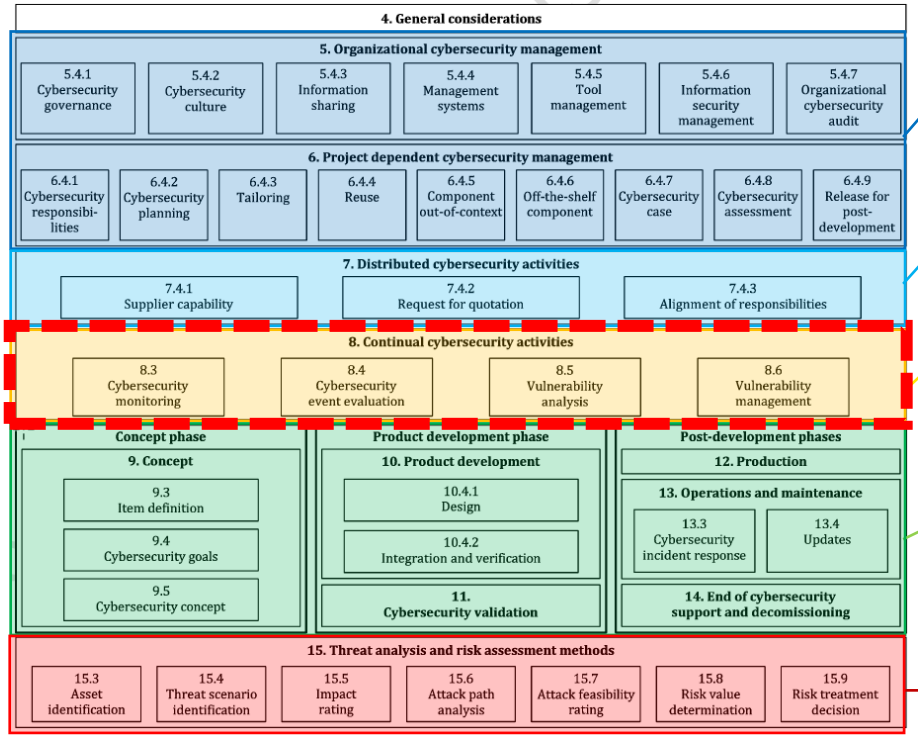
DEKRA

DEKRA DIGITAL

ISO/SAE 21434 – Continuous monitoring & Incident response

Clause 8: Continual Cybersecurity Activities

Structure of ISO 21434



Overall & project specific management processes

(similar to ISO 26262) :

- Management Systems
- Policies
- Preparation for assessment

Distributed CS activities

- Define interfaces between customer, supplier, third parties..

Continual CS Activities :

- Requirements for continuous monitoring of CS relevant information
- Framework for analysis and management of vulnerabilities

Concept, Development and Post-Development

- Add-on of CS relevant activities during concept and development :
  - Establishment of CS goals and requirements
  - TARA and vulnerability analysis during development
- Consideration of post-development requirements (during of after production, decommissioning …)
- Definition of post development processes (Production, Incident response, Update)

TARA : Threat Analysis and Risk Assessment

- Describes the steps to perform a robust risk analysis on the system
- Complex process to be performed multiple times and for multiple assets

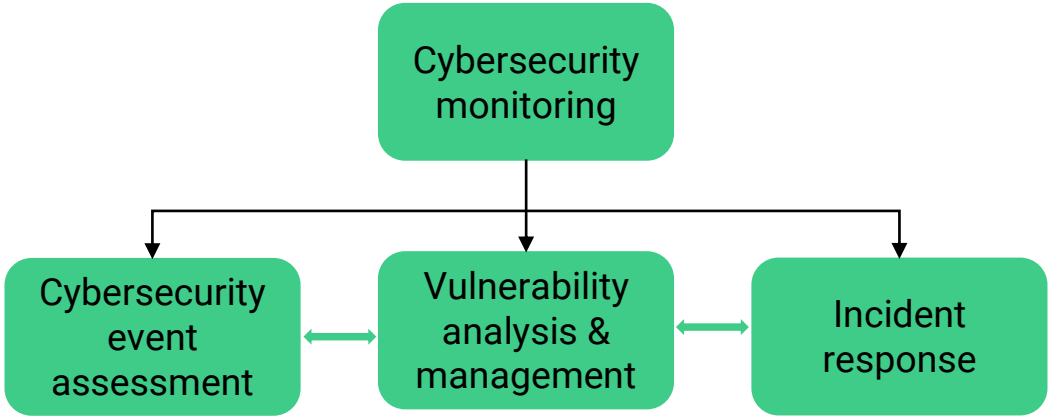
Continual Cybersecurity Activities

DEKRA DIGITAL

What are continual cybersecurity activities?

