

DOSSIER DE COMPETENCES

**CONSEILLER SENIOR EN CYBERSÉCURITÉ | OSEP | OSCP | EWPTX V2
| ECCPT V2 | CARTP | CRTP | CCSK
JIMMY NGUEGUIM (M. Sc)**

TEL: +1 (438) 465-0033

COURRIEL: contact@jimmy-ngueguim.com

LINKEDIN: [linkedin.com/in/jimmy-ngueguim/](https://www.linkedin.com/in/jimmy-ngueguim/)

COMPETENCES

POINTS FORTS

- **Maîtrise du développement et du scripting** (Python, PowerShell, Bash, javascript)
- **Communication fluide, structurée et adaptée** au niveau technique des parties prenantes
- **Expérience en encadrement d'équipes multidisciplinaires** et gestion de projets techniques
- **Détermination constante et engagement soutenu** pour atteindre les objectifs
- **Autonomie, proactivité et capacité à prioriser** en environnement complexe
- **Excellente qualité rédactionnelle** orientée livrables techniques et stratégiques

COMPETENCES FONCTIONNELLES

- Gestion des vulnérabilités, définition de scénarios d'attaque, analyse de risque opérationnel, coordination avec les parties prenantes, rédaction de livrables techniques et stratégiques, validation des contrôles de sécurité, support aux audits internes, veille stratégique.

COMPETENCES TECHNIQUES

RESEAUX	Sniffing réseau, analyse de paquets, reconnaissance passive, pivoting réseau, spoofing DHCP, évasion de filtrage, contournement WAF (Big-IP, WAF Azure), test de segmentation réseau, attaque LLMNR, tunnel inversé, persistance réseau.
DevSecOps	Intégration OWASP 10, développement sécurisé, automatisation par script, tests SAST/DAST, sécurisation du code IaC, durcissement des pipelines CI/CD (Jenkins).
Pentest Web/API	Évaluation logique applicative, authentification, validation d'entrée, contrôle d'accès, gestion de session, injections SQL/XML/JSON, fuzzing d'objets, CSRF, IDOR, entêtes HTTP, versionnage d'API, gestion des erreurs.
Pentest Interne/AD/OT	Exploitation technologies vulnérables, analyse objets AD, Kerberoasting, Pass-the-Ticket, NTLM relay, attaque LLMNR/NBT-NS, évasion antivirus, escalade privilèges locaux, exploitation ADCS, compromission trust AD, Pivoting IT-OT
Audit technique	Audit O365, Audit Active Directory, Audit de pare-feux, audit technologique

FORMATION

[2024] - MAITRISE EN INFORMATIQUE CHEMINEMENT EN CYBERSÉCURITÉ



Université de Sherbrooke

[2020] - DIPLÔME D'INGÉNIEUR EN SÉCURITÉ INFORMATIQUE



École Nationale Supérieure Polytechnique de Maroua

CERTIFICATIONS

[2024]-	 CCSK – Certificate of Cloud Security Knowledge  PECB – EBIOS Risk Manager  ECCPT v2 – Certified Professional Penetration Tester  OSEP – Offensive Security Experienced Penetration Tester	[2021]-	 NSE 1 2 3 – Fortinet Network Security Expert
[2023]-	 CARTP – Certified Azure Red Team Professional  eWPTXv2 – Web Application Penetration Tester eXtreme  OSCP – Offensive Security Certified Professional  CRTP – Certified Red Team Professional  Certified Splunk Power User		[2020]-  Mastering Web and Infrastructure Reconnaissance [2019]-  C EH – (formation) Certified Ethical Hacker  Acunetix – Vulnerability Scanner  Nessus – Vulnerability Scanner  Metasploit – Exploitation tools  Burp Suite – Vulnerability Scanner
[2022]-	 CRTP – Certified Red Team Professional  EC-Council – Mastering Pentesting Using Kali Linux  EC-Council – Advanced Cryptography Engineering  EC-Council – Mastering Database Reconnaissance&Exploitation		



