Industrialisation de la modélisation des menaces, un retour d'expérience

Stéphane Adamiste

OWASP Geneva Chapter – 3 décembre 2019

Agenda

1 — Modélisation des menaces - Aperçu

2 — Etude de cas

3 — Industrialisation de la modélisation des menaces

4 — Intégrer la modélisation des menaces dans la gouvernance sécurité d’entreprise – Proposition

5 — Conclusions

A propos de l'orateur

Stéphane Adamiste
Information Security Consultant

- Travaille pour une société de services spécialisée en sécurité de l'information (50 personnes)
- Définition de l'offre de services / avant-vente
- Assiste également les clients dans leur stratégie de gestion de la sécurité et des risques associés

PROFIL

- Spécialiste sécurité de l'information et protection des données personnelles (expérience ~18 ans)
- Appréhende la sécurité de l'information d'un point de vue technique et métier
- #Audit, #Risk management #Conformité #Gouvernance

PRÉCÉDENTS EMPLOIS

- Senior consultant dans une des grandes sociétés d'ingénierie logicielle suisse
- COO d'une société suisse d'audit et de conseil spécialisée dans en sécurité de l'information et gestion du risque informationnel
- Senior consultant et auditeur au sein de l'un des Big4 (département Enterprise Risk Management - Luxembourg)

Modélisation des menaces - Aperçu

Modélisation des menaces: Définition / caractéristiques

Processus permettant d'identifier et de documenter les menaces pesant sur un système ainsi que les contremesures les plus appropriées

Préventif

- Effectué durant la phase de design d'un projet
- Détection et mitigation des risques précoces

Editable

- Supporte les itérations
- Mise à jour au fur et à mesure qu'évolue le système évalué

Simple

- Besoin d'un stylo et d'une feuille

Elastique

- Focus sur les menaces principales vs approche hyper détaillée

Didactique

- Comble le vide entre le métier et la technique

Objectif

- Fournit des éléments rationnels de décision

Les différents façons de modéliser des menaces

Asset-centric

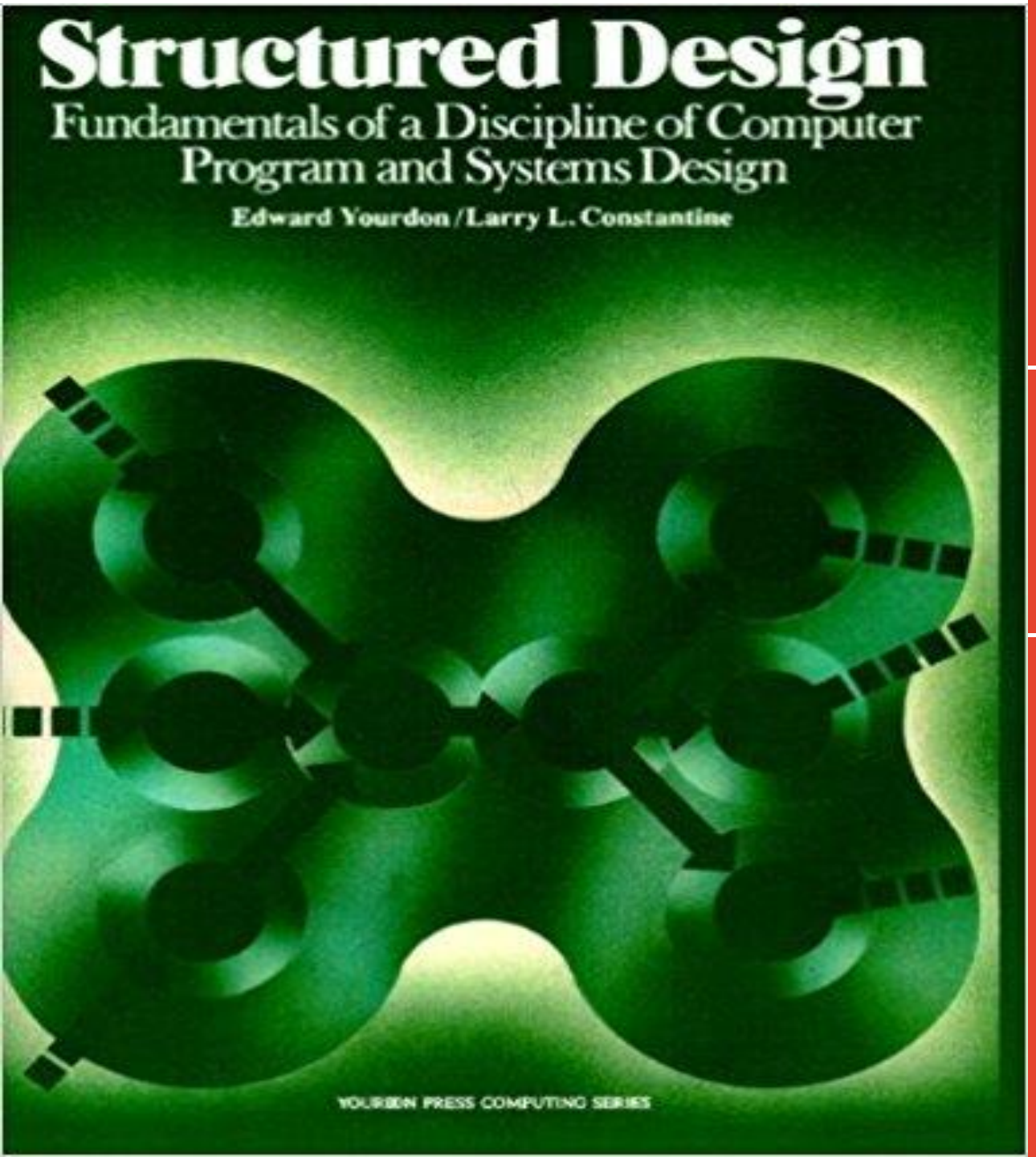
- «Asset» = Bien de valeur (vague)
- Identification des «assets»
  - Que voulons-nous protéger?
  - Que convoitent les attaquants?
  - Quelles sont les étapes pour y parvenir?
- Identification des menaces
  - Lien asset-menace peu évident?

Attacker-centric

- Identifier les «profils-type» d'attaquants
- P. ex. script kiddie vs groupe étatique
- P. ex. interne vs externe
- Subjectivité / projection

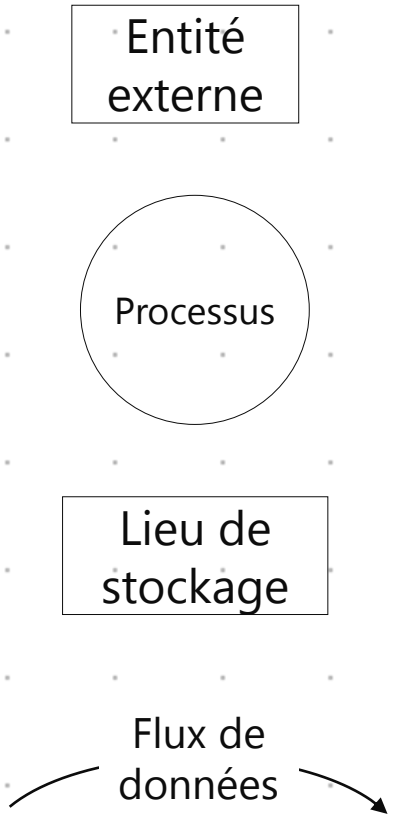
Software-centric

- Focus sur le système en cours de construction
- Basé sur une représentation graphique du système
- Plus objectif / systématique



Diagrammes de Flux de Données (DFD)

