

# **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

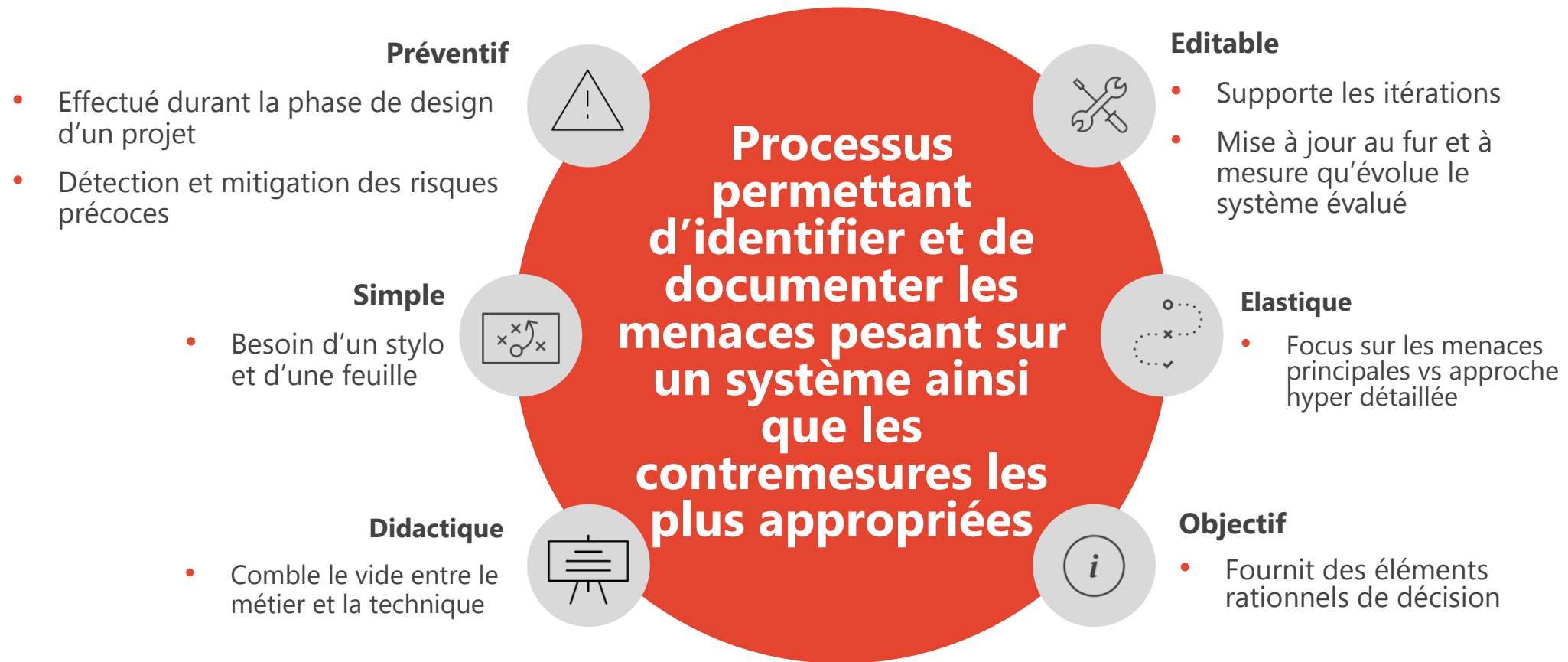
- Spécialiste sécurité de l'information et protection des données personnelles (expérience ~18 ans)
- Appréhende la sécurité de l'information d'un point de vue technique et métier
- #Audit, #Risk management #Conformité #Gouvernance