Sécurité offensive



Sécurité défensive



Gouvernance



Outils & Technologies

TABLEAU SOMMAIRE DES RÉALISATIONS

Mise à jour: Juin 2025

No	CLIENT	MANDAT	RÔLE	ENVERGURE (J-P)	PÉRIODE	EXPÉRIENCE (MOIS)
COLLEGE CDI						
12	Collège CDI – TEMPS PARTIEL –	Chargé de cours en Cybersécurité	Enseignant en Cybersécurité	90	09/2024 à ce jour	4,5
LEVIO CONSEILS INC						
11	Commission des normes, de l'équité, de la santé et de la sécurité du travail (CNESST) – MISSION AU FORFAIT –	Test d'intrusion de l'application SNRT Zone Abonné	Conseiller en cybersécurité	7	06/2025	0.3
10	Ministère de la Justice Québec (MJQ) – MISSION AU FORFAIT –	Test d'intrusion de l'API MISST	Conseiller en cybersécurité	8	04/2025	0.3
9	Quincaillerie Richelieu – MISSION AU FORFAIT –	Test d'intrusion environnement IT&OT	Conseiller en cybersécurité	12	03/2025 à 04/2025	0,5
8	Assemblée nationale du Québec (ASSNAT) – MISSION EN RÉGIE –	Offre de service de conseil en sécurité offensive	Conseiller en cybersécurité	80	02/2025 à ce jour	4
7	Mondata – MISSION AU FORFAIT –	Test d'intrusion de la solution SaaS "MD.ECO"	Conseiller en cybersécurité	22	09/2024 à 10/2024	1
6	Ministère de l'Immigration, de la Francisation et de l'Intégration (MIFI) – MISSION AU FORFAIT –	Tests d'intrusion de l'application web et API ARRIMA-PTET	Conseiller en sécurité offensive	20	02/2024 à 03/2024	1
5	Commission des normes, de l'équité, de la santé et de la sécurité du travail (CNESST) – MISSION AU FORFAIT –	Évaluation de la vulnérabilité et analyse des risques	Conseiller en sécurité offensive	20	12/2023 à 02/2024	1
4	Ministère de la Justice Québec (MJQ) – MISSION EN RÉGIE –	Offre de service de conseil en sécurité offensive	Conseiller en cybersécurité	271	10/2023 à 01/2025	15
3	Sous-traitance industrielle Québec (STIQ) – MISSION AU FORFAIT –	Tests d'intrusion de l'application web et audit de sécurité de l'environnement O356	Conseiller en sécurité offensive	37	08/2023 à 12/2023	2
2	Levio Conseils – MISSION EN INTERNE –	Lead de projet (RS&DE) En Cybersécurité	Conseiller en cybersécurité	130	03/2023 à ce jour	7
NIMBUZ						
1	Nimbuz – MISSION EN INTERNE –	Gestion de vulnérabilités et Tests d'intrusion sur des applications et serveurs d'hébergement	Analyste en tests d'intrusion	1,450	11/2018 au 03/2023	71
TOTAL						107.6 m-p. 8,96 ans

REFERENCES PROJETS – CDI Collège

Collège CDI – TEMPS PARTIEL – 12

Sept. 2024 – A nos jours

Chargé de cours en Cybersécurité

PROJET : Dispenser un cours avancé de cybersécurité à des étudiants, en mettant l'accent sur le développement de compétences pratiques et la maîtrise des concepts clés du domaine. Les étudiants sont initiés aux techniques de tests d'intrusion, à l'analyse des cyberattaques, ainsi qu'aux mécanismes de défense à mettre en œuvre pour sécuriser les systèmes d'information. Le programme couvre également les fondements de l'audit interne en cybersécurité, ainsi que les exigences de conformité aux normes et cadres réglementaires tels que l'ISO/CEI 27001 et la Loi 25. L'ensemble du cours est conçu pour favoriser une compréhension concrète et opérationnelle des enjeux contemporains en sécurité des technologies de l'information.

DOMAINE D'INTERVENTION :

- **Élaboration de contenus pédagogiques en cybersécurité :** Conception de modules structurés couvrant l'ensemble du spectre de la cybersécurité;
- **Évaluation des compétences et suivi de la progression :** Élaboration de grilles d'évaluation, d'examens pratiques, de projets finaux et de feedbacks individualisés;
- **Mise en place de simulations et de laboratoires pratiques :** Organisation des sessions de tests d'intrusion, d'analyse de vulnérabilités et de gestion des incidents de cybersécurité pour renforcer l'apprentissage pratique.
- **Intégration de la conformité et de l'éthique :** Sensibilisation aux enjeux éthiques et juridiques liés aux activités offensives avec un accent sur la responsabilité professionnelle;
- **Collaboration avec l'administration académique :** Coordination avec les responsables pédagogiques pour la validation des contenus;
- **Suivi administratif des étudiants :** Participation aux réunions pédagogiques, contribution à l'élaboration des bulletins, saisie des notes et remontée;
- **Contribution à l'assurance qualité pédagogique :** Participation aux processus d'évaluation interne des enseignements, amélioration continue des contenus sur la base des retours étudiants et des indicateurs de performance;
- **Accompagnement à l'insertion professionnelle :** Organisation de sessions de préparation à l'emploi (CV, entretiens techniques), mise en relation avec les acteurs du secteur;
- **Encadrement des stages et suivi de terrain :** Supervision des stages académiques, coordination avec les maîtres de stage, validation des missions techniques, et suivi des livrables exigés.

