AJVDEC-TOGO

ASSOCIATION DES JEUNES VOLONTAIRES POUR LE DÉVELOPPEMENT ET L'ÉCHANGES CULTURELS - TOGO

Cybersécurité • Réseaux • Systèmes & Sécurité

CATALOGUE DES PROJETS DE STAGE ET DE STAGE DE FIN D'ÉTUDES (PFE) D'INGÉNIEUR

1. PRÉSENTATION DU PROGRAMME

L'AJVDEC-TOGO propose aux étudiants des écoles d'ingénieurs et des établissements d'enseignement supérieur des projets fondés sur des problématiques concrètes. L'objectif est de leur permettre de mettre en pratique leurs connaissances tout en développant une véritable expérience de conduite de projet.

Dans le cadre du développement de ses partenariats avec des entreprises et structures technologiques au Togo, l'AJVDEC-TOGO accueille des étudiants ingénieurs et jeunes professionnels souhaitant développer leurs compétences pratiques et acquérir une expérience professionnelle dans des environnements technologiques et innovants.

À travers ces partenariats, l'AJVDEC-TOGO facilite l'intégration des stagiaires au sein de structures professionnelles togolaises, leur permettant de mettre en pratique leurs connaissances, de développer leur autonomie et de participer à des projets concrets répondant aux besoins du terrain.

Chaque étudiant travaille sur un projet défini à partir d'un cahier des charges, avec des objectifs clairement identifiés, des étapes de réalisation et des livrables précis. Selon la nature du projet, sa réalisation peut avoir lieu au sein de l'AJVDEC-TOGO ou auprès d'une structure technique partenaire disposant des équipements et compétences nécessaires.

Les sujets proposés couvrent cinq grands domaines :

- **Cybersécurité**
- **Réseaux**
- **Systèmes & Sécurité**

Projet 01 : Analyse des performances réseau et détection d'anomalies

Type	Stage ciblé
Niveau	Bac+2 à Bac+4
Durée indicative **Lieu :** Lomé	2 à 3 mois
Axe	Réseaux & supervision
Technologies principals	SolarWinds ou Zabbix, Wireshark, SNMP, Syslog
POUR CANDIDATER **PIÈCES À FOURNIR**	**CV + LETTRE DE MOTIVATION** (+ convention de votre établissement si stage conventionné) via Mail : ajvdectogo@gmail.com N'hésitez pas à nous contacter pour de plus amples informations Tél/WhatsApp : +228 90119058 SITE WEB : www.ajvdec-togo.org

Contexte et problématique : Une infrastructure peut être disponible tout en présentant des dégradations difficiles à localiser. Le projet relie la supervision de performance à l'identification de comportements réseau anormaux.

Objectif général : Construire une visibilité exploitable sur les performances et distinguer les incidents de capacité des événements potentiellement liés à la sécurité.

Travaux à réaliser :

- Cartographier les équipements et indicateurs suivis.
- Déployer les sondes et tableaux de bord.
- Définir des seuils et scénarios d'anomalie.
- Analyser quelques incidents simulés ou historiques.
- Documenter les mesures et recommandations.

Livrables attendus :

- Cartographie et inventaire.
- Tableaux de bord et seuils.
- Jeu de scénarios.
- Rapport d'analyse.

Critères de validation :

- Indicateurs cohérents et historisés.
- Anomalies identifiées avec justification.
- Rapport reproductible et documenté.

Extensions possibles : Corrélation avec un SIEM ou avec les journaux firewall.

Projet 02 : Audit et sécurisation d'une infrastructure réseau d'entreprise

Type	Stage ciblé
Niveau	Bac+2 à Bac+4
Durée indicative **Lieu :** Lomé	2 à 4 mois
Axe	Réseaux & sécurité
Technologies principals	Nmap, Wireshark, firewall, VLAN, ACL, OPNsense/pfSense
POUR CANDIDATER **PIÈCES À FOURNIR**	**CV + LETTRE DE MOTIVATION** (+ convention de votre établissement si stage conventionné) via Mail : ajvdectogo@gmail.com N'hésitez pas à nous contacter pour de plus amples informations Tél/WhatsApp : +228 90119058 SITE WEB : www.ajvdec-togo.org

Contexte et problématique : Une infrastructure réseau doit être évaluée avant de pouvoir définir une architecture de sécurité cohérente.

Objectif général : Identifier les faiblesses réseau et mettre en œuvre un ensemble de mesures de sécurisation vérifiables.

Travaux à réaliser :

- Cartographier l'existant et les flux.
- Auditer les services et règles de filtrage.
- Identifier les expositions et mauvaises configurations.
- Mettre en œuvre segmentation, filtrage et durcissement.
- Réaliser un avant/après.

Livrables attendus :

- Cartographie.
- Matrice de flux.
- Rapport d'audit.
- Configuration sécurisée.
- Plan de tests.

Critères de validation :

- Vulnérabilités classées et justifiées.
- Règles testées.
- Réduction mesurable de l'exposition.

Extensions possibles : Ajouter détection Suricata/Snort et centralisation des événements.