## 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



# 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

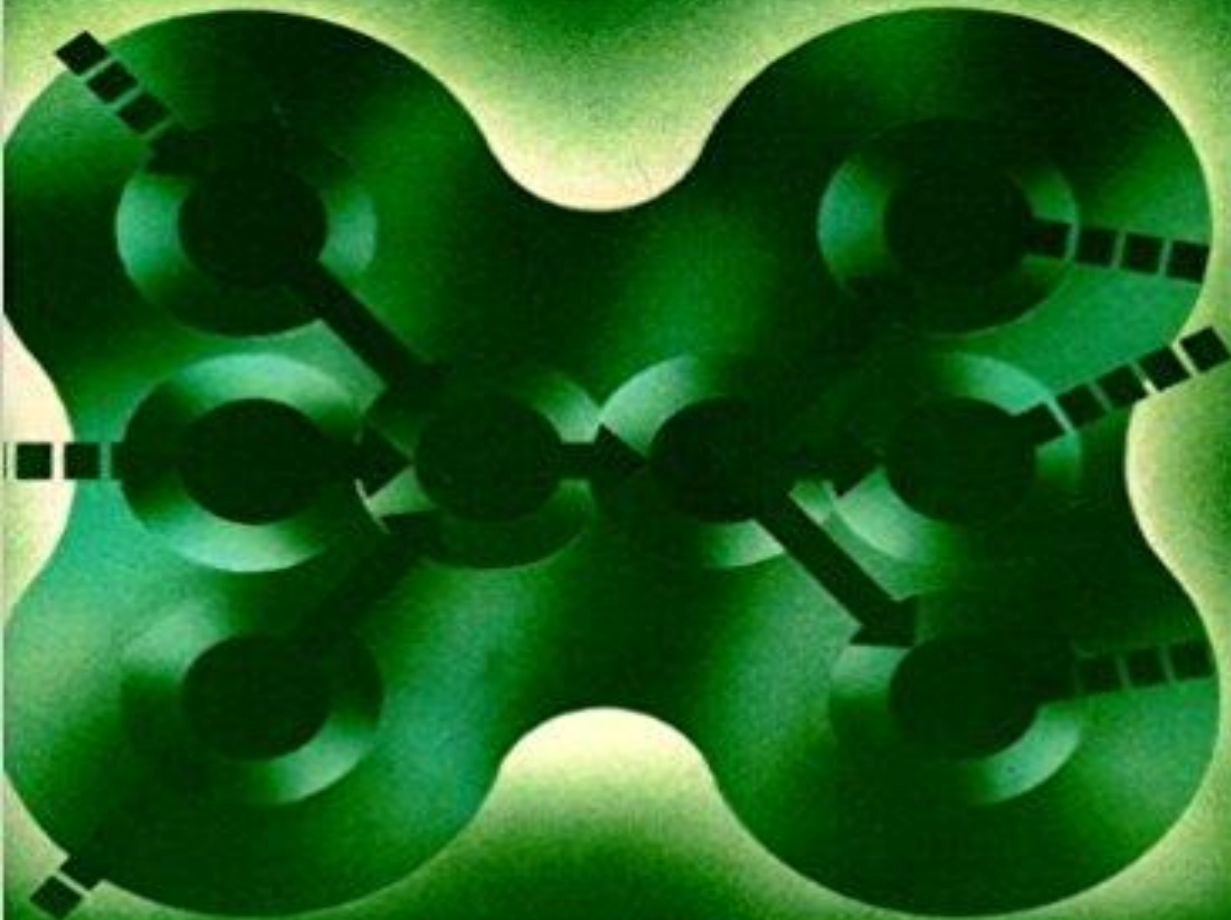
## Software-centric

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

# Structured Design

Fundamentals of a Discipline of Computer  
Program and Systems Design

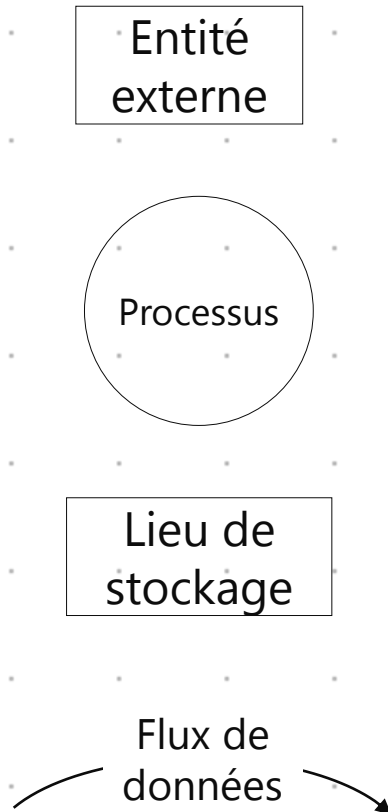
Edward Yourdon / Larry L. Constantine



YOURDON PRESS COMPUTING SERIES

## 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 système 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

Please login

Login:

Password:

**LOGIN**

[<< Register](#)



## Welcome to HacmeCasino, the best Gambling Site on the Net

Here at HacmeCasino, we aim to provide the best user experience on the web. Using Web 2.0-friendly technologies like AJAX, HacmeCasino is a state of the art online gaming experience that has to be tried to be believed. Try your hand at poker, or take a spin at the roulette wheel. Rest assured that HacmeCasino will give you the most entertaining, enjoyable, and secure user experience available online.



Fancy some blackjack?  
HacmeCasino has you covered, with the most exciting, high-stakes blackjack game this side of the computer monitor! Fun for all!



Howdy, pardner! Poker is all the rage, and HacmeCasino is ready to serve your online gaming needs, providing a state of the art online poker experience.



Round and round it goes...  
Roulette is a game for novices and experts alike to let go and have some fun. Take life for a spin, and let it ride at HacmeCasino!

