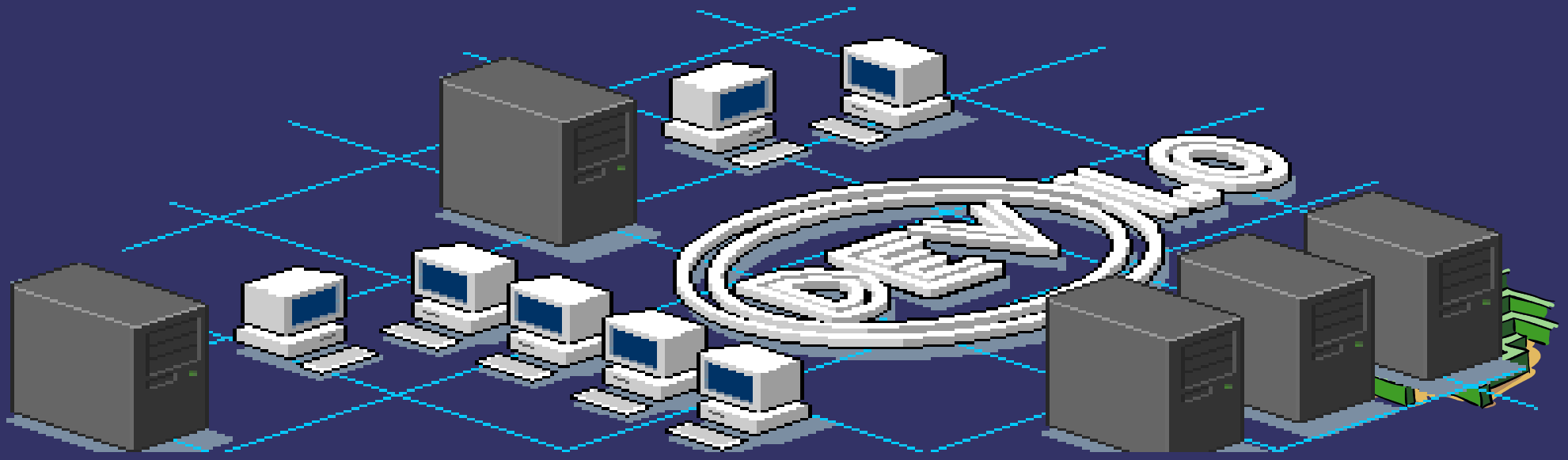
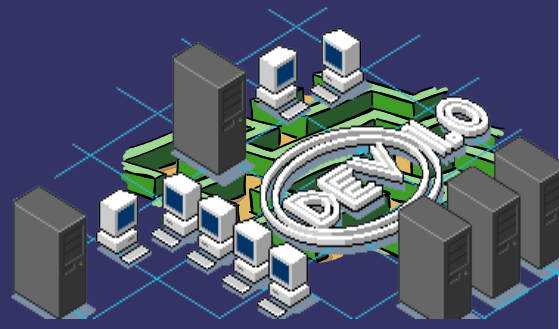
- ANALYSE DE RISQUE AVEC LA MÉTHODE MEHARI

Eric Papet
e.papet@dev1-0.com
Co-Fondateur SSII DEV1.0
Architecte Logiciel & Sécurité
Lead Auditor ISO 27001



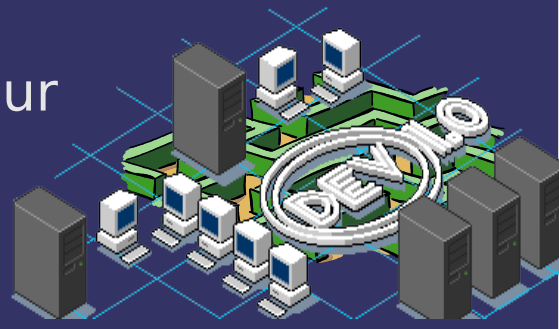
PLAN

- Introduction Générale
- Introduction MEHARI
- L'analyse des enjeux de la sécurité et la classification
- Le diagnostic de l'état des services de sécurité
- L'analyse de situation de risque
- Les automatismes MEHARI
- Modèle métier MEHARI



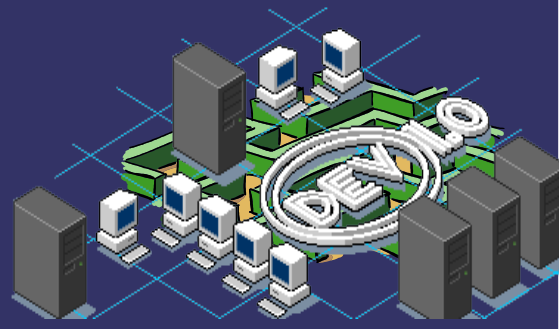
Introduction Générale

- Problématique (Sécurisation du SI)
  - L'information et les processus, systèmes, ressource humaines et réseaux qui en permettent le traitement, constituent des biens importants pour un organisme.
  - Business = confiance
    - Augmentation de l'utilisation des NTIC
    - Augmentation des Transfert EDI (B2B)
    - Augmentation des Transactions online
  - Augmentation de la cybercriminalité
    - https://www.clusif.asso.fr/fr/production/ouvrages/pdf/Pa
    - apparition réseau sociaux
    - Spam
    - Espionnage industriel (Renaud,Ferrai)
    - 80% des attaques proviennent de l'intérieur



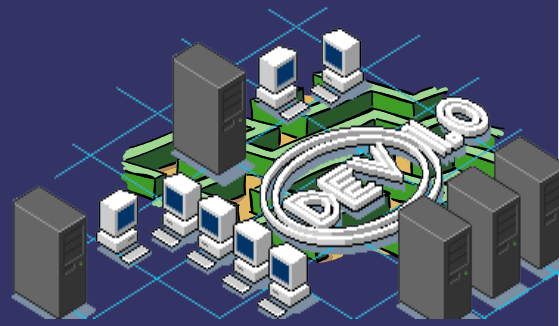
Introduction Générale

- Objectif
  - Améliorer la sécurisation des systèmes d'information, pour faire face à la concurrence, la mise en conformité avec la loi et l'image commerciale.
  - Justifier le budget alloué à la sécurisation du SI
  - Prouver la crédibilité du son SI à des donneurs d'ordre
  - Obtenir une certification ISO 27001 (mise d'un pace SMSI)



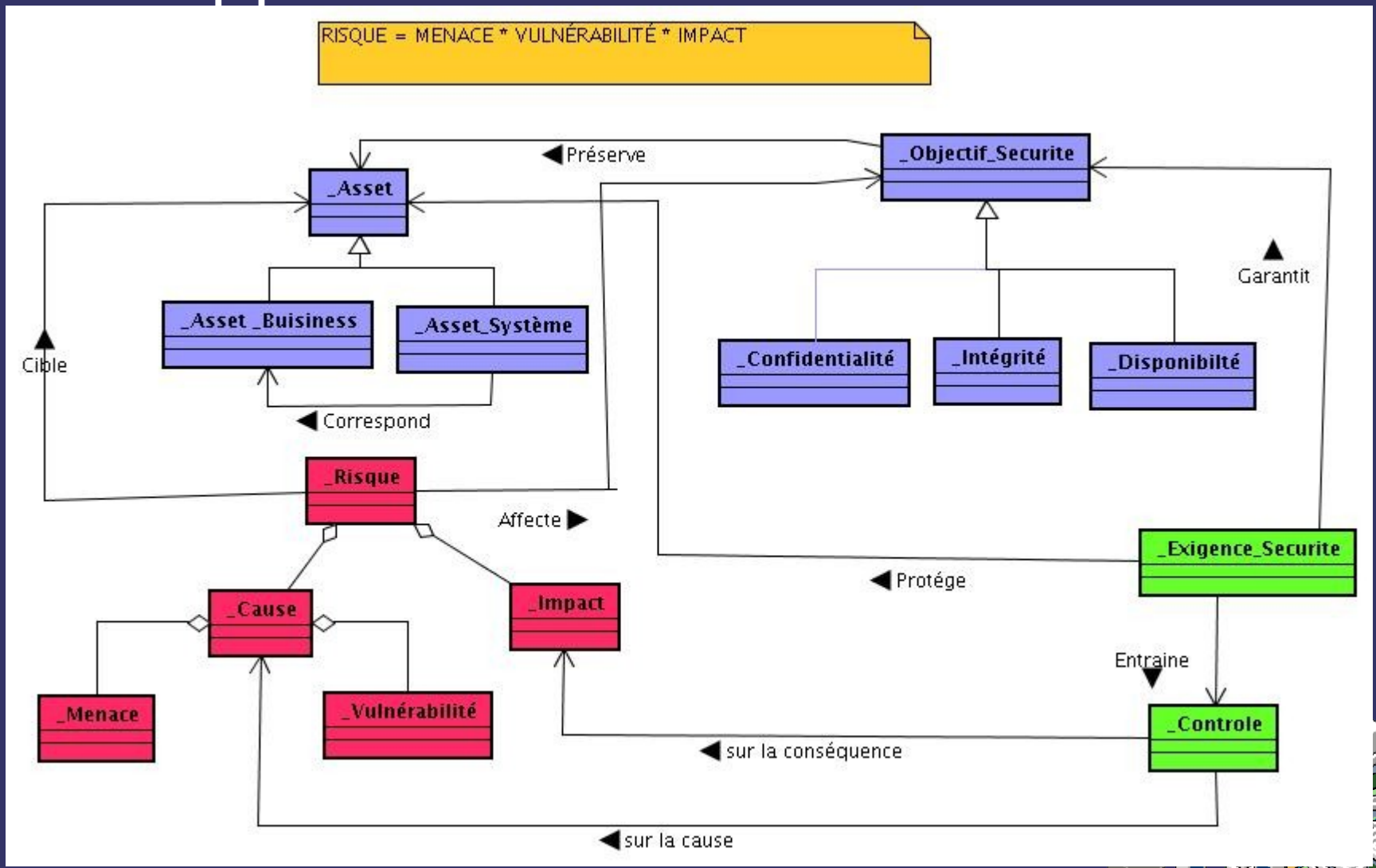
Introduction Générale

- Moyen
  - Approche basée sur la gestion des risques
  - Utilisation de méthode
    - MEHARI (Méthode Harmonisée d 'analyse de risquue), maintenu par le CLUSIF
    - EBIOS (expressions des besoins et identification des objectifs de sécurité), maintenu par la DCSSI
  - Base de connaissance de l'ISO
    - ISO 27002 (BS 17999 ; guide bonne pratique)
    - ISO 27001 (mise en place SMSI)
    - ISO 27005 (étude de risque)