Projet 03 : Conception d’une architecture NAC avec 802.1X et segmentation dynamique

Type	Projet avancé
Niveau	Bac+3 à Bac+5
Durée indicative **Lieu :** Lomé	3 à 5 mois
Axe	Réseaux & contrôle d’accès
Technologies principals	802.1X, RADIUS, VLAN dynamiques, Active Directory/LDAP, switch
POUR CANDIDATER **PIÈCES À FOURNIR**	**CV + LETTRE DE MOTIVATION** (+ convention de votre établissement si stage conventionné) via Mail : ajvdectogo@gmail.com N'hésitez pas à nous contacter pour de plus amples informations Tél/WhatsApp : +228 90119058 SITE WEB : www.ajvdec-togo.org

Contexte et problématique : Le contrôle d’accès au réseau doit tenir compte de l’identité de l’utilisateur et de l’équipement afin d’éviter un accès réseau implicite.

Objectif général : Concevoir et tester une architecture NAC capable d’autoriser, refuser ou restreindre les connexions selon des politiques définies.

Travaux à réaliser :

- Définir les profils utilisateurs et équipements.
- Mettre en œuvre authentification et politiques NAC.
- Déployer VLAN ou quarantaine dynamique.
- Tester équipements conformes et non conformes.
- Mesurer l’efficacité et les limites.

Livrables attendus :

- Architecture NAC.
- Politiques d’accès.
- Configuration.
- Scénarios et résultats.
- Guide d’exploitation.

Critères de validation :

- Accès autorisés correctement établis.
- Cas de refus/quarantaine démontrés.
- Traçabilité des authentifications.

Extensions possibles : Ajouter intégration SIEM et automatisation de réponse aux équipements non conformes.

Projet 04 : Détection et analyse des attaques DNS dans une infrastructure d'entreprise

Type	Stage avancé
Niveau	Bac+3 à Bac+5
Durée indicative **Lieu :** Lomé	3 à 4 mois
Axe	Network Security
Technologies principals	Zeek, Suricata, DNS logs, Wireshark, SIEM
POUR CANDIDATER **PIÈCES À FOURNIR**	**CV + LETTRE DE MOTIVATION** (+ convention de votre établissement si stage conventionné) via Mail : ajvdectogo@gmail.com N'hésitez pas à nous contacter pour de plus amples informations Tél/WhatsApp : +228 90119058 SITE WEB : www.ajvdec-togo.org

Contexte et problématique : Le DNS fournit des données utiles pour détecter des comportements anormaux comme les résolutions inhabituelles, certains tunnels ou l'usage de domaines malveillants.

Objectif général : Construire une chaîne de visibilité et de détection centrée sur le trafic DNS.

Travaux à réaliser :

- Collecter et normaliser les requêtes DNS.
- Définir des indicateurs et règles.
- Simuler plusieurs comportements suspects en laboratoire.
- Corréler DNS, réseau et endpoint.
- Évaluer faux positifs et couverture.

Livrables attendus :

- Architecture.
- Règles de détection.
- Jeu de tests.
- Dashboard.
- Rapport d'évaluation.

Critères de validation :

- Scénarios détectés avec traces exploitables.
- Règles expliquées et testées.
- Limites documentées.

Extensions possibles : Ajouter enrichissement Threat Intelligence via MISP.

Projet 05 : Sécurisation et détection des attaques sur un réseau Wi-Fi d'entreprise ou public

Type	Stage ciblé
Niveau	Bac+2 à Bac+4
Durée indicative **Lieu :** Lomé	2 à 4 mois
Axe	Wireless Security
Technologies principals	WPA2/WPA3, contrôleur/AP, Wireshark, Suricata, RADIUS
POUR CANDIDATER **PIÈCES À FOURNIR**	**CV + LETTRE DE MOTIVATION** (+ convention de votre établissement si stage conventionné) via Mail : ajvdectogo@gmail.com N'hésitez pas à nous contacter pour de plus amples informations Tél/WhatsApp : +228 90119058 SITE WEB : www.ajvdec-togo.org

Contexte et problématique : Les réseaux Wi-Fi exposent des risques liés à l'authentification, à l'isolation et aux points d'accès non autorisés.

Objectif général : Mettre en place une architecture Wi-Fi sécurisée puis vérifier sa résistance par des scénarios contrôlés.

Travaux à réaliser :

- Analyser la couverture et les flux.
- Définir l'authentification et l'isolation.
- Sécuriser les paramètres des AP.
- Détecter des comportements suspects dans le lab.
- Documenter la configuration et les contrôles.

Livrables attendus :

- Architecture Wi-Fi.
- Politique de sécurité.
- Configuration.
- Scénarios de test.
- Rapport.

Critères de validation :

- Segmentation effective.
- Authentification vérifiée.
- Événements suspects visibles.

Extensions possibles : Intégrer WPA-Enterprise/802.1X et supervision centralisée.