ENVIRONNEMENT TECHNIQUE

- LabSim : Comptia TestOut;
- Windows Server 2019, Hyper V, VMware, XenServeur, Kali Linux, SCVMM;
- Metasploit, SonarQube, nmap, Nessus, Metasploit, Burpsuite pro, Splunk, Autopsy, Microsoft Defender for Endpoint, Trend Micro Vision One (XDR);
- Word, Excel, Powerpoint, Visio, Jira

REFERENCES PROJETS – LEVIO

Commission des normes, de l'équité, de la santé et de la sécurité du travail (CNESST) – AU FORFAIT – 11

Juin 2025

Test d'intrusion de l'application SNRT Zone Abonné

PROJET : L'application SNRT – Zone Abonné est un service web proposé par la CNESST aux citoyens, leur permettant de soumettre des réclamations et des demandes de remboursement dans le cadre des normes du travail et de l'équité salariale. Afin de sécuriser cet actif exposé publiquement sur Internet, la Commission des normes, de l'équité, de la santé et de la sécurité du travail a mandaté l'entreprise Levio pour réaliser une évaluation approfondie de ses vulnérabilités, au moyen de tests d'intrusion en mode boîte grise.

Dans le cadre de ce mandat, M. Jimmy Nguenguim était responsable des missions suivantes :

DOMAINE D'INTERVENTION :

- Réunion de cadrage avec le client afin de définir le protocole d'exécution des tests;
- Cartographie de l'application et identification des surfaces d'attaque accessibles, incluant l'interface web, les points de terminaison API, et les flux d'authentification ;
- Réalisation de tests automatisés et semi-automatisés à l'aide de scanners spécialisés pour détecter les vulnérabilités courantes et les erreurs de configuration ;
- Conduite de tests manuels approfondis, appuyés par des outils reconnus (Burp Suite, Postman, mitmproxy) et des scripts Python personnalisés développés en interne ;
- Évaluation des vulnérabilités liées à la logique applicative;
- Vérification des failles de sécurité listées dans l'OWASP API Security Top 10;
- Tests ciblant l'authentification, la gestion des sessions, les autorisations et les contrôles d'accès;
- Analyse des injections et de la validation des entrées utilisateur;
- Tests sur les méthodes HTTP, le comportement serveur, ainsi que la sécurité des configurations réseau et applicatives;
- Formulation détaillée de recommandations pour atténuer et corriger les vulnérabilités identifiées;
- Production d'un rapport technique détaillé, incluant des preuves de concept à destination des équipes opérationnelles ;
- Élaboration d'un rapport exécutif synthétisant les risques identifiés, à l'attention des décideurs.

ENVIRONNEMENT TECHNIQUE

- Kali Linux
- Nessus, Nikto, Shcheck, sslscan, Nuclei, nmap, Burpsuite pro, Postman, proxychains
- Word, Excel, Powerpoint, Visio

Ministère de la Justice Québec (MJQ) – AU FORFAIT – 10

Avril 2025

Test d'intrusion de l'API MISST

PROJET : L'API MISST est un service web permettant la recherche, la consultation et la mise à jour des informations relatives aux employés du ministère de la Justice du Québec. Afin de sécuriser cet actif exposé publiquement sur Internet, le ministère de la Justice du Québec (MJQ) a mandaté l'entreprise Levio pour réaliser une évaluation approfondie de ses vulnérabilités, au moyen de tests d'intrusion en mode boîte grise.

Dans le cadre de ce mandat, M. Jimmy Nguenguim était responsable des missions suivantes :

DOMAINE D'INTERVENTION :

- Réunion de cadrage avec le client afin de définir le protocole d'exécution des tests;
- Exécution de tests automatisés sur les différents points de terminaison de l'API;
- Réalisation de tests avancés à l'aide d'outils reconnus et de scripts Python développés en interne;
- Évaluation des vulnérabilités liées à la logique applicative;
- Vérification des failles de sécurité listées dans l'OWASP API Security Top 10;
- Tests ciblant l'authentification, la gestion des sessions, les autorisations et les contrôles d'accès;
- Analyse des injections et de la validation des entrées utilisateur;
- Tests sur les méthodes HTTP, le comportement serveur, ainsi que la sécurité des configurations réseau et applicatives;
- Formulation détaillée de recommandations pour atténuer et corriger les vulnérabilités identifiées;
- Production d'un rapport technique détaillé, incluant des preuves de concept à destination des équipes opérationnelles ;
- Élaboration d'un rapport exécutif synthétisant les risques identifiés, à l'attention des décideurs.

