CGI | Business Consulting

Intégration de projets au SOC applicatif

Club EBIOS

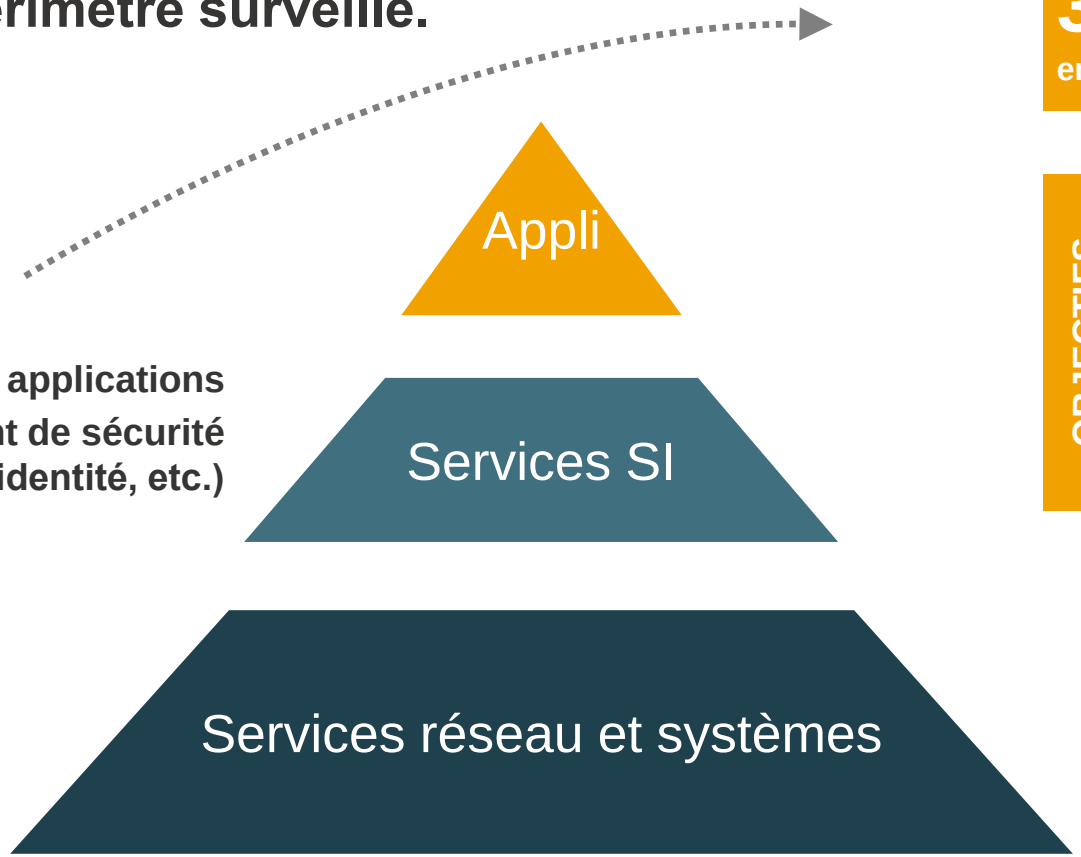
Jean Olive
14 mai 2019

CGI | Business Consulting

Sommaire

Contexte

Le déploiement des services SOC suit généralement les phases suivantes d'extension du périmètre surveillé.



2. Les services / applications transverses, notamment de sécurité (gestion d'identité, etc.)

1. Les briques d'infrastructures

3. Les applications critiques, présentant des enjeux forts ou des risques résiduels non traités

OBJECTIFS

Définir et mettre en œuvre des scénarios de surveillance, adaptés à chaque contexte projet