## Fonctionnalités de l'application

— Enregistrement

— Authentification

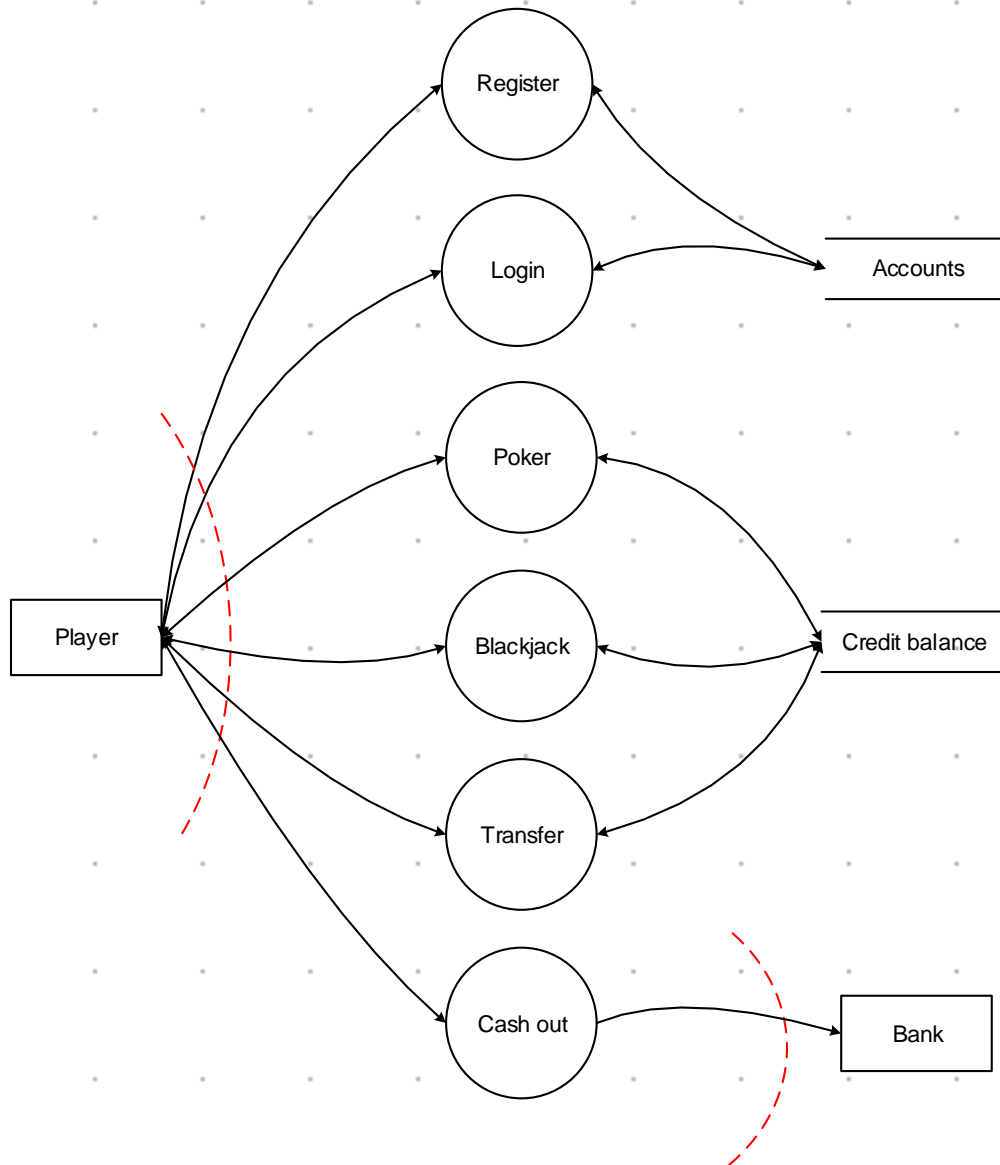
— Blackjack

— Poker

— Transfert de jetons aux autres joueurs

— Virement des gains vers une banque

— Déconnexion



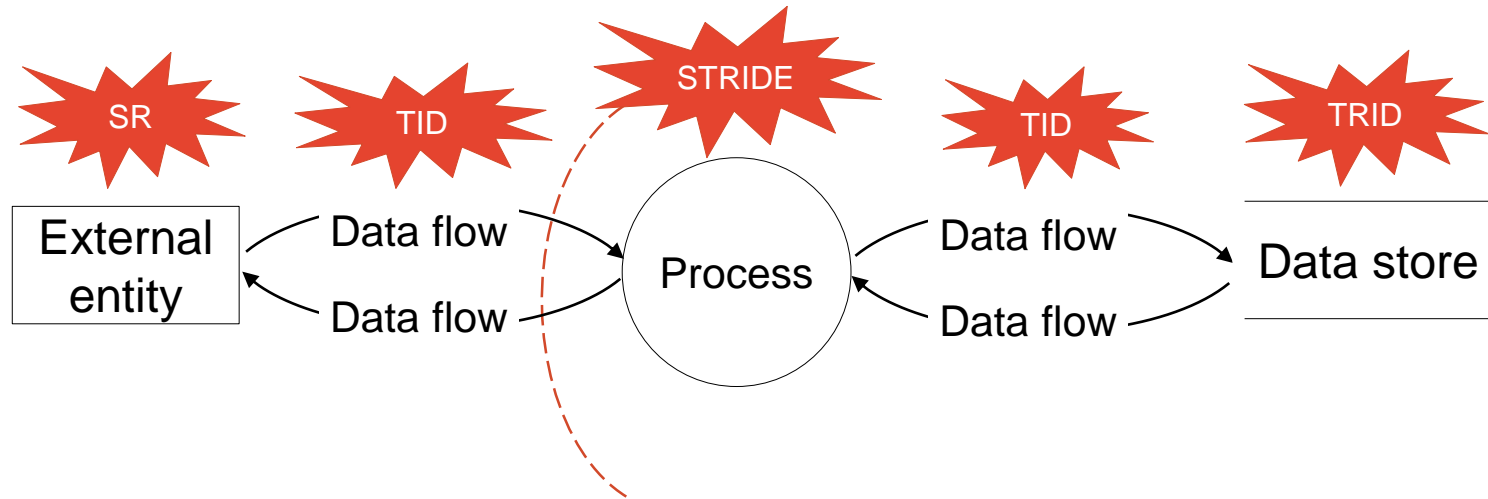
## Biens informationnels

| 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

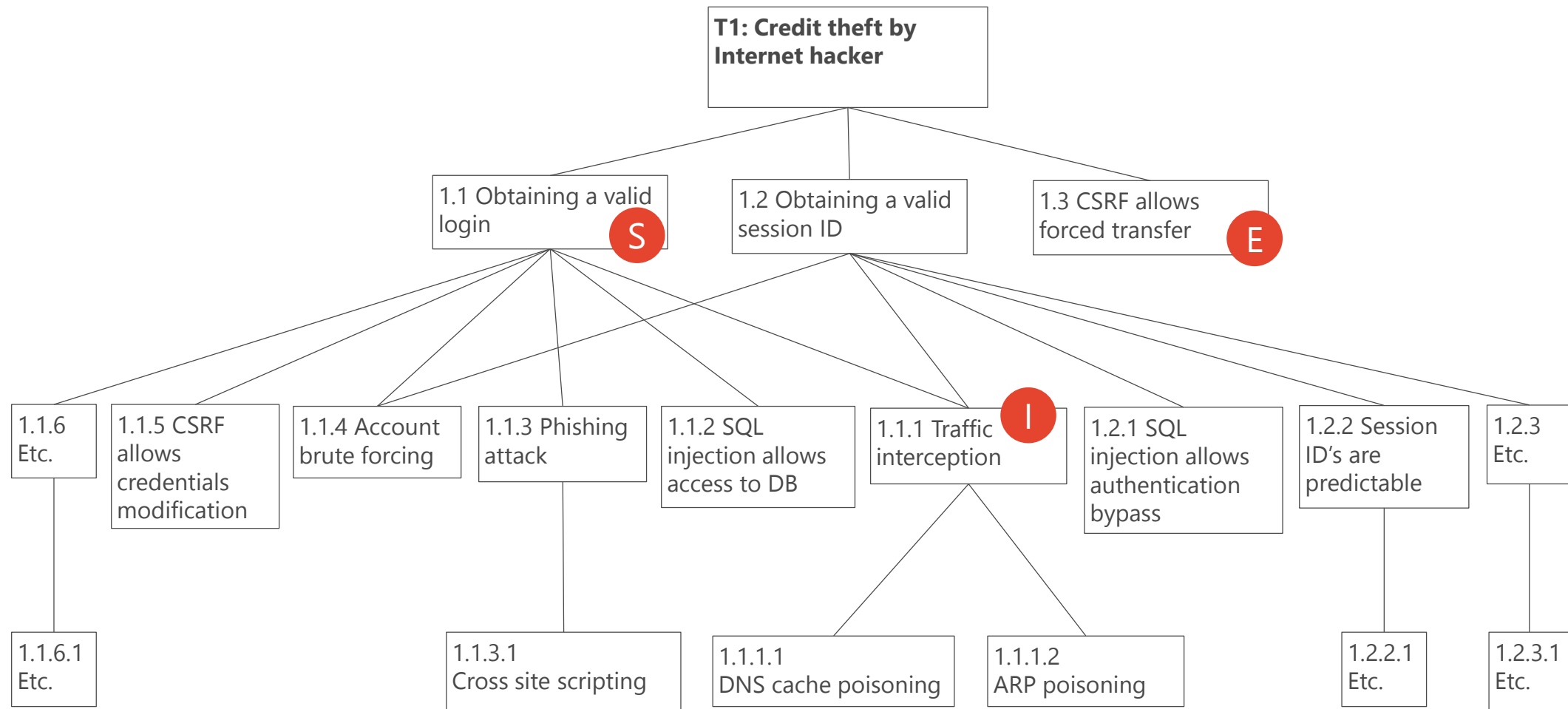
| #  | Scénario                    | Agents de menace                    |
|----|-----------------------------|-------------------------------------|
| T1 | Vols de crédits             | Joueur, Internet hacker             |
| T2 | Vol de données personnelles | Joueur, Internet hacker, concurrent |
|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