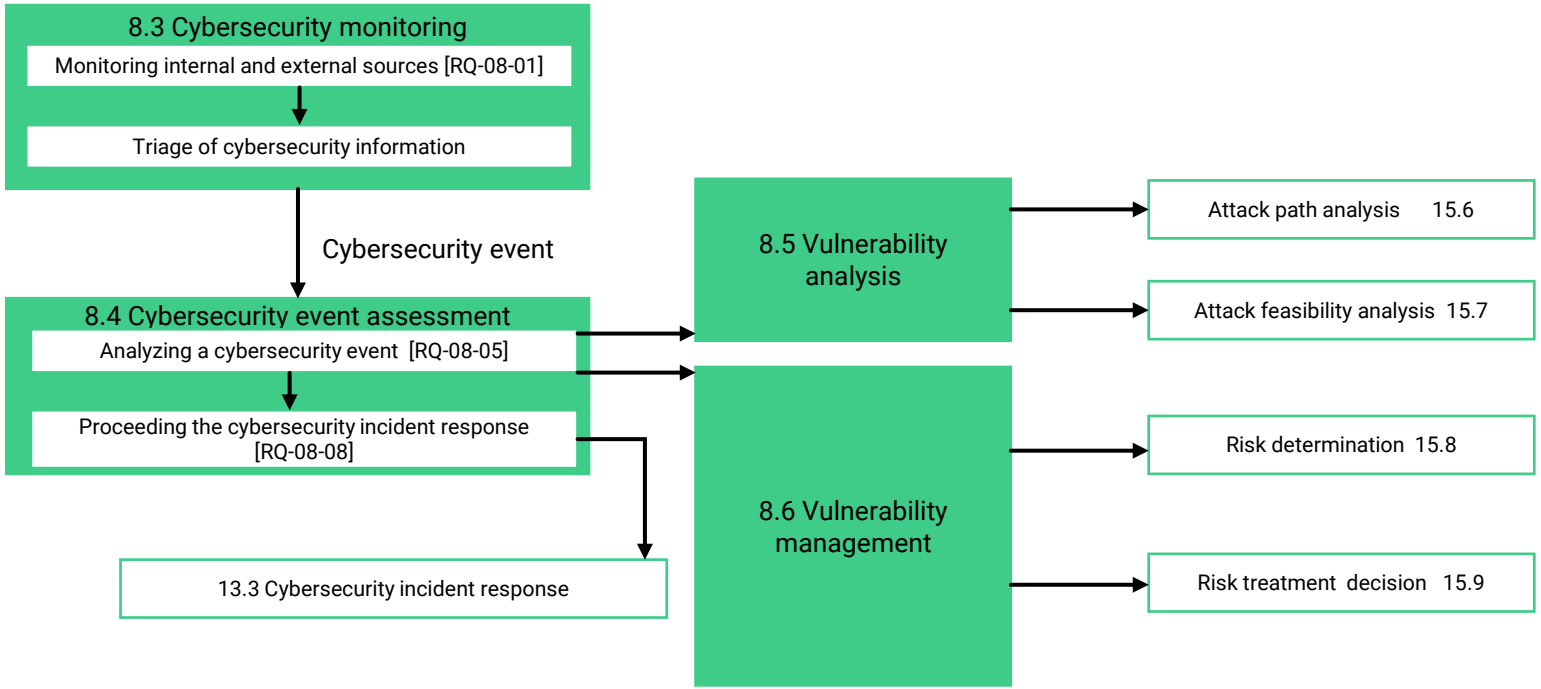
Continual cybersecurity activities are performed throughout the product life cycle and are not specific to one product or phase.

- The important activities include:
  - Collection of CS information for triage
  - Event evaluation for weakness determination
  - Vulnerability analysis to examine weakness
  - Vulnerability management to treat vulnerabilities
  - Incident response for potential threats



Continual Cybersecurity Activities

General interactions in continuous cybersecurity activities



Continual Cybersecurity Activities

DEKRA DIGITAL

How to establish good CS activities ?

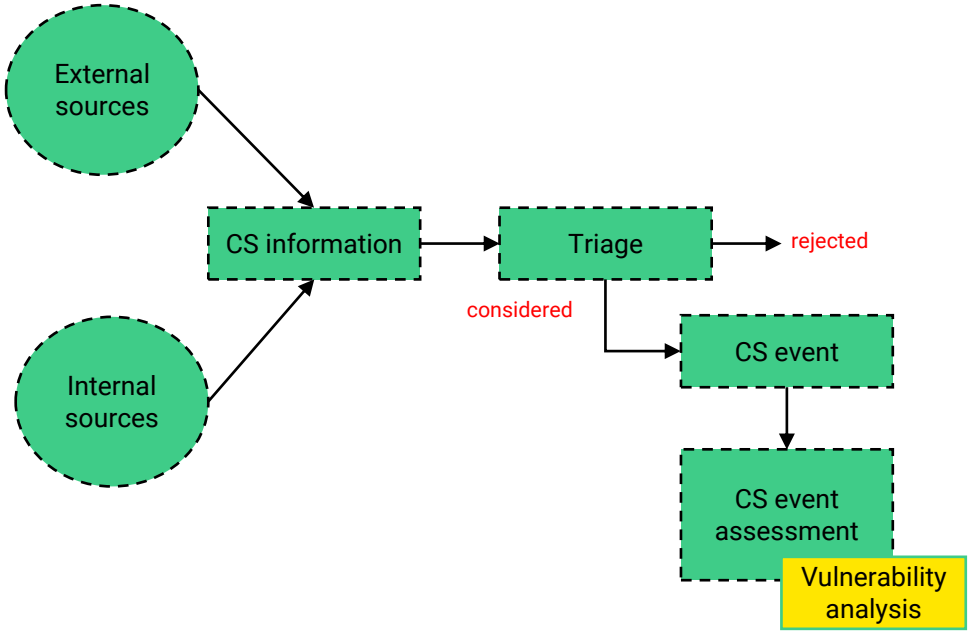
- Having a UNIQUE independent team in the company for Threat Intelligence
- Build communication channels with internal and external sources
- Actively participating in conferences, ISACs, bounty programs, etc... to promote information research and sharing
- Build competence in information gathering

Having well-established and working information gathering processes is essential to not miss potential vulnerabilities which may have an impact in the future.