ENVIRONNEMENT TECHNIQUE

- Kali Linux
- Nessus, Nikto, Shcheck, sslscan, Nuclei, nmap, Burpsuite pro, Postman
- Word, Excel, Powerpoint, Visio

Quincaillerie Richelieu – AU FORFAIT – 9**Mars – Avril 2025***Test d'intrusion environnement IT&OT***PROJET :**

Dans le cadre de sa stratégie de renforcement de la posture de sécurité face aux menaces cybernétiques, Quincaillerie Richelieu a mandaté Levio pour réaliser des tests d'intrusion en mode boîte grise. Cette initiative visait à évaluer la surface d'exposition de l'environnement externe « richelieu.com », accessible publiquement via Internet, ainsi que celle de l'environnement interne, lequel intègre une infrastructure IT/OT déployée sur site (on-premise) et accessible par VPN.

Dans le cadre de ce mandat, M. Jimmy Ngueguim était responsable des missions suivantes :

DOMAINE D'INTERVENTION :

- Planification et réunion de cadrage avec les parties prenantes afin de définir le périmètre de l'évaluation, incluant les plages d'adresses IP, les actifs critiques IT/OT, les applications exposées, ainsi que les règles d'engagement spécifiques aux environnements de production sensibles.
- Réalisation d'une cartographie active et passive des surfaces d'attaque internes et externes, intégrant les actifs réseau, les interfaces SCADA, les équipements industriels, les systèmes bureautiques, et les serveurs applicatifs.
- Exécution de tests automatisés sur l'ensemble des points d'exposition identifiés, appuyée par des outils reconnus dans l'industrie (Nessus, Burp Suite, Nmap, PingCastle, Metasploit, etc.) ;
- Conduite de tests manuels avancés ciblant les applications web, les API REST/JSON, les services d'authentification, les interfaces de supervision OT, ainsi que les ports réseau ouverts ;
- Réalisation d'attaques sur l'environnement Active Directory, incluant LLMNR/NBT-NS, NTLM relay, phishing interne, exploitation d'AD CS (ESC1/ESC8) et Kerberoasting, en vue d'une élévation de privilèges ou d'une compromission de domaine.
- Réalisation de tests spécifiques liés à la segmentation réseau, incluant la vérification des restrictions inter-VLAN, la détection de ponts non autorisés entre zones IT et OT, l'évaluation des règles de pare-feu, ainsi que la tentative d'accès transversal entre sous-réseaux isolés.
- Réalisation de tests ciblés sur l'environnement AS400, incluant l'énumération des services actifs, la validation des profils à privilèges, les tentatives contrôlées d'accès via Telnet et FTP, l'analyse des autorisations sur les

objets critiques, les transferts de fichiers, l'exécution de commandes distantes, ainsi que l'évaluation des risques liés à l'interconnexion entre les zones IT et OT.

- Formulation détaillée de recommandations pour atténuer et corriger les vulnérabilités identifiées;
- Production d'un rapport technique détaillé, incluant des preuves de concept à destination des équipes opérationnelles ;
- Élaboration d'un rapport exécutif synthétisant les risques identifiés, à l'attention des décideurs.

ENVIRONNEMENT TECHNIQUE

- Kali Linux
- Nessus, Nmap, Nikto, Nuclei, sslscan, Shcheck, Gobuster, Dirsearch, Burp Suite Pro, Postman, mitmproxy, OWASP ZAP
- CrackMapExec, Impacket, BloodHound, Rubeus, Certify, Mimikatz, Metasploit, PingCastle
- Word, Excel, Powerpoint, Visio

Assemblée nationale du Québec (ASSNAT) – EN REGIE

Févr. 2025 – A nos jours

Offre de service de conseil en sécurité offensive

PROJET : L'Assemblée nationale du Québec a mandaté Levio pour réaliser une revue de code et des tests d'intrusion sur une série d'applications manipulant des données sensibles de ses clients et utilisateurs. Le mandat inclut également le suivi des correctifs auprès des fournisseurs et des équipes de développement concernées, dans le but de s'assurer que ces applications ne présentent aucun risque de sécurité susceptible de compromettre l'image de l'Assemblée nationale ou celle de ses parties prenantes. Afin de préserver l'intégrité des systèmes en production, les tests sont menés principalement dans des environnements ISO production, de manière à limiter l'impact sur les opérations courantes.