# STRIDE

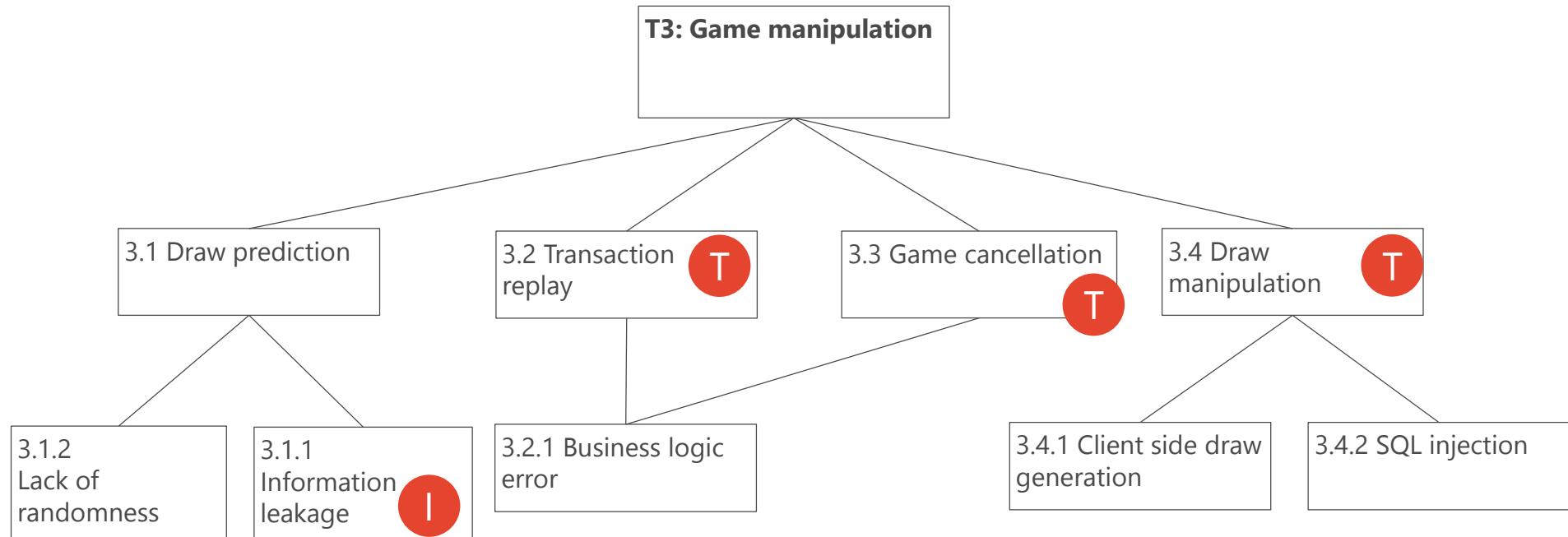


|                 | <b>S</b><br>Spoofing | <b>T</b><br>Tampering | <b>R</b><br>Repudiation | <b>I</b><br>Information disclosure | <b>D</b><br>Denial of service | <b>E</b><br>Elevation of privilege |
|-----------------|----------------------|-----------------------|-------------------------|------------------------------------|-------------------------------|------------------------------------|
| External entity | ✓                    |                       | ✓                       |                                    |                               |                                    |
| Process         | ✓                    | ✓                     | ✓                       | ✓                                  | ✓                             | ✓                                  |
| Data store      |                      | ✓                     | ✓                       | ✓                                  | ✓                             |                                    |
| Data flow       |                      | ✓                     |                         | ✓                                  | ✓                             |                                    |

# Arborescence des menaces



# Arborescence des menaces



A person wearing a light blue button-down shirt is seated at a dark wooden desk. They are holding a black pen and writing in a white notebook. A laptop is partially visible on the desk to their right. The background is a warm, orange-toned wall.