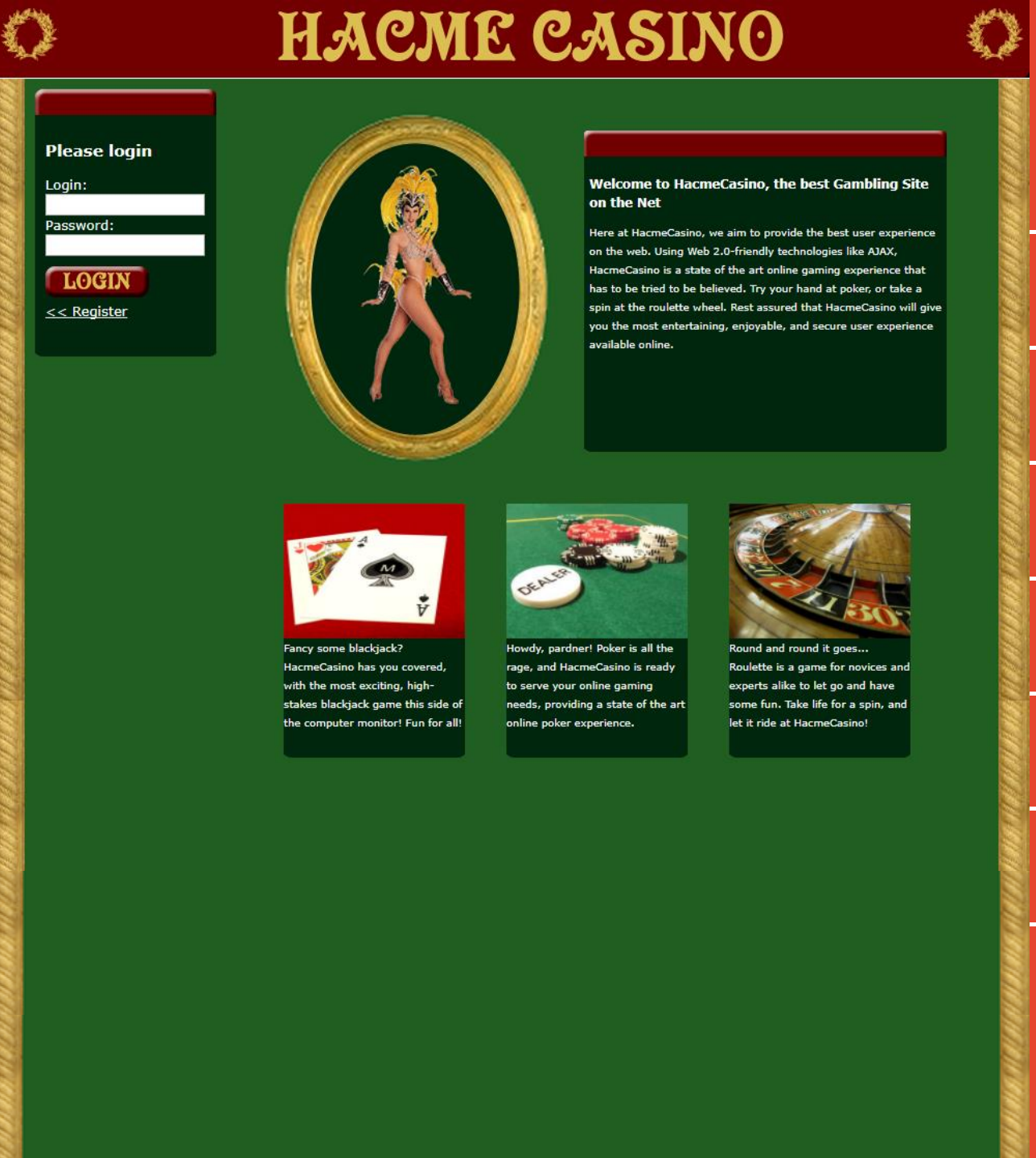
- Représentation graphique des flux de données au travers d'un système d'information modélisant les traitements qui y sont faits
- Popularisé dans les 70's par les pionniers de l'informatique Ed Yourdon et Larry Constantine dans leur livre *Structured Design*



Symboles utilisés (Yourdon/De Marco)

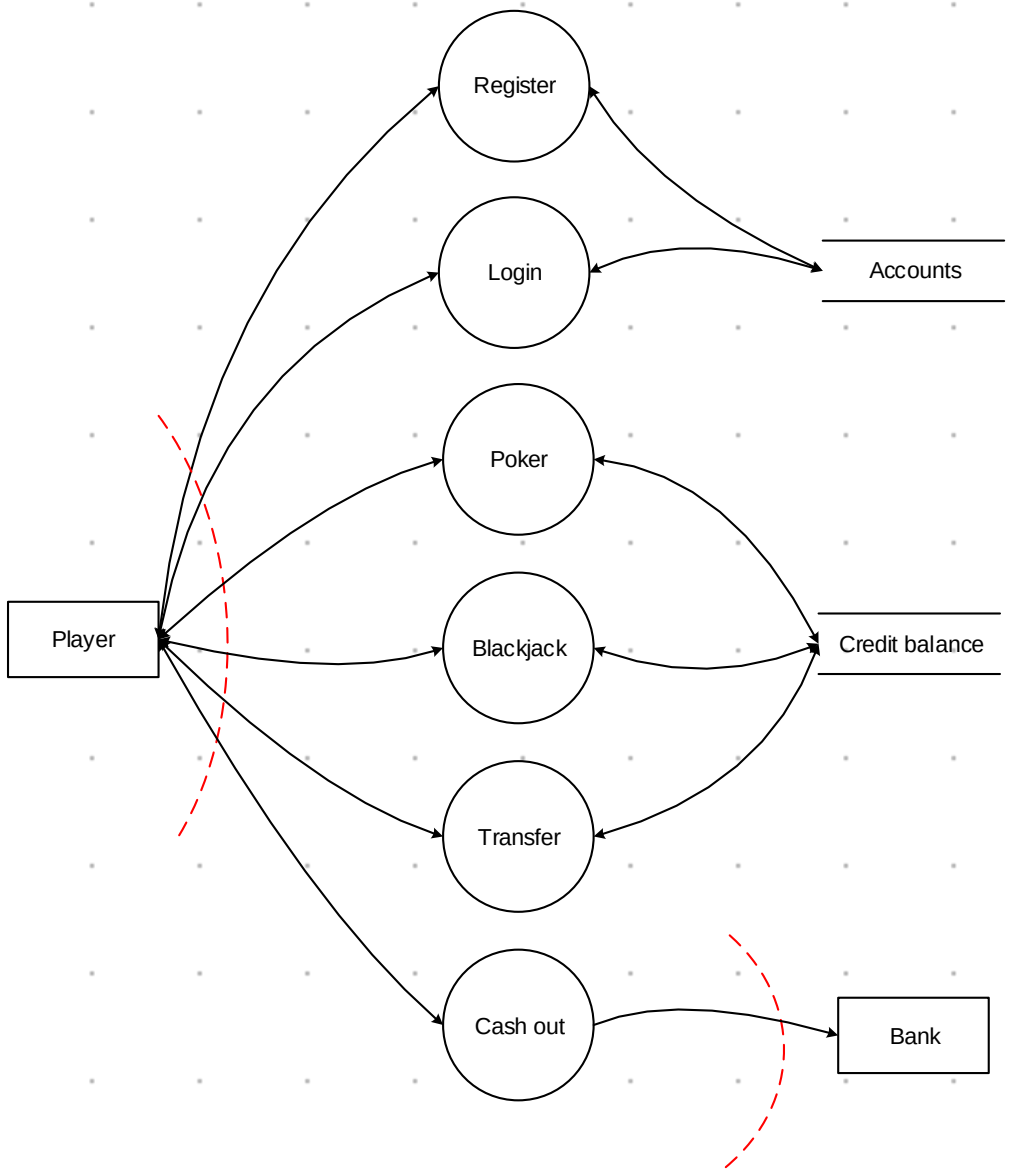
- **Entité externe**: Individu ou système externe qui communique (envoi / réception de données) avec le systéme étudié.
- **Processus:** Tout processus qui modifie les données, produisant un résultat.
- **Lieux de stockage:** Entrepôt de données qui stocke l'information pour un usage ultérieur.
- **Flux de données:** La route qui est empruntée par les données entre les entités externes, les processus et le lieux de stockage

Etude de cas



Fonctionalités de l'application

- Enregistrement
- Authentification
- Blackjack
- Poker
- Transfert de jetons aux autres joueurs
- Virement des gains vers une banque
- Déconnexion