Projet 06 : Audit et sécurisation d’un environnement Active Directory

Type	Projet avancé / PFE
Niveau	Bac+4 à Bac+5
Durée indicative **Lieu :** Lomé	4 à 6 mois
Axe	Identity & Enterprise Security
Technologies principals	Active Directory, GPO, PowerShell, BloodHound, Sysmon, Wazuh
POUR CANDIDATER **PIÈCES À FOURNIR**	**CV + LETTRE DE MOTIVATION** (+ convention de votre établissement si stage conventionné) via Mail : ajvdectogo@gmail.com N'hésitez pas à nous contacter pour de plus amples informations Tél/WhatsApp : +228 90119058 SITE WEB : www.ajvdec-togo.org

Contexte et problématique : Les erreurs de configuration et les privilèges excessifs dans Active Directory peuvent faciliter une compromission et les mouvements latéraux.

Objectif général : Évaluer la posture AD, simuler des scénarios de compromission autorisés et appliquer des mesures de remédiation.

Travaux à réaliser :

- Inventorier utilisateurs, groupes, privilèges et relations.
- Auditer les GPO et configurations sensibles.
- Construire des scénarios d’attaque en laboratoire.
- Mettre en place détection et journalisation.
- Réaliser la remédiation et un nouvel audit.

Livrables attendus :

- Cartographie AD.
- Rapport d’audit.
- Scénarios.
- Règles de détection.
- Plan de remédiation.

Critères de validation :

- Chemins de privilège identifiés.
- Scénarios détectés ou documentés.
- Écart avant/après mesuré.

Extensions possibles : Corrélation avec SIEM, SOAR et Threat Intelligence.

Projet 07 : Analyse et reconstruction d'une cyberattaque dans une infrastructure d'entreprise

Type	Projet phare
Niveau	Bac+3 à Bac+5
Durée indicative **Lieu :** Lomé	3 à 6 mois
Axe	SOC / Incident Response
Technologies principals	Wazuh, Nessus, Metasploit, Sysmon, Wireshark, MITRE ATT&CK
POUR CANDIDATER **PIÈCES À FOURNIR**	**CV + LETTRE DE MOTIVATION** (+ convention de votre établissement si stage conventionné) via Mail : ajvdectogo@gmail.com N'hésitez pas à nous contacter pour de plus amples informations Tél/WhatsApp : +228 90119058 SITE WEB : www.ajvdec-togo.org

Contexte et problématique : Une organisation doit être capable non seulement de détecter un incident, mais aussi de comprendre sa chronologie, les techniques utilisées et les traces laissées sur les systèmes.

Objectif général : Simuler une attaque multi-étapes, observer les traces produites, reconstruire la chaîne d'attaque et proposer des mesures de détection et de remédiation.

Travaux à réaliser :

- Concevoir le lab et le périmètre autorisé.
- Évaluer les vulnérabilités.
- Réaliser des simulations d'attaque contrôlées.
- Collecter logs, événements et captures.
- Construire une timeline et mapper les techniques MITRE ATT&CK.
- Rédiger les recommandations et refaire certains tests après remédiation.

Livrables attendus :

- Architecture du lab.
- Rapport de vulnérabilités.
- Timeline de l'attaque.
- Cartographie MITRE ATT&CK.
- Règles/alertes.
- Rapport d'incident.

Critères de validation:

- Chaîne d'attaque reconstruite à partir de preuves.
- Détections démontrées sur plusieurs étapes.
- Recommandations vérifiées par un second test.

Extensions possibles : Ajouter SOAR, CTI et réponse active encadrée.

Projet 08 : Conception et déploiement d'une plateforme SIEM/XDR pour la détection des incidents

Type	Projet avancé / PFE
Niveau	Bac+4 à Bac+5
Durée indicative **Lieu :** Lomé	4 à 6 mois
Axe	SOC / SIEM-XDR
Technologies principals	Wazuh, Sysmon, Suricata, agents Windows/Linux, dashboards
POUR CANDIDATER **PIÈCES À FOURNIR**	**CV + LETTRE DE MOTIVATION** (+ convention de votre établissement si stage conventionné) via Mail : ajvdectogo@gmail.com N'hésitez pas à nous contacter pour de plus amples informations Tél/WhatsApp : +228 90119058 SITE WEB : www.ajvdec-togo.org

Contexte et problématique : Les organisations ont besoin de centraliser les événements provenant des endpoints, serveurs et réseaux afin de construire une vision cohérente des incidents.

Objectif général : Construire une plateforme de détection intégrée et mesurer sa couverture sur un jeu de scénarios réalistes.

Travaux à réaliser :

- Définir les sources et use cases.
- Déployer les agents et capteurs.
- Créer ou adapter des règles de détection.
- Construire dashboards et procédures de triage.
- Mesurer couverture, bruit et temps de traitement.

Livrables attendus :

- Architecture SIEM/XDR.
- Use cases.
- Règles.
- Dashboards.
- Plan de tests.
- Rapport d'évaluation.

Critères de validation :

- Événements correctement collectés.
- Scénarios détectés.
- Mesures de couverture et faux positifs.

Extensions possibles : Intégrer SOAR, CTI, tickets et réponse endpoint.