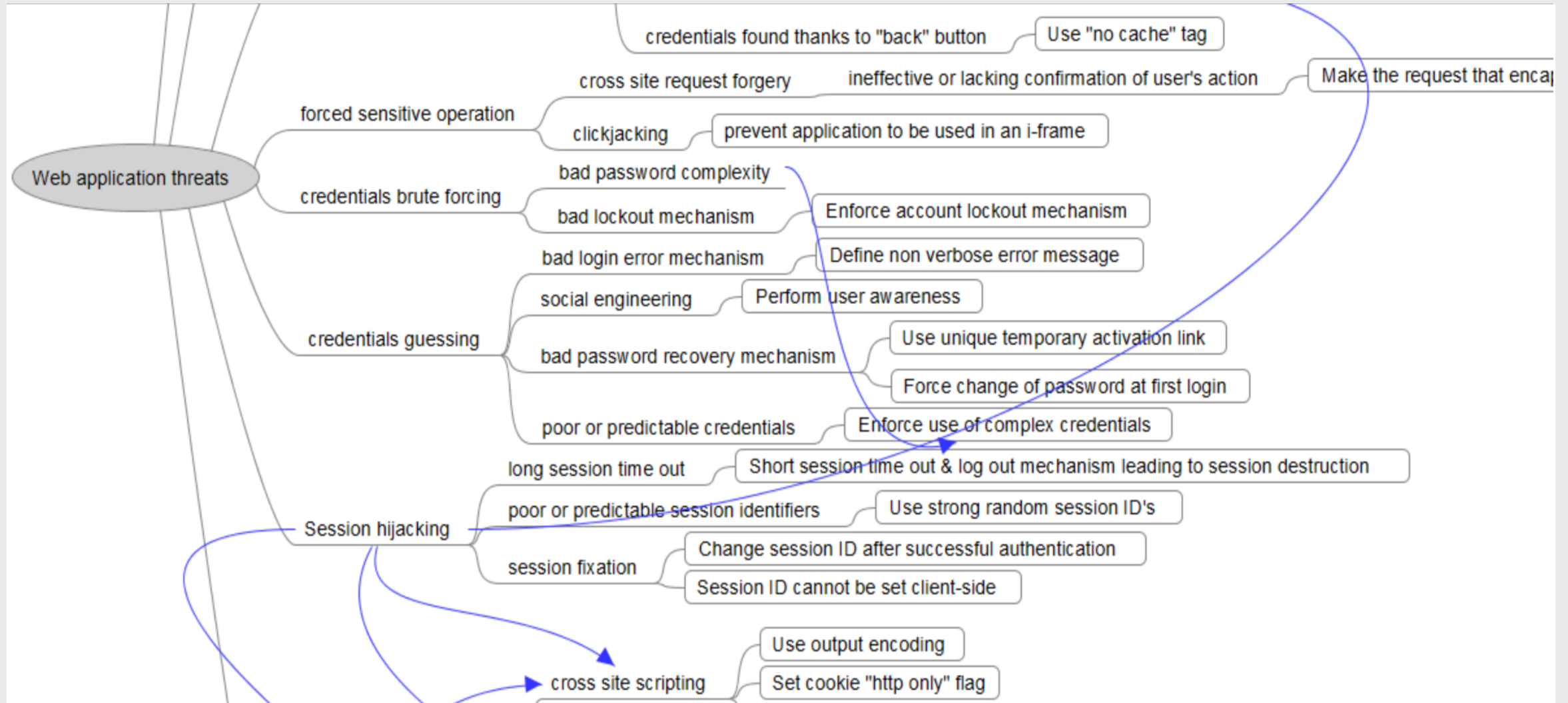
## Limites identifiées

- 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

The screenshot displays the ThreatModeler web application interface. The top navigation bar includes the ThreatModeler logo and a 'Threat Framework' dropdown. The main content area is divided into three panels. The left panel, titled 'Threats', contains a table with 737 items. The middle panel, titled 'TestCases', shows 2 items. The right panel, titled 'Description', provides details for the selected 'Absolute Path Traversal' threat, including its CAPEC-597 label and a detailed description of the adversary's goal.

| Name   | Risk      | Labels                       |
|--|-----------|------------------------------|
| Absolute Path Traversal                                  | Very High | CAPEC-597                    |
| Abuse of Functionality                                   | Very High | CAPEC-210                    |
| Accessing Functionality Not Properly Constrained by ACLs | High      | CAPEC-1                      |
| Accessing, Intercepting, Modifying HTTP Cookies          | High      | CAPEC-31, CAPEC-105, CAPEC-  |
| Account Footprinting                                     | Very High | CAPEC-575                    |
| Action Spoofing  | Very High | CAPEC-173, CAPEC-195, CAPEC- |
| Active OS Fingerprinting                                 | Low       | CAPEC-312, CAPEC-224, CAPEC- |
| Activity Hijack  | Very High | CAPEC-501                    |
| Add Malicious File to Shared Webroot                     | Very High | CAPEC-563, CAPEC-106, CAPEC- |
| Adding a Space to a File Extension                       | Medium    | CAPEC-649                    |
| Address Resolution Protocol - ARP Attacks                | Very High | VLAN                         |

**TestCases** (2 items):

- Path Traversal Test Case
- Relative Path Traversal Test Case

**SecurityRequirements** (8 items):

- Input Validation
- Input Sanitization
- Host Integrity Checking
- Implement proper access control to limit access to restricted data or function
- Run server interfaces with a non-root account
- Perform testing such as pen-testing and vulnerability scanning

**Description** (Absolute Path Traversal):

**CAPEC-597**

**Description**

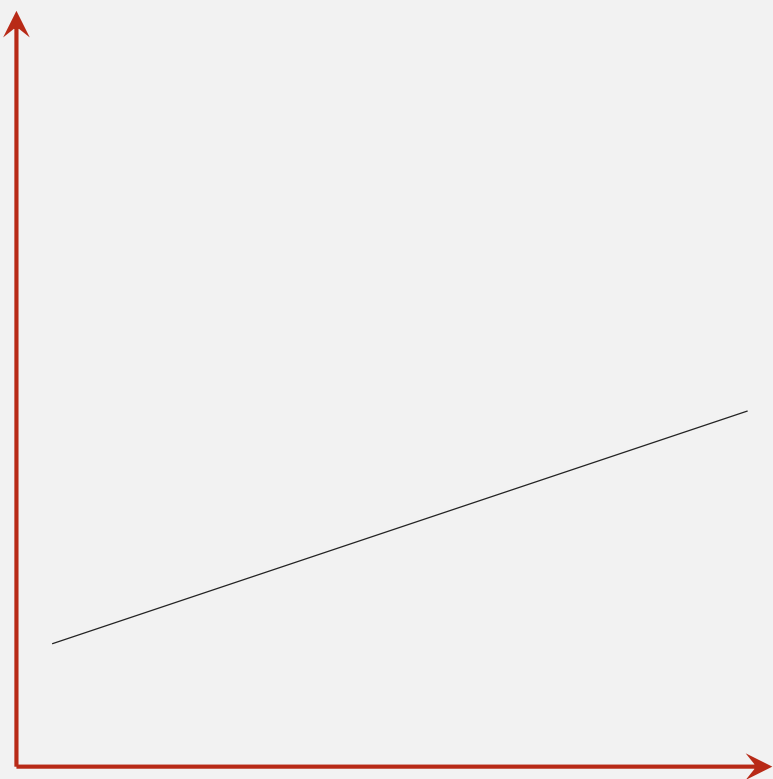
An adversary with access to file system resources, either directly or via application logic, will use various file absolute paths and navigation mechanisms such as ".." to extend their range of access to inappropriate areas of the file system.

The goal of the adversary is to access directories and files that are intended to be restricted from their access.

Reference: <https://capec.mitre.org/data/definitions/597.html>

# Evolution des besoins en termes de modélisation des menaces

Niveau d'abstraction des recommandations



Maturité des processus de sécurité

| Menace               | Vecteur d'attaque | Mitigation   |
|----------------------|-------------------|--|
| Vol des identifiants | SQL injection     | <ul style="list-style-type: none"><li>Requêtes paramétrées</li></ul> |
| Vol des identifiants | XSS               | <ul style="list-style-type: none"><li>Output encoding</li></ul>      |
| Etc.                 | Etc.              | <ul style="list-style-type: none"><li>Etc.</li></ul>                 |



| Menace               | Vecteur d'attaque                 | Mitigation  |
|----------------------|-----------------------------------|---|
| Vol des identifiants | Attaque sur la couche applicative | <ul style="list-style-type: none"><li>Pratiques de développement sécurisées</li></ul> |
| 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 logs
- 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.