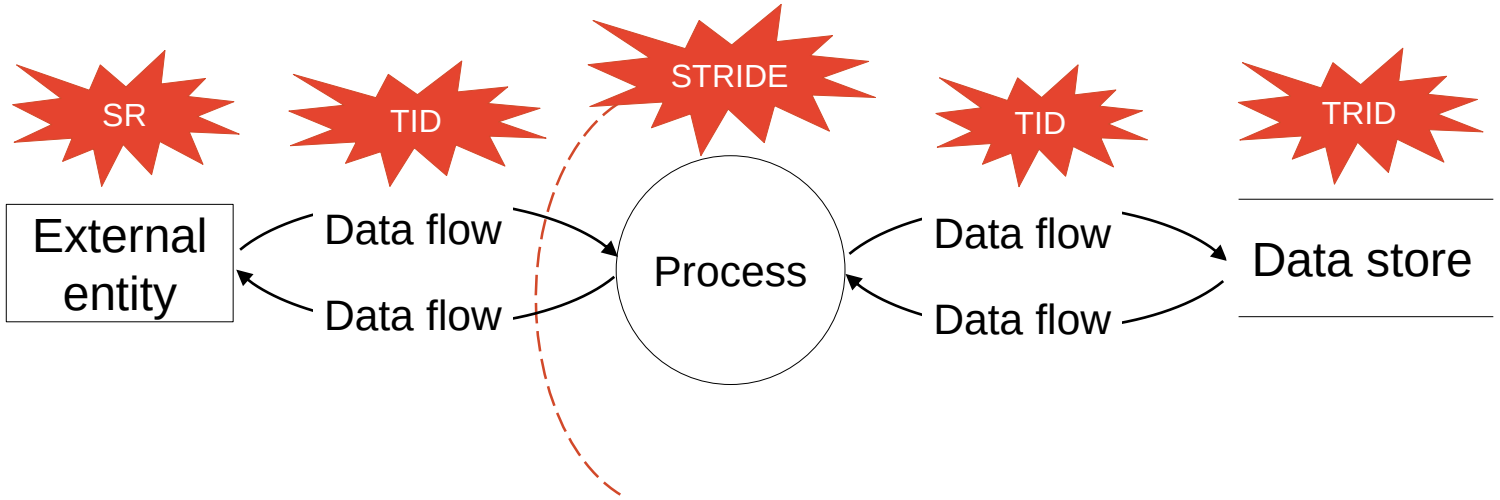
Biens informationnels

Bien informationnel	C	I	A
Crédits		X	X
Montants pariés		X	X
Cartes des joueurs		X	X
Cartes du casino	X	X	X
Données personnelles des joueurs	X	X	X

Scénarios de menace

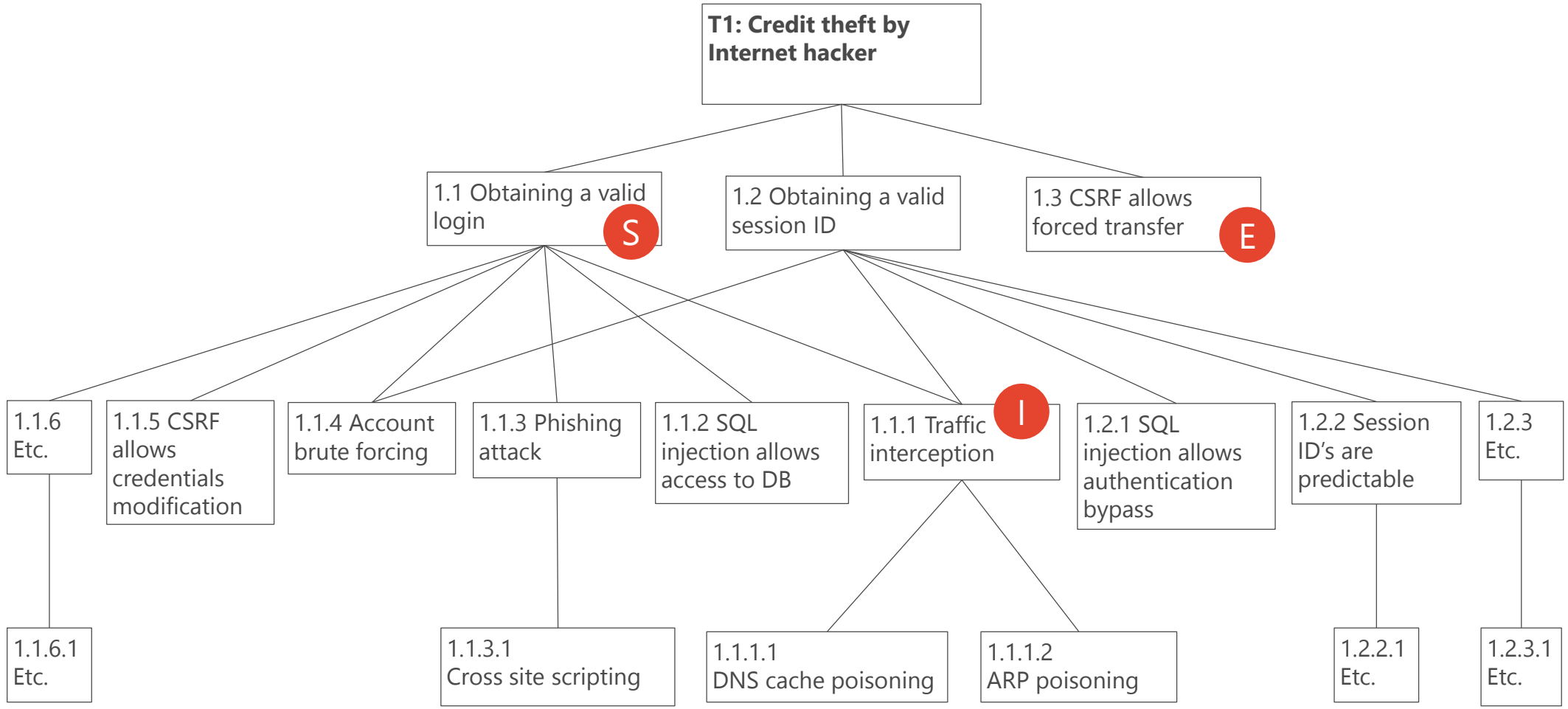
#	Scénario	Agents de menace
T1	Vols de crédits	Joueur, Internet hacker
T2	Vol de données personnelles	Joueur, Internet hacker, concurrent
T3	Manipulation d'un jeu	Joueur
T4	Déni de service	Concurrent