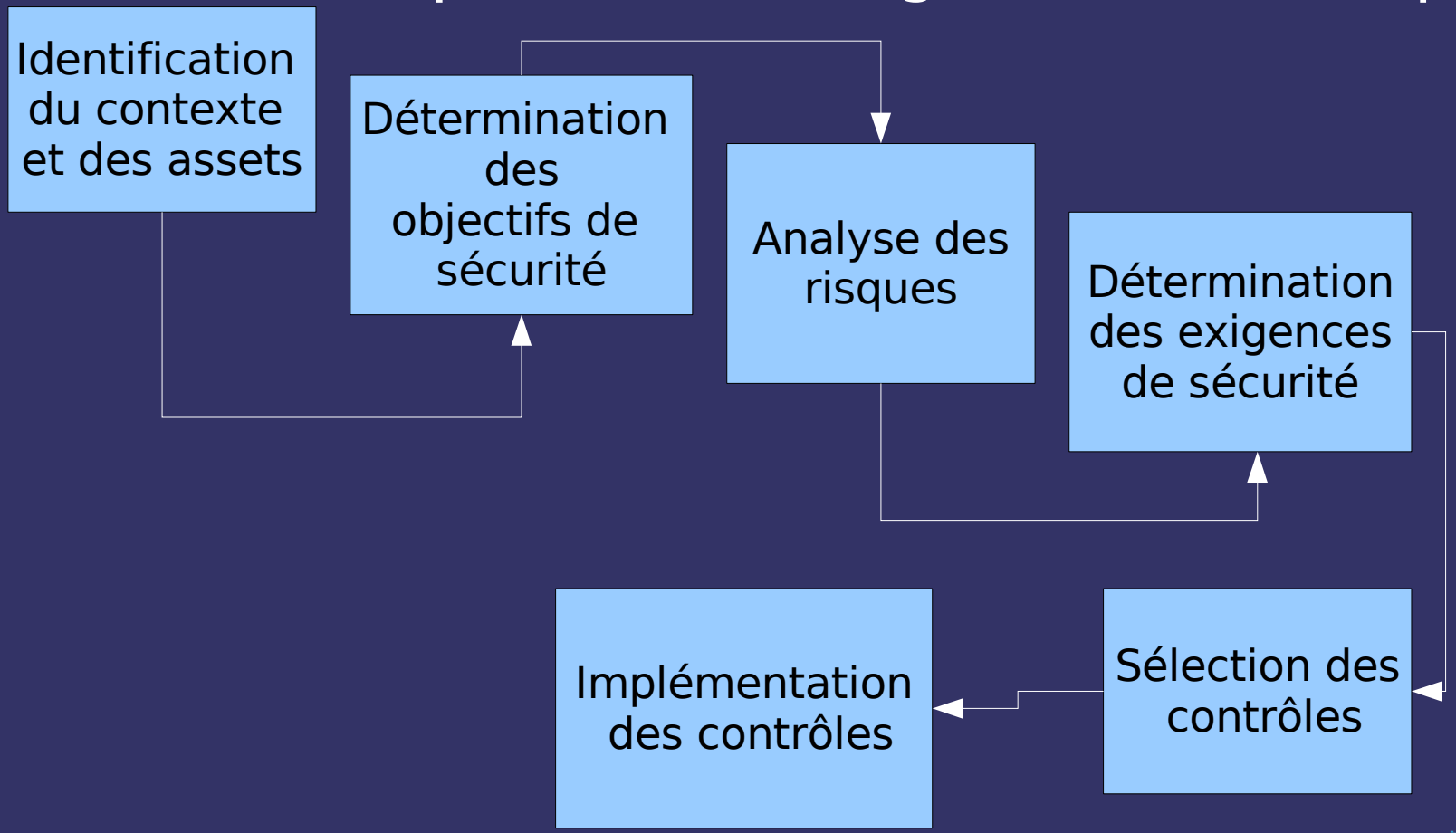
Introduction Générale

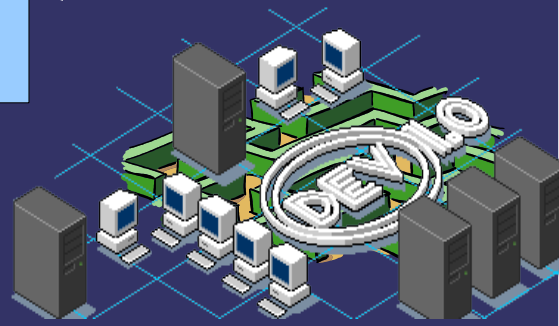
- Rappels & Definitions



Introduction Générale

- Rappels & Definitions
  - Le processus de gestion des risques



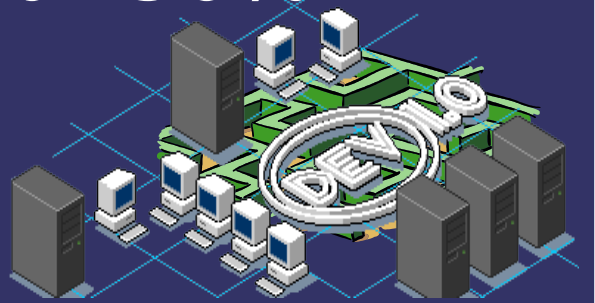


Introduction Générale

- Rappels & Definitions
  - Le processus de gestion des risques
    - Identification du contexte
      - (périmètre, organisation, ressources)
    - Détermination des objectifs de sécurité
      - (besoin en termes de confidentialité, intégrité, disponibilité)
    - Analyse de risque
      - (identification menace/vulnérabilité/impact,);
      - par audit
      - utilisation de bas de connaissances
    - Détermination des exigences
      - réduction des risques identifiés
    - Selection des contrôles
      - Définitions des choix technique (par-feu, gestion des flux, IDS, ect..)

Introduction MEHARI

- CLUSIF :
  - Club des utilisateurs de la sécurité de l'information Français
- Objectif :
  - agir pour la sécurité de l'information
- Association sans but lucratif
  - (création au début des années 80) > 600 membres (pour 50% fournisseurs et prestataires de produits et/ou services, pour 50% RSSI, DSI, managers)

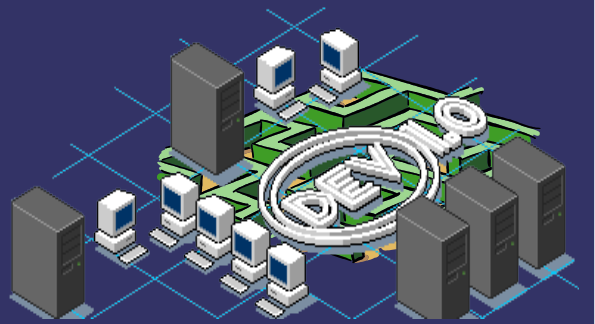


Introduction MEHARI

- Documentation MEHARI PRESENTATION
  - Présentation générales
  - Principes et mécanismes
  - Guide de l'analyses des enjeux et de la classification
  - Guide du diagnostic (audit)
  - Guide de l'analyse de risque
  - Base de connaissances (questionnaires d'audit)
  - Manuel de référence des services de sécurité
  - Manuel de référence des scénarios

Introduction MEHARI

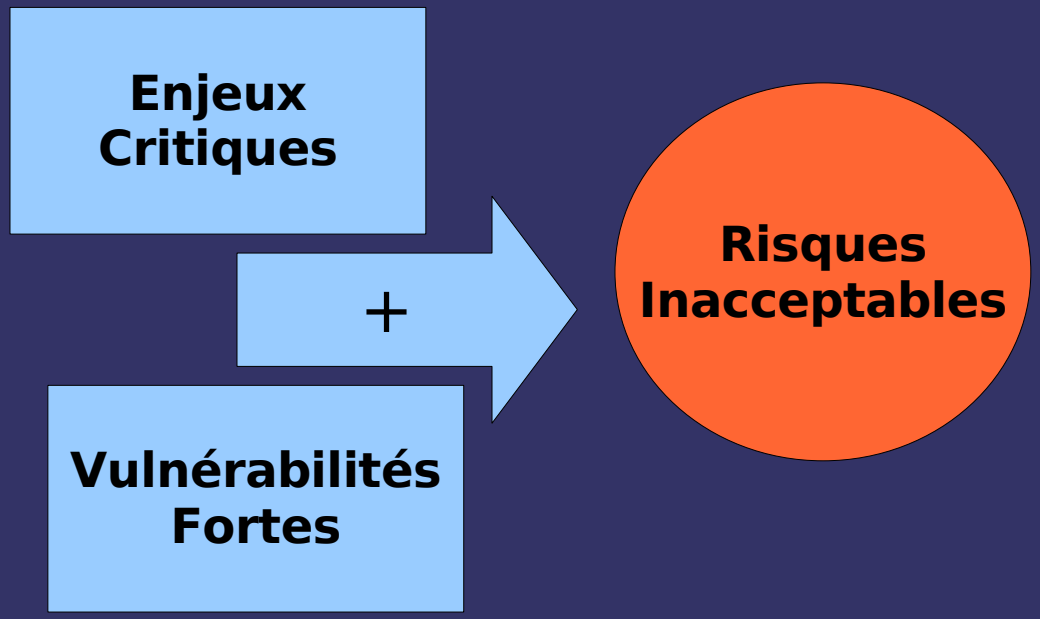
- Les 2 questions que se sont posées tous RSSI:
- Quelles est la finalité de la fonction? Quel est le but à atteindre ?
- Comment s'y prendre ? Y a-t-il des méthodes et des outils spécifiques du management de la sécurité

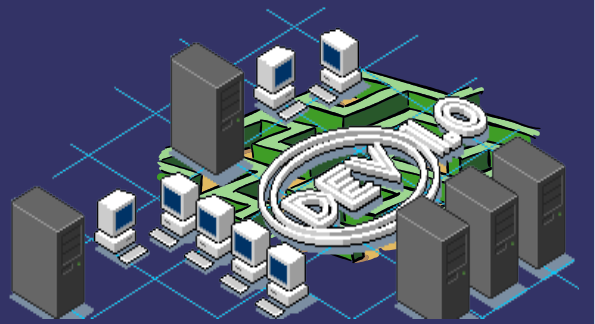


Introduction MEHARI

- Objectif:
  - Minimiser les risques encourus par l' entreprise du fait de son système d'information.
  - Faire que ces risques soient acceptables
  - Qu'est qu'un risque acceptable ?

