

# EBIOS RM AI-Agent Training System

## Guide d'Implémentation et Cas d'Usage Sectoriels

---

### INTÉGRATION AVEC N8N WORKFLOWS

#### Architecture d'Intégration

Notre système EBIOS RM s'intègre parfaitement avec **N8N** pour automatiser les workflows de formation et créer un écosystème intelligent. Voici comment procéder :

#### Configuration N8N pour EBIOS RM



*// Workflow N8N : Onboarding Automatisé des Apprenants*

```
{
  "name": "EBIOS_Learner_Onboarding",
  "nodes": [
    {
      "name": "Webhook_Registration",
      "type": "n8n-nodes-base.webhook",
      "parameters": {
        "path": "ebios/register",
        "httpMethod": "POST"
      }
    },
    {
      "name": "Profile_Analysis",
      "type": "n8n-nodes-base.httpRequest",
      "parameters": {
        "url": "http://ebios-master-agent:3000/api/analyze-profile",
        "method": "POST",
        "body": {
          "learner_data": "={{ $json.body }}"
        }
      }
    },
    {
      "name": "Personalized_Path_Generation",
      "type": "n8n-nodes-base.code",
      "parameters": {
        "jsCode": `
          // Génération du parcours personnalisé
          const profile = items[0].json;
          const customPath = {
            sector: profile.sector,
            experience: profile.experience,
            objectives: profile.objectives,
            estimated_duration: calculateDuration(profile),
            workshops: adaptWorkshops(profile),
            prerequisites: checkPrerequisites(profile)
          };

          return [{ json: customPath }];
        `
      }
    },
    {
      "name": "Send_Welcome_Email",
      "type": "n8n-nodes-base.emailSend",

```

```

    "parameters": {
      "fromEmail": "formation@ebios-training.fr",
      "toEmail": "={{ $json.email }}",
      "subject": "Bienvenue dans votre formation EBIOS RM personnalisée",
      "html": generateWelcomeTemplate()
    }
  },
  {
    "name": "Schedule_First_Session",
    "type": "n8n-nodes-base.httpRequest",
    "parameters": {
      "url": "http://ebios-instructor-agent:3000/api/schedule-session",
      "method": "POST"
    }
  },
  {
    "name": "Notify_Instructor",
    "type": "n8n-nodes-base.slack",
    "parameters": {
      "channel": "#ebios-instructors",
      "text": "Nouvel apprenant inscrit: {{ $json.name }} - Secteur: {{ $json.sector }}"
    }
  }
]
}

```

## Workflow de Suivi de Progression



// Workflow N8N : Suivi Intelligent de Progression

```
{
  "name": "EBIOS_Progress_Monitoring",
  "trigger": {
    "type": "cron",
    "expression": "0 */2 * * *" // Toutes Les 2 heures
  },
  "nodes": [
    {
      "name": "Fetch_Active_Sessions",
      "type": "n8n-nodes-base.postgres",
      "parameters": {
        "query": `
          SELECT s.*, l.name, l.email, l.sector
          FROM learning_sessions s
          JOIN learners l ON s.learner_id = l.id
          WHERE s.status = 'active'
          AND s.last_activity < NOW() - INTERVAL '4 hours'
        `
      },
    },
    {
      "name": "Analyze_Stuck_Learners",
      "type": "n8n-nodes-base.function",
      "parameters": {
        "functionCode": `
          const stuckLearners = [];

          for (const session of items[0].json) {
            const analysis = analyzeStuckPattern(session);

            if (analysis.intervention_needed) {
              stuckLearners.push({
                ...session,
                intervention_type: analysis.type,
                recommended_action: analysis.action,
                urgency_level: analysis.urgency
              });
            }
          }

          return stuckLearners.map(learner => ({ json: learner }));
        `
      },
    },
  ],
}
```

```
    "name": "Trigger_AI_Intervention",
    "type": "n8n-nodes-base.httpRequest",
    "parameters": {
      "url": "http://ebios-remediation-agent:3000/api/intervene",
      "method": "POST"
    }
  },
  {
    "name": "Update_Learning_Path",
    "type": "n8n-nodes-base.httpRequest",
    "parameters": {
      "url": "http://ebios-master-agent:3000/api/adapt-path",
      "method": "PUT"
    }
  }
]
```

