,51; 0,75]
Critical	[0,76; 1]

... consequences scale (only technical in our case):
3 values according with CVSS (also 4 if you want)

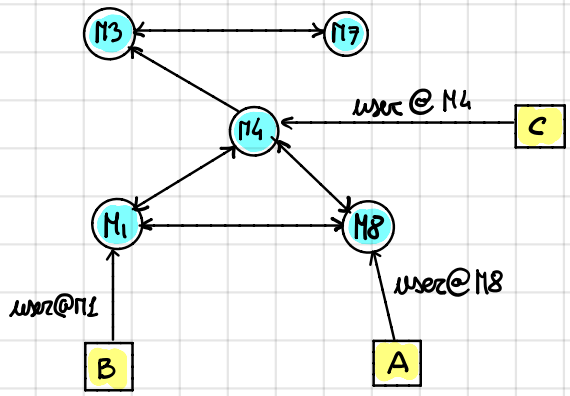
Critical			
High			
Medium			
Low			
Likelihood / Consequence	Low	Medium	High

② Reachability Matrix

from \ to		LAN 3			LAN 2		
		M1	M4	M8	M3	M7	Internet
LAN 3	M1	1	1	1			
	M4	1	1	1	1		
	M8	1	1	1			
LAN 2	M3				1	1	
	M7				1	1	
	Internet						

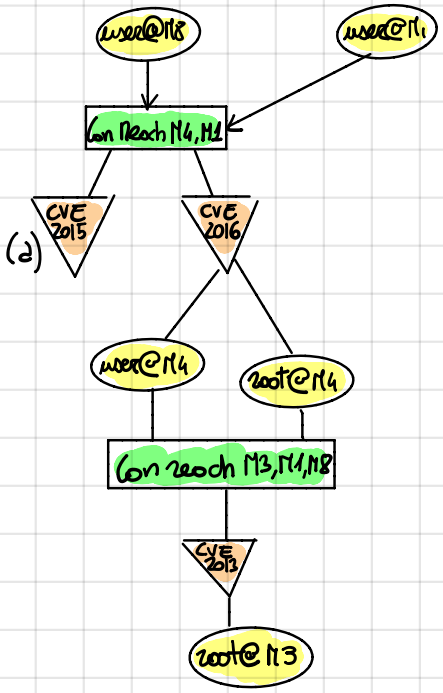
Assumptions:

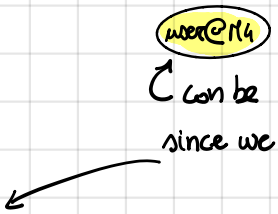
- Inside each LAN every host are reachable
- LANs not reachable from internet
- Bob has access level user@M1
- Charlie the same



③ Compute Attack Graph

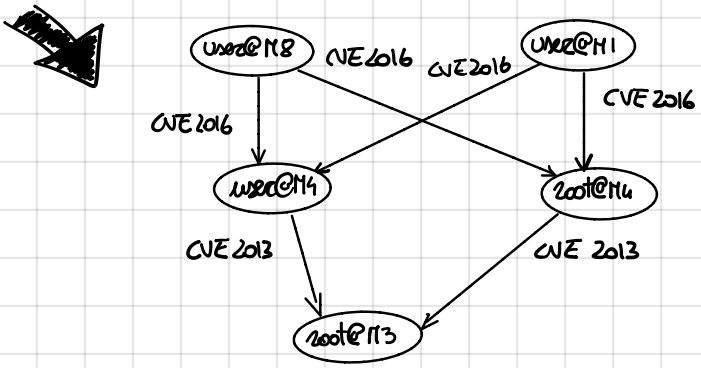
From context is legit to think that whole LAN3 is full of idiots that can be exploited as entrypoints



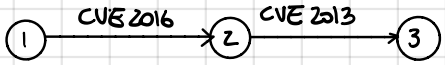


C can be removed since we reach it

Only M4 has vulnerabilities.
From vulnerabilities specifications (provided at exam) we can notice that CVE 2015 (a) can be applied only with local access while CVE 2016 can be applied and grants privileges (not specified if user/root) CVE 2013 gives root privileges.