Alerter à bon escient lors d'évènements ou de comportements suspects

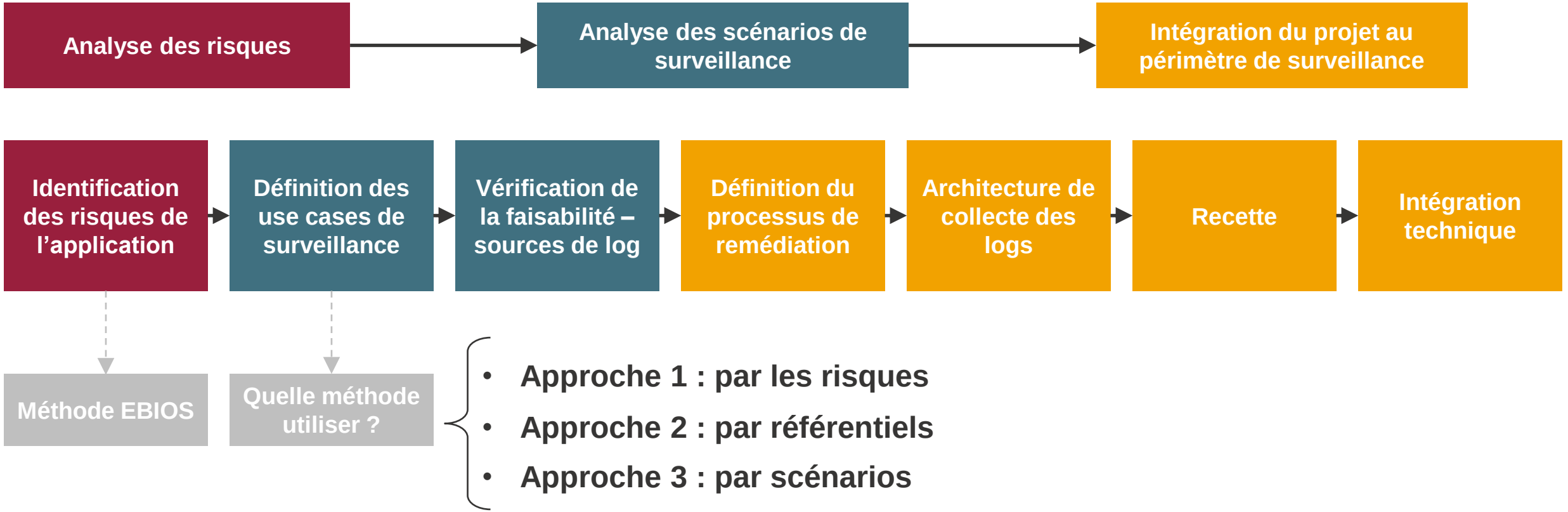
NIVEAU DES CYBER ATTAQUES

SIMPLE LARGE SPECTRE

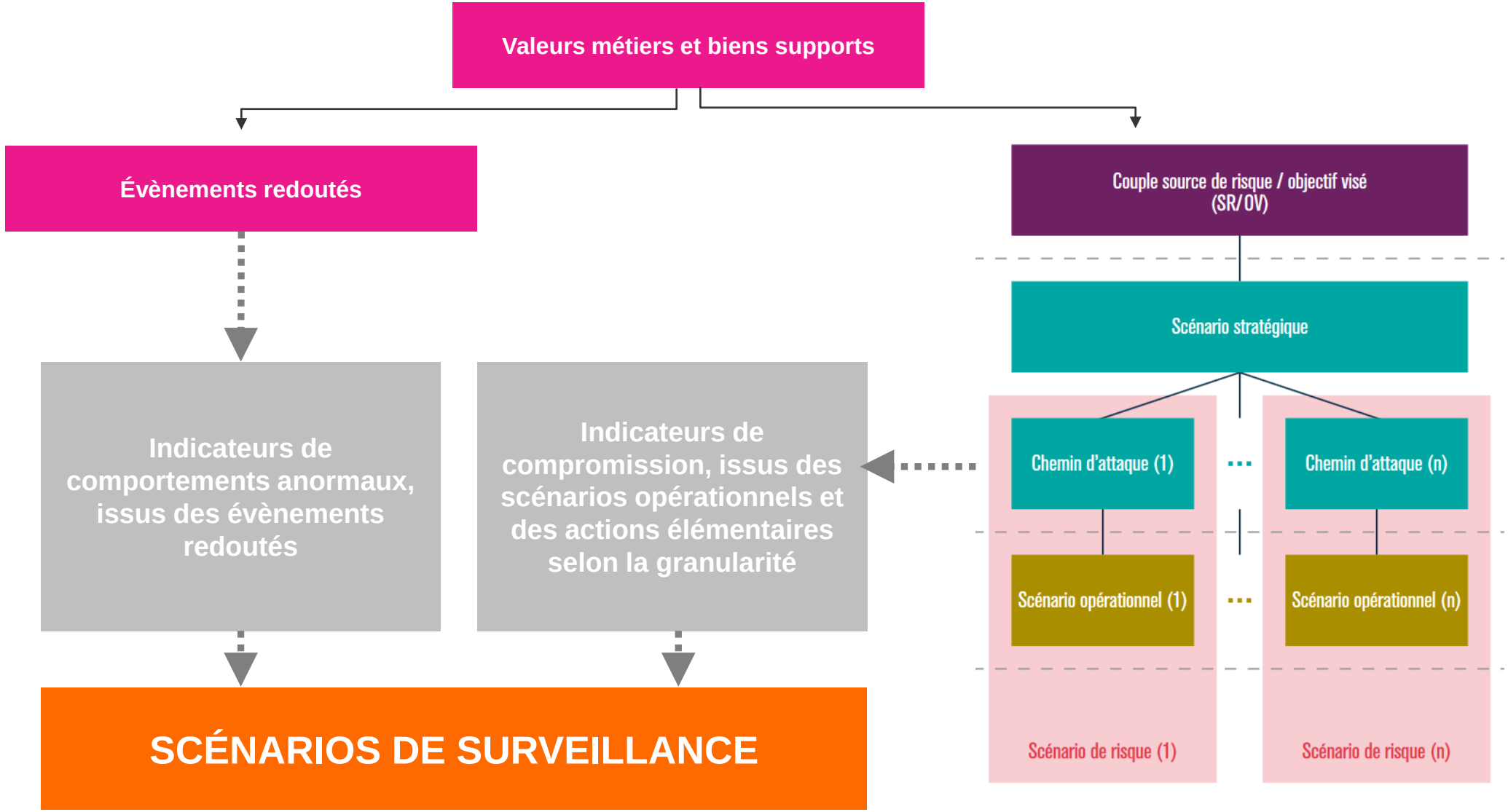
ÉLABORÉ

AVANCÉ CIBLÉ

3 approches pour identifier les incidents/scénarios



Approche 1
Détection des scénarios par l'approche par les risques



Approche 1

Surveiller les risques résiduels, appliquer une démarche de défense en profondeur

Scénario stratégique		
Les documents sont détruits suite à un abus d'un administrateur ou par le déclenchement intempestif du processus de purge.		
Événements redoutés	**Gravité**	**SROV**
Perte des documents	4	• Attaquant ou administrateur cherchant à compromettre le système en supprimant des documents probants
Scénarios opérationnels	**Vraisemblance**	
Abus de droit d'un administrateur provoquant la destruction de données par accès direct à la base	2	
Accès avec des privilèges root pour modifier la date du système	4	
Infection virale sur le poste de l'administrateur se propageant à la base de données	2	

Mesure de sécurité		
▪ Plan de sauvegarde ▪ Solution antivirale ▪ Installation d'un NTP	▪ Versement en Y (site de secours) ▪ Durcissement des OS et des middlewares	▪ Protection en écriture des documents et des preuves ▪ Traçabilité de toute opération

Scénarios de surveillance
SS1 Détection de connexion directe à la base de données en dehors de période de maintenance
SS2 Détection d'opérations impactant un gros volume de données (destruction)

Approche 2
Base de scénarios courants

- ✓ **Comportemental**
  - ➢ Tentative répétées d'échecs de connexion sur un même compte
  - ➢ Connexion à un compte resté longtemps inactif
  - ➢ …

- ✓ **Technique**
  - ➢ Échec de connexion d'un compte de service, présentation d'un ticket SAML non valide
  - ➢ Usurpation d'un compte de service (IP différente)
  - ➢ …