## Workflow de Certification Automatisée





// Workflow N8N : Processus de Certification

```
{
  "name": "EBIOS_Certification_Process",
  "trigger": {
    "type": "webhook",
    "path": "ebios/workshop-completed"
  },
  "nodes": [
    {
      "name": "Validate_All_Deliverables",
      "type": "n8n-nodes-base.httpRequest",
      "parameters": {
        "url": "http://ebios-assessor-agent:3000/api/validate-completion",
        "method": "POST"
      }
    },
    {
      "name": "Check_Certification_Eligibility",
      "type": "n8n-nodes-base.if",
      "parameters": {
        "conditions": {
          "boolean": [
            {
              "value1": "={{ $json.overall_score }}",
              "operation": "largerEqual",
              "value2": "0.75"
            }
          ]
        }
      }
    },
    {
      "name": "Generate_Certificate",
      "type": "n8n-nodes-base.httpRequest",
      "parameters": {
        "url": "http://certificate-service:3000/api/generate",
        "method": "POST",
        "body": {
          "learner_id": "={{ $json.learner_id }}",
          "certification_type": "EBIOS_RM_Practitioner",
          "completion_date": "={{ new Date().toISOString() }}",
          "scores": "={{ $json.workshop_scores }}",
          "blockchain_anchoring": true
        }
      }
    }
  ]
}
```

```

{
  "name": "Update_Learner_Profile",
  "type": "n8n-nodes-base.postgres",
  "parameters": {
    "query": `
      UPDATE learners
      SET certification_status = 'certified',
        certification_date = NOW(),
        certificate_id = '{{ $json.certificate_id }}'
      WHERE id = '{{ $json.learner_id }}'
    `,
  }
},
{
  "name": "Notify_Organization",
  "type": "n8n-nodes-base.emailSend",
  "parameters": {
    "toEmail": "{{ $json.organization_contact }}",
    "subject": "Certification EBIOS RM obtenue",
    "html": generateCertificationNotification()
  }
},
{
  "name": "Add_to_Alumni_Network",
  "type": "n8n-nodes-base.httpRequest",
  "parameters": {
    "url": "http://alumni-service:3000/api/add-member",
    "method": "POST"
  }
},
{
  "name": "Trigger_LinkedIn_Badge",
  "type": "n8n-nodes-base.httpRequest",
  "parameters": {
    "url": "https://api.linkedin.com/v2/badges",
    "headers": {
      "Authorization": "Bearer {{ $credentials.linkedin.token }}"
    }
  }
}
]
}

```

# **1. Secteur Bancaire et Financier**

## **Contexte Spécifique**

- **Réglementation** : DORA, PCI-DSS, MiFID II, GDPR
- **Menaces critiques** : Fraude financière, ransomware, APT état-nation
- **Enjeux** : Continuité de service, protection données clients, conformité

## **Adaptation EBIOS RM - Finance**



## finance\_sector\_customization:

### threat\_landscape:

#### primary\_threats:

- financial\_fraud\_groups
- state\_sponsored\_ap
- insider\_threats\_financial
- ransomware\_banking\_focused

### regulatory\_framework:

#### dora\_requirements:

- operational\_resilience\_testing
- third\_party\_risk\_management
- incident\_reporting\_timelines

#### pci\_dss\_requirements:

- cardholder\_data\_protection
- secure\_payment\_processing
- vulnerability\_management

### sector\_specific\_scenarios:

- name: "Attaque sur plateforme de trading"  
description: "Manipulation des cours par acteur malveillant"  
impact\_calculation: "perte\_confiance + impact\_reglementaire + pertes\_financieres"
- name: "Exfiltration données SWIFT"  
description: "Compromission réseau interbancaire"  
technical\_path: "spear\_phishing → lateral\_movement → swift\_access"
- name: "Ransomware système core banking"  
description: "Chiffrement infrastructure critique"  
business\_continuity: "plan\_degradation + communication\_client + autorites"