④ Compute Likelihood



$MTAO = \sum_k \frac{1}{\lambda_k}$ with λ_k = value given for each vulnerability, in our case $\lambda_{2016} = 0.43$, $\lambda_{2013} = 0.4$

$\Rightarrow MTAO = 1/0.43 + 1/0.4 = 4.83$

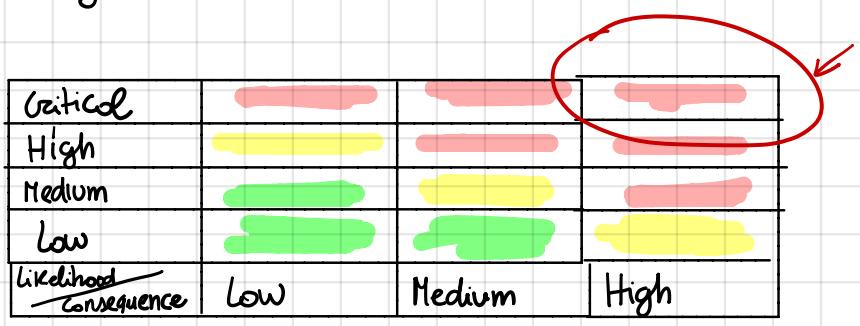
lowest possible value for MTAO = simplest attack path, composed of one attack step exploiting the easiest possible CVSS

$$Likelihood = -20 \log_{10}\left(\frac{MTAO - MTAO_{min}}{MTAO}\right) = -20 \log_{10}\left(\frac{4.83 - 1}{4.83}\right) = 2.04$$

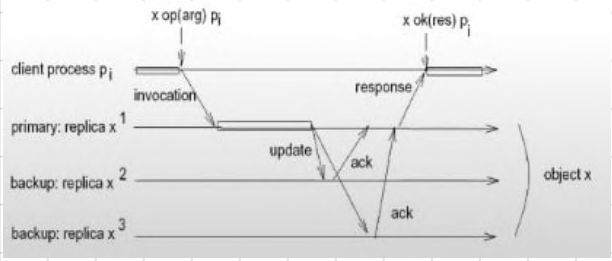
↳ Normalized = $\frac{4.83 - 1}{4.83} = 0.79$

Critical!

From CVE 2013 spec we see that consequence on AVAILABILITY (asked from the text) is Complete
→ High!



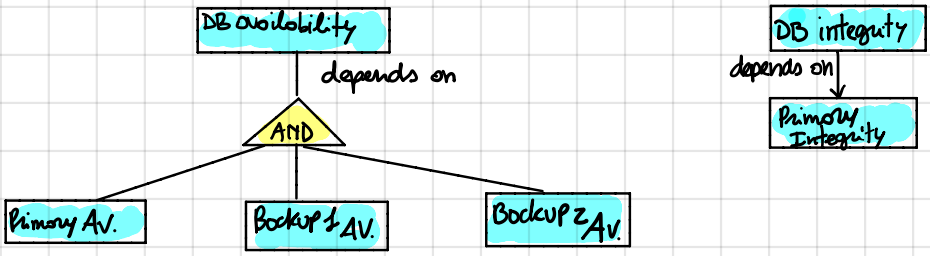
Ex Lets consider the XYZ company owning a private cloud where all relevant data are stored in a replicated database X. The database is composed of 3 replicas r_1, r_2 and r_3 located on 3 different machines m_1, m_2 and m_3, two inside XYZ main building (m_1, m_2) and one located in a secondary building 100 m far away (m_3).
The replication schema adopted is the primary-backup as described in the following figure where m_1 acts as primary and m_2 and m_3 are backups.



