



# SERVICES DE CYBERSÉCURITÉ DE MOTOROLA SOLUTIONS



## TENDANCE ACTUELLE

VS.

## PRATIQUES ACTUELLES

**87%**

SONT EXTRÊMEMENT OU ASSEZ CONFIANTS DANS LA CYBERSÉCURITÉ DE LEURS SYSTÈMES RADIO. MAIS DOIVENT-ILS L'ÊTRE ? SEULEMENT...

**53%**

PRATIQUENT UNE SURVEILLANCE ACTIVE DE LA SÉCURITÉ

**48%**

ONT DES RÈGLES ET DES PROCÉDURES DE SÉCURITÉ DOCUMENTÉES

**42%**

APPLIQUENT DES CORRECTIFS À LEURS SYSTÈMES LMR

**30%**

EFFECTUENT DES ÉVALUATIONS PÉRIODIQUES DES RISQUES

**22%**

NE FONT AUCUNE DES OPÉRATIONS PRÉCÉDENTES

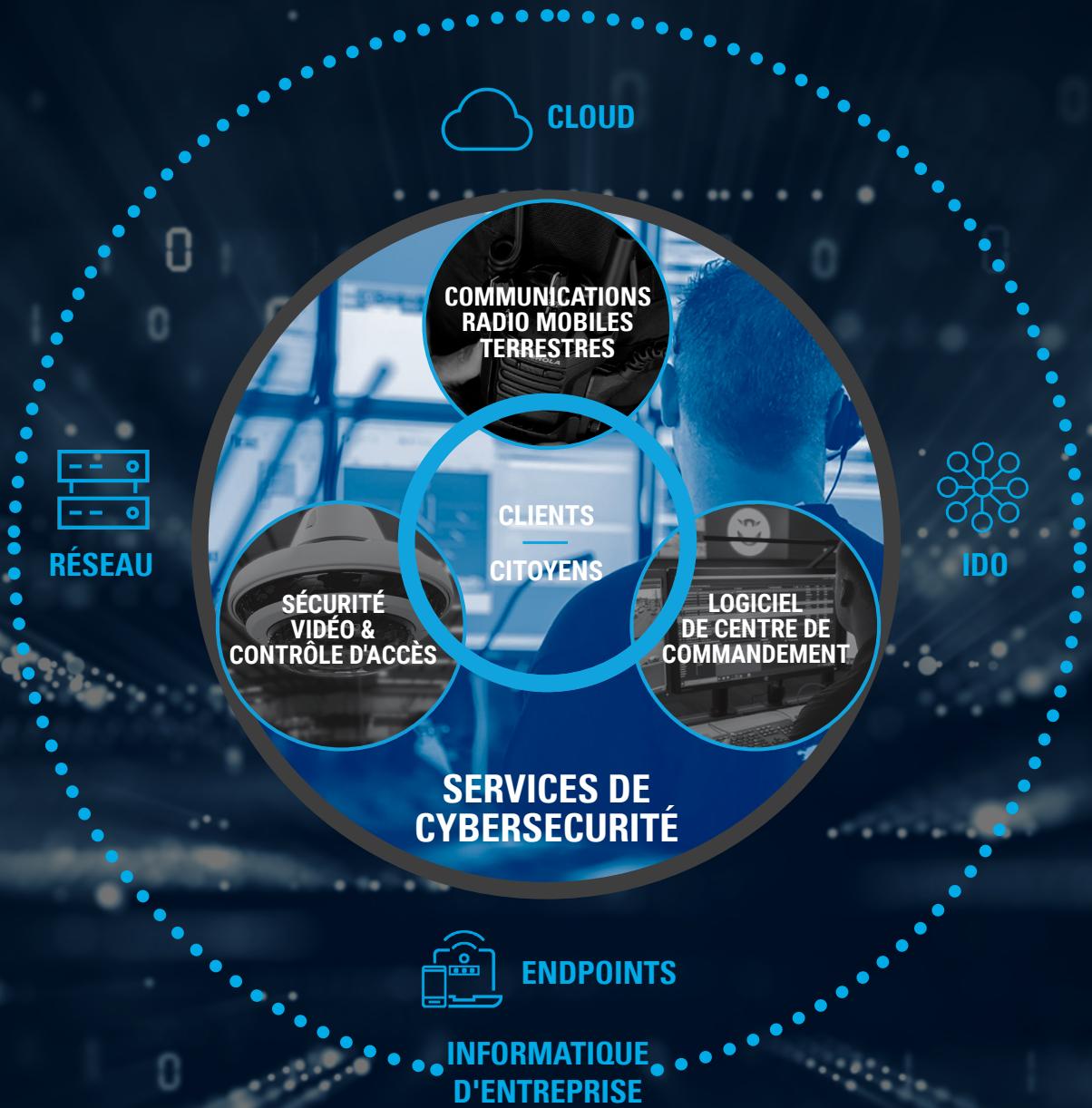
Toutes les données sont issues de l'enquête comparative 2018 de Motorola Solutions sur la gestion des systèmes LMR.