Limites de ces approches

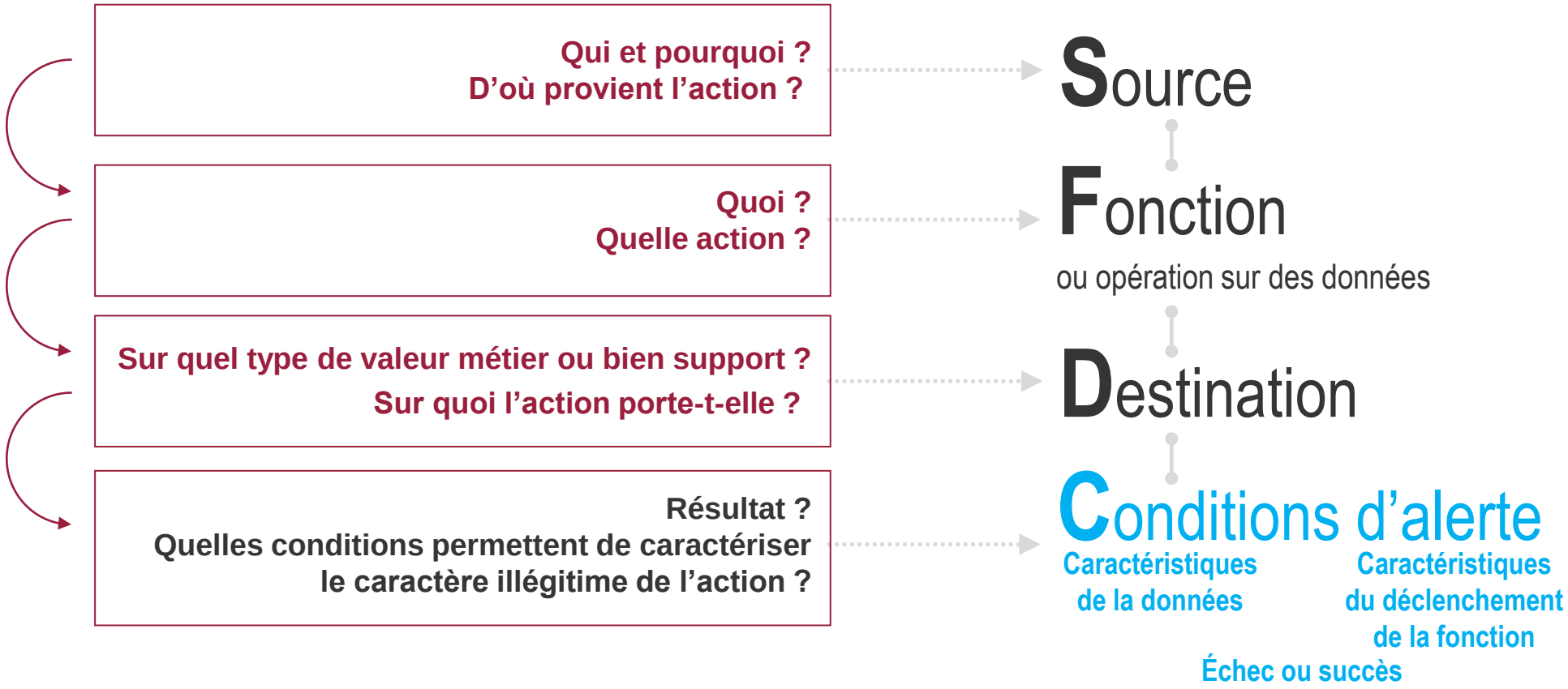
Comment vérifier que des scénarios importants n'ont pas été oubliés ?

- L'analyse des risques n'est pas exhaustive
- Les comportements ou évènements techniques sont trop nombreux pour tous les dénombrer
  - *Même s'il existe des scénarios "génériques" utilisables par défaut*
- Manque une vue globale des scénarios
- Absence de "fil directeur" ➔ méthode empirique s'appuyant sur les scénarios

Définir une approche complémentaire consistant en un modèle et la construction d' une représentation. Approche 3 : *Framework* de surveillance applicative

Approche 3
Le modèle SFDC - Décomposition d'un scénario

Pour caractériser complètement un scénario de surveillance, il faut se poser les questions suivantes :



Approche 3

Le modèles SFDC – exemples

Conditions

Connexion directe à la **base de données** en ***dehors de période de maintenance***

Fonction — Destination

Quelle que soit la **S**ource

Altération ***réussie*** d'un ***gros volume*** **de données**

Fonction — Destination

Quelle que soit la **S**ource

Connexions ***réussies simultanées*** à un même **compte** de **l'application**

Fonction — Source — Destination

Connexion ***réussie*** avec un compte **applicatif** interne au projet depuis une **adresse IP** ***inhabituelle***