STRIDE

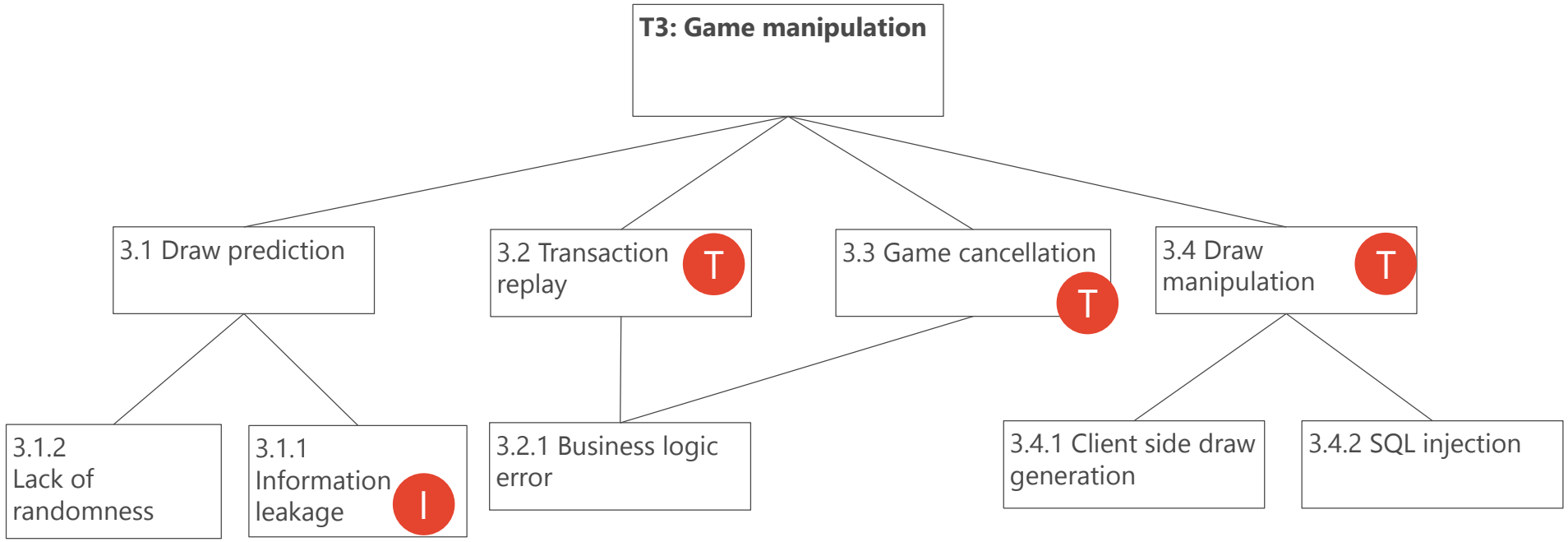


	S Spoofing	T Tampering	R Repudiation	I Information disclosure	D Denial of service	E Elevation of privilege
External entity	✓		✓			
Process	✓	✓	✓	✓	✓	✓
Data store		✓	✓	✓	✓	
Data flow		✓		✓	✓	

Arborescence des menaces



Arborescence des menaces

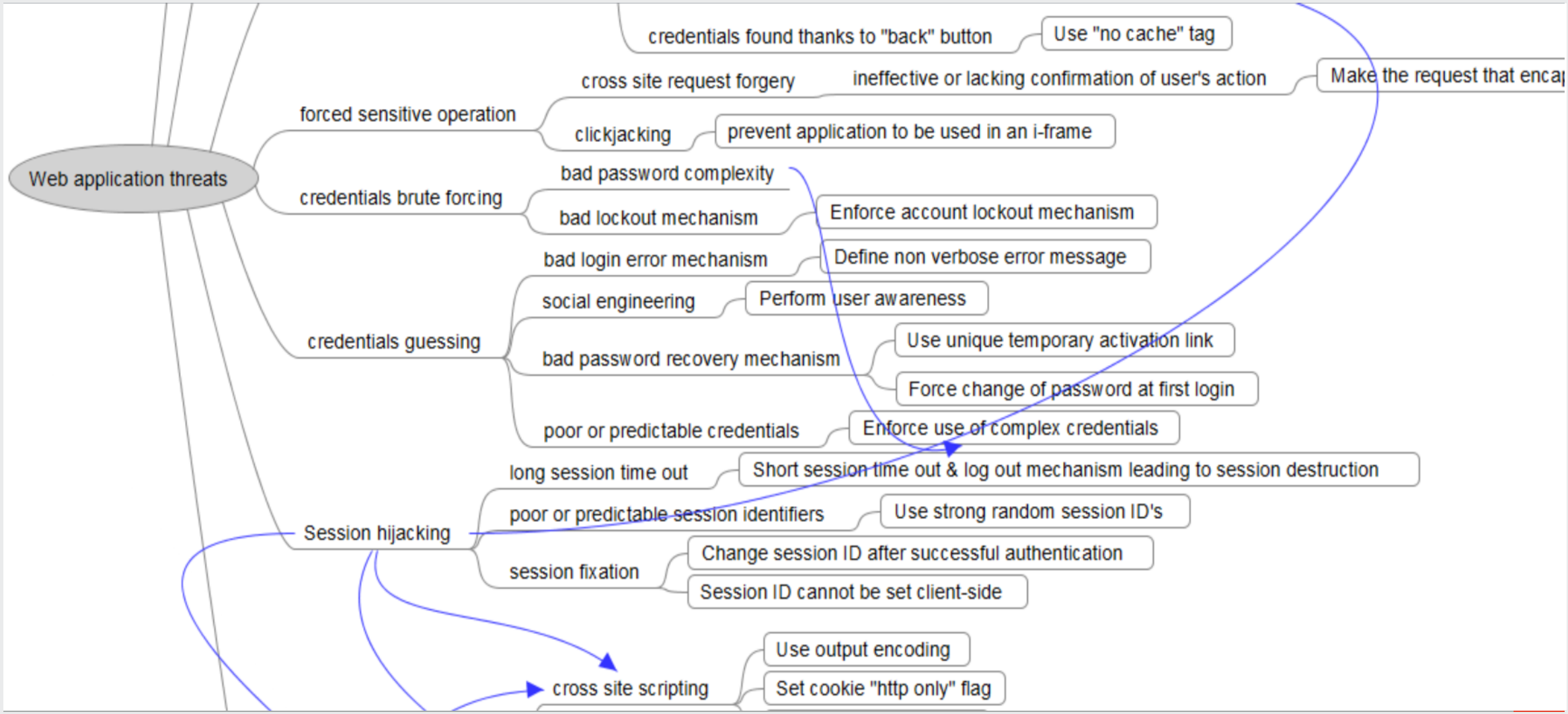


Limites identifiées

- Activité chronophage, fastidieuse, nécessitant des connaissances en hacking
- Produit des rapports pléthoriques
- Ne supporte pas la montée en maturité des équipes de développement
- Ne traite souvent que les menaces humaines intentionnelles

Industrialisation de la modélisation des menaces

Arbre des menaces génériques



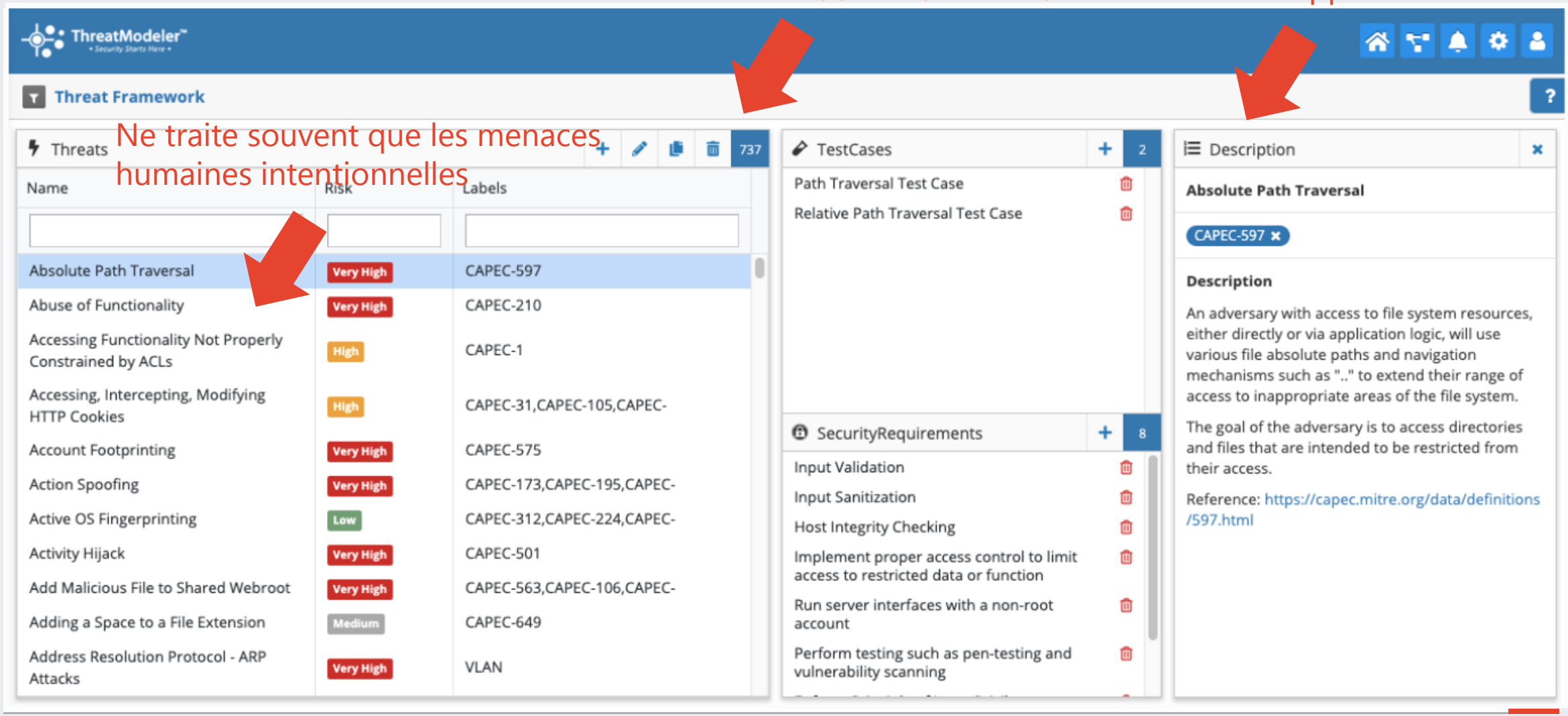
Outils

- Iriusrisk https://www.continuumsecurity.net/
- Microsoft TMT https://blogs.msdn.microsoft.com/secdevblog/2017/04/21/whats-new-with-microsoft-threat-modeling-tool-preview/
- SecuriCAD https://www.foreseeti.com/
- SD Elements https://www.securitycompass.com/sdelements
- Threat modeler http://threatmodeler.com