## LES CYBERMENACES QUI PÈSENT SUR LES ÉCOGRAPHIES DE LA SÉCURITÉ PUBLIQUE SONT EN AUGMENTATION, MAIS LES DISPOSITIFS DE PROTECTION DE NOMBREUSES ORGANISATIONS NE SONT PAS SUFFISAMMENT EFFICACES. DES ACTIONS PLUS POUSSÉES DOIVENT ENCORE ÊTRE MENÉES POUR EMPÊCHER LES ATTAQUES MALVEILLANTES ET LA CYBERHYGIÈNE DOIT ÊTRE ANALYSÉE MINUTIEUSEMENT.

Aucune entité n'est à l'abri de la menace mondiale croissante de la cybercriminalité. Presque toutes les agences de renseignement du monde ont publié des directives sur les mesures à prendre en matière de cybersécurité en cas de risque élevé. Cependant, si vous étudiez ces recommandations, vous verrez un thème commun. Effectuez les opérations de base, testez-les et répétez-les.

Les solutions de cybersécurité de Motorola Solutions peuvent fournir les outils, les solutions et l'assistance nécessaires pour garantir la robustesse et la protection de votre environnement informatique et de votre réseau de communication critique.

Notre équipe créera une feuille de route pour votre programme de cybersécurité en fonction de vos objectifs, elle vous permettra de déterminer le niveau actuel de conformité de votre organisation aux règles internationales de sécurité de l'information et aux normes sectorielles. Elle vous fournira une feuille de route pour améliorer les contrôles de sécurité par ordre de priorité en fonction de l'impact opérationnel.



**MOTOROLA SOLUTIONS EST VOTRE PARTENAIRE MONDIAL POUR LES SERVICES DE CYBERSÉCURITÉ. NOUS PROPOSONS UNE OFFRE INTÉGRÉE CONFORME AUX DISPOSITIONS RÉGIONALES ET NATIONALES POUR IDENTIFIER LES LACUNES DES PROGRAMMES DE SÉCURITÉ, DÉTECTOR LES MENACES AU SEIN DES RÉSEAUX ET PRÉPARER NOS CLIENTS À INTERVENIR EN CAS D'INCIDENT.**



#### SERVICES DE CONSEIL

Identifient les lacunes dans votre dispositif de cybersécurité et définissent une stratégie pour lutter contre les cybermenaces.



#### GESTION DES DÉTECTIONS ET DES INTERVENTIONS

Détecte les menaces telles que les Ransomware dans vos réseaux et votre infrastructure. Les menaces sont bloquées et neutralisées.



#### SERVICE DE MISES À JOUR DE SÉCURITÉ

L'application de correctifs est l'une des méthodes les plus économiques pour réduire la vulnérabilité aux cybermenaces.



#### CRYPTAGE ET AUTHENTIFICATION

N'autorisez que les appareils que vous souhaitez intégrer à votre réseau de communication et assurez-vous que vos communications sont sécurisées.



#### FORMATION ET ENSEIGNEMENT

Une formation pour vous donner les compétences nécessaires pour comprendre les cybermenaces, les combattre et les prévenir.