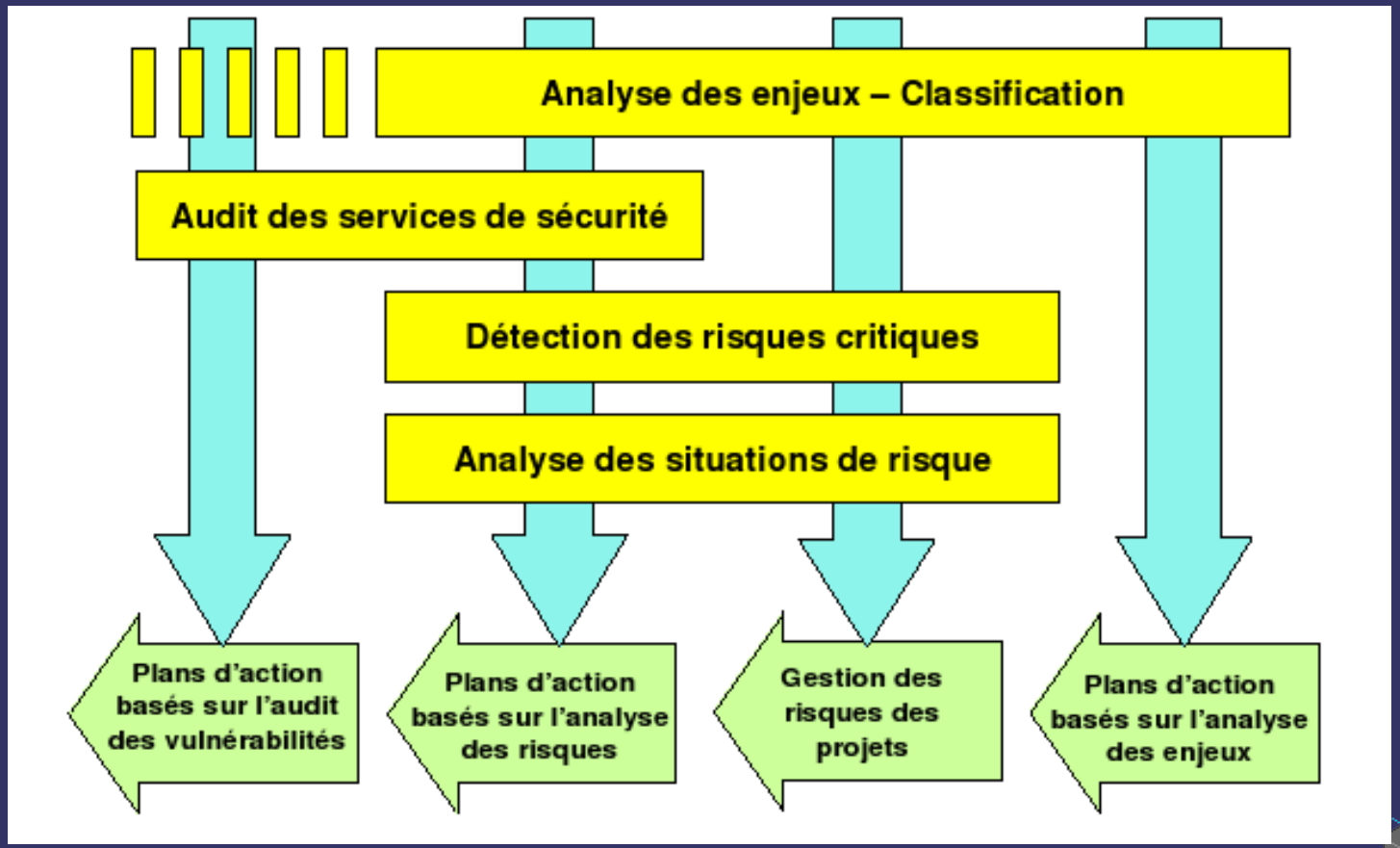
«La sécurité est l'absence de risques inacceptables »

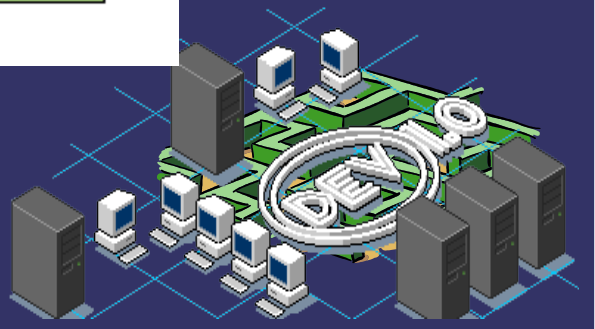




Introduction MEHARI

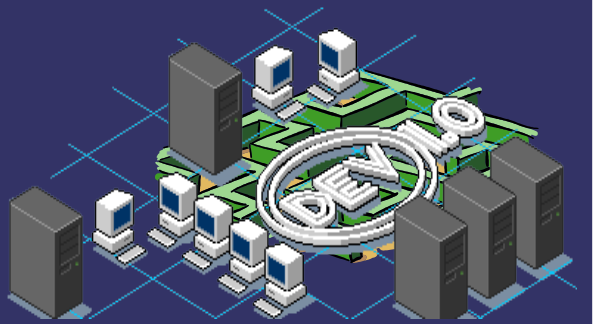
- Principe MEHARI: GRAVITE





Introduction MEHARI

- Les différentes Démarches:
  - Partir des enjeux majeurs, et analyser, pour chacun, comment il pourrait être attaqués, puis prendre les mesures en conséquence.
  - Partir des vulnérabilités et les réduire toutes jusqu'à ce que les risques deviennent acceptable.
  - Partir des situations de risque combinant les enjeux et les vulnérabilités et procéder à une analyse de risque.