Projet 09 : Network Detection & Response (NDR) pour la visibilité et l'investigation réseau

Type	Projet avancé / PFE
Niveau	Bac+4 à Bac+5
Durée indicative **Lieu :** Lomé	4 à 6 mois
Axe	Network Security Operations
Technologies principals	Zeek, Suricata, Wireshark, Wazuh/Elastic, SPAN/TAP
POUR CANDIDATER **PIÈCES À FOURNIR**	**CV + LETTRE DE MOTIVATION** (+ convention de votre établissement si stage conventionné) via Mail : ajvdectogo@gmail.com N'hésitez pas à nous contacter pour de plus amples informations Tél/WhatsApp : +228 90119058 SITE WEB : www.ajvdec-togo.org

Contexte et problématique : Les métadonnées réseau peuvent compléter les journaux endpoint et révéler des scans, communications atypiques, anomalies DNS/HTTP/TLS ou mouvements latéraux.

Objectif général : Concevoir une chaîne NDR permettant de collecter, détecter, corréler et investiguer les activités réseau.

Travaux à réaliser :

- Concevoir le point de visibilité.
- Collecter métadonnées et alertes.
- Créer des règles ou signatures adaptées.
- Corréler avec endpoint et identité.
- Évaluer les scénarios et la qualité des détections.

Livrables attendus :

- Architecture NDR.
- Capteurs.
- Règles.
- Jeu de données.
- Dashboard.
- Rapport.

Critères de validation :

- Scénarios de scans/anomalies détectés.
- Investigation reproductible.
- Couverture et limites mesurées.

Extensions possibles : Ajouter Threat Hunting et enrichissement IOC.

Projet 10 : Détection et réponse aux attaques sur les endpoints avec une plateforme EDR

Type	Projet avancé / PFE
Niveau	Bac+4 à Bac+5
Durée indicative **Lieu :** Lomé	4 à 6 mois
Axe	Endpoint Security
Technologies principals	Wazuh, Sysmon, osquery ou EDR équivalent, PowerShell, Sigma
POUR CANDIDATER **PIÈCES À FOURNIR**	**CV + LETTRE DE MOTIVATION** (+ convention de votre établissement si stage conventionné) via Mail : ajvdectogo@gmail.com N'hésitez pas à nous contacter pour de plus amples informations Tél/WhatsApp : +228 90119058 SITE WEB : www.ajvdec-togo.org

Contexte et problématique : Les événements de processus, fichiers et connexions peuvent révéler des comportements malveillants qui échappent à une protection uniquement fondée sur les signatures.

Objectif général : Déployer une capacité de détection endpoint et démontrer plusieurs actions de réponse encadrées.

Travaux à réaliser :

- Déployer les agents.
- Construire des règles de comportement.
- Simuler exécution suspecte, persistance et élévation dans un lab.
- Analyser les chronologies endpoint.
- Tester isolation ou remédiation selon la solution.

Livrables attendus :

- Architecture EDR.
- Politiques.
- Règles.
- Scénarios.
- Playbooks.
- Rapport.

Critères de validation :

- Télémétrie exploitable.
- Détections reproductibles.
- Réponses contrôlées et tracées.

Extensions possibles : Intégration SIEM/NDR/SOAR.

Projet 11 : Plateforme SOAR pour l'automatisation de la réponse aux incidents

Type	Projet avancé / PFE
Niveau	Bac+4 à Bac+5
Durée indicative **Lieu :** Lomé	4 à 6 mois
Axe	SOC Automation
Technologies principals	Shuffle ou SOAR équivalent, Wazuh, MISP, APIs, Python, firewall
POUR CANDIDATER **PIÈCES À FOURNIR**	**CV + LETTRE DE MOTIVATION** (+ convention de votre établissement si stage conventionné) via Mail : ajvdectogo@gmail.com N'hésitez pas à nous contacter pour de plus amples informations Tél/WhatsApp : +228 90119058 SITE WEB : www.ajvdec-togo.org

Contexte et problématique : Une partie des actions de triage et de réponse est répétitive. L'automatisation peut réduire les délais tout en conservant des points de contrôle humains.

Objectif général : Concevoir et évaluer des playbooks automatisés pour plusieurs types d'incidents.

Travaux à réaliser :

- Identifier les tâches automatisables.
- Concevoir les playbooks.
- Connecter SIEM, CTI et outils d'action.
- Ajouter validations humaines pour les actions sensibles.
- Mesurer temps gagné, erreurs et échecs.

Livrables attendus :

- Architecture SOAR.
- Playbooks.
- Connecteurs.
- Scénarios.
- Journal d'exécution.
- KPI.

Critères de validation :

- Déclenchement correct.
- Actions tracées.
- KPI comparant manuel et automatisé.

Extensions possibles : Ajouter réponse firewall, quarantaine endpoint et gestion de tickets.

Projet 12 : Plateforme de Cyber Threat Intelligence intégrée à la défense

Type	Projet avancé / PFE
Niveau	Bac+4 à Bac+5
Durée indicative **Lieu :** Lomé	4 à 6 mois
Axe	Threat Intelligence
Technologies principals	MISP, STIX/TAXII, VirusTotal, SIEM, Python/API
POUR CANDIDATER **PIÈCES À FOURNIR**	**CV + LETTRE DE MOTIVATION** (+ convention de votre établissement si stage conventionné) via Mail : ajvdectogo@gmail.com N'hésitez pas à nous contacter pour de plus amples informations Tél/WhatsApp : +228 90119058 SITE WEB : www.ajvdec-togo.org

Contexte et problématique : Les IOC perdent de leur valeur s'ils ne sont pas qualifiés, enrichis, dédupliqués et reliés aux outils de défense.