# ÉVALUER VOTRE PERSONNEL, VOS PROCESSUS ET VOTRE TECHNOLOGIE POUR TROUVER ET COMBLER LES LACUNES EN MATIÈRE DE SÉCURITÉ

Motorola Solutions utilise une approche multidimensionnelle de votre patrimoine protégé et de l'informatique d'entreprise traditionnelle, qui intègre la recherche et une analyse technique approfondie. Notre approche consiste à étudier les informations disponibles ou ayant fait l'objet de divulgations publiques, le manque de contrôles, les mauvaises configurations et les vulnérabilités du système, comme le ferait un pirate informatique malveillant. À travers des tests de pénétration, des évaluations de vulnérabilité, des tests effectués sur des scénarios, des évaluations de maturité et des exercices de simulation.

**30%**

EFFECTUENT DES ÉVALUATIONS PÉRIODIQUES DES RISQUES



## DÉTECTEZ

### IDENTIFIEZ LES VULNÉRABILITÉS

Bénéficiez d'une visibilité complète sur l'efficacité de vos contrôles, règles et procédures de sécurité pour protéger le réseau de votre entreprise, vos environnements Cloud, vos terminaux et vos réseaux de sécurité publique.



## ANALYSEZ

### REPRODUISEZ LES MENACES

La reproduction des menaces internes et externes sur vos réseaux, vos applications et vos sites opérationnels permet d'identifier les failles que des pirates ou des employés malveillants pourraient exploiter.



## ENQUÊTEZ

### EXPERTISE EN MATIÈRE DE SÉCURITÉ

Nous utilisons une approche multidimensionnelle, qui associe l'expertise de notre équipe avec de nombreux outils et de moyens techniques sophistiqués.



**TOTALEMENT CONFORME AU CADRE DE CYBERSÉCURITÉ DU NIST**

## PROCESSUS REPRODUCTIBLES, VIGILANCE ET ÉVALUATION PERMANENTES

### PRÉ-ÉVALUATION

ÉVALUE LES BESOINS DE L'ENTREPRISE ET LE PÉRIMÈTRE

Situation opérationnelle réelle et pratiques en matière de cybersécurité  
Planification, confirmation du périmètre, livrables et résultats attendus

### ÉVALUATION SUR SITE

EFFECTUE DES ÉVALUATIONS DE CONFORMITÉ AUX NORMES DU NIST, DE VULNÉRABILITÉ TECHNIQUE ET DES RENSEIGNEMENT SUR LES MENACES

Collecte de données  
Harmonisation des activités, des outils, des compétences et des processus

### POST-ÉVALUATION

FOURNIT UNE FEUILLE DE ROUTE ET DES RECOMMANDATIONS

Analyse des lacunes et rapports

Services de remédiation

**STRATÉGIE CONTINUE DE CYBER-RÉSILIENCE**

**ÉVALUATION HOLISTIQUE DE L'ENSEMBLE DE L'ENVIRONNEMENT TECHNOLOGIQUE DE VOTRE ORGANISME DE SÉCURITÉ PUBLIQUE**

# LA PLATEFORME DE GESTION DE LA SÉCURITÉ ACTIVE EYE BÉNÉFICIEZ D'UNE VISIBILITÉ SUR LES SYSTÈMES LMR, LES RÉSEAUX DE MATÉRIELS INFORMATIQUES ET LES RÉSEAUX CLOUD

La plateforme de sécurité avancée ActiveEye vous offre une visibilité complète sur vos systèmes, réseaux et les autres éléments de votre infrastructure. Connectez-vous à tout moment pour obtenir une vision immédiate de la situation dans votre environnement et des actions qui ont été prises pour protéger vos infrastructures vitales. Grâce à la constitution d'une base de données des menaces, il détecte activement les comportements inhabituels qui peuvent annoncer des menaces. Qu'il s'agisse d'Office 365, de Google Workspace, d'AWS ou d'Azure, ActiveEye protège vos actifs lorsque vous migrez vers les applications Cloud.