Introduction MEHARI

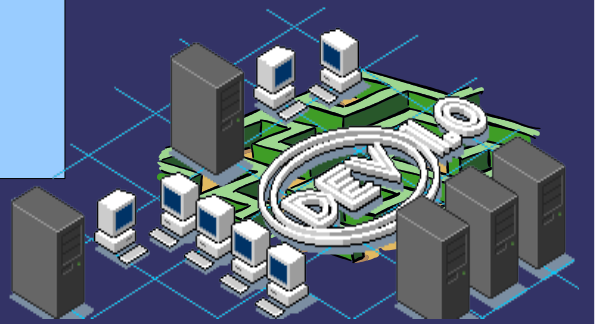
- Résumé de l'Utilisation MEHARI

Identifier vos principaux enjeux Métiers

Diagnostiquez vos vulnérabilités

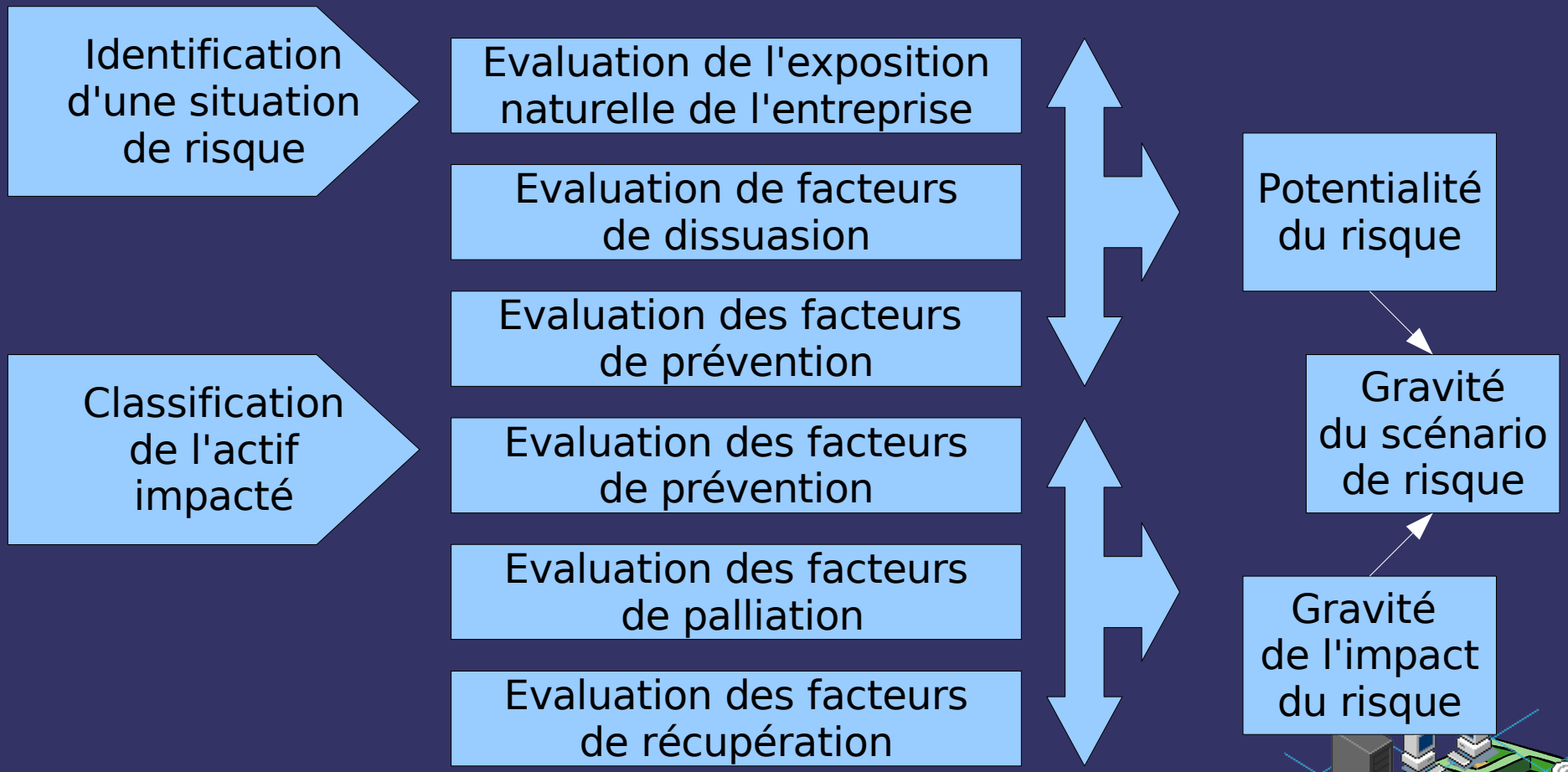
Évaluez vos Risques

Construisez vos Plan d'actions



Introduction MEHARI

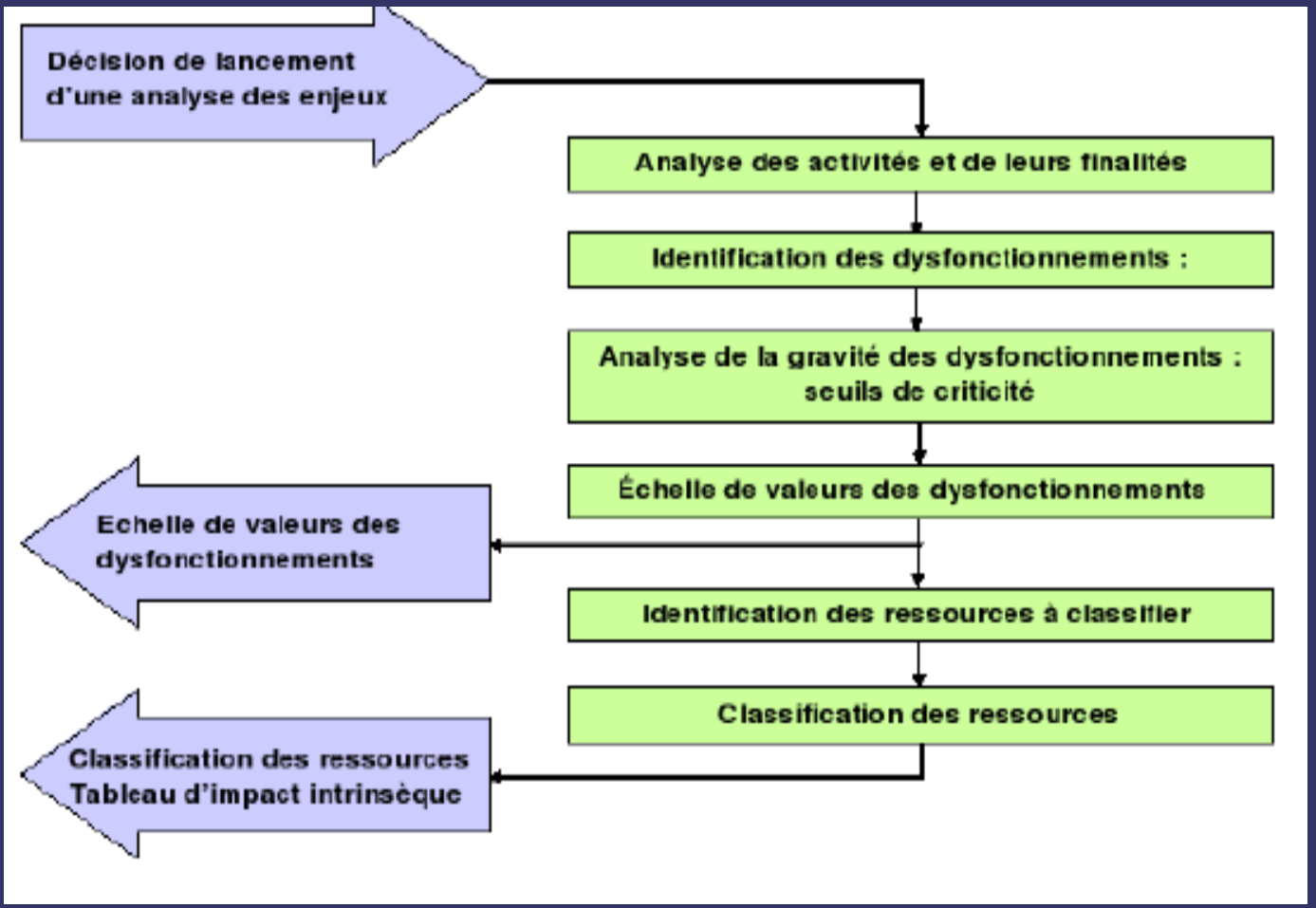
- Le processus d'analyse de risque de MEHARI

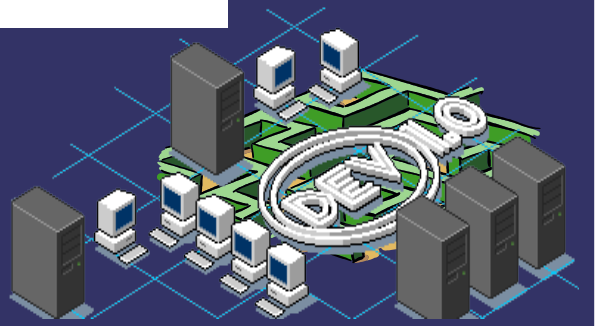


L'analyse des enjeux de la sécurité et la classification

- « Les enjeux de la sécurité, ne sont pas d'accroître les opportunités de gain mais de limiter les possibilités de perte. »
- Objectif:
  - « Que peut-on redouter et, si cela devait arriver, serait-ce grave?
- Quand :
  - Dés lors qu'il y a plusieurs choix;
  - Dés que l'on demande des budgets.

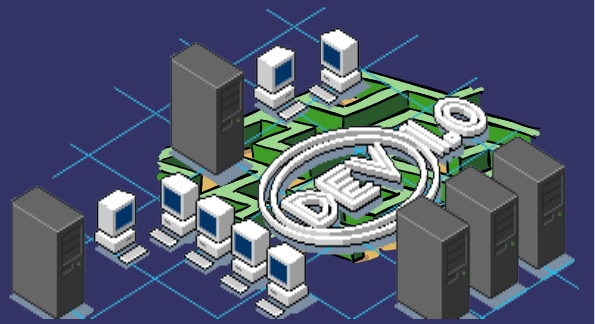
L'analyse des enjeux de la sécurité et la classification





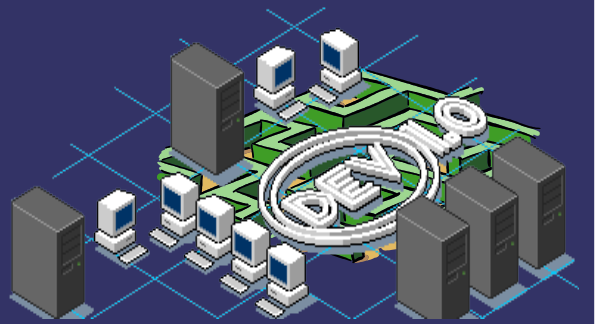
L'analyse des enjeux de la sécurité et la classification

- Identifications des activités majeures et de leurs finalités.
- Identification des dysfonctionnements redoutés de chaque activités (de l'activité et de la fonction)
- Evaluation du niveau de gravité de ces dysfonctionnements par activité.
- Determination et validation d'une échelle de valeurs
  - Exemple



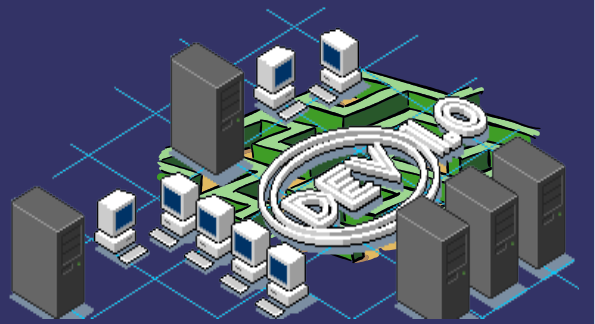
L'analyse des enjeux de la sécurité et la classification

- Pour chaque type d'informations et pour chaque ressources du SI et pour chaque critère de classification. On va classifier.
- Les critères :
  - Disponibilité
  - Confidentialité
  - Intégrité
  - etc .. (non répudiation, auditabilité)



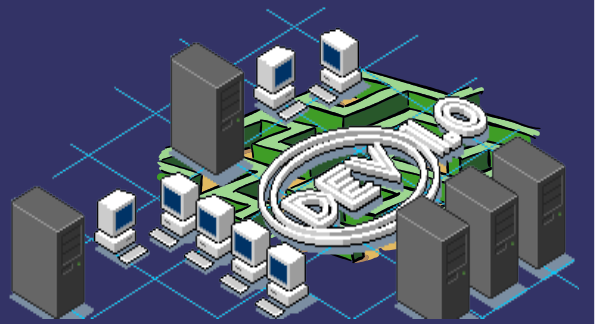
L'analyse des enjeux de la sécurité et la classification

- Les tableaux de classification MEHARI:
  - T1 : Identification des éléments liés à des processus métiers:
    - Les serveurs applicatifs
    - Les serveurs bureautiques
    - Les postes de travail
  - T2 : Identification des éléments liés à des services communs
    - Messagerie
    - Archivage