Considering that:
- m_3 fully dedicated to manage replica of DB
- m_1 and m_2 also host other application
- m_1 is exposed to internet
- m_1, m_2 can be accessed by XYZ's employs with user privileges and by admin with root privileges

- m_1 and m_2 have vulnerabilities CVE 2013 and CVE 2016 (detailed at exam)

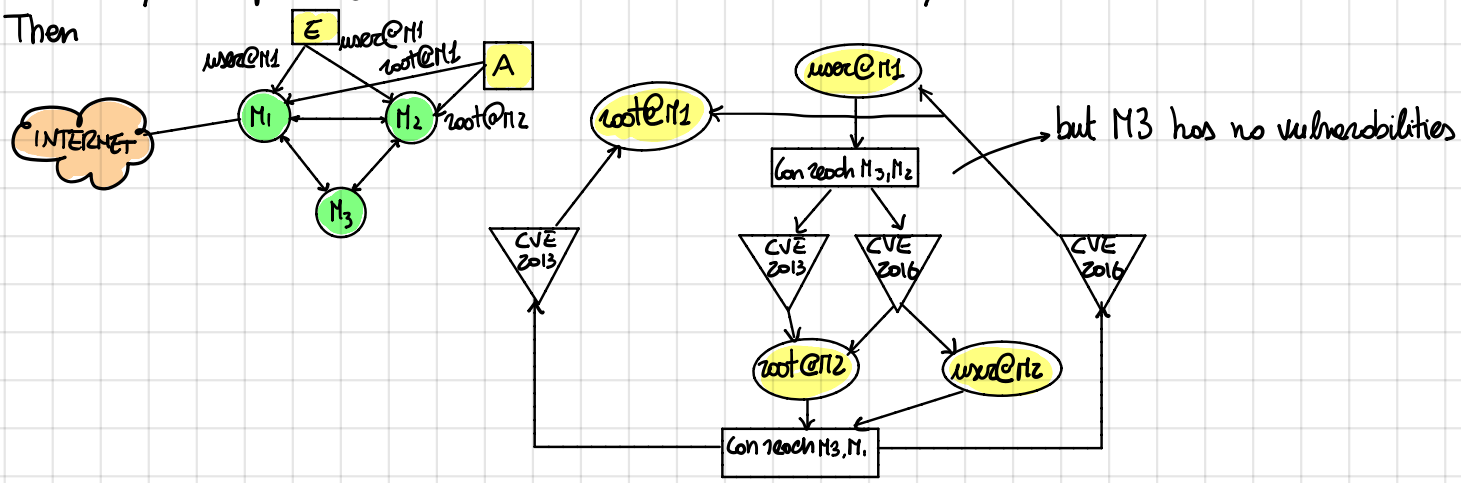
Evaluate following risks:
- loss of availability of database (whole DB)
- loss of integrity of data stored in replicated DB



So:
- for risk #1 → assess risk of loss of availability on all machines
- for risk #2 → assess risk of loss of integrity on primary backup.

As always compute Context Establishment and Reachability Matrix.

Then



- CVE 2013 lead to root privileges on M_1 → Integrity compromised.
- No way to compromise M3 → likelihood of compromise Availability extremely low.

Post questions with MY possible answer.

1) Discuss the role of Best Practices and Standards in the design and realization of an Information Security Governance System.
An Information Security Governance System aims to specify the behaviour inside an organisation about Information Security and to verify that is compliant to its guidelines.
The model is based on 2 core principles:
- cover 3 well known level of management – Strategic, Tactical and Operational – that overlap most of the time
- 3 distinct action – Direct, Execute, Control – over these 3 levels.

Direct: WHAT to do at Strategic level, the directives of organisation about Information Security
HOW to do it at Tactical level, what are the security standards to follow inside organisation
WHO has to do it at Operational level, assign duties following formal guidelines coming from standards.

Control: check compliance "bottom-up" analyzing data extracted from a wide range of sources (electonic and not) and verify the correct application of standards (at tactical level) and of directives (at Strategic level)
Best Practices are the best known methods/techniques/proven processes used to achieve an end goal – a standard.
Standards are usually established by an authority or general consent as a basis of comparison. Typically used to achieve a specific look/quality/grade about Information Security.