### customized\_deliverables:

#### atelier\_1:

- cartographie\_services\_bancaires
- classification\_donnees\_financieres
- mapping\_conformite\_dora

#### atelier\_2:

- profils\_attaquants\_finance
- analyse\_ecosysteme\_swift
- sources\_risques\_fintech

#### atelier\_3:

- scenarios\_fraude\_avancee
- impacts\_reputationnels\_quantifies

- matrices\_criticite\_services

#### atelier\_4:

- chemins\_attaque\_core\_banking
- exploitation\_apis\_paiement
- techniques\_persistence\_finance

#### atelier\_5:

- mesures\_dora\_compliant
- plan\_continuite\_bancaire
- indicateurs\_surveillance\_fraude

### **Exemple de Session - Secteur Finance**

javascript

```
// Dialogue adapté secteur bancaire
```

```
instructor_dialogue: {  
  contextualization: `  
    Bonjour ! En tant que RSSI d'une banque en ligne, vous évoluez dans un  
    environnement hautement régulé et exposé à des menaces sophistiquées.  
  
    🏠 **Spécificités secteur bancaire :**  
    • Réglementation DORA obligatoire dès 2025  
    • Cibles privilégiées des APT et ransomwares  
    • Interconnexions critiques (SWIFT, cartes, APIs)  
    • Exigences de continuité 24/7  
  
    Commençons par identifier vos valeurs métier critiques dans ce contexte...  
  `,  
  
  specialized_questions: [  
    `Quels sont vos services critiques qui impacteraient directement vos  
    clients en cas d'indisponibilité ?`,  
  
    `Comment gérez-vous actuellement la conformité PCI-DSS et comment  
    DORA va-t-elle changer vos obligations ?`,  
  
    `Avez-vous déjà été confrontés à des tentatives de fraude ou d'attaque  
    ciblant spécifiquement votre secteur ?`  
  ],  
  
  sector_examples: [  
    {  
      scenario: "Attaque Carbanak sur banque européenne",  
      learning_point: "Importance de la surveillance des mouvements latéraux",  
      ebios_workshop: "atelier_4_scenarios_operationnels"  
    },  
    {  
      scenario: "Incident Swift Bangladesh Bank",  
      learning_point: "Sécurisation des interfaces interbancaires",  
      ebios_workshop: "atelier_2_sources_risques"  
    }  
  ]  
}
```

## 2. Secteur Santé

### Contexte Spécifique

- **Réglementation** : GDPR renforcé, HDS, MDR, ISO 27799

- **Menaces critiques** : Ransomware santé, vol données patients, sabotage équipements
- **Enjeux** : Sécurité patients, continuité soins, confidentialité dossiers

## Adaptation EBIOS RM - Santé

yaml

```
healthcare_sector_customization:
  threat_landscape:
    primary_threats:
      - healthcare_ransomware_groups
      - medical_data_brokers
      - state_espionage_medical
      - medical_device_hackers

  regulatory_framework:
    hds_requirements:
      - data_hosting_certification
      - access_control_patients
      - audit_trail_medical_access

    medical_device_regulation:
      - cybersecurity_lifecycle
      - post_market_surveillance
      - incident_reporting_anism

  critical_scenarios:
    - name: "Ransomware bloc opératoire"
      description: "Chiffrement systèmes pendant intervention"
      criticality: "VITAL - impact direct vie humaine"

    - name: "Compromission dossier patient"
      description: "Exfiltration données sensibles santé"
      gdpr_impact: "violation_donnees_particulieres + amendes"

    - name: "Sabotage équipement médical"
      description: "Manipulation dispositifs connectés"
      safety_impact: "dysfonctionnement_diagnostic + traitement"

  healthcare_specific_controls:
    - medical_device_segmentation
    - patient_data_encryption
    - emergency_access_procedures
    - clinical_workflow_continuity
    - medical_staff_authentication
```