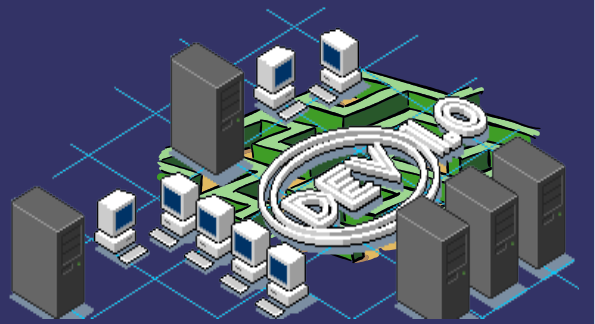
L'analyse des enjeux de la sécurité et la classification

- T3 : Tableaux d'impact intrinsèque
- C'est l'évaluation des conséquences de l'occurrence du risque, indépendamment de toute mesure de sécurité.
  - S'appuie sur les tableaux de classifications T1 et T2.
  - EXEMPLE



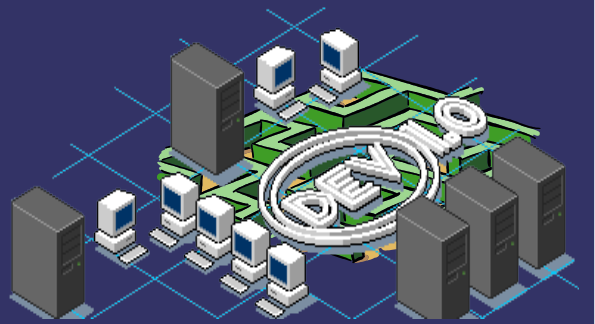
Le diagnostic de l'état des services de sécurité (Vulnérabilités)

- C'est la mesure de la qualité des services de sécurité
- C'est l'état des vulnérabilité de l'entreprise devant des risques divers :
  - Accidents
  - Erreurs
  - Actes Malveillants Volontaires



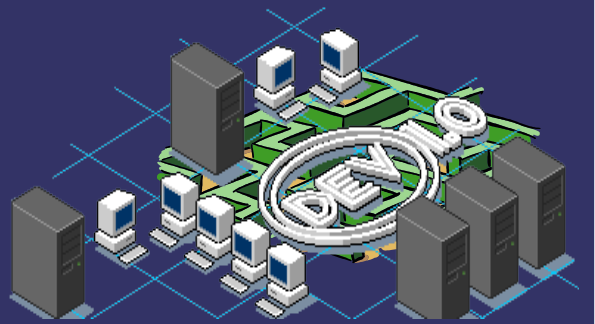
Le diagnostic de l'état des services de sécurité (Vulnérabilités)

- Un services de sécurité est une réponse à un besoin de sécurité, généralement en référence à certain types de menaces.
- Le service de sécurité est assuré par un ou plusieurs sous services de sécurités. (ex: contrôles accès = authentification + autorisation + filtrages)



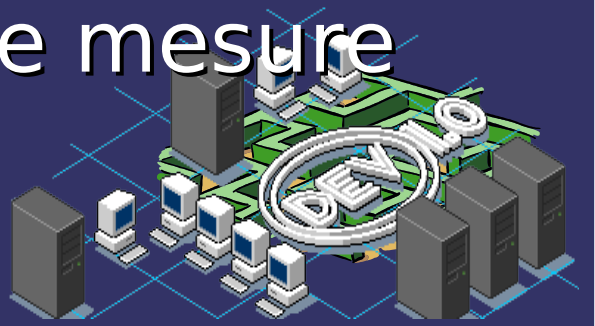
Le diagnostic de l'état des services de sécurité (Vulnérabilités)

- Un mécanismes est une manière d'assurer, totalement ou partiellement, la fonction du service ou du sous service.
- Certain service peuvent être considérés comme des mesures générales, d'autre comme des services techniques.
- EXEMPLE



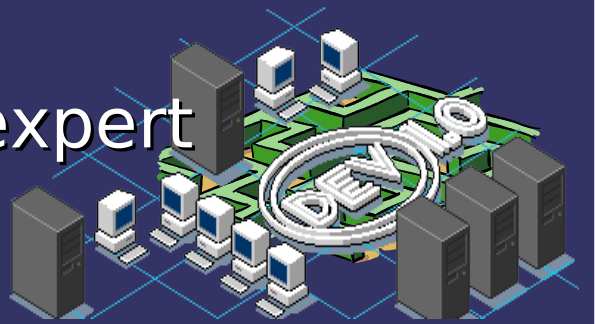
Le diagnostic de l'état des services de sécurité (Vulnérabilités)

- On mesure la qualité selon les critères:
  - Efficacité du service
  - Robustesse du service (attaque, contournement)
  - Moyen de contrôle (supervision)
- Les réponse sont évaluées à partir d'une formule et de coefficient de pondération pour fournir une mesure de la qualité du service.



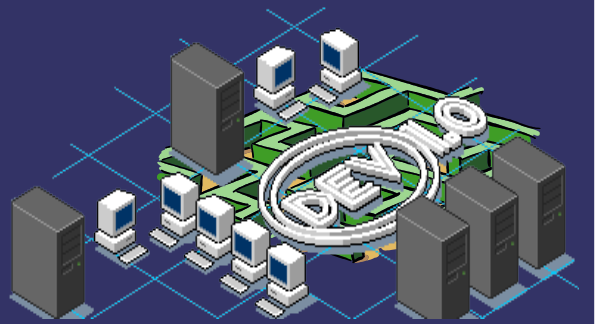
Le diagnostic de l'état des services de sécurité (Vulnérabilités)

- Les niveaux de qualité de services de sécurité
  - Qualité de service évaluée à 1
    - Qualité minimale, peu efficace à une attaque.
  - Qualité de service évaluée à 2
    - Efficace face une attaque de faible expertise
  - Qualité de service évaluée à 3
    - Efficace face à une attaque de moyenne expertise
  - Qualité de service évaluée à 4
    - Efficace face à une attaque d'expert



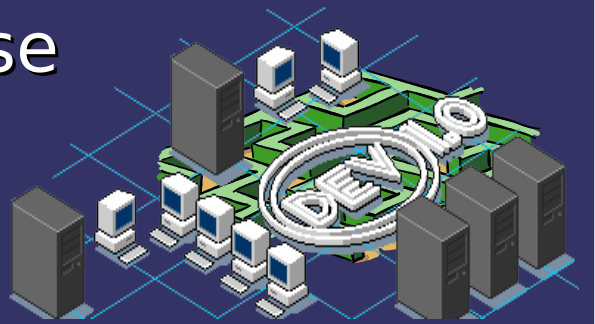
Le diagnostic de l'état des services de sécurité (Vulnérabilités)

- Deux méthodes
  - Evaluation par questionnaire
    - EXEMPLE
  - Evaluation Directe de la qualité de service
    - EXEMPLE



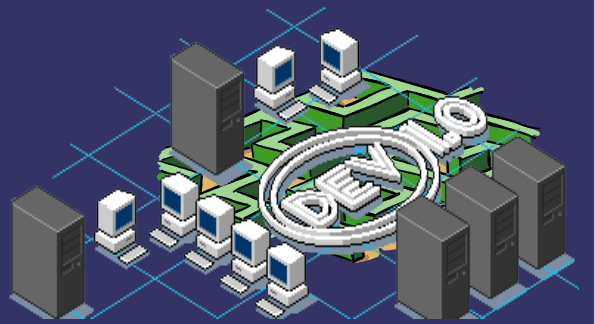
L'analyse de situations de risque

- Un scénario de risque est la description d'un dysfonctionnement et de la manière dont ce dysfonctionnement peut survenir et quel est le sinistre.
- Chaque scénario sera décrit par :
  - Le type de conséquence;
  - Le type de ressources impliquées;
  - Les types de causes;
- Paramètre associé aux risques d'un scénario
  - La potentialité de l'exécution du scénario (probabilité d'occurrence)
  - L'impact du risque sur l'entreprise



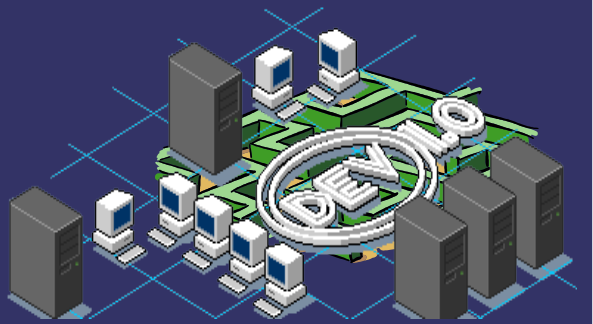
L'analyse de situations de risque

- Evaluation de la potentialité : (selection des scénarios)
  - Niveau 4 (très probable)
  - Niveau 3 (Probable)
  - Niveau 2 (Improbable)
  - Niveau 1 (Tés improbable)
  - Niveau 0 (Non envisagé)



L'analyse de situations de risque

- L'évaluation direct de cette potentialité est très difficile; MEHARI propose d'analyse préalablement plusieurs facteurs.
  - L'exposition naturelle à la situation de risque
  - Le risque pris par les auteurs (actes volontaires)
  - Les conditions de survenance du scénarios

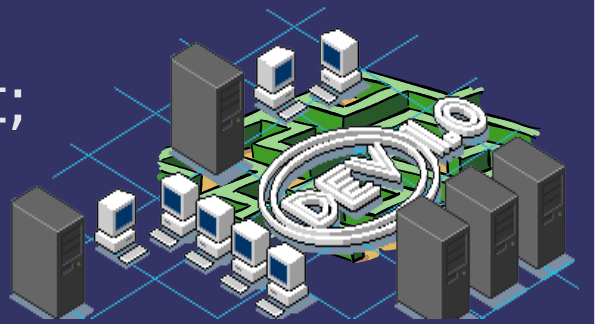


L'analyse de situations de risque

- L'exposition naturelles
  - Devant une situation de risque donnée, les entreprises ne sont pas égales.
  - Les niveaux :
    - N1 : exposition très faible
    - N2 : exposition faible
    - N3 : exposition moyenne
    - N4 : exposition forte