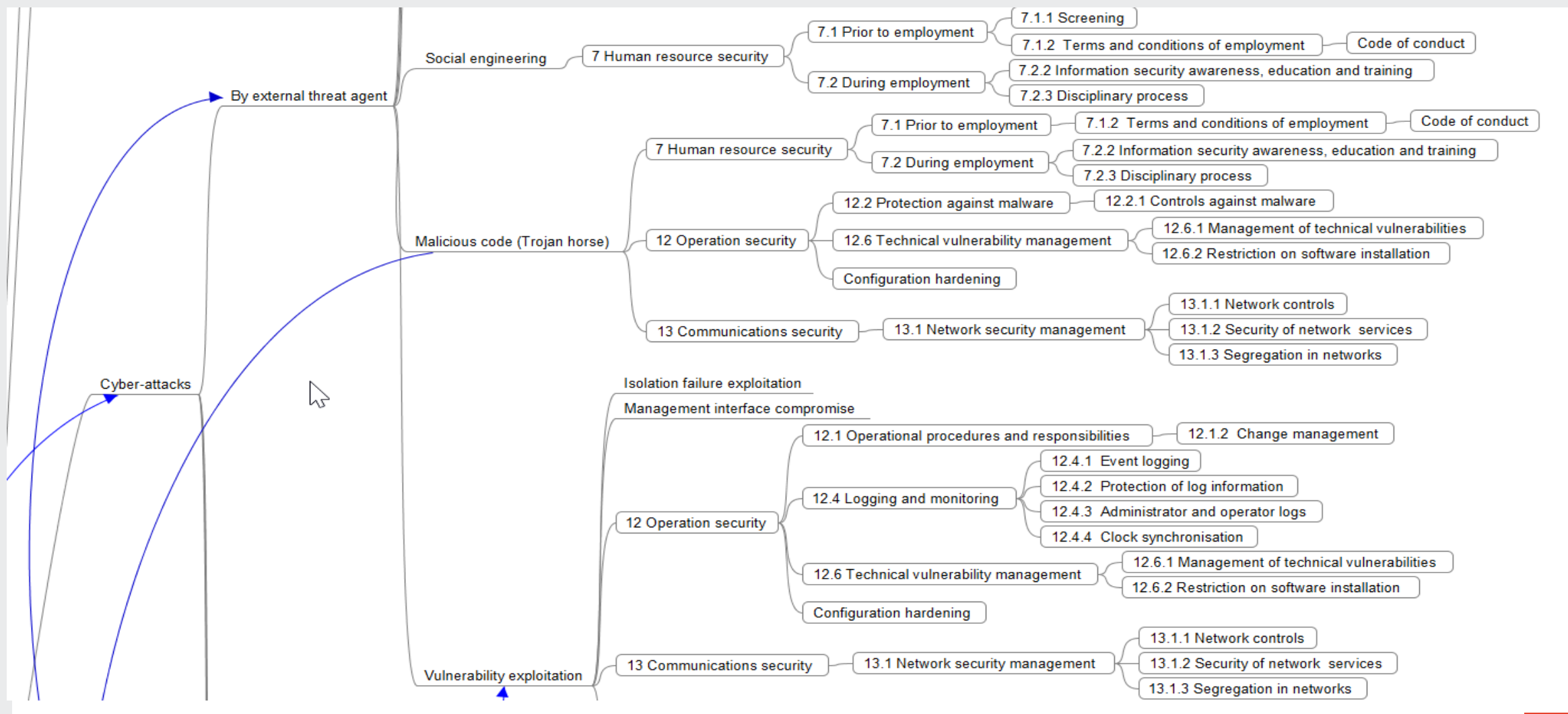
# Profils de menaces

| Item            | Menaces   | Mitigations  | Mesures ISO27001  |
|-----------------|---|--|---|
| Base de données | <ul style="list-style-type: none"> <li>Accès non autorisé</li> </ul>                          | <ul style="list-style-type: none"> <li>Authentification</li> <li>Autorisation</li> <li>Audit</li> <li>Hardening</li> </ul> | <ul style="list-style-type: none"> <li>7.1.1 Vérification des antécédents</li> <li>9.1 Besoins métier en contrôle d'accès</li> <li>9.2 Gestion des accès utilisateurs</li> <li>9.3 Responsabilités des utilisateurs</li> <li>9.4 Contrôle d'accès aux systèmes et applications</li> <li>10.1 Contrôles cryptographiques</li> <li>12.3 Backup</li> <li>12.6 Gestion des vulnérabilités techniques</li> <li>17.2 Redondances</li> <li>Etc.</li> </ul> |
|                 | <ul style="list-style-type: none"> <li>Accès non autorisé par un admin malveillant</li> </ul> | <ul style="list-style-type: none"> <li>Chiffrement au niveau applicatif</li> <li>Stockage distant des journaux</li> </ul>  |   |
|                 | <ul style="list-style-type: none"> <li>Vol de support physique</li> </ul>                     | <ul style="list-style-type: none"> <li>Transparent Data Encryption (TDE)</li> <li>Sécurité physique</li> </ul>             |   |
|                 | <ul style="list-style-type: none"> <li>Perte ou corruption de données</li> </ul>              | <ul style="list-style-type: none"> <li>Backups</li> <li>DRP</li> </ul>   |   |
|                 | <ul style="list-style-type: none"> <li>Exploitation de vulnérabilité</li> </ul>               | <ul style="list-style-type: none"> <li>Patch management</li> <li>Hardening</li> </ul>                                      |   |
|                 | <ul style="list-style-type: none"> <li>Etc.</li> </ul>  | <ul style="list-style-type: none"> <li>Etc.</li> </ul>   |   |

114 mesures  
Parfois peu explicites



# Catalogue de menaces & mitigations ISO27001



# Démo outil ISDPTool

ISDPTool

Home > ISDP Concepts > Hackme Casino

🔍

🔗

+

🗑️

⚙️

?

👤

🏠 Home

🕒 Recent

📌 Pinned

Information Security

🕒 ISO27002 Maturity

🔗 ISDP Concepts

🕒 Threats

🛡️ ISO27002 Controls

🛡️ Protection Profiles

Information Assets

💎 Critical Information ...

📄 Compliance Require...

Data Privacy

📄 RPA

🕒 Main Purposes

📄 Data Subjects Categ...

👤 Recipients / Processors

Dashboard

📄 ISDP

📄 ISDP 2

🕒

🔄 GENERATE

➕ New

🚫 Deactivate

🗑️ Delete

🔄 Refresh

👤 Assign

🔗 Share

📧 Email a Link

📄 Flow

📄 Word Templates

HC

Hackme Casino

ISDP Concept

General

Threat Agent(s)

Critical Asset(s)

Applicable Threats

Applicable Controls

General Controls

Protection Profile

Dashboard

Related

Name

Hackme Casino

Description

Online game platform developed in ruby  
Commercial solution (COTS)  
Hosted in a remote center

Hosting Mode

In remote data center

Internal Software Development Involved

☐ No

External Software Development Involved

☐ No

Data Extract

☐ No

Value for baseline

N/A

🔒 Total Applicable Controls

80

🔒 Total Applicable Threats

23

🔒 Total General Controls

19

🔒 Implemented controls (%)

13

Timeline

Enter a note...