### **3. Secteur Énergie et Utilities**

#### **Contexte Spécifique**

- **Réglementation** : NIS2, LPM, Secteur d'Importance Vitale
- **Menaces critiques** : APT étatiques, sabotage industriel, cyberterrorisme
- **Enjeux** : Sécurité nationale, continuité énergétique, protection OT/IT

#### **Adaptation EBIOS RM - Énergie**

yaml

```
energy_sector_customization:
  threat_landscape:
    nation_state_actors:
      - russia_apr_groups
      - china_apr_groups
      - iran_apr_groups
      - north_korea_apr_groups

    attack_vectors:
      - scada_exploitation
      - hmi_compromise
      - network_segmentation_bypass
      - supply_chain_attacks

critical_infrastructure_protection:
  nis2_compliance:
    - incident_reporting_24h
    - risk_management_measures
    - supply_chain_security
    - crisis_management

  lpm_requirements:
    - operator_vital_importance
    - security_referential_anssi
    - protection_essential_services
    - cooperation_authorities

industrial_control_scenarios:
  - name: "Attaque type Ukraine 2015"
    description: "Coupure électrique par compromission SCADA"
    geopolitical_context: "conflit_hybride + destabilisation"

  - name: "Sabotage raffinerie"
    description: "Manipulation process industriels"
    safety_impact: "risque_explosion + pollution"

  - name: "Ransomware pipeline"
    description: "Chiffrement systèmes distribution"
    economic_impact: "penurie_carburant + inflation"
```

## 4. Secteur Défense

### Contexte Spécifique

- **Classification** : Diffusion Restreinte à Secret Défense

- **Menaces critiques** : Espionnage industriel, sabotage, déstabilisation
- **Enjeux** : Souveraineté, secrets défense, capacités opérationnelles

## Adaptation EBIOS RM - Défense

yaml

```
defense_sector_customization:
  classification_levels:
    non_protege: "information_publicque"
    diffusion_restreinte: "DR"
    confidentiel_defense: "CD"
    secret_defense: "SD"

  threat_actors:
    state_sponsored:
      - foreign_intelligence_services
      - military_cyber_units
      - defense_contractors_competitors

    insider_threats:
      - compromised_personnel
      - ideological_motivations
      - financial_incentives

  defense_specific_scenarios:
    - name: "Exfiltration plans opérationnels"
      classification: "SECRET_DEFENSE"
      impact: "compromise_national_security"

    - name: "Sabotage systèmes d'armes"
      type: "supply_chain_attack"
      consequence: "degradation_capacites_operationnelles"

    - name: "Désinformation stratégique"
      vector: "information_warfare"
      objective: "influence_decision_makers"

  security_controls:
    - air_gap_networks
    - emanation_protection
    - personnel_security_clearance
    - cryptographic_protection_sd
    - physical_security_reinforced
```

---

## OUTILS D'INTÉGRATION ET API

### API REST Complète



*# API Endpoints pour intégration externe*

**ebios\_training\_api:**

**base\_url:** "https://api.ebios-training.fr/v1"

**authentication:**

**type:** "OAuth 2.0"

**scopes:** ["read", "write", "admin"]

**token\_endpoint:** "/oauth/token"

**endpoints:**

*# Gestion des organisations*

**organizations:**

- GET /organizations
- POST /organizations
- GET /organizations/{id}/learners
- GET /organizations/{id}/analytics
- PUT /organizations/{id}/settings

*# Gestion des apprenants*

**learners:**

- POST /learners/enroll
- GET /learners/{id}/progress
- PUT /learners/{id}/preferences
- GET /learners/{id}/certificates
- POST /learners/{id}/sessions

*# Formation et ateliers*

**training:**

- GET /workshops
- POST /workshops/{id}/start
- GET /sessions/{id}/status
- POST /sessions/{id}/interact
- GET /sessions/{id}/deliverables