2) Describe the structure of the NIST CSF and explain how it can be used to plan investment related to cyber security.
The National Institute of Standards and Technology Cyber Security Framework is a set of guidelines that aims to improve CS risk management in critical infrastructure (typically) but can be used in any organisation where Information Security has an important role.
Supports CS assessment, planning and monitoring activities.
CORE: set of activities needed to achieve specific goals in terms of CS
- Identify = what need protection inside the organisation (assets)
- Protect = implement safeguard mechanisms to ensure protection
- Detect = alert in case of CS incidents
- Respond = countermeasures to CS incidents
- Recover = processes to restore organisation state

IMPLEMENTATION TIER: describe criteria to evaluate the state of an organisation in terms of security, from Partial (Low) to Adaptive (High).
PROFILES: describe prototypes of organisation according to its functions and objectives from a CS point of view. Used to compare "current" state to "target" one and analyse needed improvements
Identifying assets to protect, their risks and countermeasures and current state of organisation help the management to decide future investments on a cost-benefits basis.

③ With reference to threat modelling, describe the asset-centric, the attack-centric and the software centric approaches highlighting for each the advantages and disadvantages.
ASSET CENTRIC: focus on the assets we want to protect. Involves analysis of information loss and business impact. It can be extended identifying the motivations and goals of attacker and can be used as attack-centered brainstorm
ATTACK-CENTRIC: focus on the attacks from attacker's point of view. Aims to identify which threat can be succesfully executed also profiling attacker's characteristic, skill set and motivations. Most likely to bring up possibilities that are human-centered.
SOFTWARE-CENTRIC: focus on the software that could be attacked and to its closer entities such as network and hosts. Ideally should be done during software design, before deployment but in practice threat models of this kind are often created for existing systems and their maintenance.

④ Discuss taxonomy of Intrusion Detection System putting particular emphasis on the different techniques that can be used to perform the analysis.
IDS is composed by 5 elements:
- INFORMATION SOURCE = how and from where the IDS takes info to analyse. From a single host (HOST BASED), on a specified portion of network (NETWORK BASED), over wireless connections, from logs or using sensors.
- ANALYSIS STRATEGY = how the analysis is performed. Divided in Misuse and Anomaly detection
  - MISUSE DETECTION: IDS knowledge is based on attack's behaviour and it try to match them during the analysis. Easy to implement with high accuracy for known attacks but can't identify new threats and must be kept updated with attack's signatures
  - ANOMALY DETECTION: the complementary of misuse detection, IDS knowledge is based on a working system model, everything that differ from it is a potential attack.
- TIME ASPECTS: online if checks data in realtime or offline if execute post-analysis
- ARCHITECTURE: centralized or distributed according to the fact that analysis is performed on a single machine or multiple ones (scalable but complex)
- RESPONSE: passive if it only alarms to human admin or active if perform some actions (typically only increases sensitivity of sensors to gather more details)

⑤ Discuss taxonomy of IDS and the main challenge that can be faced when detecting port scans.
Answer ④ +
Port scanning is not always a malicious event since also system admin use it to check vulnerabilities of available ports, so the main challenge is to detect when the scan is performed by an attacker. Scan footprint is the set of port the attacker wants to characterize and he will use different techniques to avoid detection:
- change scan order = don't scan sequentially to add noise
- slow down = slower scan are harder to detect since IDS works on time windows
- random timing = add random wait between each scan
- change connection fields = to avoid identification
- distribute scanning = similar to DDOS but for scanning

Solutions depends on how we want to manage the problem: monitor frequency of scan, create profile for each IP, keep track of anomalous packets for longer time

⑥ Describe NIST CSF, the Italian CSF and discuss the main differences

Answer ② +

National CSF is based on NIST CSF with some addition: priority and maturity levels. Each subcategory has a priority level that aim to reach target profile of the company as fast as possible and a maturity level that determine current status respect to it. Key point of National CSF is Contestualization: using priority and maturity levels any organisation can model the framework to its context and target profile.