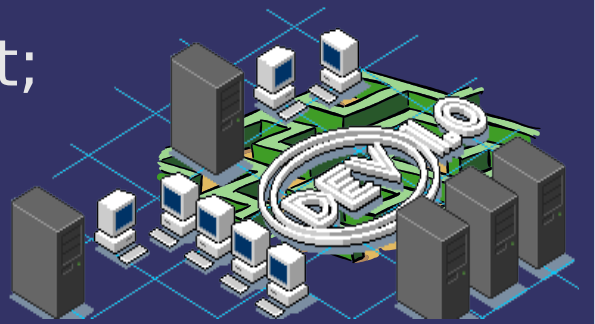
L'analyse de situations de risque

- Le risque ressenti par l'auteur d'une action volontaire
  - « Plus le risque ressenti par l'auteur est grand, moins probable est sa tentative »
  - Mesures Dissuasives : la détection, l'immutabilité, l'authentification, les sanctions, la communication;
  - Les niveaux :
    - N1 : effet dissuasif très faible ou nul;
    - N2 : effet dissuasif moyen;
    - N3 : effet dissuasif important;
    - N4 : effet dissuasif très important;



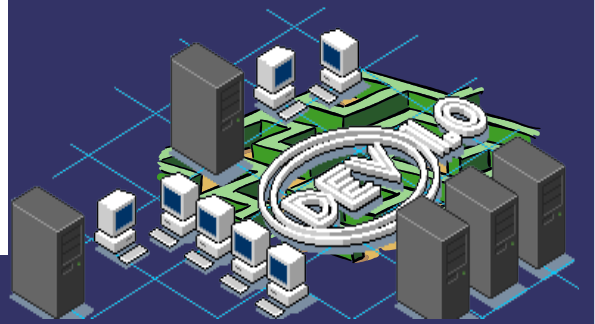
L'analyse de situations de risque

- Les conditions de survenance;
  - « Le déclenchement d'un scénario de risque n'aboutira à un sinistre réel que si certaines conditions sont réunies. »
  - Mesures Préventives :
    - mesures de sécurité physique;
    - mesures de contrôles d'accès;
  - Les niveaux :
    - N1 : effet préventif très faible ou nul;
    - N2 : effet préventif moyen;
    - N3 : effet préventif important;
    - N4 : effet préventif très important;



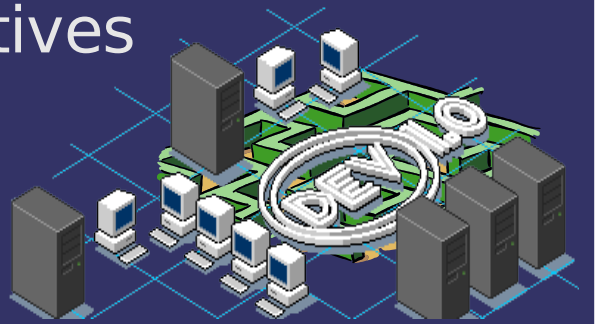
L'analyse de situations de risque

- Evaluation globale la potentialité
  - L'évaluation de l'exposition naturelle et des l'efficacité des mesures dissuasives et préventives.



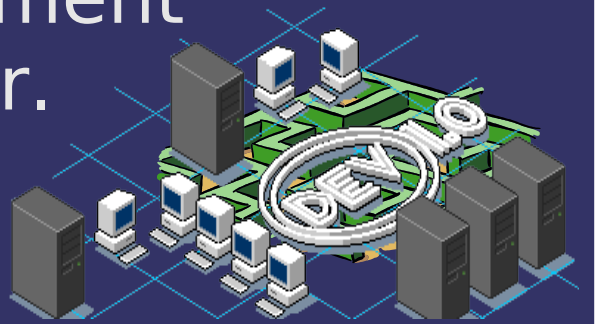
L'analyse de situations de risque

- Evaluation de l'impact: « Si le risque analysé se produit, quelle sera la gravité finale de ses conséquences ? »
  - Échelles de l'impact:
    - N4 : Vital
    - N3 : très Grave
    - N2 : Important
    - N1 : Non Significatifs
  - L'évaluation direct difficile
    - Evaluation de la gravité intrinsèque
    - Evaluation des mesures de confinements
    - Evaluation des mesures de palliatives
    - Transfert du risque sur des tiers



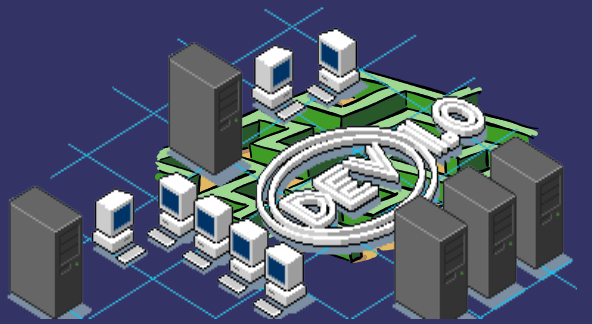
L'analyse de situations de risque

- Evaluation de la gravité intrinsèque
  - La première évaluation de l'impact, déduite d'une échelle de valeur (étude des enjeux métier), peut être considérée comme impact intrinsèque;
  - C'est à dire comme une estimation maximaliste des conséquences du risque, en dehors de toute mesure de sécurité.
  - EX : destruction des données de la base concernant le règlement de paye (calcul et paramétrage) due à un effacement volontaire par un collaborateur.



L'analyse de situations de risque

- Evaluation du Confinement du risque (limitation des conséquence direct)
  - « Les conséquences directes d'un risque qui se réalise peuvent s'étendre et se propager, dans l'espace et le temps, ou re confinées. Moins ces conséquences sont confinées, plus le risque est grand.
  - Mesures de PROTECTION:
    - mesures de detection;
    - mesures d'isolement physique (incendie, inondation)



L'analyse de situations de risque

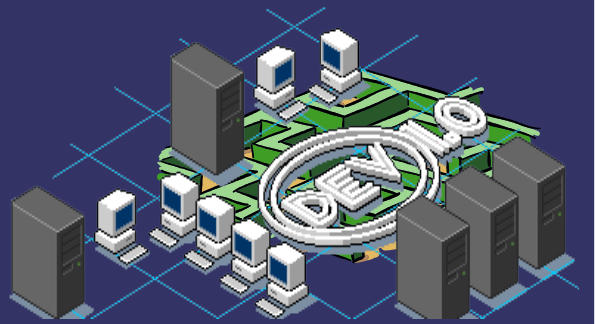
- Efficacité des mesures de confinement ou de protection
  - N 1 : l'effet de confinement et de limitation des conséquences direct est très faible ou nul;
  - N 2 : l'effet de confinement et de limitation des conséquences direct est moyen;
  - N 3 : l'effet de confinement et de limitation des conséquences direct est important;
  - N 4 l'effet de confinement et de limitation des conséquences direct est très important;

L'analyse de situations de risque

- Evaluation des mesures Palliatives du risque (limitation des conséquence indirect)
  - «La situation de crise engendrée par l'occurrence d'un risque peut être anticipée et préparée. Moins cette situation de crise est préparée, plus le risque est grand.»
  - Mesures PALLIATIVES:
    - Étude préalable des modes dégradés acceptables (plan de maintenance de secours).
    - Formation des hommes en prévision de situation de crise.

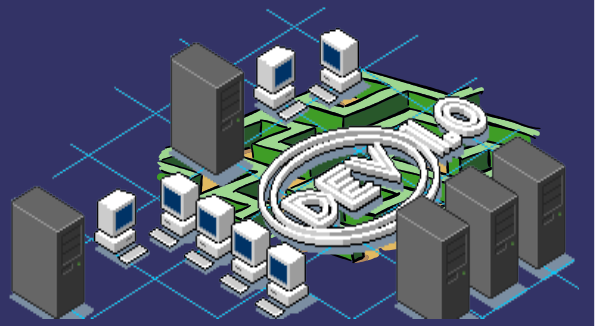
L'analyse de situations de risque

- Efficacité des mesures Palliatives
  - N 1 : L'effet de limitation des conséquences indirectes est très faible ou nul;
  - N 2 : L'effet de limitation des conséquences indirectes est moyen;
  - N 3 : L'effet de limitation des conséquences indirectes est important;
  - N 4 : L'effet de limitation des conséquences indirectes est très important;



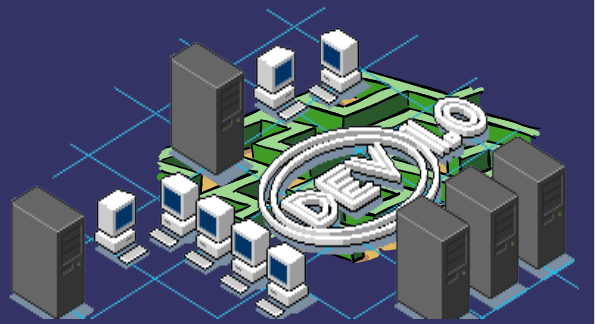
L'analyse de situations de risque

- Le transfert du risque (limitations des pertes finales)
  - « Les pertes finales peuvent éventuellement être transférées en parties sur des tiers par l'assurance et le recours en justice »
  - Mesures de RECUPERATION
    - analyse spécifique des risque à couvrir par l'assurance
    - préparation spécifique des actions en justice



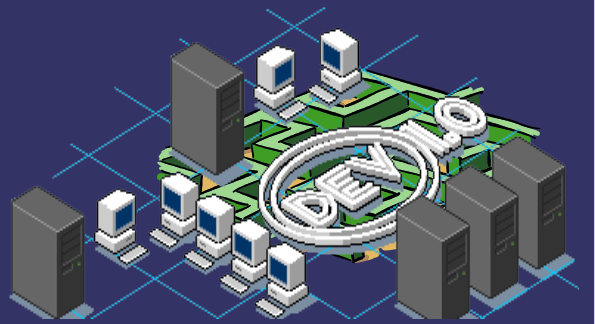
L'analyse de situations de risque

- Efficacité des mesures de Récupération
  - N 1 : L'effet de récupération est très faible ou nul;
  - N 2 : 'effet de récupération est moyen;
  - N 3 : 'effet de récupération est important;
  - N 4 : L'effet de récupération est très important (risque résiduel niveau 2);