SA

Note modified by Stéphane Adamiste

Hackme casino DFD

12/2/2019

Capture.PNG

```
graph LR; Player[Player] --> Register((Register)); Player --> Login((Login)); Player --> Play((Play)); Player --> Blackjack((Blackjack)); Player --> Transfer((Transfer)); Player --> CashOut((Cash out)); Register --> Accounts[Accounts]; Login --> Accounts; Play --> Blackjack; Blackjack --> CreditBalance[Credit balance]; Transfer --> CreditBalance; CashOut --> User[User];
```



# Démo outil ISDPTool

The screenshot displays the ISDPTool web application interface. The top navigation bar includes the ISDPTool logo, a breadcrumb trail (Home > ISDP Concepts > Hackme Casino), and a series of utility icons (search, share, add, filter, settings, help, user). Below the navigation bar is a toolbar with actions like GENERATE, New, Deactivate, Delete, Refresh, Assign, Share, Email a Link, Flow, and Word Templates. The left sidebar contains a menu with categories: Information Security (ISO27002 Maturity, ISDP Concepts, Threats, ISO27002 Controls, Protection Profiles), Information Assets (Critical Information, Compliance Requirements), Data Privacy (RPA, Main Purposes, Data Subjects Categories, Recipients / Processors), and Dashboard (ISDP, ISDP 2). The main content area shows the 'Hackme Casino' ISDP Concept with tabs for General, Threat Agent(s), Critical Asset(s), Applicable Threats, Applicable Controls, General Controls, Protection Profile, Dashboard, and Related. The 'Threat Agent(s)' tab is active, displaying a table of threat agents. The table has columns for 'Label' and 'Threat Agent Type'. The data rows are: 'Casino player' (Human external with technical means - Other), 'Data center employee with physical access' (Human external with physical access - Supplier), 'Data center employee with technical access' (Human external with technical means - Supplier), 'DB admin' (Human internal with technical means), and 'Internet hacker' (Human external with technical means - Other). The table includes a 'New Threat Agent' button, a 'Refresh' button, and an 'Excel Templates' dropdown menu.

| Label                                      | Threat Agent Type                              |
|--|--|
| Casino player                              | Human external with technical means - Other    |
| Data center employee with physical access  | Human external with physical access - Supplier |
| Data center employee with technical access | Human external with technical means - Supplier |
| DB admin                                   | Human internal with technical means            |
| Internet hacker                            | Human external with technical means - Other    |

# Démo outil ISDPTool

The screenshot displays the ISDPTool interface. The top navigation bar includes the ISDPTool logo, a breadcrumb trail (Home > ISDP Concepts > Hackme Casino), and a set of utility icons (search, link, add, filter, settings, help, user). A secondary toolbar contains actions like GENERATE, New, Deactivate, Delete, Refresh, Assign, Share, Email a Link, Flow, and Word Templates. The left sidebar is a navigation menu with categories: Information Security (ISO27002 Maturity, ISDP Concepts, Threats, ISO27002 Controls, Protection Profiles), Information Assets (Critical Information, Compliance Requirements), Data Privacy (RPA, Main Purposes, Data Subjects Categories, Recipients / Processors), and Dashboard (ISDP, ISDP 2). The main content area is titled 'Hackme Casino ISDP Concept' and features a tabbed interface with 'Critical Asset(s)' selected. Below the tabs is a table of critical assets with columns for Name, Owner, Confidentiality Requirement, Integrity Requirement, Availability Requirement, and Impact Area(s). The table lists five assets: 'Casino's cards', 'Credits', 'Customer personal data', 'Gambling amount', and 'Players' cards', each with its respective owner and requirements.

| ✓ | Name                   | ↑ | Owner                       | Confidentiality Requirement | Integrity Requirement | Availability Requirement | Impact Area(s)                      |
|---|------------------------|---|-----------------------------|-----------------------------|-----------------------|--------------------------|-------------------------------------|
|   | Casino's cards         |   | Chief Technical Officer     | High                        | High                  | Medium                   | Finance; Reputation                 |
|   | Credits                |   | Chief Technical Officer     | Low                         | High                  | Medium                   | Finance; Reputation                 |
|   | Customer personal data |   | Head of marketing and sales | Medium                      | Medium                | Medium                   | Finance; Legal/Compliance; Reput... |
|   | Gambling amount        |   | Chief Technical Officer     | Low                         | High                  | Medium                   | Finance; Reputation                 |
|   | Players' cards         |   | Chief Technical Officer     | Low                         | High                  | Medium                   | Finance; Reputation                 |

# Démo outil ISDPTool

ISDPTool

Home > ISDP Concepts > Hackme Casino

🔍

🔗

+

🔼

⚙️

?

☰

Home

Recent

Pinned

Information Security

ISO27002 Maturity

ISDP Concepts

Threats

ISO27002 Controls

Protection Profiles

Information Assets

Critical Information ...

Compliance Require...

Data Privacy

RPA

Main Purposes

Data Subjects Categ...

Recipients / Processors

Dashboard

ISDP

ISDP 2

GENERATE

New

Deactivate

Delete

Refresh

Assign

Share

Email a Link

Flow

Word Templates

HC

Hackme Casino

ISDP Concept

General

Threat Agent(s)

Critical Asset(s)

Applicable Threats

Applicable Controls

General Controls

Protection Profile

Dashboard

Related

+ New Applicable Threat

Refresh

Excel Templates

...