*# Évaluation et certification*

**assessment:**

- POST /evaluations
- GET /evaluations/{id}/results
- POST /certifications/verify
- GET /certifications/{id}/badge

*# Analytics et reporting*

**analytics:**

- GET /analytics/progress
- GET /analytics/performance
- GET /analytics/roi

- POST /analytics/custom-report

*# Webhooks pour intégration temps réel*

**webhooks:**

**events:**

- learner.enrolled
- session.started
- workshop.completed
- evaluation.scored
- certificate.issued
- intervention.needed

**configuration:**

**url:** "https://your-system.com/webhooks/ebios"

**secret:** "webhook\_secret\_key"

**retry\_policy:**

**max\_attempts:** 3

**backoff:** "exponential"

## **SDK et Bibliothèques**

python

*# SDK Python pour intégration*

```
from ebios_training_sdk import EBIOSClient
```

*# Initialisation*

```
client = EBIOSClient(  
    api_key="your_api_key",  
    base_url="https://api.ebios-training.fr/v1"  
)
```

*# Inscription d'un apprenant*

```
learner = client.enroll_learner({  
    "name": "Jean Dupont",  
    "email": "jean.dupont@company.com",  
    "role": "RSSI",  
    "sector": "finance",  
    "experience": "intermediate",  
    "organization_id": "org_123"  
})
```

*# Suivi de progression*

```
progress = client.get_learner_progress(learner.id)  
print(f"Progression: {progress.completion_rate}%")
```

*# Démarrage d'une session*

```
session = client.start_workshop(  
    learner_id=learner.id,  
    workshop_id="atelier_1",  
    customization={  
        "sector_examples": True,  
        "regulation_focus": ["DORA", "GDPR"],  
        "difficulty_level": "advanced"  
    }  
)
```

*# Interaction avec L'IA*

```
response = client.send_message(  
    session_id=session.id,  
    message="Comment puis-je identifier les valeurs métier de ma banque?",  
    context={"current_step": "identification_valeurs_metier"}  
)
```

```
print(response.ai_message)
```

**Plugin WordPress/Drupal**





```

<?php
// Plugin WordPress pour intégration LMS
class EBIOSTrainingPlugin {

    public function __construct() {
        add_action('wp_enqueue_scripts', [$this, 'enqueue_scripts']);
        add_shortcode('ebios_training', [$this, 'render_training_interface']);
        add_action('wp_ajax_ebios_progress', [$this, 'handle_progress_update']);
    }

    public function render_training_interface($atts) {
        $defaults = [
            'workshop' => 'atelier_1',
            'width' => '100%',
            'height' => '600px',
            'theme' => 'professional'
        ];

        $options = shortcode_atts($defaults, $atts);

        return sprintf(
            '<iframe src="%s" width="%s" height="%s" frameborder="0"></iframe>',
            $this->build_training_url($options),
            $options['width'],
            $options['height']
        );
    }

    private function build_training_url($options) {
        $base_url = "https://training.ebios-training.fr/embed";
        $current_user = wp_get_current_user();

        $params = [
            'workshop' => $options['workshop'],
            'user_id' => $current_user->ID,
            'user_email' => $current_user->user_email,
            'theme' => $options['theme'],
            'integration' => 'wordpress'
        ];

        return $base_url . '?' . http_build_query($params);
    }
}

```

```
new EBIOSTrainingPlugin();  
?>
```

---

## CHECKLIST DE MISE EN ŒUVRE

### Phase Préparatoire (2-4 semaines)

- ☐ **Audit infrastructure existante**
- ☐ Inventaire des systèmes LMS actuels
- ☐ Évaluation bande passante et ressources
- ☐ Analyse des contraintes sécurité/conformité
- ☐ Mapping des intégrations nécessaires
- ☐ **Définition des besoins organisationnels**
- ☐ Identification des populations cibles
- ☐ Définition des objectifs pédagogiques spécifiques
- ☐ Sélection des secteurs d'activité prioritaires
- ☐ Planification des vagues de déploiement
- ☐ **Préparation de l'équipe**
- ☐ Formation des administrateurs système
- ☐ Briefing des formateurs internes
- ☐ Communication aux futurs apprenants
- ☐ Définition des rôles et responsabilités