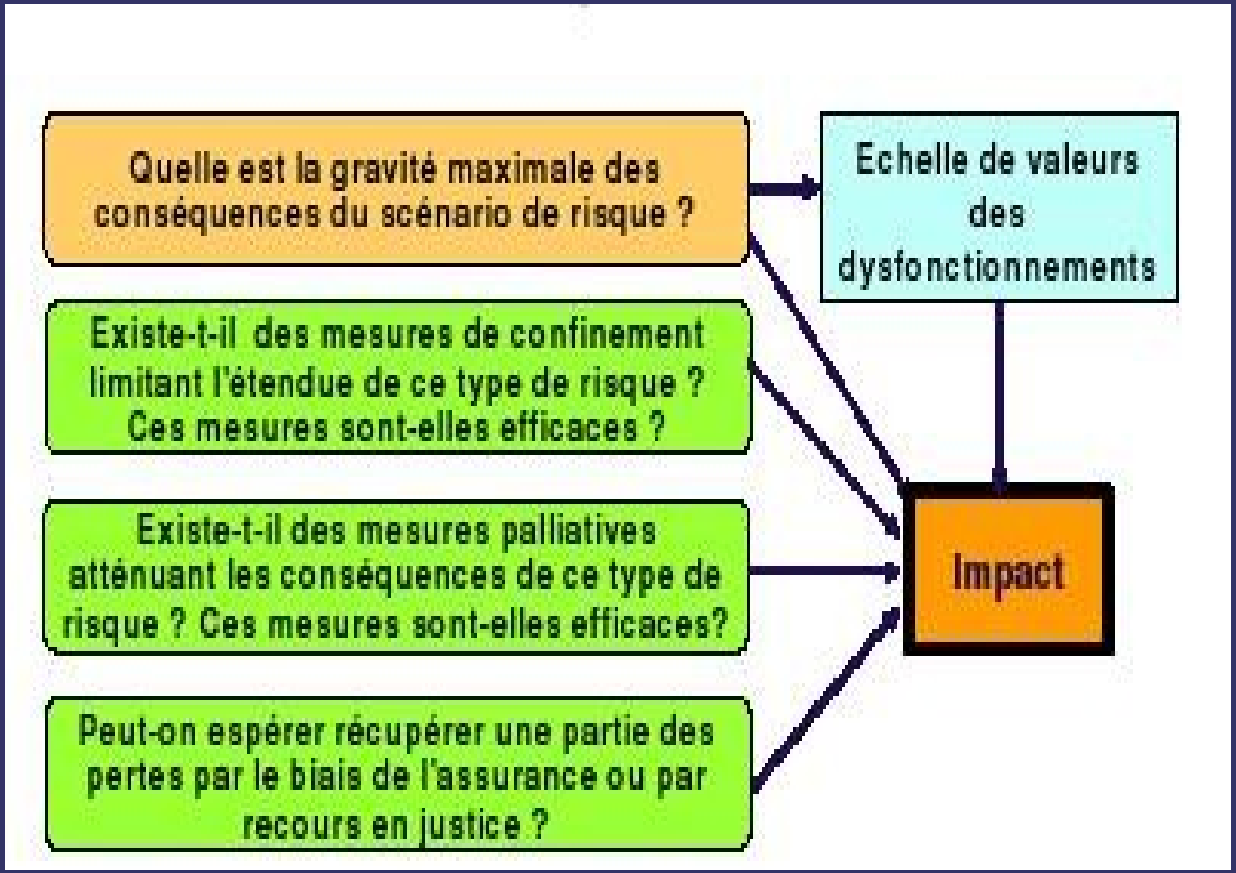
L'analyse de situations de risque

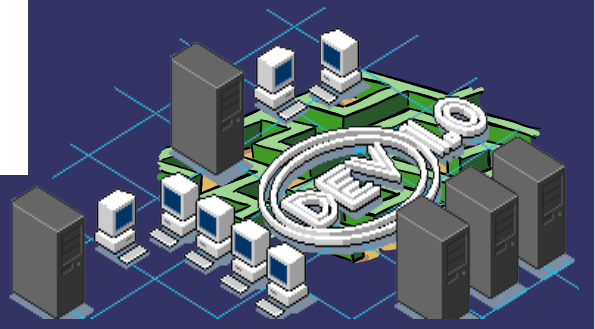
- Evaluation de l'impact globale du scénario de risque
  - L'impact intrinsèque déterminé par l'échelle de valeurs et l'évaluation de l'efficacité des mesures d'atténuation du risque pouvant limiter cet impact (mesure de protection, palliatives et de récupération) mèneront à l'évaluation de l'impact globale du scénario.



L'analyse de situations de risque

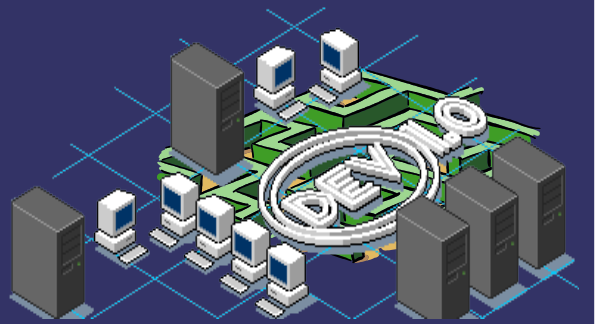
- Evaluation de l'impact globale du scénario de risque





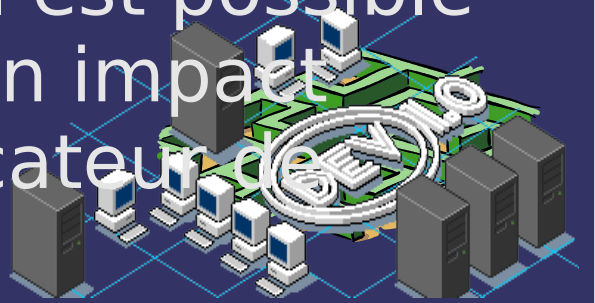
L'analyse de situations de risque

- Gravité résultante de la situation de risque
  - La gravité du scénario résulte à la foi de sa potentialité et de son impact.
  - « Cette situation de risque est-elle acceptable en l'état ou sinon que proposer ?
  - MEHARI propose trois type de risques et des grille d'acceptabilité des risques
    - Risques insupportable (4)
    - Risques inadmissible (3)
    - Risques tolérés (1,2)



L'analyse de situations de risque

- Résumé de la démarche d'analyse de risque
  - Une situation de risque peut être caractérisée par une potentialité et un impact intrinsèque en l'absence de toute mesure de sécurité. Potentialité et impact intrinsèque peuvent être évalués.(Expo-Nat; Tab d'impact intrinsèque)
  - Des mesures de sécurité peuvent venir réduire ce risque intrinsèque.
  - Sur la base de ces éléments, il est possible d'évaluer une potentialité et un impact résiduel et de déduire un indicateur de gravité de risque.



