

Your Cyber INSURANCE



Plan de formation : Cyber Intelligence and Monitoring (CIM)

Jours	thème de formation	Contenu
2 jours	Cyber Threat Intelligence Technologies de réponse aux incidents	1. Détection et réponse sur les terminaux (EDR – Endpoint Detection & Response). 2. Gestion des informations et des événements de sécurité de nouvelle génération (NG-SIEM – Next-Generation Security Information and Event Management). 3. Analyse du comportement des utilisateurs et des entités (UEBA – User and Entity Behavior Analytics). 4. Orchestration, automatisation et réponse aux incidents de sécurité (SOAR – Security Orchestration, Automation and Response).
1 à 2 jours	Supervision de la cybersécurité Fondamentaux d'un Centre des Opérations de Sécurité (SOC)	1. Les enjeux et les bonnes pratiques de la supervision de la sécurité. 2. Centre des Opérations de Sécurité (SOC) : fonctionnement et modèles. 3. Technologies et exploitation d'un SIEM (Security Information and Event Management).
3 jours	Supervision de la cybersécurité Responsable de la mise en œuvre d'un SIEM	1. Sources de données et collecte des journaux (logs). 2. Centralisation des alertes avec la pile ELK (Elasticsearch, Logstash, Kibana). 3. Détection et analyse des scénarios d'attaque à l'aide de la matrice MITRE ATT&CK. 4. Analyses tactiques réalisées avec un SIEM.