Dans le cadre de ce mandat, M. Jimmy Nogueuim était responsable des missions suivantes :

DOMAINE D'INTERVENTION :

- Rencontrer le client afin de définir le protocole d'exécution des tests ;
- Surveiller les potentielles fuites de données liées aux clients sur le dark web ;
- Répondre aux incidents de sécurité en collaboration avec l'équipe de sécurité opérationnelle de l'Assemblée nationale ;
- Contribuer activement à la gestion des incidents de sécurité ;
- Réaliser les tests d'intrusion conformément aux méthodologies reconnues (OWASP, PTES, NIST, etc.) ;
- Rédiger et présenter des rapports détaillés, incluant les vulnérabilités identifiées et des recommandations techniques adaptées aux équipes du client ;
- Effectuer des tests de validation à la suite de la mise en œuvre des correctifs recommandés ;
- Assurer un suivi continu en répondant aux demandes du client dans le cadre du mandat.

ENVIRONNEMENT TECHNIQUE

- Kali Linux
- Nessus, Nmap, Nikto, Nuclei, sslscan, Shcheck, Gobuster, Dirsearch, Burp Suite Pro, Postman, mitmproxy, OWASP ZAP
- CrackMapExec, Impacket, BloodHound, Rubeus, Certify, Mimikatz, Metasploit, PingCastle
- Word, Excel, Powerpoint, Visio

Mondata – AU FORFAIT – 7

Sept – Oct 2024

Test d'intrusion de la solution SaaS "MD.ECO"

PROJET : Mondata est une entreprise spécialisée dans la cybersécurité, offrant aux organisations et à leurs employés une défense optimale contre les cyberattaques grâce à sa solution "MD.ECO". Cette dernière est une plateforme SaaS de détection et de réponse managée (MDR) qui adopte une approche unique en matière de

cybersécurité, visant à aider les entreprises à développer les réflexes appropriés face aux menaces numériques croissantes. MD.ECO permet la personnalisation des processus de réponse aux incidents, offrant ainsi la flexibilité d'adapter les mesures en fonction de la disponibilité et des capacités des équipes internes. Dans le cadre de cette mission, j'ai été mandaté pour réaliser des tests d'intrusion sur le périmètre de la solution, y compris sur la plateforme MD.ECO elle-même et sur le site corporatif de Mondata. De plus, j'ai analysé les risques associés aux vulnérabilités détectées. L'objectif de cette mission est de garantir la sécurité, l'intégrité et la fiabilité de la solution MD.ECO de Mondata, tout en assurant sa conformité avec les meilleures pratiques de développement sécurisé de produits et les réglementations en matière de protection des données.

Dans le cadre de ce mandat, M. Jimmy Ngueguim était responsable des missions suivantes :

DOMAINE D'INTERVENTION :

- Réunion de cadrage avec le client afin de définir le protocole d'exécution des tests;
- Exécution de tests automatisés sur les différents points de terminaison des APIs;
- Réalisation de tests avancés à l'aide d'outils reconnus et de scripts Python développés en interne;
- Évaluation des vulnérabilités liées à la logique applicative, la segmentation des rôles et les fonctionnalités;
- Vérification des failles de sécurité listées dans l'OWASP API Security Top 10;
- Tests ciblant l'authentification, la gestion des sessions, les autorisations et les contrôles d'accès;
- Analyse des injections et de la validation des entrées utilisateur;
- Tests sur les méthodes HTTP, le comportement serveur, ainsi que la sécurité des configurations réseau et applicatives;
- Formulation détaillée de recommandations pour atténuer et corriger les vulnérabilités identifiées;
- Production d'un rapport technique détaillé, incluant des preuves de concept à destination des équipes opérationnelles ;
- Élaboration d'un rapport exécutif synthétisant les risques identifiés, à l'attention des décideurs.

ENVIRONNEMENT TECHNIQUE

- Kali Linux
- Nessus, Nikto, Shcheck, sslscan, Nuclei, nmap, Burpsuite pro, Postman
- Word, Excel, Powerpoint, Visio

Ministère de l'Immigration, de la Francisation et de l'Intégration (MIFI) – AU FORFAIT-6

Fevri – Mars 2024

Tests d'intrusion de l'application web et API ARRIMA-PTET

PROJET : Le ministère de l'Immigration, de la Francisation et de l'Intégration (MIFI) est l'organisme gouvernemental du Québec responsable de la sélection des immigrants, de leur francisation et de la mise en place des services facilitant leur intégration dans la société québécoise. Il met à disposition un portail permettant aux utilisateurs du monde entier de soumettre une déclaration d'intérêt pour immigrer au Québec, que ce soit de façon permanente ou temporaire, notamment pour étudier ou travailler. Un portail distinct est également offert aux entreprises afin de soumettre des demandes d'accompagnement, de validation d'offres d'emploi et d'Études d'impact sur le marché du travail (EIMT) pour les candidats recrutés à l'international. Dans ce contexte, j'ai été mandaté pour réaliser un test d'intrusion sur l'application web PTET du MIFI et évaluer les risques associés aux vulnérabilités identifiées. L'objectif de cette mission est d'assurer la sécurité et l'intégrité de l'application, en conformité avec les exigences du gouvernement du Québec et les lois en vigueur sur la protection des renseignements personnels.