Objectif général : Construire une chaîne CTI capable de collecter, enrichir et exploiter des indicateurs dans la détection.

Travaux à réaliser :

- Définir sources et modèle de données.
- Collecter et normaliser les IOC.
- Enrichir et qualifier les indicateurs.
- Dédupliquer et gérer la confiance.
- Publier les informations vers un SIEM ou IDS.

Livrables attendus :

- Architecture CTI.
- Connecteurs.
- Modèle de données.
- Flux d'intégration.
- Dashboard.
- Rapport.

Critères de validation :

- IOC correctement normalisés.
- Enrichissement démontré.
- Intégration opérationnelle avec la défense.

Extensions possibles : Ajouter TAXII et automatisation SOAR.

Projet 13 : Threat Hunting dans une infrastructure d'entreprise

Type	Projet avancé / PFE
Niveau	Bac+4 à Bac+5
Durée indicative **Lieu :** Lomé	4 à 6 mois
Axe	SOC / Detection Engineering
Technologies principals	Wazuh/Elastic, Sysmon, Sigma, Zeek, MITRE ATT&CK
POUR CANDIDATER **PIÈCES À FOURNIR**	**CV + LETTRE DE MOTIVATION** (+ convention de votre établissement si stage conventionné) via Mail : ajvdectogo@gmail.com N'hésitez pas à nous contacter pour de plus amples informations Tél/WhatsApp : +228 90119058 SITE WEB : www.ajvdec-togo.org

Contexte et problématique : La détection ne doit pas reposer uniquement sur les alertes. Le Threat Hunting cherche activement des comportements révélateurs d'une compromission.

Objectif général : Mettre en place une démarche reproductible de chasse aux menaces fondée sur des hypothèses et des preuves.

Travaux à réaliser :

- Choisir des hypothèses de menace.
- Identifier les sources nécessaires.
- Construire des requêtes et règles.
- Analyser les traces et confirmer ou infirmer les hypothèses.
- Documenter les résultats et détections créées.

Livrables attendus :

- Hypothèses de chasse.
- Requêtes/règles.
- Jeux de données.
- Rapports de chasse.
- Nouveaux use cases.

Critères de validation :

- Hypothèses testables.
- Résultats justifiés par des traces.
- Nouvelles détections réutilisables.

Extensions possibles : Automatiser l'enrichissement par CTI.

Projet 14 : Détection et réponse à un ransomware en environnement contrôlé

Type	Projet phare / PFE
Niveau	Bac+4 à Bac+5
Durée indicative **Lieu :** Lomé	4 à 6 mois
Axe	Ransomware / Incident Response
Technologies principals	Wazuh, Sysmon, FIM, Suricata, Python, SOAR
POUR CANDIDATER **PIÈCES À FOURNIR**	**CV + LETTRE DE MOTIVATION** (+ convention de votre établissement si stage conventionné) via Mail : ajvdectogo@gmail.com N'hésitez pas à nous contacter pour de plus amples informations Tél/WhatsApp : +228 90119058 SITE WEB : www.ajvdec-togo.org

Contexte et problématique : Les attaques par ransomware imposent une détection rapide, un confinement maîtrisé et une capacité à analyser la chronologie et l'impact.

Objectif général : Simuler un comportement de ransomware non destructif dans un laboratoire et démontrer une chaîne de détection, confinement et récupération.

Travaux à réaliser :

- Préparer un environnement de test et des données fictives.
- Simuler des comportements représentatifs sans utiliser de charge destructive.
- Détecter changements massifs, processus et communications.
- Déclencher quarantaine ou actions de réponse.
- Évaluer temps de détection et de réaction.

Livrables attendus :

- Architecture.
- Scénario.
- Règles de détection.
- Playbooks.
- Rapport d'incident.
- KPI.

Critères de validation :

- Détection du scénario.
- Réponse déclenchée de façon maîtrisée.
- Mesures TTD/TTR et limites.

Extensions possibles : Ajouter sauvegarde, restauration et enrichissement CTI.

Projet 15: Exercice Red Team / Blue Team d'une entreprise simulée

Type	Projet phare / PFE
Niveau	Bac+4 à Bac+5
Durée indicative **Lieu :** Lomé	4 à 6 mois
Axe	Offensive & Defensive Security
Technologies principals	Kali, Metasploit, Nmap, Burp Suite, Wazuh, Suricata, MITRE ATT&CK
POUR CANDIDATER **PIÈCES À FOURNIR**	**CV + LETTRE DE MOTIVATION** (+ convention de votre établissement si stage conventionné) via Mail : ajvdectogo@gmail.com N'hésitez pas à nous contacter pour de plus amples informations Tél/WhatsApp : +228 90119058 SITE WEB : www.ajvdec-togo.org

Contexte et problématique : Une architecture de sécurité doit être testée de manière réaliste pour vérifier les capacités de prévention, détection et réponse.

Objectif général : Construire un exercice répétable dans lequel une équipe offensive mène des scénarios autorisés et une équipe défensive surveille, détecte et répond.

