

## Session 3 : Gestion d'incidents et de crise de cyberattaque de grande ampleur

### Formateur

**Imad Abounasr**, Consultant en sécurité des systèmes d'information, Imad Abounasr a accompagné depuis le début de sa carrière des grands Groupe Français et internationaux dans la mise en œuvre de leur stratégie de cyber sécurité. Issu d'une formation spécialisée en sécurité des systèmes d'information de l'université de Limoges en France et de l'Université de Sherbrooke au Canada, il a toujours été animé par la passion de la sécurité de l'information et participe activement à la communauté au Maroc et à l'étranger, notamment, La Commission Thématique « sécurité et confiance numérique » du Maroc Numeric Cluster qu'il a présidé. Il intervient aussi, en tant qu'enseignant, dans plusieurs master spécialisés en France et au Maroc. M. Abounasr est Senior Manager, en charge des activités cyber sécurité, au sein d'un grand cabinet de conseil international.

### Animateur

**Khalid Chougali**, Professeur universitaire à l'Université Ibn Tofail - Kénitra, Chercheur en sécurité informatique.

## Ateliers nationaux et Séminaires de Formation de Cybersécurité et Lutte Contre la Cybercriminalité

### Sous l'égide

Royaume du Maroc  
Ministère de l'Industrie,  
du Commerce, de l'Investissement  
et de l'Economie Numérique



المملكة المغربية  
وزارة الصناعة  
والتجارة والاستثمار  
والاقتصاد الرقمي



المركز المغربي للأبحاث المتعددة التقنيات والابتكار  
Le Centre Marocain de Recherches Polytechniques et d'Innovation

[www.cmrpi.ma](http://www.cmrpi.ma)



La Campagne Nationale de Lutte Contre la Cybercriminalité  
Maroc 2014-2017

4<sup>ème</sup> édition

## AGENDA

07, 08 et 09 Mars 2017

## Session 3 : Gestion d'incidents et de crise de cyberattaque de grande ampleur

### Programme du Mardi 07 Mars 2017

Matin	<p><b>Lancement officiel des ateliers</b>  <b>Séances 1 - M. ABOUNASR</b>                  Comment prévenir les risques d'attaques et d'intrusion ?</p> <ul style="list-style-type: none"> <li>- Présentations</li> <li>- Introduction</li> <li>- Les principes d'hygiènes de sécurité</li> </ul>
Après-midi	<p><b>Séances 2 - M. ABOUNASR</b>                  Comment prévenir les risques d'attaques et d'intrusion ?</p> <ul style="list-style-type: none"> <li>- Les bonnes pratiques de sécurité pour prévenir les incidents de sécurité</li> <li>- L'organisation et la gouvernance de la sécurité en cas de crise</li> </ul>
	<p><b>Séances 3 - M. ABOUNASR</b>                  Détection des incidents de sécurité à travers la vision d'un SOC (Security Operation Center) efficace</p> <ul style="list-style-type: none"> <li>- Les principes d'un SOC efficace</li> <li>- L'outillage : SIEM, IDS, IPS</li> <li>- L'organisation : les équipes (niveau 1, niveau 2, niveau 3), les compétences (analystes, forensics, ...), ...</li> <li>- Les processus: la gestion d'alerte, l'escalade, la gestion de crise</li> </ul>

### Programme du Mercredi 08 Mars 2017

Matin	<p><b>Séances 4 - M. ABOUNASR</b>                  Une gestion de crise : de la détection à la réponse à l'incident</p> <ul style="list-style-type: none"> <li>- Constitution d'une cellule de crise</li> <li>- Les processus d'escalade</li> </ul>
	<p><b>Séances 5 - M. ABOUNASR</b>                  Une gestion de crise : de la détection à la réponse à l'incident</p> <ul style="list-style-type: none"> <li>- La gestion des équipes multidisciplinaires (IT, Sécurité, Juridique, Communication)</li> <li>- Les interactions avec les autorités</li> </ul>

## Session 3 : Gestion d'incidents et de crise de cyberattaque de grande ampleur

### Programme du Mercredi 08 Mars 2017

Après-midi	<p><b>Séances 6 &amp; 7 - M. ABOUNASR</b>                  Exercice de simulation d'une gestion de crise en temps réel d'une attaque informatique de grande ampleur (exercice participatif impliquant la participation des stagiaires). Chaque participant endossera un rôle dans l'exercice (Responsable informatique, Responsable sécurité, Directeur Financier, Autorité de régulation, Directeur de la communication, ...) pour mener à bien la gestion de crise.</p>
------------	---

### Programme du Jeudi 09 Mars 2017

Matin	<p><b>Séminaire animée par M. CHOUGDALI</b>                  Etat de l'art sur les cyberattaques des OIV à l'international</p>
Après-midi	<p><b>Table ronde d'experts animée par M. ABOUNASR</b>                  Autour des directives nationales de la DNSSI</p>

### Déroulement des journées

#### Mardi 07 Mars 2017

Matin	09h00 à 10h00 Accueil et inscription des participants avec thé d'accueil	10h00 à 12h00 Séance 1	
	12h00 à 14h00 Pause Déjeuner		
Après midi	14h30 à 15h45 Séance 2	15h45 à 16h00 Pause-café	16h à 17h15 Séance 3

#### Mercredi 08 Mars 2017

Matin	09h00 à 10h20 Séance 4	10h20 à 10h40 Pause-café	10h40 à 12h00 Séance 5
	12h00 à 14h00 Pause Déjeuner		
Après midi	14h30 à 15h45 Séance 6	15h45 à 16h00 Pause-café	16h à 17h15 Séance 7

#### Jeudi 09 Mars 2017

Matin	09h00 à 10h20 Séminaire	10h20 à 10h40 Pause-café	10h40 à 12h00 Séminaire
	12h00 à 14h00 Pause Déjeuner		
Après midi	14h30 à 15h45 Table ronde	15h45 à 16h00 Pause-café	16h à 17h15 Synthèse