An effort might be needed but this is **profitable in the long term**

Continual Cybersecurity Activities

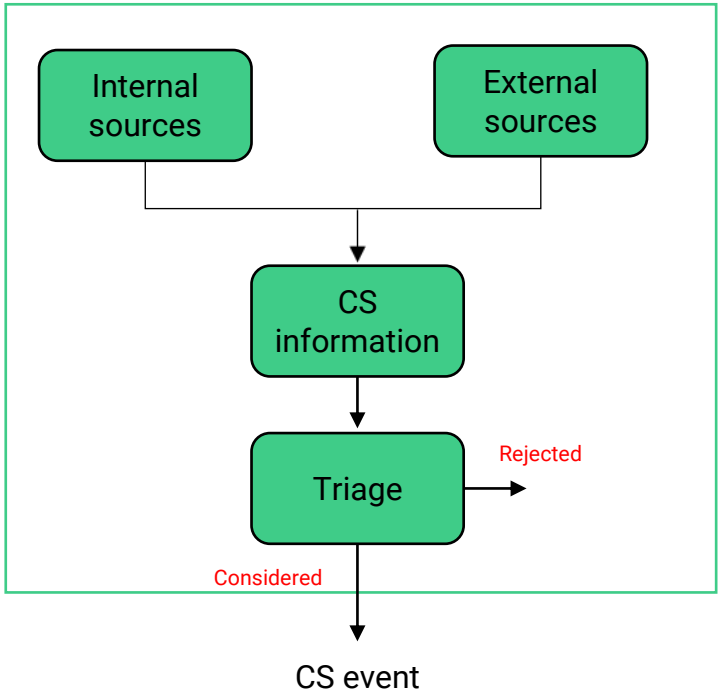
Continuous monitoring according to ISO/SAE 21434



Cybersecurity monitoring

Cybersecurity monitoring

- Cybersecurity monitoring is a process of collecting information on potential vulnerabilities, weaknesses, and CS threats
- Internal and external information sources should be documented, and triggers should be defined for monitoring
- CS monitoring assists in the treatment of existing threats and new threats
- Provides inputs to carry out vulnerability management and incident response activities

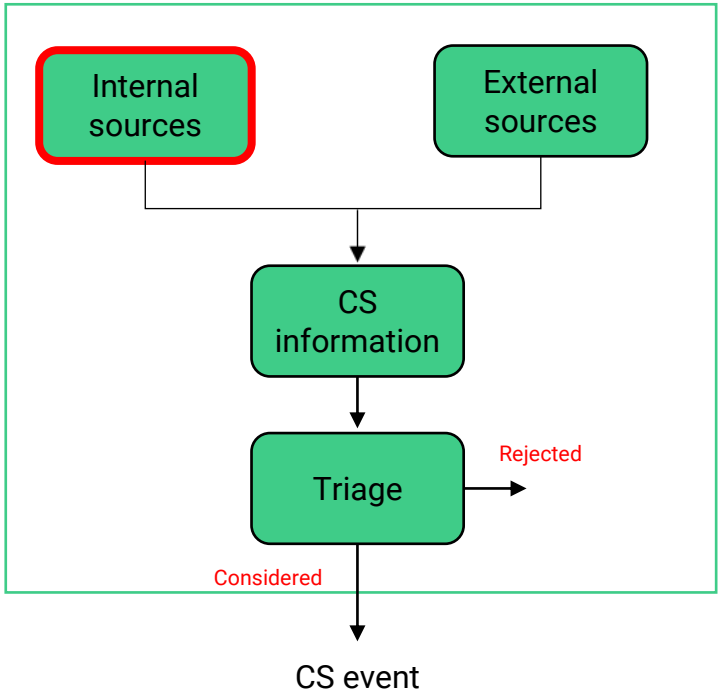


Cybersecurity monitoring

DEKRA DIGITAL

Internal sources

- Results of vulnerability analysis at the project level:
  - Testing
  - Vulnerability analysis during concept, design, development, verification, and validation
- Abnormal behavior detected on the vehicle (consumer usage information, intrusion detection, repair information ..)
- Inputs from designers, developers, integrators, testers
- Cybersecurity specifications and claims