Dans le cadre de ce mandat, M. Jimmy Ngueguim était responsable des missions suivantes :

DOMAINE D'INTERVENTION :

- Réunion de cadrage avec le client afin de définir le protocole d'exécution des tests;
- Exécution de tests automatisés sur les différents points de terminaison des APIs;
- Réalisation de tests avancés à l'aide d'outils reconnus et de scripts Python développés en interne;
- Évaluation des vulnérabilités liées à la logique applicative, la segmentation des rôles et les fonctionnalités;

- Vérification des failles de sécurité listées dans l'OWASP API Security Top 10;
- Tests ciblant l'authentification, la gestion des sessions, les autorisations et les contrôles d'accès;
- Analyse des injections et de la validation des entrées utilisateur;
- Tests sur les méthodes HTTP, le comportement serveur, ainsi que la sécurité des configurations réseau et applicatives;
- Formulation détaillée de recommandations pour atténuer et corriger les vulnérabilités identifiées;
- Production d'un rapport technique détaillé, incluant des preuves de concept à destination des équipes opérationnelles ;
- Élaboration d'un rapport exécutif synthétisant les risques identifiés, à l'attention des décideurs.

ENVIRONNEMENT TECHNIQUE

- Kali Linux
- Nessus, Nikto, Shcheck, sslscan, Nuclei, nmap, Burpsuite pro, Postman
- Word, Excel, Powerpoint, Visio

Commission des normes, de l'équité, de la santé et de la sécurité du travail (CNESST) – AU FORFAIT – 5

Dece. 2023 – Févr. 2024

Évaluation de la vulnérabilité et analyse des risques

PROJET : La Commission des normes, de l'équité, de la santé et de la sécurité du travail (CNESST) joue un rôle central dans l'application des lois du travail au Québec, en veillant au respect des droits et obligations des travailleurs et des employeurs. Pour soutenir ses activités, elle s'appuie sur un environnement interne destiné à son personnel, ainsi que sur plusieurs applications web accessibles au public. Dans ce contexte, j'ai été mandaté pour effectuer une évaluation approfondie des vulnérabilités, une analyse des risques, ainsi qu'une estimation du niveau de résilience de l'infrastructure face aux attaques de type rançongiciel. J'ai également réalisé des tests d'intrusion ciblés sur l'application web LMRST M37. Cette mission vise à garantir la sécurité et l'intégrité des systèmes informatiques de la CNESST, tout en renforçant leur capacité à résister aux menaces actuelles, notamment celles liées aux logiciels malveillants de type rançongiciel.

Dans le cadre de ce mandat, M. Jimmy Nogueuim était responsable des missions suivantes :

DOMAINE D'INTERVENTION :

- Mise en œuvre d'une simulation d'attaque par rançongiciel sur le périmètre de l'organisation.
- Évaluation de la capacité d'un rançongiciel à contourner les mécanismes de sécurité (antivirus, EDR) et à exécuter des activités malveillantes.
- Analyse de la capacité d'un rançongiciel à élever les privilèges sur un poste client de la CNESST.
- Évaluation de la propagation potentielle d'un rançongiciel à travers l'ensemble de l'infrastructure de la CNESST.
- Analyse des risques associés aux vulnérabilités identifiées.
- Réalisation d'un test d'intrusion sur l'application LMRST M37.
- Tests de vulnérabilités sur la logique de l'application.
- Conduite de tests avancés à l'aide d'outils spécialisés et de scripts Python développés en interne.
- Formulation de recommandations détaillées pour atténuer et corriger les vulnérabilités identifiées.
- Production d'un rapport technique détaillé, incluant des preuves de concept à destination des équipes opérationnelles ;
- Élaboration d'un rapport exécutif synthétisant les risques identifiés, à l'attention des décideurs.