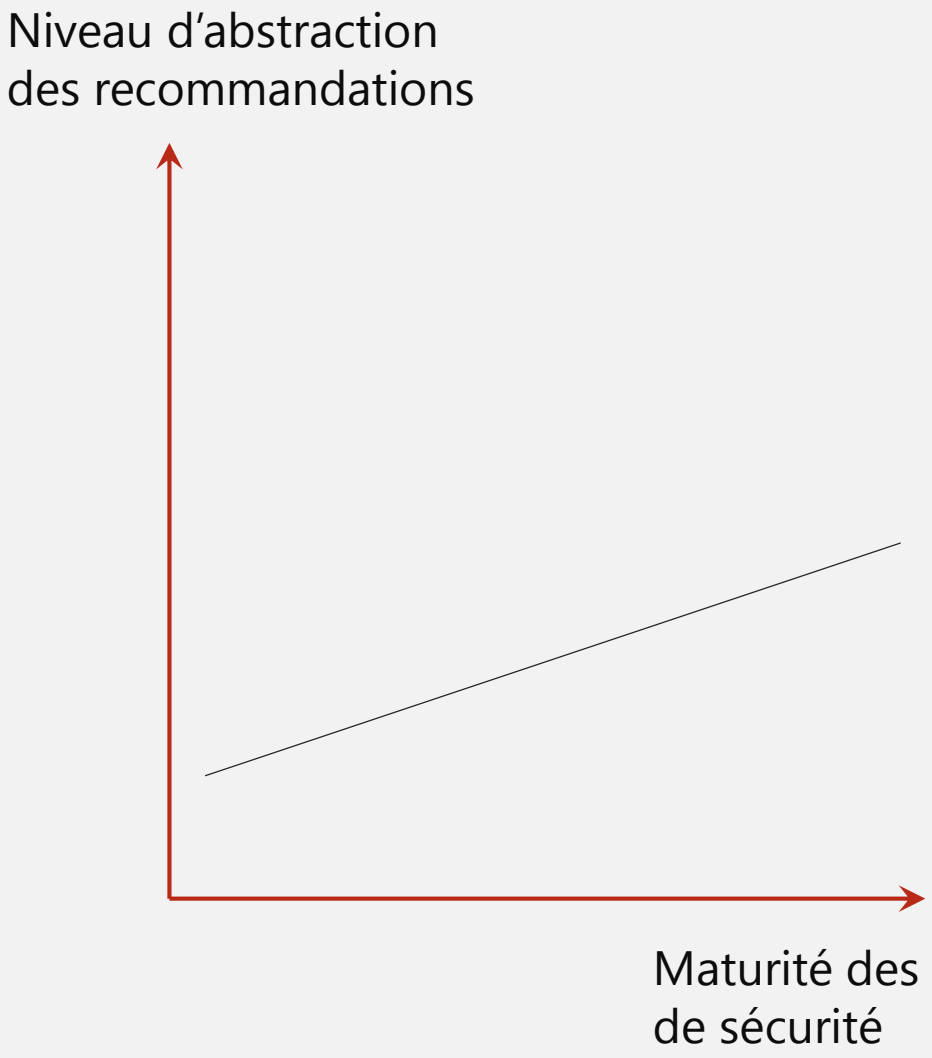
Limites identifiées - illustration

Produit des rapports pléthoriques

Ne supporte pas la montée en maturité des équipes de développement



Evolution des besoins en termes de modélisation des menaces



Menace	Vecteur d'attaque	Mitigation
Vol des identifiants	SQL injection	• Requêtes paramétrées
Vol des identifiants	XSS	• Output encoding
Etc.	Etc.	• Etc.

Menace	Vecteur d'attaque	Mitigation
Vol des identifiants	Attaque sur la couche applicative	• Pratiques de développement sécurisées
Etc.	Etc.	

Granularité des recommandations dans un modèle de menaces

e.g. Journalisation et surveillance:
- Journaliser toute tentative d'accès
- Stocker les journaux séparément
- Vérifier l'intégrité des lods
- Conserver les journaux durant 1 an
- Etc.

```
If (COBIT_maturity >=2)
```

Spécificités de l'application (métier / technologiques)

Pratiques immatures dans l'organisation

Pratiques matures (socle de sécurité / security baseline)

Fournir des recommandations détaillées

Se référer aux processus d'entreprise

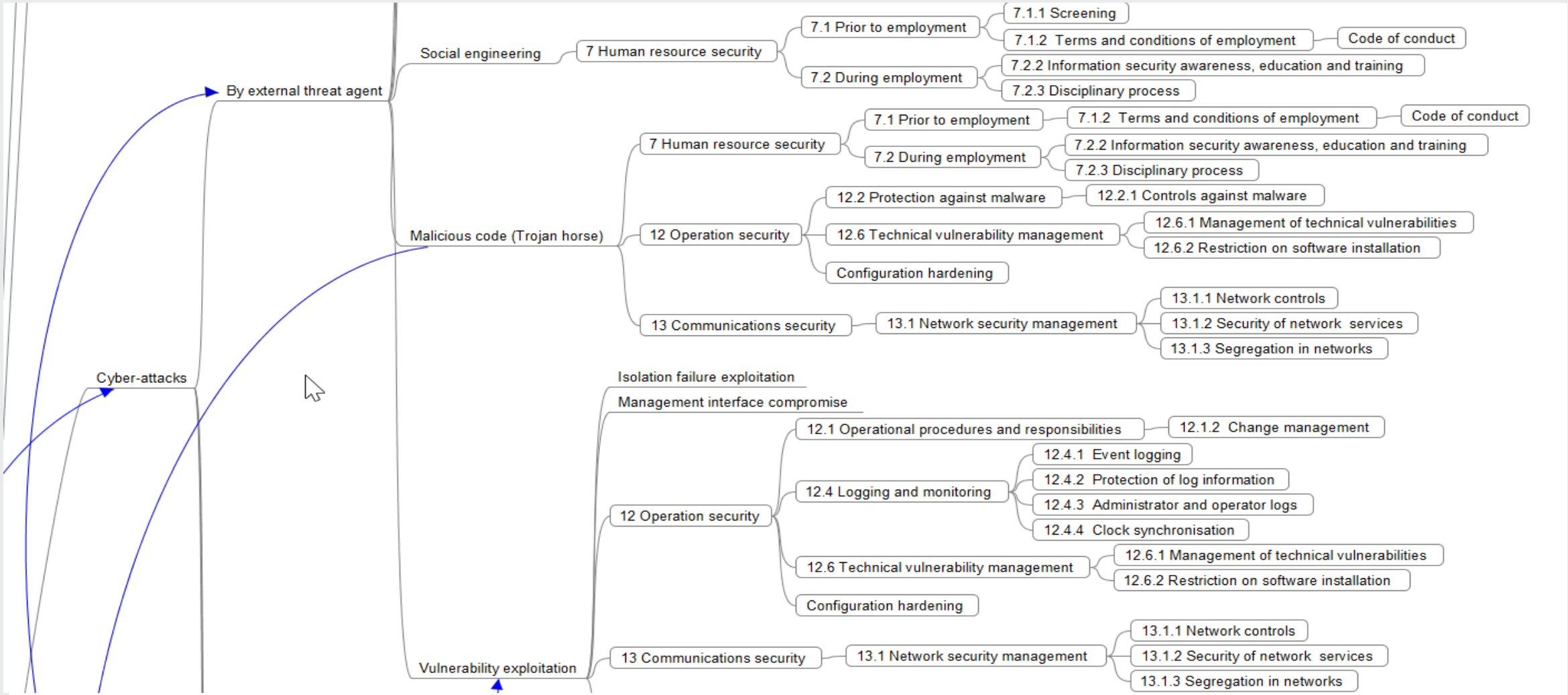
e.g. ISO27001
- A9.1.1 Access Control Policy
- Etc.