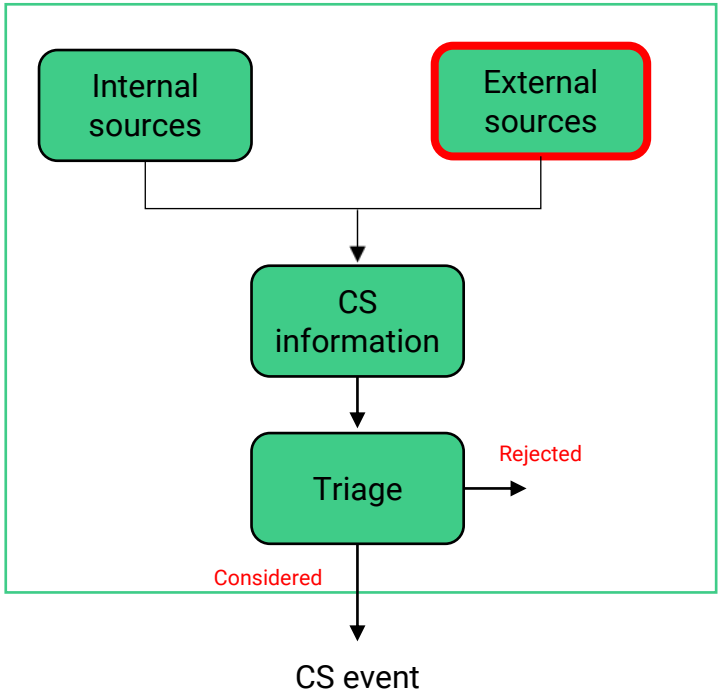


Cybersecurity monitoring

DEKRA DIGITAL

External sources

- Incident data from partners/customers
- ISACs (Information Sharing and Analysis Center)
- Research papers
- Cybersecurity conferences (DEF CON, BlackHat, etc..)
- Information from hacker websites, forums, chat channels...
- Open-source information
  - White hacker's blogs and repositories
  - Common Vulnerabilities and Exposures (CVEs)
  - Common Weakness Enumeration (CWEs)
- Government resources (CERTs : Computer emergency response team: BSI CERT, TWNCERT, ...)



Cybersecurity monitoring

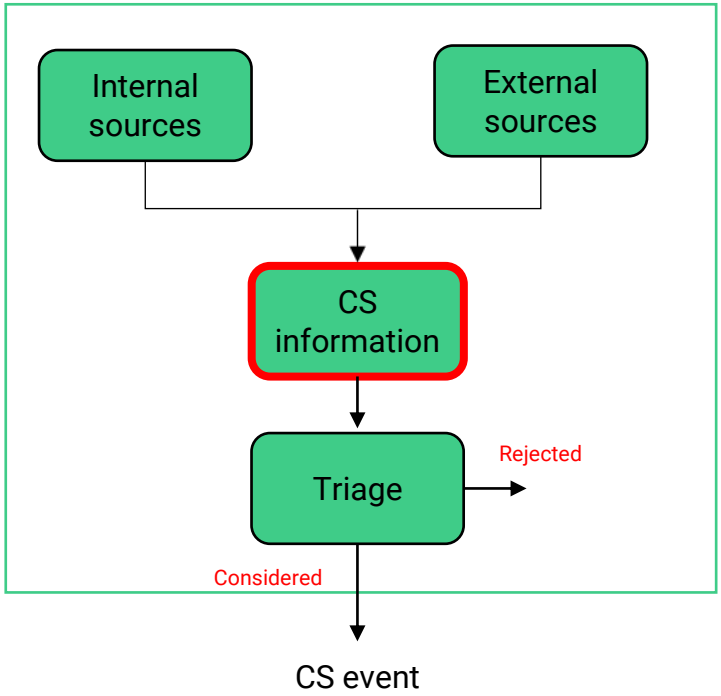
Cybersecurity information and triggers

Triggers are used to identify necessary cybersecurity information and give hints on which information to look for. (e.g., helps to automate monitoring process using software tools)

The cybersecurity information obtained may involve,

- Information about system weaknesses
- New attack vectors
- Exploits in similar components
- Reports from research firms
- Vulnerabilities from white hat hackers

- And triggers are used to perform triage activities
  - Example: source (name and type of the source)
  - Product name, function name, name of libraries
  - Name of vulnerabilities or threats



Cybersecurity monitoring

Triage

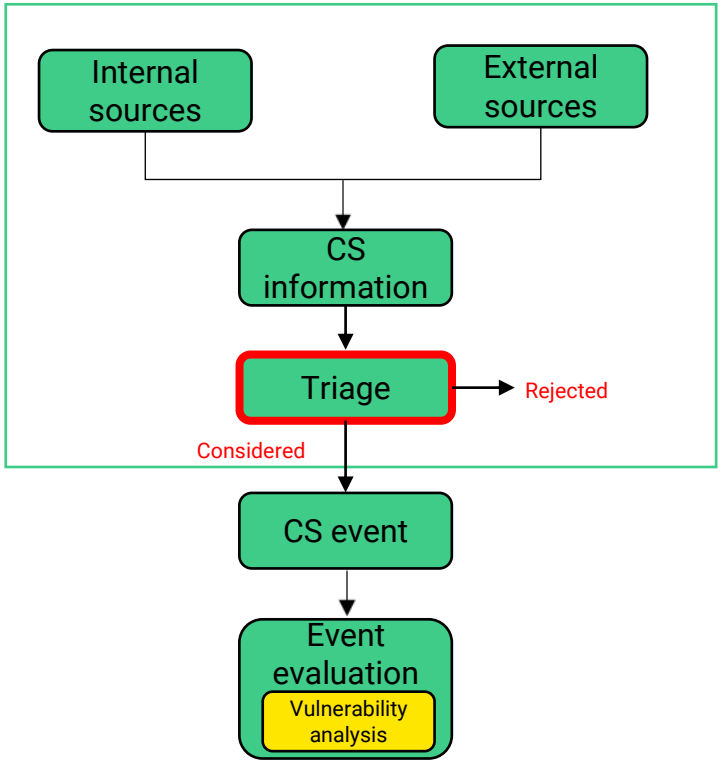
Triage is the process of filtering cybersecurity information to what is relevant and eliminating irrelevant information.

- Defines rules to evaluate CS information to determine whether it results in CS events or not
- Generally, triage is performed using software tools

Example of criteria for triage:

- Keywords, name of components and/or suppliers
- Potential new damage scenarios, threats...
- Type of information (research, attack, etc..)