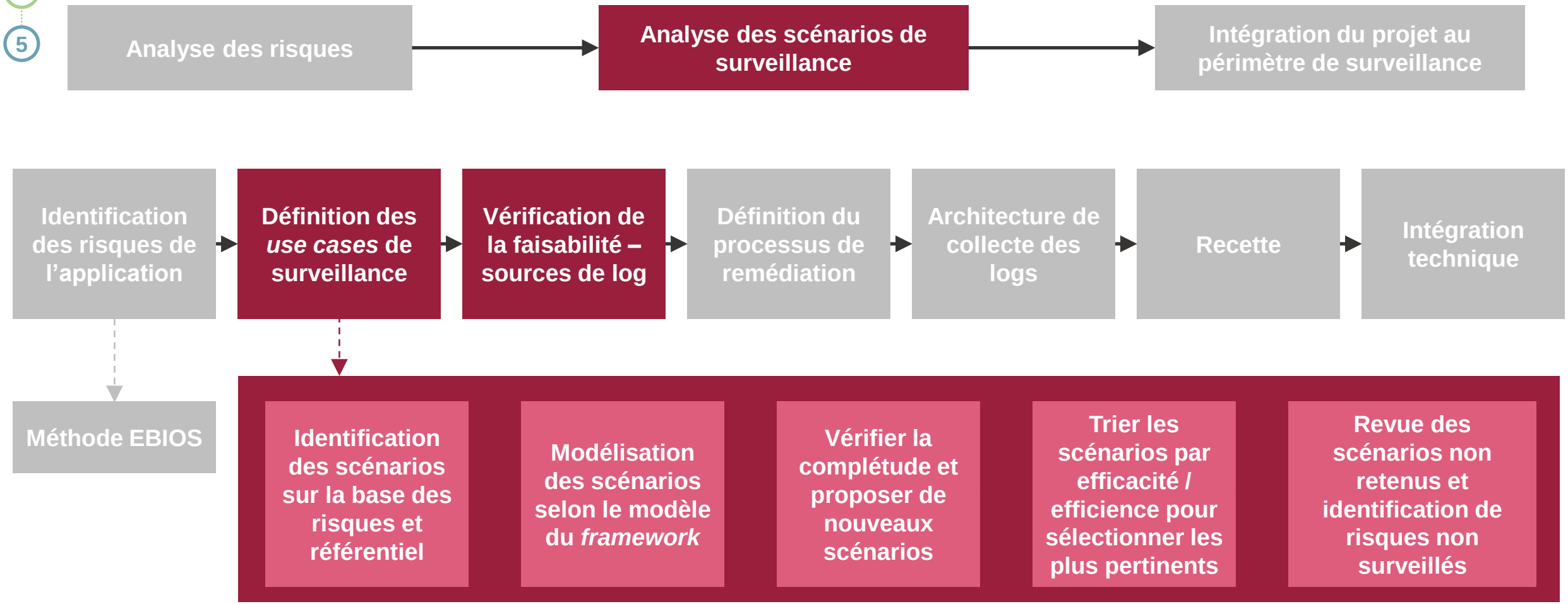
Fonction — Destination — Source

Méthode d'utilisation du framework

- Personnaliser les éléments du framework (sources retenues, fonctions essentielles, biens supports, etc.)
- Analyser les combinatoires pour vérifier la complétude
- Analyser l'intérêt des scénarios (faux positifs)
- Identifier les risques associés
- Arbitrer sur l'intérêt croissant des scénarios retenus

source	bien	fonction	condition	retei	scénario
Tout	Bases de données	Connexion	Hors période de maintenance	O	Connexion directe à la base de données
Tout	Bases de données	Service de sauvegarde	Arrêt du service	O	Arrêt du processus de sauvegarde
Tout	Bases de données	Suppression	Gros volume ou table	O	Détection d'opérations impactant un gros volume de données
Utilisateur	Bases de données	Purge	HNO	N	Détection d'une purge en HNO
Admin	Serveur	Connexion	HNO	O	Connexion d'un administrateur en HNO
Admin	Serveur	Connexion	Hors période de maintenance	O	Connexion d'un administrateur hors période de maintenance
Tout	Serveur	Service NTP	Modification du service	O	Détection de toute modification du service NTP
Tout	Serveur	Gestion des droits	Modification du groupe Administrateur	O	Détection de toute modification des groupes d'utilisateurs à priviléges

Intégration des 3 approches



Communiquez avec nous pour poursuivre la conversation.

Jean Olive
Vice-Président
jean.olive@cgi.com
06 74 33 29 42