Profils de menaces

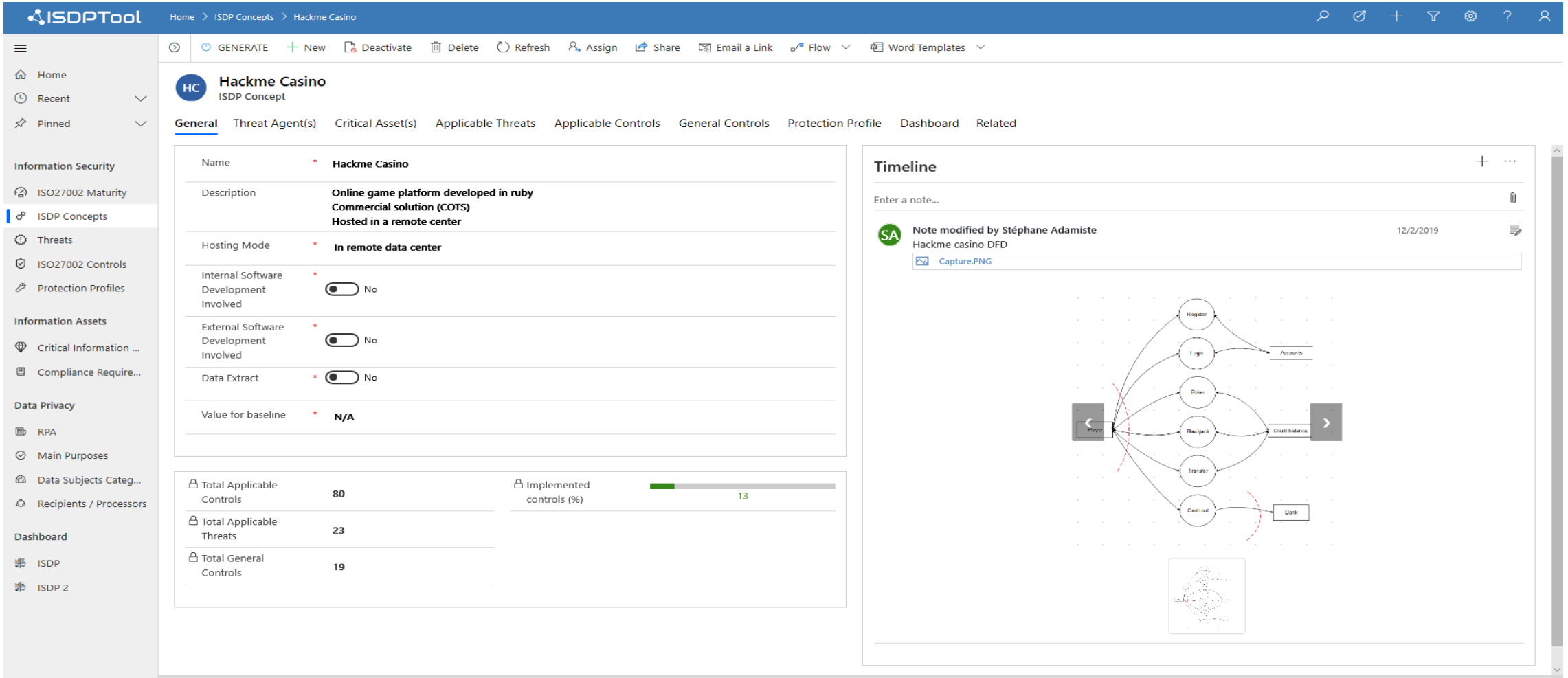
114 mesures
Parfois peu explicites

Item	Menaces	Mitigations	Mesures ISO27001
Base de données	• Accès non autorisé	• Authentification • Autorisation • Audit • Hardening	• 7.1.1 Vérification des antécédents • 9.1 Besoins métier en contrôle d'accès • 9.2 Gestion des accès utilisateurs • 9.3 Responsabilités des utilisateurs • 9.4 Contrôle d'accès aux systèmes et applications • 10.1 Contrôles cryptographiques • 12.3 Backup • 12.6 Gestion des vulnérabilités techniques • 17.2 Redondances • Etc.
	• Accès non autorisé par un admin malveillant	• Chiffrement au niveau applicatif • Stockage distant des journaux	
	• Vol de support physique	• Transparent Data Encryption (TDE) • Sécurité physique	
	• Perte ou corruption de données	• Backups • DRP	
	• Exploitation de vulnerabilité	• Patch management • Hardening	
	• Etc.	• Etc.	

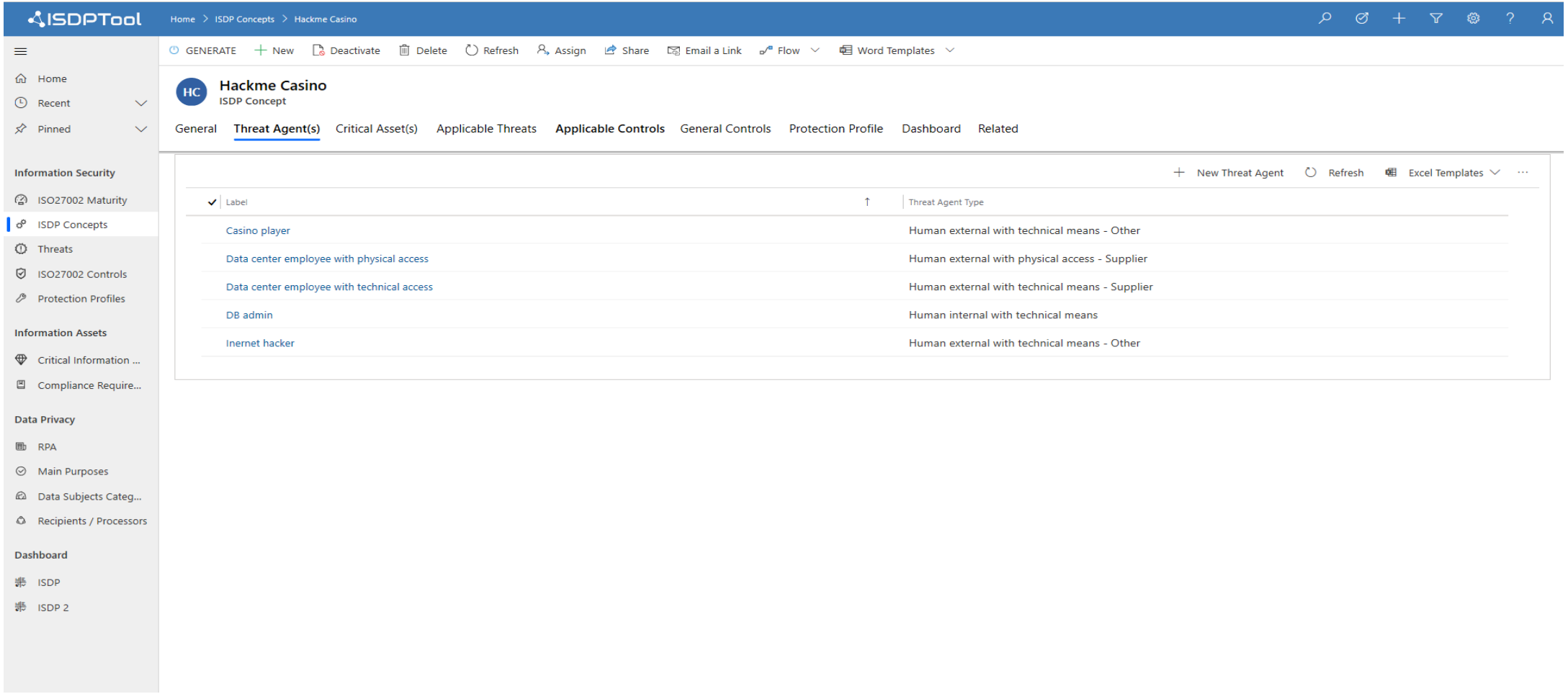
Catalogue de menaces & mitigations ISO27001