ENVIRONNEMENT TECHNIQUE

- Kali Linux
- Nessus, Nmap, Nikto, Nuclei, sslscan, Shcheck, Gobuster, Dirsearch, Burp Suite Pro, Postman, mitmproxy, OWASP ZAP
- CrackMapExec, Impacket, BloodHound, Rubeus, Certify, Mimikatz, Metasploit, PingCastle

- Word, Excel, Powerpoint, Visio

Ministère de la Justice Québec (MJQ) – EN REGIE – 4

Octo. 2023 – Janv. 2025

Offre de service de conseil en sécurité offensive

PROJET : Le ministère de la Justice du Québec (MJQ) a pour mission de promouvoir la confiance des citoyens et de garantir le respect des droits individuels et collectifs, en assurant un système de justice accessible, intègre et fondé sur la primauté du droit. Il œuvre en collaboration avec plusieurs entités intégrées ou affiliées, et propose une gamme de services en ligne destinés à faciliter les interactions des utilisateurs avec le ministère. Dans ce contexte, M. Ngueguim a été mandaté pour réaliser des tests d'intrusion sur l'ensemble des applications web du MJQ, ainsi que pour analyser les risques liés aux vulnérabilités identifiées. Cette mission vise à assurer la sécurité et l'intégrité des plateformes numériques du ministère et de ses entités associées, tout en garantissant leur conformité avec les directives du gouvernement du Québec et les lois en vigueur sur la protection des renseignements personnels.

Dans le cadre de ce mandat, M. Jimmy Ngueguim était responsable des missions suivantes :

DOMAINE D'INTERVENTION :

- Rencontrer le client afin de définir le protocole d'exécution des tests ;
- Surveiller les potentielles fuites de données liées aux clients sur le dark web ;
- Répondre aux incidents de sécurité en collaboration avec l'équipe de sécurité opérationnelle du MJQ;
- Contribuer activement à la gestion des incidents de sécurité ;
- Réaliser les tests d'intrusion conformément aux méthodologies reconnues (OWASP, PTES, NIST, etc.) ;
- Rédiger et présenter des rapports détaillés, incluant les vulnérabilités identifiées et des recommandations techniques adaptées aux équipes du client ;
- Effectuer des tests de validation à la suite de la mise en œuvre des correctifs recommandés ;
- Assurer un suivi continu en répondant aux demandes du client dans le cadre du mandat.

ENVIRONNEMENT TECHNIQUE

- Kali Linux
- Nessus, Nmap, Nikto, Nuclei, sslscan, Shcheck, Gobuster, Dirsearch, Burp Suite Pro, Postman, mitmproxy, OWASP ZAP
- CrackMapExec, Impacket, BloodHound, Rubeus, Certify, Mimikatz, Metasploit, PingCastle

Word, Excel, Powerpoint, Visio

Sous-traitance industrielle Québec (STIQ) – AU FORFAIT

Août. 2023 – Dece. 2023

Tests d'intrusion web et audit de sécurité

PROJET : STIQ est une association représentant divers secteurs d'entreprises industrielles québécoises, dont la mission est de favoriser le développement des relations d'affaires et d'accroître la compétitivité des entreprises manufacturières afin de stimuler la croissance économique au Québec. Pour atteindre ses objectifs, STIQ s'appuie sur une gamme d'applications métier conçues pour simplifier les opérations et coordonner l'ensemble de ses processus internes. Dans ce contexte, j'ai été mandaté pour réaliser des tests d'intrusion sur les applications web InfoStiq+, InfoStiq, Stiq et Podium, ainsi qu'un audit de sécurité sur l'environnement Microsoft 365 de STIQ. L'objectif de cette mission est de garantir la sécurité et l'intégrité de leurs systèmes informatiques, tout en renforçant leur résilience face aux menaces potentielles, conformément aux normes de sécurité en vigueur.

Dans le cadre de ce mandat, M. Jimmy Ngueguim était responsable des missions suivantes :

DOMAINE D'INTERVENTION :

- Réunion de cadrage avec le client afin de définir le protocole d'exécution des tests;
- Évaluation des vulnérabilités liées à la logique applicative, la segmentation des rôles et les fonctionnalités;
- Vérification des failles de sécurité listées dans l'OWASP API Security Top 10;
- Conduite de tests avancés à l'aide d'outils spécialisés et de scripts Python développés en interne.

- Tests sur les méthodes HTTP, le comportement serveur, ainsi que la sécurité des configurations réseau et applicatives;
- Analyse des injections et de la validation des entrées utilisateur;
- Formulation détaillée de recommandations pour atténuer et corriger les vulnérabilités identifiées;
- Production d'un rapport technique détaillé, incluant des preuves de concept à destination des équipes opérationnelles ;
- Élaboration d'un rapport exécutif synthétisant les risques identifiés, à l'attention des décideurs.