| ✓ | 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...  |

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

27

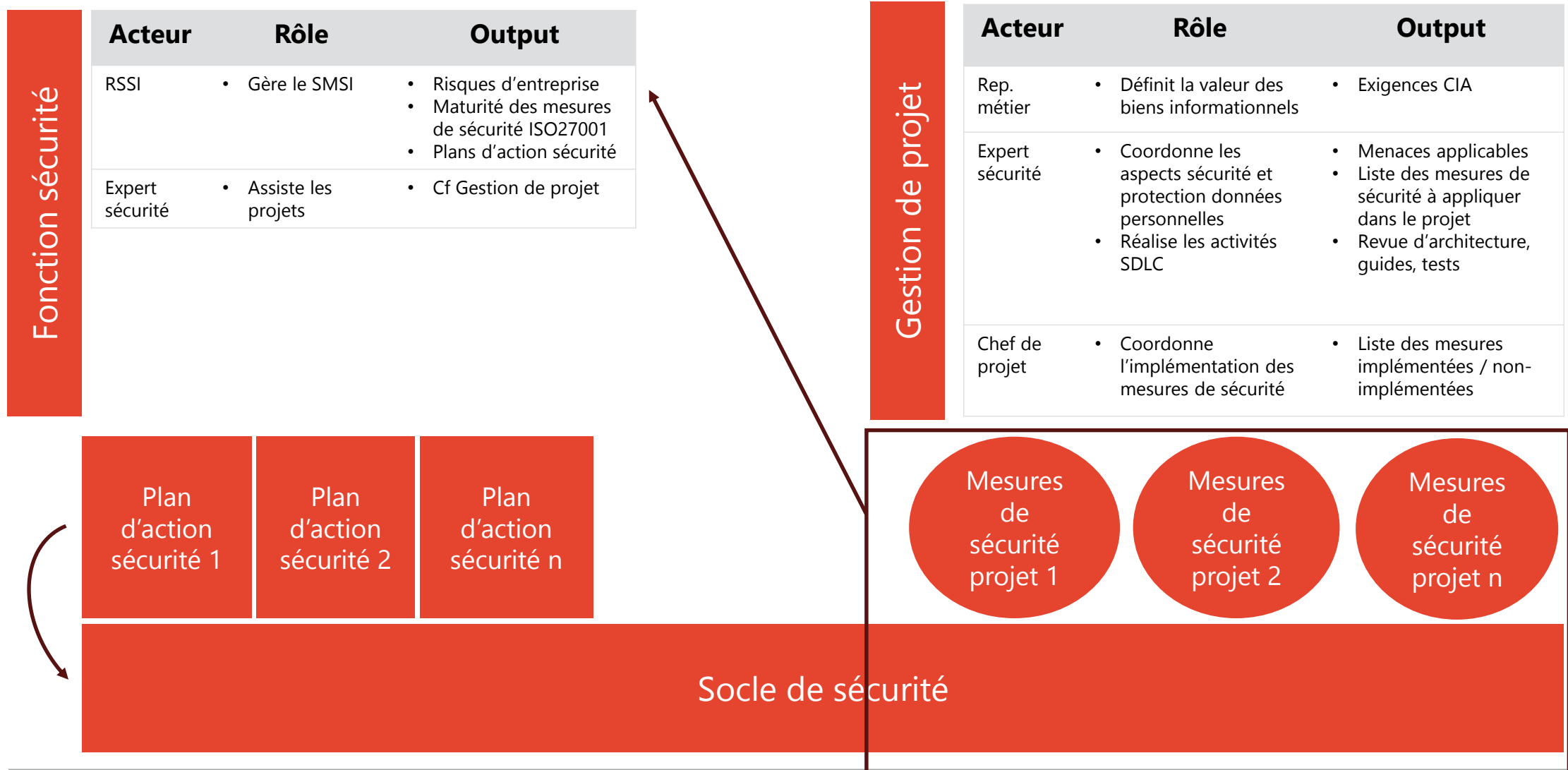
# Démo outil ISDPTool

The screenshot displays the ISDPTool interface for a project named 'Hackme Casino'. The left sidebar contains navigation menus for 'Information Security', 'Information Assets', 'Data Privacy', and 'Dashboard'. The main area shows the 'Applicable Controls' tab, which lists various controls and their associated threats. A tooltip is visible over the 'Threats' column for the control '15.1.2 - Addressing security within supplier...'. The table has columns for 'Chapter (ISO27002 Control Maturity)', 'Control', 'Threats Count', and 'Threats'. The 'Threats' column lists specific threats like 'Abuse of access rights', 'Access to data by foreign authorities', 'Account hijacking', etc. The 'Applicable Control' column shows the status of each control, with 'Yes' for '15.1.2 - Addressing security within supplier...' and 'No' for others.

| Chapter (ISO27002 Control Maturity)             | Control                                     | Threats Count | Threats   | Applicable Control |
|---|---|---------------|---|--------------------|
| 15.1.1 - Information security policy for sup... | Information security requirements for ...   | 14            | - Abuse of access rights                                | ---                |
| 15.2.2 - Managing changes to supplier ser...    | Changes to the provision of services b...   | 14            | - Abuse of access rights                                | ---                |
| 15.1.3 - Information and communication t...     | Agreements with suppliers should incl...    | 14            | - Abuse of access rights                                | ---                |
| 15.2.1 - Monitoring and review of supplier...   | Organizations should regularly monito...    | 14            | - Abuse of access rights                                | ---                |
| 15.1.2 - Addressing security within supplie...  | All relevant information security requir... | 14            | - Abuse of access rights - Access to data by foreign... | Yes                |
| 18.1.3 - Protection of records                  | Records should be protected from los...     | 9             | - Abuse of access rights - Access to data by foreign... | No                 |
| 07.1.2 - Terms and conditions of employm...     | The contractual agreements with empl...     | 8             | - Abuse of access rights - Accidental data alterati...  | ---                |
| 07.2.3 - Disciplinary process                   | There should be a formal and commu...       | 8             | - Abuse of access rights - Accidental data alterati...  | No                 |
| 17.2.1 - Availability of information process... | Information processing facilities shoul...  | 7             | - Damage on equipment - IT hardware componen...         | No                 |
| 07.1.1 - Screening                              | Background verification checks on all ...   | 6             | - Abuse of access rights - Account hijacking - Den...   | No                 |
| 09.1.2 - Access to networks and network s...    | Users should only be provided with ac...    | 6             | - Abuse of access rights - Account hijacking - Den...   | No                 |
| 13.1.2 - Security of network services           | Security mechanisms, service levels an...   | 6             | - Denial of service -> Distributed denial of service... | No                 |
| 08.1.3 - Acceptable use of assets               | Rules for the acceptable use of inform...   | 6             | - Account hijacking - Compliance breach with leg...     | No                 |
| 13.1.3 - Segregation in networks                | Groups of information services, users ...   | 6             | - Account hijacking - Denial of service -> Distribu...  | No                 |
| 12.4.2 - Protection of log information          | Logging facilities and log information ...  | 6             | - Abuse of access rights - Account hijacking - Den...   | No                 |
| 12.4.4 - Clock synchronisation                  | The clocks of all relevant information ...  | 6             | - Abuse of access rights - Account hijacking - Den...   | No                 |
| 13.1.1 - Network controls                       | Networks should be managed and co...        | 6             | - Denial of service -> Distributed denial of service... | No                 |

# **Intégrer la modélisation des menaces dans la gouvernance sécurité d'entreprise - Proposition**

# Organisation type



# 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](mailto:sadamiste@hotmail.com)

LinkedIn: Stéphane Adamiste

Twitter: [@sadamiste](https://twitter.com/sadamiste)