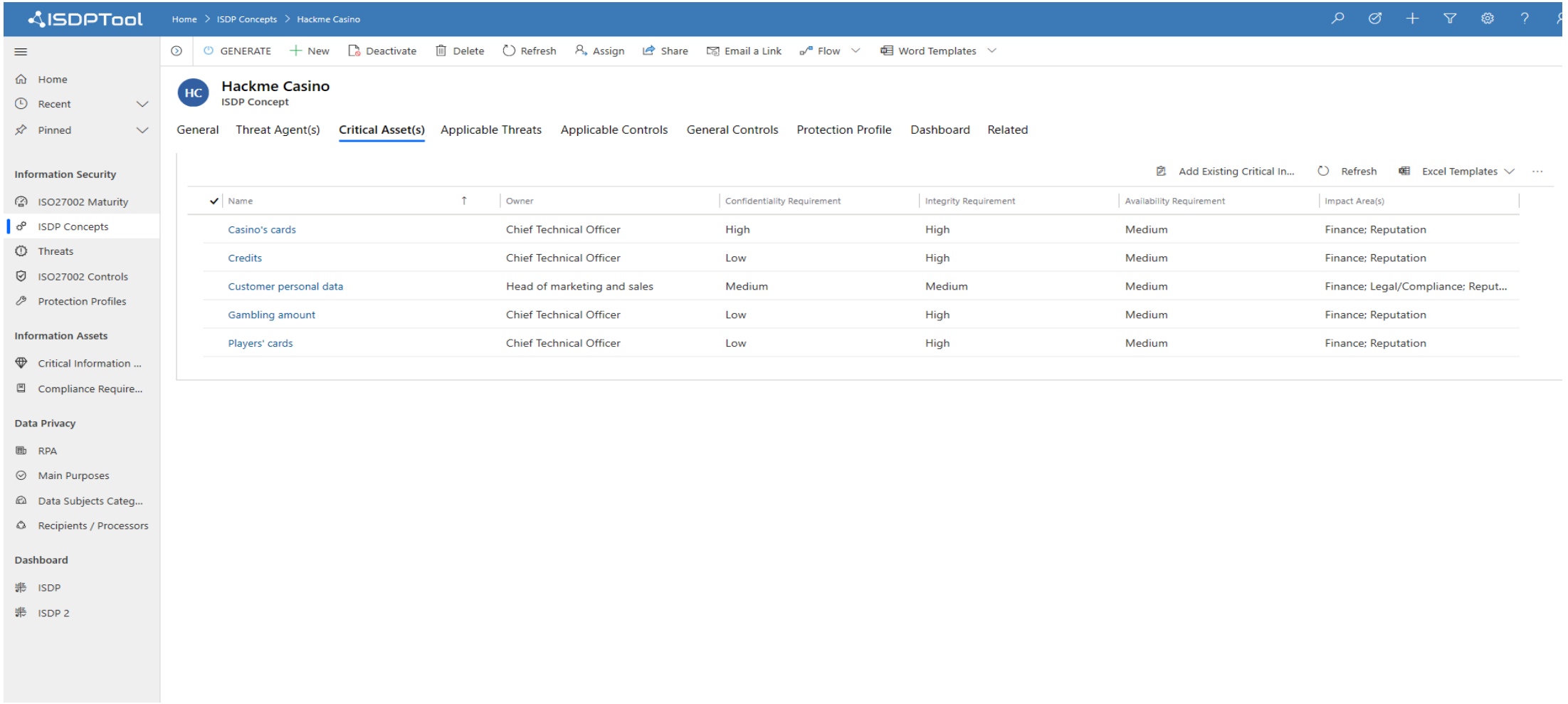
Démo outil ISDPTool



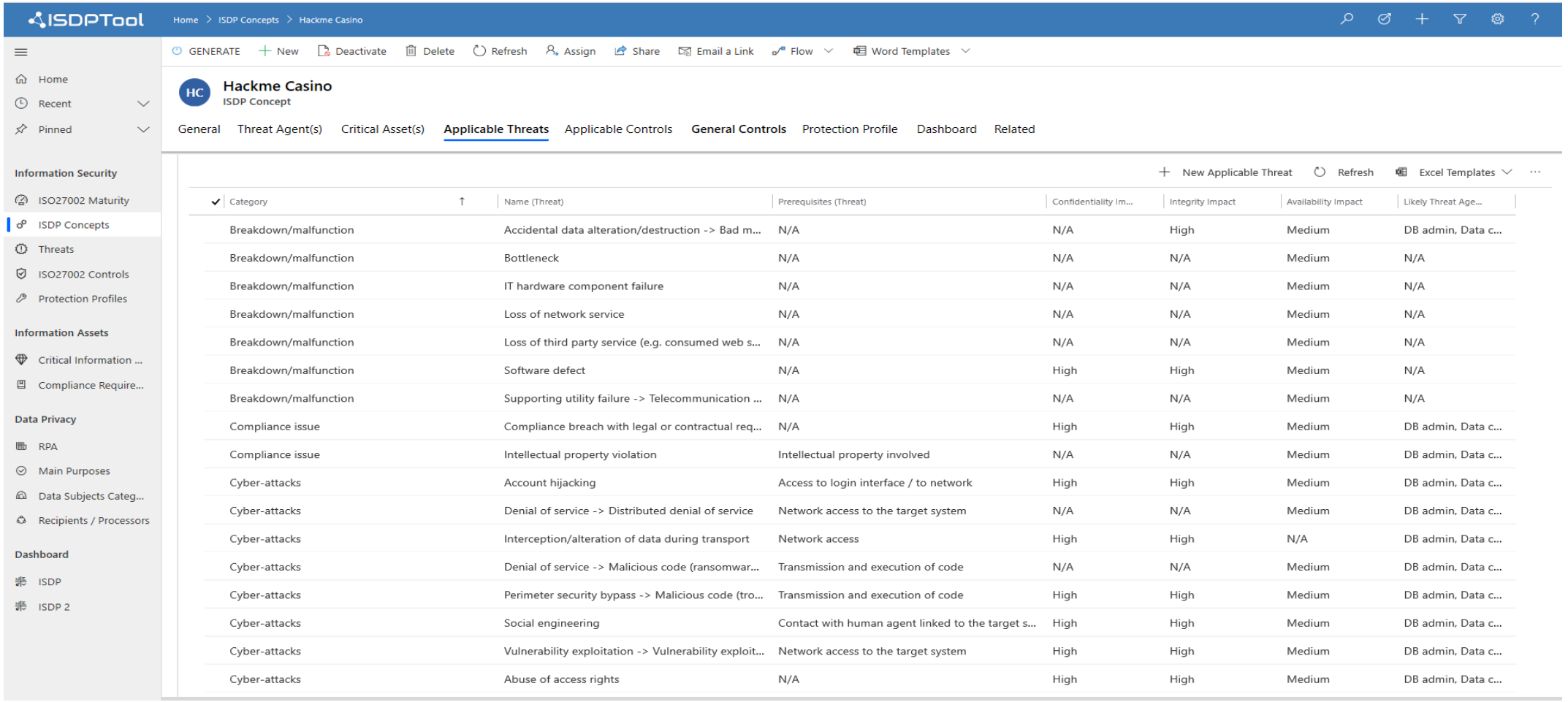
Démo outil ISDPTool



Démo outil ISDPTool

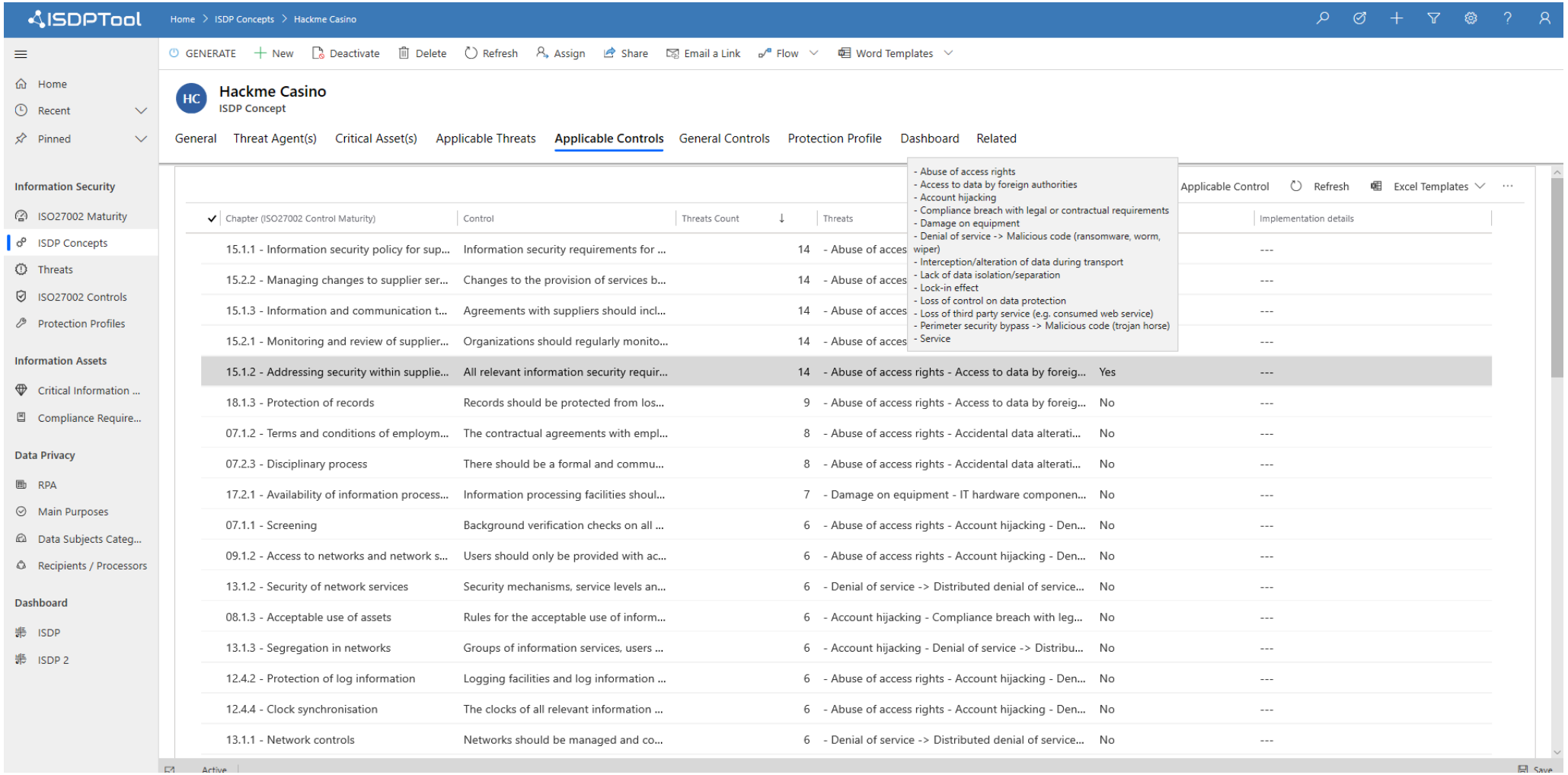


Démo outil ISDPTool



Category	Name (Threat)	Prerequisites (Threat)	Confidentiality Im...	Integrity Impact	Availability Impact	Likely Threat Age...
Breakdown/malfunction	Accidental data alteration/destruction -> Bad m...	N/A	N/A	High	Medium	DB admin, Data c...
Breakdown/malfunction	Bottleneck	N/A	N/A	N/A	Medium	N/A
Breakdown/malfunction	IT hardware component failure	N/A	N/A	N/A	Medium	N/A
Breakdown/malfunction	Loss of network service	N/A	N/A	N/A	Medium	N/A
Breakdown/malfunction	Loss of third party service (e.g. consumed web s...	N/A	N/A	N/A	Medium	N/A
Breakdown/malfunction	Software defect	N/A	High	High	Medium	N/A
Breakdown/malfunction	Supporting utility failure -> Telecommunication ...	N/A	N/A	N/A	Medium	N/A
Compliance issue	Compliance breach with legal or contractual req...	N/A	High	High	Medium	DB admin, Data c...
Compliance issue	Intellectual property violation	Intellectual property involved	N/A	N/A	Medium	DB admin, Data c...
Cyber-attacks	Account hijacking	Access to login interface / to network	High	High	Medium	DB admin, Data c...
Cyber-attacks	Denial of service -> Distributed denial of service	Network access to the target system	N/A	N/A	Medium	DB admin, Data c...
Cyber-attacks	Interception/alteration of data during transport	Network access	High	High	N/A	DB admin, Data c...
Cyber-attacks	Denial of service -> Malicious code (ransomwar...	Transmission and execution of code	N/A	N/A	Medium	DB admin, Data c...
Cyber-attacks	Perimeter security bypass -> Malicious code (tro...	Transmission and execution of code	High	High	Medium	DB admin, Data c...
Cyber-attacks	Social engineering	Contact with human agent linked to the target s...	High	High	Medium	DB admin, Data c...
Cyber-attacks	Vulnerability exploitation -> Vulnerability exploit...	Network access to the target system	High	High	Medium	DB admin, Data c...
