**BTIB**
19 Avenue de la Division Leclerc
92160 Antony
+33 (0)1 41 24 20 07
www.btib.fr

# Descriptif et programme de formation Cybersécurité NIAGARA 4

| | |
|---|---|
| ***Intitulé du stage :*** | **Sécuriser la plateforme de développement NIAGARA⁴**. Formation de niveau intermédiaire. |
| ***Public visé :*** | Ingénieurs ou techniciens de programmation et d'intégration des systèmes d'information technique du bâtiment.<br>Il est recommandé d'avoir une expérience dans le métier de la Gestion Technique du Bâtiment, la supervision technique et les infrastructures informatiques réseaux d'au moins 2 ans. |
| ***Près requis :*** | 1) Maitriser la plateforme de développement NIAGARA⁴<br>2) Connaissance de quelques notions élémentaires sur la topologie d'un réseau informatique (IPV4, SubnetMask, etc.)<br>3) Une expérience avec les fonctionnalités de sécurités Windows (Active Directory) est recommandée<br>4) Connaissance de quelques protocoles de communication classiques (Modbus, BACnet, SNMP) |
| ***Objectifs :*** | Programmer le logiciel de supervision NIAGARA⁴ de manière sécurisée afin de répondre aux enjeux de la cybersécurité et de protéger la supervision des cyberattaques. |
| **Méthodes et pédagogie :** | La formation est assurée par un formateur professionnel interne à l'entreprise BTIB. Durant la formation le stagiaire dispose de supports de cours et d'un poste informatique avec la plateforme logicielle NIAGARA⁴ pour pratiquer les exercices et travaux pratiques |
| **Méthode d'évaluation :** | Evaluation en pourcentage de réussite à la suite d'un exercice pratique et d'un QCM. Une attestation de suivi sera délivrée à chaque candidat |
| **Type d'action de formation :** | Perfectionnement des connaissances de second niveau. Formation permettant de comprendre et d'utiliser de façon sécurisée le logiciel de supervision NIAGARA⁴. |
| **Durée et organisation :** | 3 jours (7h / jour).<br>Formation en groupe de 12 personnes maximum.<br>Formation inter-entreprises. |
| **Lieu et accessibilité :** | En présentiel (Lieu défini par BTIB) - Pour toutes situations de handicap merci de nous contacter |
| **Délais d'accès :** | Il est possible de s'inscrire jusqu'à 48h maximum avant le début de la formation. |
| **Tarifs et modalités :** | 1950 € HT / personne<br>Une commande ou le devis de BTIB signé vous engage dans le processus d'organisation.<br>Arrhes de 750 € TTC à la commande, solde à la fin de la formation à réception de facture.<br>En cas de dédit ou d'abandon par l'entreprise à moins de 15 jours francs avant le début de l'action de formation, ou abandon en cours de formation par un ou plusieurs stagiaires, l'entreprise acquittera le coût total, diminué des sommes que BTIB n'aura pas réellement dépensées ou engagées pour la réalisation de ladite action (article L. 920-9 du code du travail).<br>Si une contestation ou un différend ne peut être réglés à l'amiable, le tribunal du siège de BTIB sera seul compétent pour régler le litige. |
| **Moyens d'encadrement :** | Le formateur (Mr Bruno SOUYRIS) dispose de plus 20 ans d'expériences sur la technologie de ladite formation.<br>Le formateur est également le directeur technique de BTIB sur la technologie NIAGARA⁴. |

**Contact Commerciaux et inscription :** formation@btib.fr | 01 41 24 20 07

**BTIB**
19 Avenue de la Division Leclerc
92160 Antony
+33 (0)1 41 24 20 07
www.btib.fr

# Programme de la formation

| 3 JOURS (9h-18h) | Sujets |
|---|---|
| | Accueil et présentation |
| | Pourquoi mieux sécuriser ? |
| | Le rôle de l'intégrateur système GTB |
| | Les organismes CISA, ANSSI et R2S |
| | Ransomware et Malware |
| | Défense en profondeur |
| | L'environnement OT : DMZ, VLAN, VPN |
| | Matrice de flux de sécurité |
| | Secure By Design et Security Dashboard |
| | TLS et Certificats |
| | Foxs, BACnet/SC et SNMPv3 |
| | Https, Webservices |
| | Architecture PKI |
| | Gestion utilisateur : rôles, permissions, catégories |
| | SAML et SSO Single Sign-on |
| | LDAP |
| | Radius 802.1X |
| | Syslog |

Compétences visées :

- Comprendre et maitriser les outils de cybersécurités sur la plateforme logicielle NIAGARA[4] afin de protéger la supervision contre les cyberattaques.

## PLANNING 2026

- Du 10 au 12 mars
- Du 3 au 5 novembre