Travaux à réaliser :

- Concevoir l'environnement et les règles d'engagement.
- Préparer les scénarios offensifs.
- Définir les use cases défensifs.
- Exécuter les scénarios et collecter les preuves.
- Mesurer détection, confinement et remédiation.

Livrables attendus :

- Architecture.
- Rules of engagement.
- Scénarios Red Team.
- Matrice détection/réponse.
- Rapport final.

Critères de validation :

- Tous les scénarios documentés.
- Preuves techniques disponibles.
- Mesures avant/après amélioration.

Extensions possibles : Étendre au Cloud ou à l'Active Directory.

Projet 16 : Audit de sécurité et exploitation contrôlée d'une infrastructure d'entreprise

Type	Projet avancé
Niveau	Bac+3 à Bac+5
Durée indicative **Lieu :** Lomé	3 à 5 mois
Axe	Offensive Security
Technologies principals	Nmap, Nessus, Burp Suite, Metasploit, Nuclei, Wireshark
POUR CANDIDATER **PIÈCES À FOURNIR**	**CV + LETTRE DE MOTIVATION** (+ convention de votre établissement si stage conventionné) via Mail : ajvdectogo@gmail.com N'hésitez pas à nous contacter pour de plus amples informations Tél/WhatsApp : +228 90119058 SITE WEB : www.ajvdec-togo.org

Contexte et problématique : Un audit de sécurité utile doit aller au-delà d'un scan automatique et relier vulnérabilités, exploitation contrôlée, impact et remédiation.

Objectif général : Réaliser un audit offensif encadré sur une infrastructure de laboratoire et fournir un plan de correction priorisé.

Travaux à réaliser :

- Définir le périmètre.
- Effectuer reconnaissance et énumération.
- Analyser les vulnérabilités.
- Valider quelques failles sans détruire le système.
- Documenter les preuves et recommandations.

Livrables attendus :

- Plan de test.
- Rapport de vulnérabilités.
- Preuves techniques.
- Plan de remédiation.
- Rapport de re-test.

Critères de validation :

- Périmètre respecté.
- Constats reproductibles.
- Risque et correction clairement expliqués.

Extensions possibles : Corréler les résultats avec SIEM/CTI.

Projet 17 : Sécurité d’une application Web : audit, exploitation contrôlée et remédiation

Type	Projet avancé
Niveau	Bac+3 à Bac+5
Durée indicative **Lieu :** Lomé	3 à 5 mois
Axe	Application Security
Technologies principals	Burp Suite, OWASP ZAP, Nuclei, Semgrep, OWASP ASVS
POUR CANDIDATER **PIÈCES À FOURNIR**	**CV + LETTRE DE MOTIVATION** (+ convention de votre établissement si stage conventionné) via Mail : ajvdectogo@gmail.com N'hésitez pas à nous contacter pour de plus amples informations Tél/WhatsApp : +228 90119058 SITE WEB : www.ajvdec-togo.org

Contexte et problématique : Les applications web concentrent des risques d’authentification, autorisation, validation d’entrée et exposition de données.

Objectif général : Évaluer une application de laboratoire, démontrer des vulnérabilités autorisées puis vérifier les correctifs.

Travaux à réaliser :

- Cartographier les fonctionnalités.
- Tester authentification, autorisation et entrées.
- Analyser les composants et configurations.
- Documenter les preuves sans compromettre les données.
- Appliquer les correctifs et réaliser un re-test.

Livrables attendus :

- Cartographie.
- Rapport d’audit.
- Preuves.
- Correctifs.
- Rapport de validation.

Critères de validation :

- Constats reproductibles.
- Correctifs testés.
- Réduction des vulnérabilités démontrée.

Extensions possibles : Ajouter CI/CD et sécurité du code.

Projet 18 : Analyse forensique et reconstruction d'un incident numérique

Type	Projet avancé / PFE
Niveau	Bac+3 à Bac+5
Durée indicative	3 à 5 mois
Axe	DFIR
Technologies principals	Autopsy, FTK Imager ou équivalent, Volatility, Wireshark, logs, Windows/Linux
POUR CANDIDATER **PIÈCES À FOURNIR**	**CV + LETTRE DE MOTIVATION** (+ convention de votre établissement si stage conventionné) via Mail : ajvdectogo@gmail.com N'hésitez pas à nous contacter pour de plus amples informations Tél/WhatsApp : +228 90119058 SITE WEB : www.ajvdec-togo.org

Contexte et problématique : Après un incident, les équipes doivent déterminer ce qui s'est passé à partir d'artefacts, journaux, fichiers et traces mémoire.

Objectif général : Mettre en œuvre une démarche d'investigation reproductible et reconstruire une chronologie à partir d'éléments de preuve.

Travaux à réaliser :

- Préserver et identifier les éléments.
- Analyser disque, mémoire et journaux selon le scénario.
- Extraire les artefacts utiles.
- Construire la timeline.
- Distinguer faits observés, hypothèses et limites.

Livrables attendus :

- Chaîne de traitement.
- Rapport forensique.
- Timeline.
- IOC/artefacts.
- Annexes techniques.

Critères de validation :

- Méthodes documentées.
- Résultats reproductibles.
- Chronologie justifiée.