- As a result, a trigger must be defined and maintained
  - For example, a score applied to a checklist



Triage

DEKRA DIGITAL

Example

OEM A is producing a car model B who is integrating ECU C in charge of managing 5G communication in the vehicle.

Car model B, and ECU C can be considered as a automatic trigger to classify CS information as relevant.

Specific car configurations shall also be detected in the CS information if applicable.

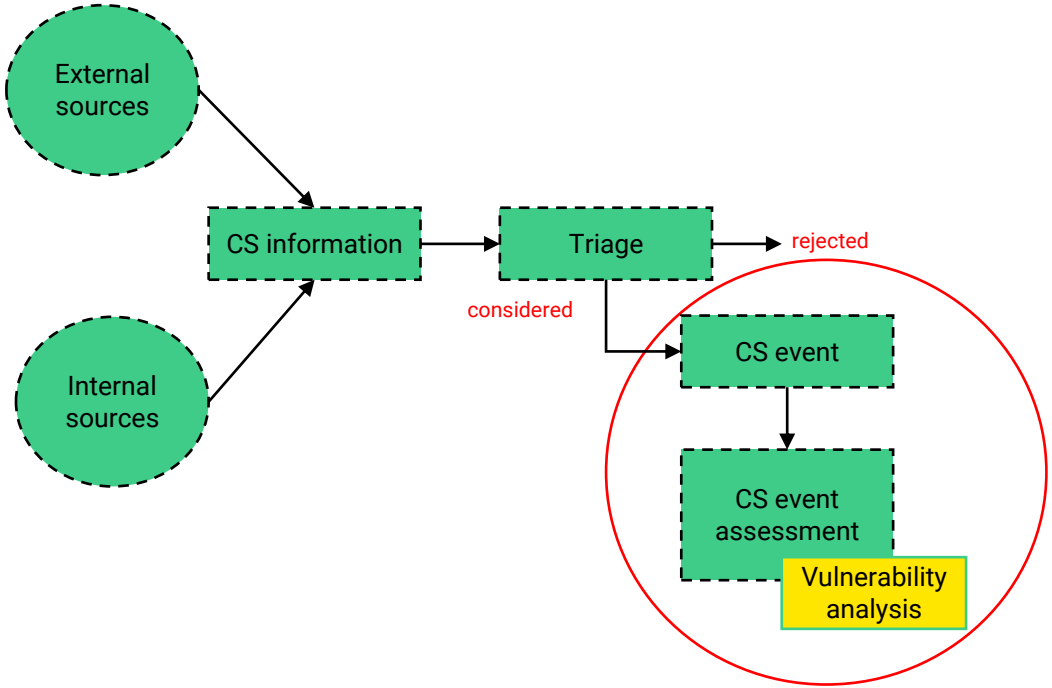
Additionally, keywords like “5G MitM attack”, could be a set of keywords to track.

Cybersecurity Event Evaluation

DEKRA DIGITAL

Objective

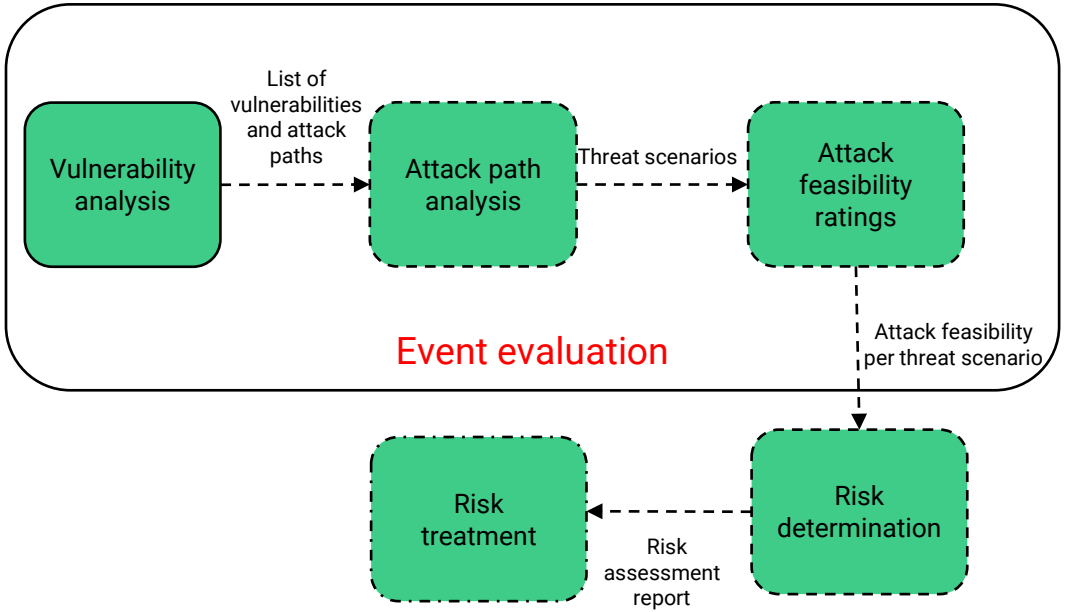
- Analyse the potential risks involved by this CS information (new vulnerabilities, existing rationale not valid anymore, etc...). TARA-like
- Each accepted CS information should be tracked
- In post-development phase, a CS information can become a CS incident, and therefore the CS Incident Response team processes will be applied