Cyber-attacks	Abuse of access rights	N/A	High	High	Medium	DB admin, Data c...

Démo outil ISDPTool



Intégrer la modélisation des menaces dans la gouvernance sécurité d’entreprise - Proposition

Organisation type

Fonction sécurité

Acteur	Rôle	Output
RSSI	• Gère le SMSI	• Risques d'entreprise • Maturité des mesures de sécurité ISO27001 • Plans d'action sécurité
Expert sécurité	• Assiste les projets	• Cf Gestion de projet

Gestion de projet

Acteur	Rôle	Output
Rep. métier	• Définit la valeur des biens informationnels	• Exigences CIA
Expert sécurité	• Coordonne les aspects sécurité et protection données personnelles • Réalise les activités SDLC	• Menaces applicables • Liste des mesures de sécurité à appliquer dans le projet • Revue d'architecture, guides, tests
Chef de projet	• Coordonne l'implémentation des mesures de sécurité	• Liste des mesures implémentées / non-implémentées

Mutualisation des efforts

Modélisation des menaces dans les projets

- Biens informationnels
- Menaces / risques
- Contre-mesures

Gestion de la sécurité de l'information

- Biens informationnels
- Risk management (p. ex. ISO27005)
- Mesures de sécurité (p. ex. ISO27001)

Protection des données personnelles

- Biens informationnels (données personnelles)
- Data Protection Impact Assessment
- Mesures techniques et informationnelles (p. ex. RGPD Art. 32)

Conclusions

Conclusions

- La modélisation des menaces est une technique à forte valeur ajoutée
  - Permet de fixer le périmètre de la sécurité dans les projets
  - Penser à intégrer la valeur des données
- Elle est toutefois souvent cantonnée au monde du développement
- Il faut chercher à rendre le processus plus simple
  - Liste de menaces standard
  - Mapping automatique menaces <-> mesures de sécurité
  - Niveau d'abstraction plus élevé
  - Prise en compte de la maturité des processus sécurité d'entreprise
- Opportunité de lier sécurité dans les projets avec sécurité d'entreprise
  - Référentiel commune (p. ex. ISO27001)

Merci de votre attention!

Contact:

Mail: sadamiste@hotmail.com
LinkedIn: Stéphane Adamiste
Twitter: @sadamiste