Extensions possibles : Corréler avec SIEM et CTI.

Projet 19 : Conception d’une plateforme de Privileged Access Management (PAM)

Type	Projet avancé / PFE
Niveau	Bac+4 à Bac+5
Durée indicative	4 à 6 mois
Axe	Identity Security
Technologies principals	PAM/bastion, AD/LDAP, MFA, RBAC, coffre de secrets
POUR CANDIDATER **PIÈCES À FOURNIR**	**CV + LETTRE DE MOTIVATION** (+ convention de votre établissement si stage conventionné) via Mail : ajvdectogo@gmail.com N'hésitez pas à nous contacter pour de plus amples informations Tél/WhatsApp : +228 90119058 SITE WEB : www.ajvdec-togo.org

Contexte et problématique : Les comptes privilégiés concentrent des risques importants. Le contrôle doit couvrir identité, moindre privilège, secrets et traçabilité des sessions.

Objectif général : Concevoir et prototyper une architecture PAM adaptée à une infrastructure d’entreprise.

Travaux à réaliser :

- Inventorier les comptes privilégiés.
- Définir RBAC et politiques.
- Mettre en place bastion/coffre.
- Activer MFA et traçabilité.
- Tester élévation, révocation et revue des accès.

Livrables attendus :

- Architecture PAM.
- Politiques.
- Prototype.
- Journalisation.
- Plan de revue.

Critères de validation :

- Accès nominatif et contrôlé.
- Sessions tracées.
- Revue des droits démontrée.

Extensions possibles : Ajouter accès juste-à-temps et intégration SIEM.

Projet 20 : Conception et expérimentation d’une architecture Zero Trust

Type	Projet avancé / PFE
Niveau	Bac+4 à Bac+5
Durée indicative	4 à 6 mois
Axe	Zero Trust
Technologies principals	IAM, MFA, SSO, ZTNA, micro-segmentation, firewall
POUR CANDIDATER **PIÈCES À FOURNIR**	**CV + LETTRE DE MOTIVATION** (+ convention de votre établissement si stage conventionné) via Mail : ajvdectogo@gmail.com N'hésitez pas à nous contacter pour de plus amples informations Tél/WhatsApp : +228 90119058 SITE WEB : www.ajvdec-togo.org

Contexte et problématique : Les environnements hybrides rendent insuffisant le simple fait d’être sur le réseau interne. Les accès doivent être fondés sur identité, contexte et ressources.

Objectif général : Concevoir une architecture Zero Trust, prototyper ses contrôles et mesurer leurs effets sur l’exposition.

Travaux à réaliser :

- Cartographier ressources, identités et flux.
- Définir politiques d’accès.
- Mettre en place MFA et segmentation.
- Prototyper ZTNA ou accès applicatif.
- Évaluer les écarts avant/après.

Livrables attendus :

- Cartographie.
- Modèle de menace.
- Architecture cible.
- Prototype.
- Politiques.
- Plan de migration.

Critères de validation :

- Accès limités aux ressources prévues.
- Politiques testées.
- Mesure de la visibilité et des écarts.

Extensions possibles : Ajouter posture des appareils et contrôle adaptatif.

Projet 21 : Détection et réponse aux incidents de sécurité dans un environnement Cloud

Type	Projet avancé / PFE
Niveau	Bac+4 à Bac+5
Durée indicative	4 à 6 mois
Axe	Cloud Security
Technologies principals	AWS ou Azure, IAM, CloudTrail/Azure Monitor, SIEM, SOAR
POUR CANDIDATER **PIÈCES À FOURNIR**	**CV + LETTRE DE MOTIVATION** (+ convention de votre établissement si stage conventionné) via Mail : ajvdectogo@gmail.com N'hésitez pas à nous contacter pour de plus amples informations Tél/WhatsApp : +228 90119058 SITE WEB : www.ajvdec-togo.org

Contexte et problématique : Les environnements Cloud introduisent des journaux, identités et chemins d'accès spécifiques qui doivent être surveillés comme une infrastructure d'entreprise.

Objectif général : Mettre en place une chaîne de détection et de réponse centrée sur les événements Cloud et les identités.

Travaux à réaliser :

- Définir l'architecture et les rôles.
- Activer la journalisation Cloud.
- Construire des scénarios de compromission contrôlés.
- Détecter les comportements anormaux.
- Automatiser certaines actions de réponse.

Livrables attendus :

- Architecture Cloud.
- Politiques IAM.
- Use cases.
- Dashboards.
- Playbooks.
- Rapport.

Critères de validation :

- Logs exploitables.
- Scénarios détectés.
- Réponse tracée.

Extensions possibles : Ajouter détection comportementale des identités.

Projet 22 : Détection d’anomalies des identités et des accès dans le Cloud

Type	Projet avancé / PFE
Niveau	Bac+4 à Bac+5
Durée indicative	4 à 6 mois
Axe	Cloud / IAM Analytics
Technologies principals	AWS/Azure logs, Python, SIEM, règles comportementales, API
POUR CANDIDATER **PIÈCES À FOURNIR**	**CV + LETTRE DE MOTIVATION** (+ convention de votre établissement si stage conventionné) via Mail : ajvdectogo@gmail.com N'hésitez pas à nous contacter pour de plus amples informations Tél/WhatsApp : +228 90119058 SITE WEB : www.ajvdec-togo.org

Contexte et problématique : Des comportements d’identité atypiques peuvent constituer un signal précoce de compromission, même lorsque les authentifications réussissent.