Cybersecurity Event Evaluation

Cybersecurity event evaluation

- The goal of the CS event evaluation is to determine the risk associated with the event
- The event is analyzed to identify the item or component's weaknesses
- Cybersecurity event evaluation could be performed in combination with triage activities
- The weaknesses should be analyzed to identify vulnerabilities

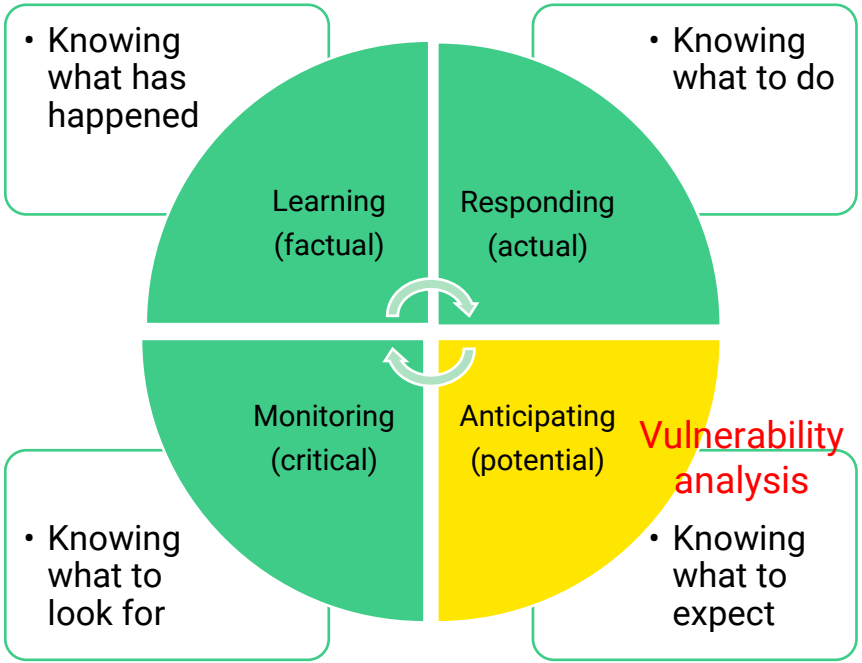


Cybersecurity Event Evaluation

DEKRA DIGITAL

Vulnerability analysis

- The illustration depicts the role of vulnerability analysis in contributing to the overall objective of enhancing item security
- Performed when a potential vulnerability or weakness is identified
- Weaknesses are analyzed to identify possible vulnerabilities
- Vulnerability analysis is performed in a bottom-up approach (attacker's view)
- An analysis following the TARA approach shall be performed
    - Identified vulnerabilities are mapped to threat scenarios or targeted assets
    - The feasibility to launch an attack by exploiting the vulnerability is then identified



Cybersecurity Event Evaluation

Vulnerability analysis

Inputs / Supporting Information

Item definition (item)

CS specification (Component)