From the union of National CSF and Data protection comes the GDPR.

⑦ Describe main steps of a risk management process and discuss peculiarities of handling cyber risks

Main steps of risk management are: context establishment, risk identification, risk analysis, risk evaluation and risk treatment.

- Context establishment is about identifying the attack surface i.e. potential attack points all over the system.
- Risk identification is when we identify possible threats. Actions order depends on the fact we are looking for malicious or non malicious threat.

In first case we start from source identification i.e who and why would attack us (attacker profile). For each of them we identify possible threat that may happen (threat identification) and which vulnerability they may exploit. Last step is identifying possible consequences (incident identification)

If we are looking for non malicious threat we have to follow previous step backwards: from assets incidents find out possible vulnerabilities which have generate them using standards and possible threat that have exploited them. Last, understand who caused the incident and how.

- Risk Analysis: quantify level of incidents in term of likelihood and impact keeping in mind that likelihood of malicious threats is hard to compute
- Risk Evaluation: check risk analysis results, check if some risks could be evaluated as single and group risks with common elements and solutions
- Risk Treatment is when we (try) to solve the risks reducing likelihood, accepting them or avoiding the activities that were the causes. Treatments may change from malicious and non malicious risks.

⑧ Describe what is a SOC, its main responsabilities and design principles.

The Security Operation Centre is a centralized security organization (internal or not) that assists the company with security functions. Its goal is to improve security level by detecting and responding to threats before it is too late. Responsabilities of soc go from Log Management, monitoring, alerting to more evolved features like threat intelligence (also overlapping CERT).

SOC should be implemented in presence of sensitive data/processes or when current information security policies are not enough anymore.

SOC principles are:

PEOPLE = who will partecipate in the response team, can be internal or external (or hybrid). Staff must be well trained to ded with constantly changing and challenging Jobs of cybersecurity. It is divided in tiers according to their role inside soc

eg Tier 1 → endpoint monitoring

Tier 3 → in-depth knowledge of network, more complex duties

PROCESSES = the repeatable workflow of the SOC, from triage to investigation actions. Standardized

to define responsabilities for each Tier of the staff.

TECHNOLOGY - on enterprisewide data collection, aggregation, detection, analytic and management solution, core of a successful SOC. Data gathered from monitoring network and endpoints can be used as investigative tool to prevent incidents or as a management tool to respond to them.

(9) Provide the definition of attack graph and then describe and discuss the main phases involved in the attack graph generation process, highlighting their main issues.

Attack graph is the graphical representation of the ponible ways an attacker could violate the target network exploiting a series of vulnerabilities all over it.

A typical attack graph uses node to represent privileges gained by attacker on specific hosts and edges for vulnerabilities.

Main phases of attack graph creation are:

- Reachability Analysis = core process, utilizes network data to compute reachability matrix. The matrix is used to evaluate possible targets for the attacker from each host he could be on

The more network information (topology, IDS conf, trust relations etc) we have the more accurate the attack graph will be.

- Attack Template Determination = attack graph contains privileges gained and ponible vulnerabilities that could be exploited with. This relationships are determined using an attack template which specifies the conditions required to perform a succesful attack and the ones gained after it. Attack templates together form the attack model.

Increasing the detail of the templates increases also the precision of resulting chains but requires lot of more time and space during process.

- Attack Graph Structure Determination = space complexity may reach exponential order for full stack attack graph so is important to decide the structure of the graph depending on its complexity also introducing elements to reduce space complexity.
- Attack Graph Core Building Mechanism = initial attacker's privileges are given as input for attack path determination. From them, using some sort of search algorithm we traverse the graph until we reach target privileges, the one that can exploit vulnerabilities.

Main issue of Attack Graph is scalability, possible countermeasures are:

- Monotonicity assumption: an attack can't negate any privileges obtained by attacker so far
- Pruning attack paths based on depth and/or likelihood of success of traversed attack path
- Compute just the shortest attack path (or fixed length)
- Cycle-free attack graph