**53%**

PRATIQUENT UNE SURVEILLANCE ACTIVE DE LA SÉCURITÉ

## DÉCOUVREZ & ASSIMILEZ



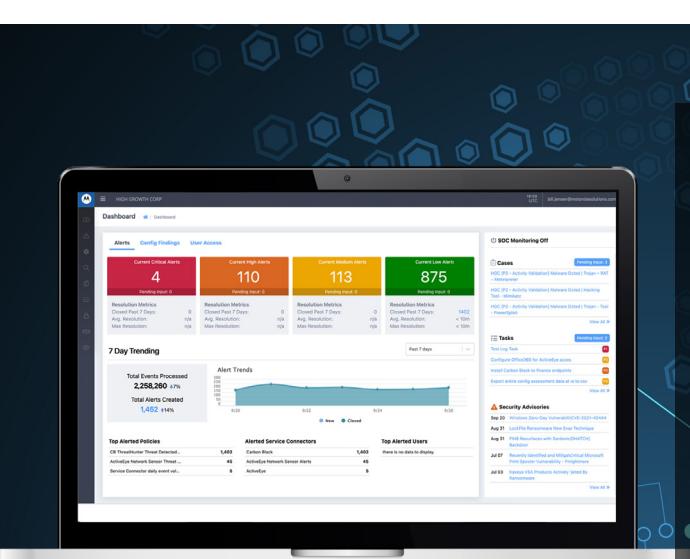
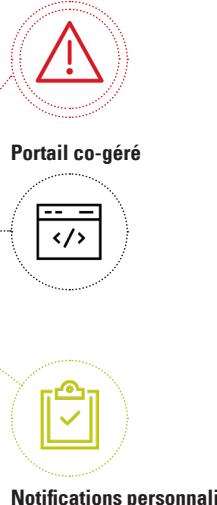
## ANALYSEZ & ENQUÊTEZ

Renseignements sur les menaces



## CORRIGEZ & INTERVENEZ

Réduction des menaces



## SERVICE DE DÉTECTION DES RÉSEAUX GÉRÉS

- Identifie les menaces encore inconnues
- Identifie les applications inconnues exécutées sur le réseau
- Alerte sur les attaques grâce à la détection des anomalies des flux
- Particulièrement utile lorsque les Endpoint Agents ne sont pas possibles

## SOC (SECURITY OPERATIONS CENTER)

- Plus de 300 experts en sécurité sont chargés de surveiller et d'intervenir 24 heures sur 24 et 7 jours sur 7 dans des SOC (Security Operations Centres) dédiés
- Organise une intervention et émet des recommandations
- Les services standards du SOC peuvent être renforcés grâce à des informations approfondies sur les menaces

# LES CORRECTIFS : VOTRE PREMIÈRE DÉFENSE CONTRE LES ATTAQUES

Dans un système critique tel que la LMR (Land Mobile Radio), il est capital que le système suive le rythme régulier des mises à jour de sécurité logicielle ou "correctifs". Cependant, seulement 42 % des entreprises appliquent des correctifs pour différentes raisons, telles que le manque de ressources et de compétences. Motorola Solutions propose à ses clients des offres qui leur permettent de résoudre ces problèmes.

42%

APPLIQUENT DES CORRECTIFS  
À LEURS SYSTÈMES LMR

DÉCOUVREZ ET TÉLÉCHARGEZ ► ANALYSEZ ET VÉRIFIEZ ► DIFUSEZ ET DEPLOYEZ



SYSTÈME  
D'EXPLOITATION



ASTRO



VIRTUALISATION



PASSERELLE POUR  
RADIOS WAVE



APPLICATION



MOTOROLA  
SOLUTIONS



TEST ET VALIDATION DES CORRECTIFS



SIGNATURES ANTIVIRUS MCAFEE - HEBDOMADAIRE  
MICROSOFT WINDOWS - MENSUEL  
AUTRES FOURNISSEURS - TRIMESTRIELLE



SERVICE DE MISES À JOUR DE SÉCURITÉ  
INSTALLATION PAR LE CLIENT



MISE À JOUR DE SÉCURITÉ À DISTANCE  
GESTION DU DÉPLOIEMENT DES CORRECTIFS



MISE À JOUR DE SÉCURITÉ SUR SITE  
GESTION DU DÉPLOIEMENT DES CORRECTIFS SUR SITE

## SUS (SECURITY UPDATE SERVICE)



### AUTO-INSTALLATION

Couverture complète des correctifs de sécurité pré-testés disponibles sur le site Web sécurisé de Motorola Solutions.