Attack paths

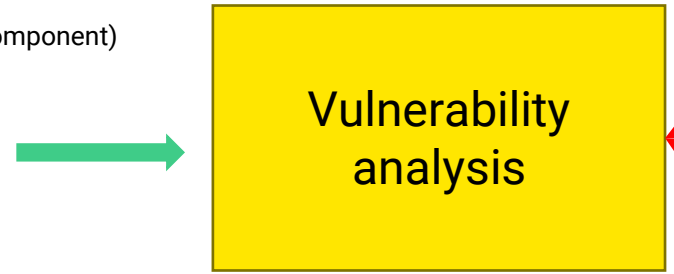
Past vulnerability

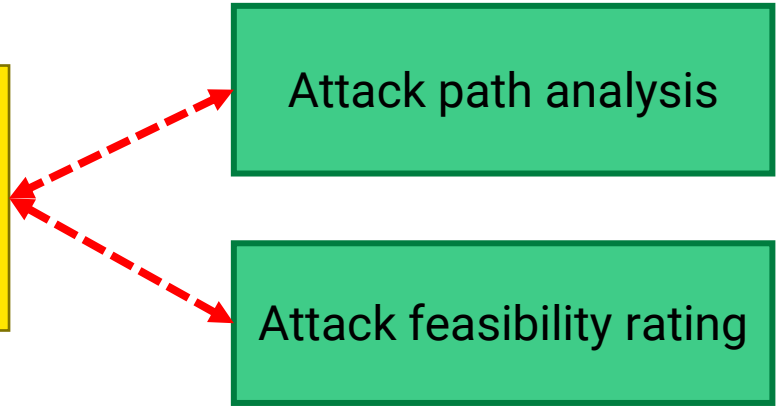
Verification reports

Past incident reports

Weaknesses from the development phase

Weaknesses from CS events



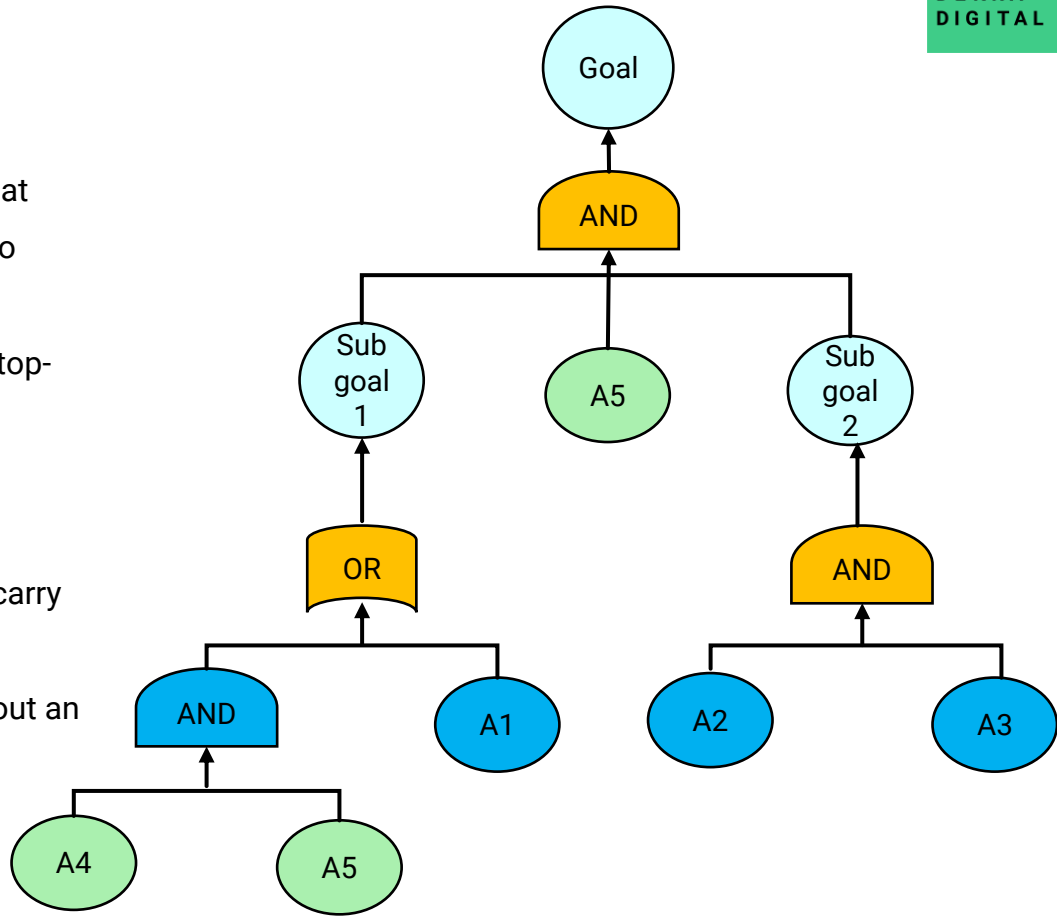


Cybersecurity Event Evaluation

DEKRA DIGITAL

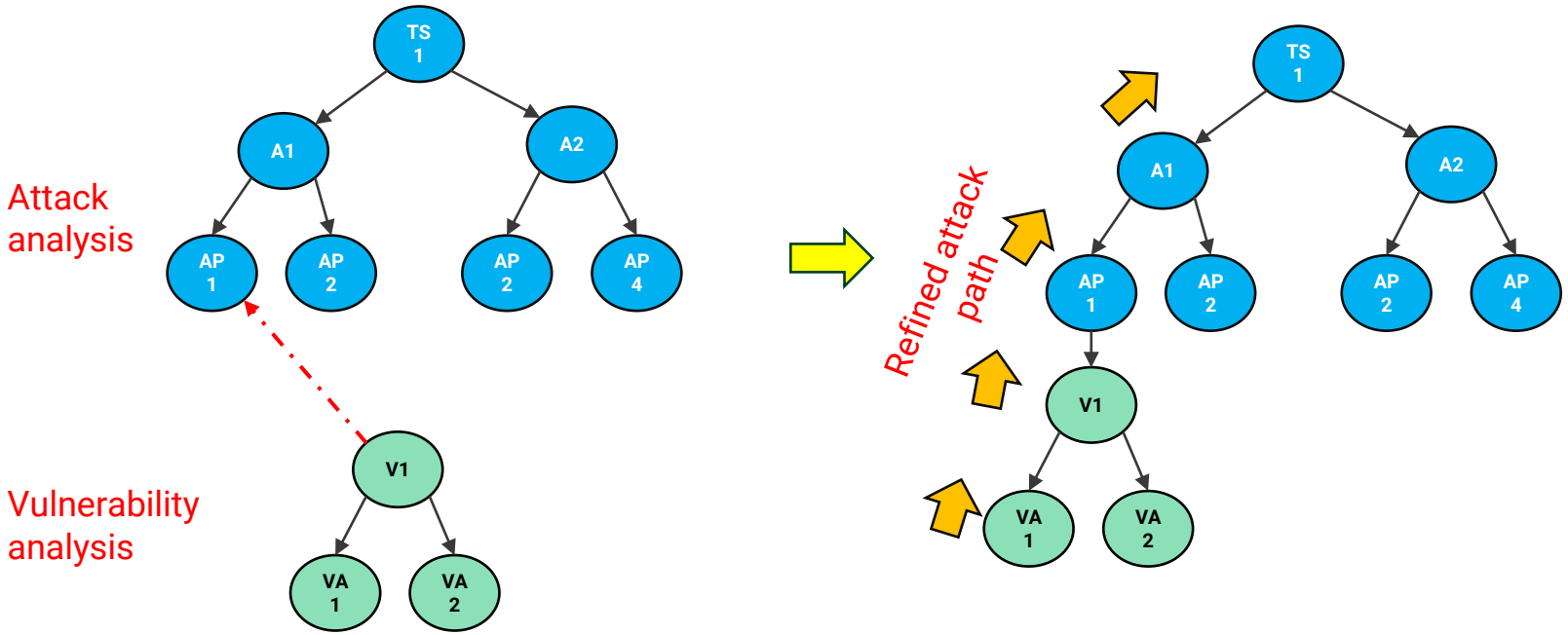
Attack analysis

- Attack trees are hierarchical conceptual diagrams that show how low-level activities interact and combine to reach the attacker's goal
- Attack analysis is performed in both bottom-up and top-down approach
- The attack trees consist of:
  - Root: Goal of an attacker (threat scenario)
  - Intermediate node: Basic actions required to carry out an attack
  - Leave nodes: Basic actions required to carry out an attack
- Non-leaf nodes are designated as AND or OR nodes