Les automatismes de MEHARI

- Rappel du processus d'analyse de risque

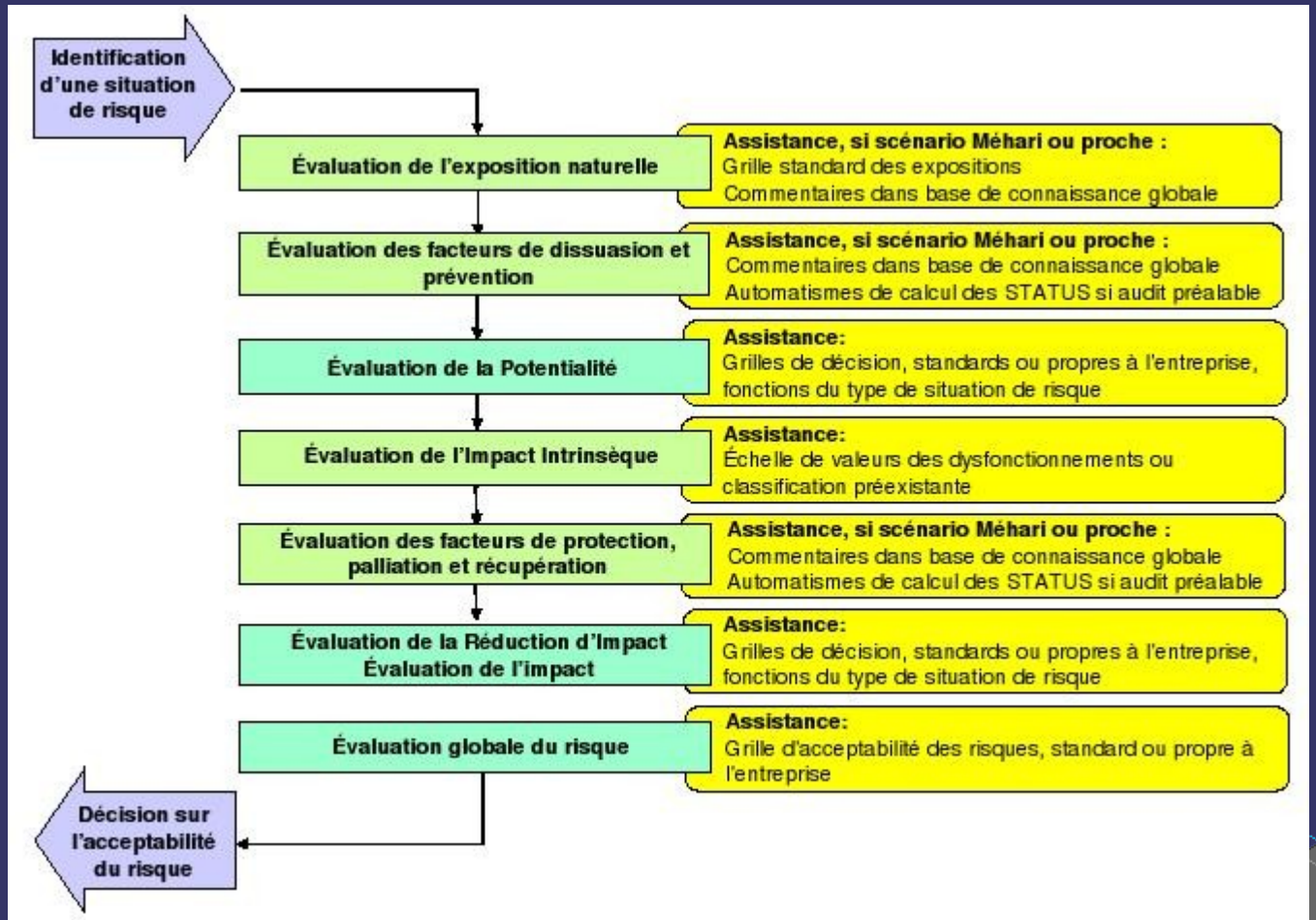


Figure 1 : Le processus d'analyse de risque et les assistances de MEHARI

Les automatismes de MEHARI

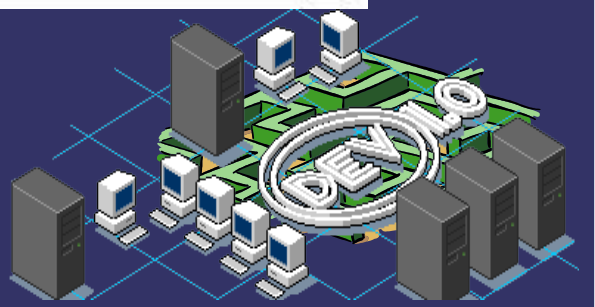
- Indicateurs d'efficacité des des services de sécurité par scénario et par type de mesures.
  - **EFF-DISS** pour l'efficacité des mesures dissuasives
  - **EFF-PREV** pour l'efficacité des mesures de prévention
  - **EFF-PROT** pour l'efficacité des mesures de protection
  - **EFF-PALL** pour l'efficacité des mesures palliatives
  - **EFF-RECUP** pour l'efficacité des mesures de récupération

Les automatismes de MEHARI

- Indicateurs d'efficacité des des services de sécurité par scénario et par type de mesures.

10.31 : Perte de fichier de données, par effacement malveillant de supports par le personnel d'exploitation

Potentialité	TYP-EXPO	EFF-DISS	EFF-PREV
	MA010	MAX(MIN(07C02;08E02);08C01)	08A02
Impact	TYP-PROT	EFF-PALL	EFF-RECUP
	max(08C01;08C05)	MAX(MIN(08D05 ;09D03);09D02)	01D02

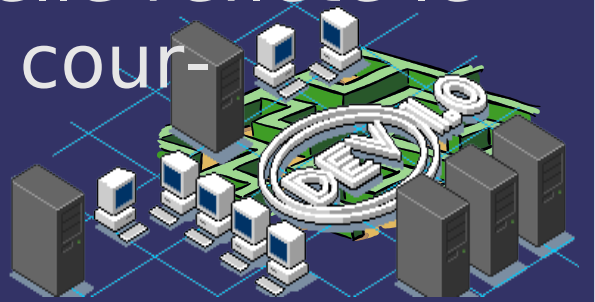


Les automatismes de MEHARI

- Indicateurs d'efficacité des des services de sécurité par scénario et par type de mesures.
  - Ces indicateurs sont calculés à partir de vos résultats d'audit.
  - La qualité du sous service de sécurité est évaluée par l'audit.
  - L'efficacité des mesures (ci-dessous) est calculée à partir des algorithmes MEHARI utilisant ces qualités de service.
    - MIN : les services sont complémentaires, si l'un d'eux est faible, l'ensemble est faible.
    - MAX : les services sont alternatifs, si l'un d'eux est de bonne qualité, l'ensemble y sera.

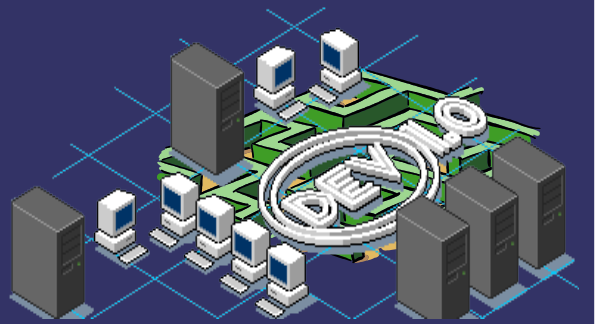
Les automatismes de MEHARI

- Calcul de la qualité de service
  - Les services de sécurité peuvent avoir des niveaux de performances différents celon leur mécanismes.
  - On évalue la qualité des service par un audit ou à partir du manuel de référence des services. AUDIT/ REF
  - Paramètre (efficacité, robustesse, contrôles(audit))
  - La qualité de service est notée sur une échelle de de 0 à 4. Cette échelle reflète le niveau de force qu'il faut pour cour-circuiter le mécanisme.



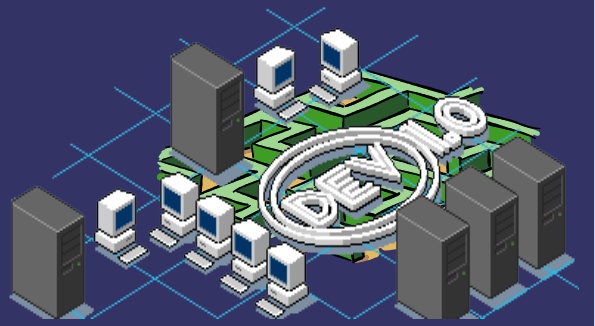
Les automatismes de MEHARI

- Evaluation de la potentialité : Le STATUS-P
  - Evaluation automatisé par des grilles à partir :
    - STATUS-EXPO
    - STATUS-DISS
    - STATUS-PREF
  - 3 grilles en fonctions du type de cause
    - Événement naturel ou accident
    - Erreur humaine
    - Acte volontaire (malveillant ou non)
    - EXEMPLE



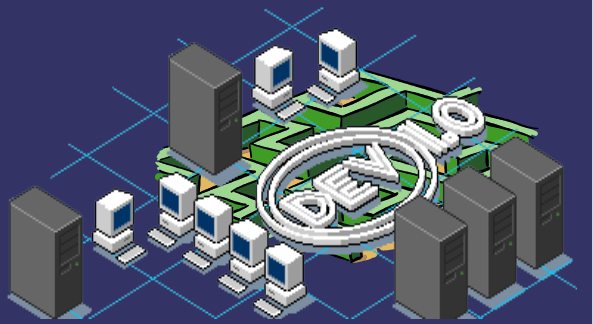
Les automatismes de MEHARI

- Evaluation de l'impact : Le STATUS-I
  - Evaluation automatisé par des grilles à partir :
    - STATUS-RI
    - Impact intrinsèque
  - Cette évaluation se fait en deux temps:
    - évaluation d'un indicateur de réduction d'impact : STATUS-RI
    - évaluation de l'impact : STATUS-I



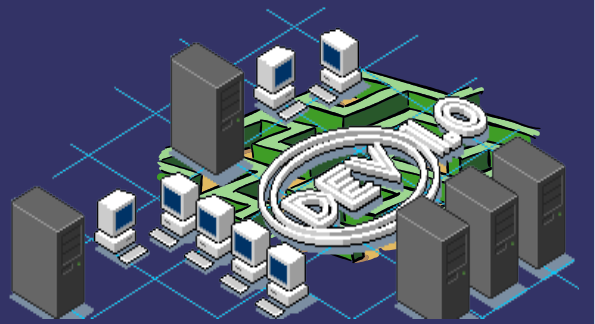
Les automatismes de MEHARI

- Evaluation de la réduction d'impact : Le STATUS-RI
  - Evaluation automatisé par des grilles à partir :
    - STATUS-PROT
    - STATUS-PALL
    - STATUS-RECUP
  - 3 grilles en fonction des types de conséquences
    - Perte de disponibilité
    - Perte d'intégrité
    - Perte de confidentialité



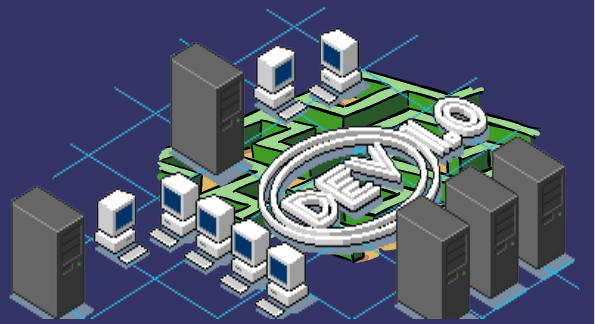
Les automatismes de MEHARI

- Evaluation d'impact résiduel : Le STATUS-I
  - l'impact résiduel est déduit de l'impact intrinsèque et de l'indicateur de réduction d'impact par la formule suivante:
    - I = MIN (IMPACT INTRINSÈQUE; 5-STATUS-RI)
    - STATUS-RI a un effet de plafonnement sur l'impact



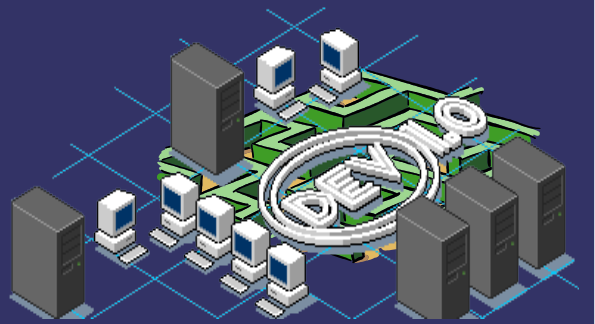
Les automatismes de MEHARI

- Evaluation de la gravité du scénario
  - La gravité du scénario sera déduite des évaluations de la Potentialité et de l'inpact (STATUS-P et STATUS-I), par des grilles d'acceptabilité des risques.
  - EXEMPLE



Les automatismes de MEHARI

- Expression des besoins de sécurité
  - un besoin de service de sécurité est établi pour chaque scénario en s'appuyant sur :
    - les services de sécurité associés au scénario
    - une formule fournie par MEHARI
- La synthèse des besoins de service
  - Sur quel service de sécurité agir en priorité pour diminuer le risque de mes scénario ?
  - MEHARI fournie une formule de calcul



Modèle UML métiers