ENVIRONNEMENT TECHNIQUE

- Kali Linux
- Nessus, Nikto, Shcheck, sslscan, Nuclei, nmap, Burpsuite pro, Postman
- Word, Excel, Powerpoint, Visio

Levio Conseils – EN INTERNE – 2

Mars. 2023 – A nos jours

Lead de projet (RS&DE) En Cybersécurité et Tests d'Intrusion

PROJET : Face à l'évolution constante des cybermenaces, les entreprises doivent surveiller et analyser en continu les vulnérabilités afin de protéger efficacement leurs infrastructures. Levio, acteur clé du domaine de la cybersécurité, aspire à devenir un partenaire stratégique pour ses clients, au-delà du simple rôle de prestataire de services. Dans cette optique, Levio développe une approche méthodologique ainsi qu'une solution opérationnelle permettant d'agréger en temps réel les vulnérabilités détectées. Cette solution générera des bulletins d'alerte périodiques afin de sensibiliser les clients aux nouvelles menaces et de les accompagner dans leur remédiation. J'ai été mandaté pour piloter ce projet de recherche, en collaboration avec une équipe de 26 conseillers composée de développeurs, d'architectes logiciel et sécurité, d'analystes en infrastructure et d'un scrum master.

Dans le cadre de ce mandat, M. Jimmy Ngueguim était responsable des missions suivantes :

DOMAINE D'INTERVENTION :

- Élaborer un plan de projet détaillé, incluant les objectifs, l'échéancier et les ressources nécessaires ;
- Mener des activités de recherche afin d'alimenter la conception de la solution ;
- Faciliter la collaboration et la communication entre les membres de l'équipe ;
- Assurer la coordination des tâches afin de respecter les jalons et les délais établis ;
- Organiser des rencontres régulières (mêlées quotidiennes) pour suivre l'avancement du projet ;
- Identifier et évaluer les risques associés, et élaborer des stratégies d'atténuation pour en réduire l'impact ;
- Superviser la documentation des processus, des résultats de recherche et des décisions techniques ;
- Adapter la stratégie en fonction des résultats obtenus et des rétroactions des clients.

REFERENCES PROJETS – Nimbuz

Nimbuz – EN INTERNE – 1

Nove.2018 – Mars 2023

Gestion de vulnérabilités et Tests d'intrusion sur des applications et serveurs d'hébergement

PROJET : Nimbuz Cameroun opère dans les domaines de l'hébergement web, des audits et du conseil en sécurité informatique, du développement web ainsi que du marketing numérique. L'entreprise met son expertise au service des administrations, ainsi que des organisations publiques et privées, afin de sécuriser leurs infrastructures, protéger leurs applications et préserver la confidentialité de leurs données. Elle propose une gamme complète de services, allant du conseil stratégique à la mise en œuvre technique, pour répondre aux besoins spécifiques en cybersécurité. Dans ce cadre, M. Ngueguim a été mandaté pour effectuer les tests d'intrusion mensuels sur les systèmes de Nimbuz et de ses filiales. Cette mission vise à assurer la sécurité des environnements informatiques en identifiant les vulnérabilités potentielles et en contribuant à leur remédiation proactive, afin de prévenir toute compromission susceptible d'affecter l'entreprise ou ses clients.

Dans le cadre de ce mandat, M. Jimmy Ngueguim était responsable des missions suivantes :

DOMAINE D'INTERVENTION :

- Exécution de tests manuels et automatisés sur des cibles en vue d'obtenir un accès initial
- Révision du code pour identifier les vulnérabilités potentielles dans la logique de l'application
- Conduite de tests avancés à l'aide d'outils bien connus et de scripts Python développés en interne
- Organisation d'ateliers de travail avec les développeurs pour promouvoir les meilleures pratiques de l'OWASP Top 10
- Rédaction d'un rapport détaillé sur les vulnérabilités détectées, incluant des preuves de concept pour les équipes opérationnelles
- Préparation d'un rapport de test de haut niveau comprenant une analyse des risques pour les cadres supérieurs
- Animation d'ateliers de restitution avec les cadres supérieurs pour présenter les vulnérabilités et les risques associés
- Proposition détaillée de correctifs pour atténuer et résoudre les vulnérabilités identifiées
- Assistance aux développeurs dans la correction des vulnérabilités

ENVIRONNEMENT TECHNIQUE

- Kali Linux
- Nessus, Nikto, Shcheck, sslscan, Nuclei, nmap, Burpsuite pro, Postman
- Word, Excel, Powerpoint, Visio