Téléchargés et installés par :

le client

Redémarré par : le client



### SUS SUR SITE

Des techniciens MSI formés procèdent aux mises à jour des correctifs et au redémarrage des serveurs et des postes de travail sur le site du client.

Téléchargés et installés par :

Motorola Solutions

Redémarré par : le client ou Motorola Solutions



### À DISTANCE

Nos techniciens installeront à distance les mises à jour de sécurité sur votre réseau radio.

Téléchargés et installés par :

Motorola Solutions

Redémarré par : le client

85%

DES ATTAQUES  
CIBLÉES PEUVENT  
ÊTRE ÉVITÉES AVEC  
DES CORRECTIFS

[https://www.us-cert.gov/ncas/  
alerts/TA15-119A](https://www.us-cert.gov/ncas/alerts/TA15-119A)

# MAÎTRISEZ TOTALEMENT LA SÉCURITÉ DE VOTRE RÉSEAU, AVEC DES SOLUTIONS DE CRYPTAGE SÛRES, ÉVOLUTIVES ET ÉPROUVÉES

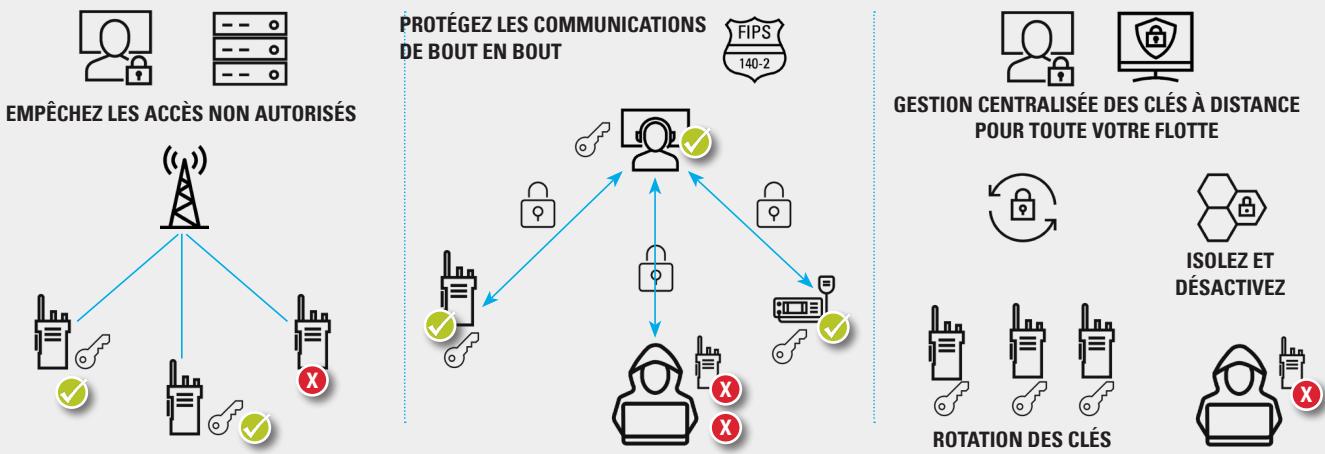
Vous devez prévoir et vous préparer à des attaques hostiles et ciblées contre votre réseau. Sécurisez vos communications critiques afin de pouvoir répondre rapidement et facilement aux menaces sans compromettre vos communications voix et données sensibles.

L'authentification fournit plusieurs couches de sécurité pour garantir que seuls les appareils disposant d'une clé valide et actualisée peuvent s'enregistrer sur le système. Le cryptage de bout en bout signifie que chaque communication est cryptée avant de quitter l'appareil et que seul le destinataire auquel elle est destinée peut la déchiffrer. Grâce à l'authentification et au cryptage, vos messages et vos données ne sont interprétés que par les personnes que vous avez sélectionnées.