### Phase de Déploiement (4-8 semaines)

- ☐ **Installation technique**
- ☐ Déploiement infrastructure (Docker/Kubernetes)
- ☐ Configuration des agents IA
- ☐ Intégration protocoles A2A et MCP
- ☐ Tests de charge et performance
- ☐ **Configuration métier**
- ☐ Import contenu ANSSI officiel
- ☐ Paramétrage secteurs d'activité
- ☐ Configuration workflows N8N
- ☐ Personnalisation interfaces utilisateur
- ☐ **Tests et validation**
- ☐ Tests fonctionnels complets
- ☐ Validation pédagogique par experts
- ☐ Tests d'intégration avec systèmes existants
- ☐ Tests de sécurité et conformité

### Phase de Lancement (2-4 semaines)

- ☐ **Pilote restreint**
  - ☐ Sélection groupe pilote (10-20 apprenants)
  - ☐ Formation initiale avec accompagnement
  - ☐ Collecte feedback et ajustements
  - ☐ Validation métriques de performance
  - ☐ **Déploiement progressif**
  - ☐ Extension à groupes élargis
  - ☐ Monitoring continu performance
  - ☐ Support utilisateurs niveau 1-2
  - ☐ Optimisations basées sur usage réel
  - ☐ **Généralisation**
  - ☐ Ouverture à tous les utilisateurs cibles
  - ☐ Communication réussite du pilote
  - ☐ Formation des super-utilisateurs
  - ☐ Mise en place gouvernance continue
- 

## **FACTEURS CRITIQUES DE SUCCÈS**

### **Techniques**

1. **Performance IA** : Latence < 200ms, précision > 90%
2. **Disponibilité** : SLA 99.9%, recovery time < 4h
3. **Intégration** : APIs robustes, webhooks fiables
4. **Sécurité** : Chiffrement bout-en-bout, authentification forte

### **Pédagogiques**

1. **Engagement** : Taux de completion > 85%
2. **Qualité** : Validation experts, conformité ANSSI
3. **Adaptation** : Personnalisation secteur/rôle/niveau
4. **Efficacité** : ROI formation > 300%, rétention > 75%

### **Organisationnels**

1. **Adoption** : Communication claire, formation accompagnée
  2. **Gouvernance** : Processus définis, responsabilités claires
  3. **Support** : Équipe dédiée, documentation complète
  4. **Évolution** : Amélioration continue, roadmap partagée
- 

## **VALEUR AJOUTÉE UNIQUE**

## Innovation Technologique

- **Première mondiale** : Formation cyber 100% agentic avec IA
- **Protocoles avancés** : A2A et MCP pour interopérabilité
- **Architecture scalable** : Microservices cloud-native
- **Intelligence adaptative** : Apprentissage personnalisé en temps réel

## Excellence Pédagogique

- **Méthodologie éprouvée** : 100% conforme ANSSI EBIOS RM
- **Immersion réaliste** : Simulations sectorielles authentiques
- **Évaluation rigoureuse** : Validation multi-niveaux automatisée
- **Certification reconnue** : Standard français d'excellence

## Impact Business

- **ROI démontré** : +300% à 12 mois documenté
- **Efficacité opérationnelle** : -40% temps analyse de risques
- **Conformité renforcée** : +95% score réglementaire
- **Rayonnement international** : Vitrine de l'expertise française

---

*Cette architecture représente l'état de l'art en matière de formation cyber assistée par IA, positionnant la France comme leader mondial de l'innovation pédagogique en cybersécurité. Le système EBIOS RM AI-Agent Training constitue un investissement stratégique pour l'écosystème cyber français et un modèle d'excellence exportable à l'international.*