Cybersecurity Event Evaluation

DEKRA DIGITAL

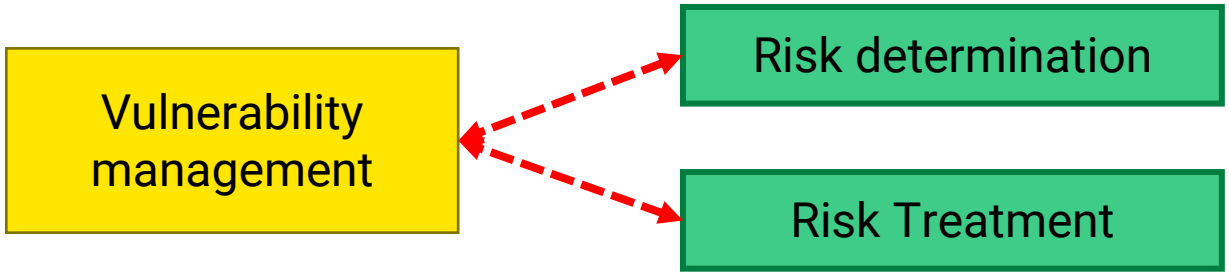


Relation between Attack analysis (TARA) and Vulnerability analysis

Vulnerability Management

Vulnerability Management

- Documenting the vulnerabilities
- Identifying risks due to the vulnerabilities
- Document the mitigation measures applied



Vulnerability Management

DEKRA DIGITAL

Vulnerability Management

- The information required to perform vulnerability management are
    - Cybersecurity assessment
    - Vulnerability analysis reports
- Risk due to the vulnerability should be determined according to TARA in clause 15 of ISO 21434
- Risk treatment decision according to clause 15 (avoidance, sharing, retention, and reduction)
- If any change is made in an item or component due to risk treatment, change management is applied
- If the change must be done while the car is already released, an incident response plan shall be created in accordance with clause 13. In this case, the plan can be applied independently of TARA.

CS Incident response

Context

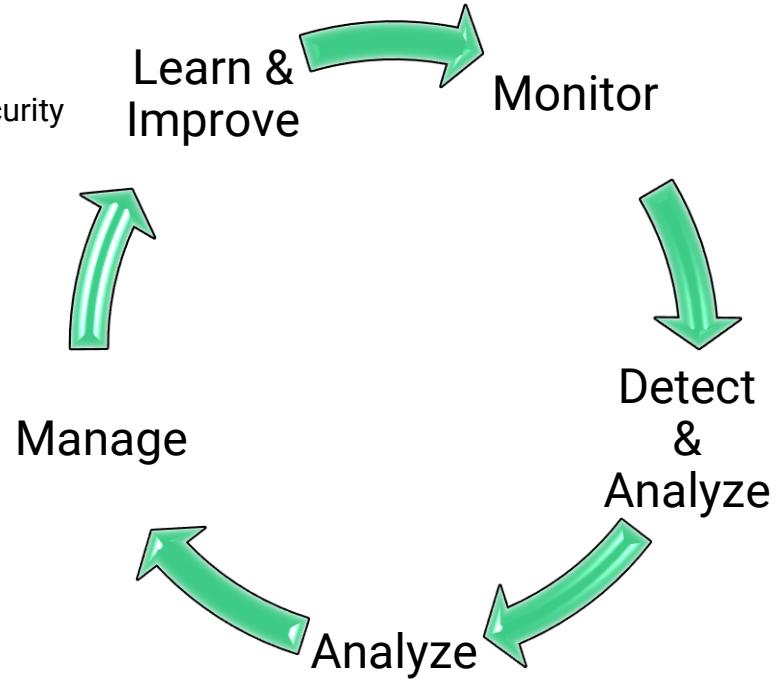
- Incidents are CS Information that may need a change of SW or HW through updates or maintenance.
- Only applicable in post-development phase as changes during development can follow the change management processes
- Triggered by continuous monitoring activities, the CS incident must define processes to follow closely
- The Incident response will follow the following steps
- This will be covered in detail in clause 13 of this training

Continual Cybersecurity Activities

DEKRA DIGITAL

Summary

- Monitor cybersecurity information to identify cybersecurity events
  - Collect CS related information
  - Triage CS information to refine CS events
- Evaluate cybersecurity events to identify weaknesses;
  - Identify vulnerabilities from weaknesses
  - Perform Vulnerability analysis
- Manage identified vulnerabilities
  - Trigger incident response if necessary



Continual cybersecurity activities

Summary of work products

- [WP-08-01] Sources for cybersecurity information
- [WP-08-02] Triggers
- [WP-08-03] Cybersecurity events
- [WP-08-04] Weaknesses from cybersecurity events
- [WP-08-05] Vulnerability analysis
- [WP-08-06] Evidence of managed vulnerabilities

DEKRA

DEKRA DIGITAL

Thank you for your attention