**48%**

ONT DES RÈGLES ET DES PROCÉDURES DE SÉCURITÉ DOCUMENTÉES

## AUTHENTIFICATION RADIO ► CRYPTAGE VOIX ET DONNÉES ► GESTION DES CLÉS



CONTRÔLE CENTRALISÉ OU MANUEL DES CLÉS DE CRYPTAGE. SUPPRIMEZ LA COMPLEXITÉ DE LA GESTION DES CLÉS. GRÂCE À LA DISTRIBUTION À DISTANCE PAR ONDES RADIO. LES APPAREILS AUTORISÉS QUI SONT COMPROMIS PEUVENT ÊTRE IMMÉDIATEMENT VERROUILLÉS ET/OU DÉSACTIVÉS.

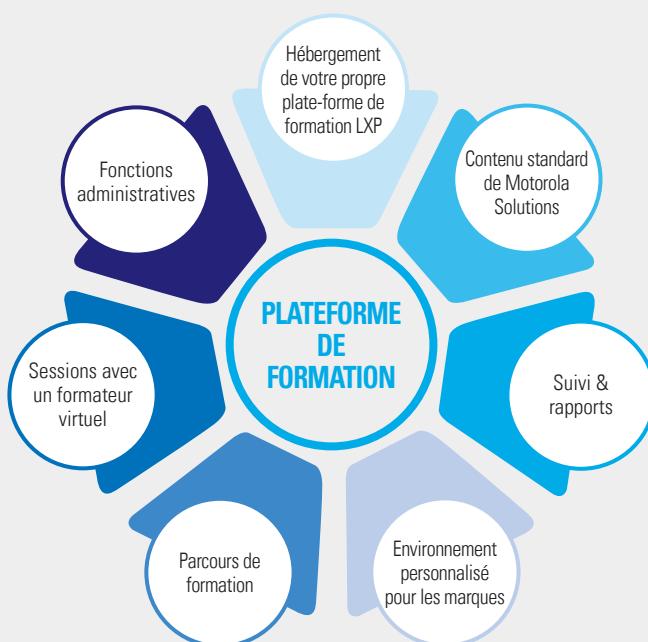
# DÉVELOPPEZ VOTRE EXPERTISE PARTOUT ET À TOUT MOMENT, GRÂCE À LA FORMATION CONTINUE

Pour vous aider à maintenir à jour vos compétences, nous proposons un abonnement à une plateforme Cloud de formation hébergée de manière centralisée, ce qui vous permet de modifier votre abonnement en fonction de vos besoins.

Notre centre de cybersécurité propose des formations formelles et informelles dispensées de différentes manières, telles que des cours animés par un formateur et des cours en ligne, pour vous fournir des formations à la cybersécurité qui soient disponibles rapidement, pertinentes et adaptées à vos besoins.

## PARCOURS DE FORMATION

- Initiation à la cybersécurité
- Prévention des logiciels malveillants
- Menaces et attaques en matière de cybersécurité
- Intervention en cas d'incident
- Enquêtes et analyses judiciaires de cybersécurité
- Évaluation des vulnérabilités



## COMMENCEZ VOTRE PARCOURS DE CYBERSÉCURITÉ

L'établissement et la mise en œuvre d'une stratégie de cyber-sécurité suscitent de nombreuses réflexions. Si votre entreprise ne dispose pas d'experts en cybersécurité, vous pouvez collaborer avec nous. Nos experts sont des professionnels qualifiés en cybersécurité, qui sont prêts à travailler avec votre entreprise pour améliorer votre capacité à identifier les cybermenaces, à les gérer et à intervenir.

Pour en savoir plus, veuillez-vous rendre sur : [motorolasolutions.com/cybersecurity](http://motorolasolutions.com/cybersecurity)

Motorola Solutions France SAS Parc Les Algorithmes Saint Aubin 91193 Gif - sur - Yvette, France motorolasolutions.fr

Les disponibilités dépendent des lois et des réglementations des pays. Sauf stipulation contraire, toutes les caractéristiques indiquées sont standards et peuvent être modifiées sans préavis.

MOTOROLA, MOTO, MOTOROLA SOLUTIONS et le logo M sont des marques commerciales ou des marques déposées de Motorola Holdings, LLC et sont utilisés sous licence de marques.  
Toutes les autres marques sont la propriété de leurs propriétaires respectifs. ©2022 Motorola Solutions, Inc. Tous droits réservés. (10-22)