Objectif général : Construire un prototype de détection comportementale basé sur les événements IAM et mesurer sa pertinence.

Travaux à réaliser :

- Collecter des événements d’identité.
- Définir les comportements de référence.
- Créer indicateurs et règles d’anomalie.
- Simuler des comportements suspects.
- Évaluer précision, faux positifs et limites.

Livrables attendus :

- Modèle de détection.
- Jeu de données.
- Règles.
- Dashboard.
- Rapport d’évaluation.

Critères de validation :

- Scénarios clairement définis.
- Anomalies détectées et expliquées.
- Mesures quantitatives.

Extensions possibles : Comparer règles déterministes et modèle ML.

Projet 23 : Sécurité des systèmes utilisant l'intelligence artificielle : menaces, contrôles et tests

Type	Projet de recherche appliquée / PFE
Niveau	Bac+4 à Bac+5
Durée indicative	4 à 6 mois
Axe	AI Security
Technologies principals	LLM local ou API de test, applications RAG, logs, red teaming encadré
POUR CANDIDATER **PIÈCES À FOURNIR**	**CV + LETTRE DE MOTIVATION** (+ convention de votre établissement si stage conventionné) via Mail : ajvdectogo@gmail.com N'hésitez pas à nous contacter pour de plus amples informations Tél/WhatsApp : +228 90119058 SITE WEB : www.ajvdec-togo.org

Contexte et problématique : Les applications utilisant des modèles d'IA introduisent de nouvelles surfaces d'attaque et de nouvelles exigences de contrôle.

Objectif général : Étudier des scénarios de sécurité sur une application IA de laboratoire et proposer des mécanismes de réduction du risque.

Travaux à réaliser :

- Cartographier les composants et flux.
- Identifier menaces pertinentes pour le cas d'usage.
- Construire un banc de test.
- Tester robustesse des contrôles.
- Documenter les résultats et limites.

Livrables attendus :

- Architecture.
- Modèle de menace.
- Jeu de tests.
- Contrôles.
- Rapport.

Critères de validation :

- Scénarios reproductibles.
- Mesures de contrôle documentées.
- Distinction claire entre comportement attendu et vulnérabilité.

Extensions possibles : Ajouter sécurité des données, secrets et journaux.

Projet 24 : Triage et analyse assistés par IA des alertes d'un SOC

Type	Projet de recherche appliquée / PFE
Niveau	Bac+4 à Bac+5
Durée indicative	4 à 6 mois
Axe	SOC + IA
Technologies principals	Wazuh/Elastic, Python, LLM local ou API de test, MISP, ticketing
POUR CANDIDATER **PIÈCES À FOURNIR**	**CV + LETTRE DE MOTIVATION** (+ convention de votre établissement si stage conventionné) via Mail : ajvdectogo@gmail.com N'hésitez pas à nous contacter pour de plus amples informations Tél/WhatsApp : +228 90119058 SITE WEB : www.ajvdec-togo.org

Contexte et problématique : Le volume d'alertes peut ralentir les analystes. Une assistance IA peut aider à résumer, enrichir et prioriser sans remplacer la validation humaine.

Objectif général : Prototyper un système d'assistance au triage qui explique ses sorties et conserve un contrôle humain sur les décisions.

Travaux à réaliser :

- Définir les cas d'usage.
- Construire le pipeline d'extraction d'alertes.
- Ajouter enrichissement CTI et contexte.
- Générer résumés et suggestions de classification.
- Évaluer qualité, erreurs et risques d'hallucination.

Livrables attendus :

- Architecture.
- Pipeline.
- Jeu de tests.
- Interface ou rapports.
- Métriques d'évaluation.

Critères de validation :

- Sorties traçables et vérifiables.
- Évaluation humaine documentée.
- Aucune action sensible exécutée sans validation.

Extensions possibles : Ajouter recommandation de playbooks et retour analyste.

Règles communes de réalisation

- Tout test d’intrusion, simulation d’attaque, collecte de données ou exploitation doit rester dans un périmètre explicitement autorisé.
- Les environnements de laboratoire doivent être isolés lorsque les scénarios présentent un risque de propagation ou d’altération.
- Les données sensibles doivent être fictives ou protégées et ne doivent être utilisées que pour le besoin autorisé.
- Chaque projet doit comporter un plan de tests, des preuves de fonctionnement et une documentation des limites.
- Les actions automatisées à impact doivent comporter des garde-fous et, pour les projets concernés, une validation humaine.
- La démonstration finale doit montrer le problème initial, l’architecture, les tests, les résultats et les améliorations apportées.

Livrables communs

- Rapport technique ou mémoire.
- Schéma d’architecture et cartographie.
- Configurations, scripts ou playbooks.
- Plan de tests et résultats.
- Captures, journaux, tableaux de bord ou preuves techniques.
- Guide d’exploitation et recommandations.
- Présentation et démonstration finale.