

EXPERT en Cybersécurité

Expert en cybersécurité, il intervient sur la gestion des vulnérabilités, des incidents, et l'amélioration des outils et processus de sécurité. Il accompagne également les projets IT en apportant son expertise, en évaluant les risques et en contribuant à la sensibilisation des équipes.

FORMATIONS & CERTIFICATIONS

- Juillet 2014
Master 2 en Informatique, Université d'Avignon et des Pays de Vaucluse, Avignon, Spécialité Réseaux Informatique et Sécurité.
- Juin 2012 Licence en Informatique, Université d'Avignon et des Pays de Vaucluse, Avignon, Spécialité Réseaux Informatiques et Systèmes Mobiles.
- Mars 2022 Certified Red Team Professional, CRTP. Active Directory ATTACK and DEFENSE
- May 2020 Offensive Security Certified Expert, OSCE. Advanced Exploitation, Anti-Virus Evasion, Backdoored Files, Debugging, Egghunter, Exploit Development, Network Attacks, Advanced Web Attacks
- Septembre 2018 Offensive Security Certified Professional, OSCP. Antivirus Exploitation, Buffer Overflow Exploits, Client Side Attacks Exploitation, Information Gathering, Kali Linux, Metasploit, Network Vulnerability, Scanning Password Attacks, Pivoting, Port Scanning, Privilege Escalation, Web Exploitation.
- Mai 2013 Cisco Certified Network Associate Niveau 4, CCNA 4. Technologie WAN et Sécurité

LANGUES :

Anglais : Courant
Français : Langue maternelle

COMPÉTENCES FONCTIONNELLES :

- Analyse des vulnérabilités et amélioration des processus de remédiation
- Contribution à la gestion des incidents de sécurité
- Optimisation des outils de sécurité opérationnelle
- Gestion des demandes de dérogation sécurité
- Suivi des tests d'intrusion et programmes de bug bounty
- Support sécurité aux projets IT et évaluation des risques
- Interface avec les architectes pour les enjeux de sécurité
- Rédaction de procédures et documentation sécurité
- Sensibilisation à la cybersécurité
- Configuration d'une solution PAM

COMPÉTENCES TECHNIQUES :

- Active Directory : Enumeration Active Directory, Escalade de privilèges locaux, Escalade de privilèges domaine (Kerberoast, Délégation Kerberos, Abus des groupes protégés, Abus des applications d'entreprise), Persistance et domination de domaine (Golden ticket, Silver ticket, Skeleton key, DSRM abuse, AdminSDHolder, DCSync, Abus des ACLs, Descripteurs de sécurité hôtes), Escalade de privilèges inter-forêts (Cross trust attacks, Inter-forest trust attacks)
- Attaques Réseaux : ARP poisoning, DHCP spoofing, IP spoofing, DNS spoofing, Scan zombie, Scan à travers pare-feu, Sniffing de paquets, DOS, DDOS

CONTACT COMMERCIAL

Tatopoulos Talia

Tel : 06.58.12.93.34

Email:

Talia.Tatopoulos@tilencia.com

- **Attaques Web** : LFI, RFI, Upload de fichiers, SQL injection, LDAP injection, Directory traversal, Fichiers de sauvegarde, XSS, CSRF, Obfuscation JavaScript
- **Attaques Système** : Escalade de privilèges, Programmes SUID, Exécution de code à distance, Obfuscation de malware, Encodage de malware, Packers

EXPÉRIENCES

Société

Poste :

Réalisations :

Confidentiel

Analyste SOC

Avril 2024 – Mai 2025

- Build d'un SIEM basé sur Logpoint
- Développement d'alertes de détection
- Réalisation de mission purple et threat hunting
- Mise en place d'une solution EDR Harfanglab
- Forensic sur les postes de travaux d'utilisateurs infectés
- Réponse à incident niveau 3
- Mise en place d'un SOAR open source Shuffle

Société

Poste :

Réalisations :

Groupe Duval

Expert cybersécurité / Analyste SOC

Novembre 2023 à Mars 2024

- Build d'un SIEM basé sur SEKOIA
- Déploiement d'agents NetSkope
- Configuration des journalisations détaillées sur l'environnement Windows (WinEvent)
- Mise en place et déploiement de SYSLOG/RSYSLOG sur les environnements Linux/UNIX
- Mise en place d'une machine de puits de logs sur le Cloud Azure
- Déploiement des agents Velociraptor via GPO et via Cloud Itune (Azure)
- Réalisation d'une mission de Threat Hunting
- Analyse d'incidents niveau 3 en se basant sur les outils : Microsoft Defender Endpoints, SentinelOne et Sekoia
- Développement d'alerte de détection sur SEKOIA
- Reverse Engineering sur des malwares reçus via phishing

Société

Poste :

Réalisations :

Valeo

PENTEST Automotive

Novembre 2023 à Février 2024

- Analyse de PCB, détection de GPIO
- Test de continuité pour détecter les ports UART ou JTAG
- Soudage et dessoudage sur PCB sur des petites composantes

- Connexion sur différents type de BUS série/parallèle
- Dumpde mémoire flash qui utilise le protocole SPI
- Debuggage JTAG en utilisant OpenOCD
- Audit de code source C, C++ et Java Android
 - Développement de script de fuzzing
- Reverse Engineering et Binary Exploitation x86/x64 et ARM
- Utilisation d'outils d'analyse du protocole CAN BUS
- Analyse de trame Bluetooth BLE

Société

Poste :

Réalisations :

M1VH

Mai 2023 à Novembre 2023

Gouvernance Sécurité SI

- Pilotage d'un SOC managé, revue des analyses d'incidents critiques
- Suivi des alertes et corrections des faux positifs
 - Planification de développement de nouveaux Uses Cases
- Revue des KPI hebdomadaire avec le SOC managé
- Suivie des SLA d'incidents traités par le SOC managé
- Pilotage de Test d'intrusion
- Réalisation des détections périodiques des vulnérabilités avec RAPID7
 - Suivi de plan d'action de correction vulnérabilité
- Suivi de déploiement de solution de sécurité
- Audits d'architecture d'infrastructure et applicatif
 - Suivi et validation de demandes d'ouverture de flux

Société

Poste :

Réalisations :

ATOS - Avantix

Décembre 2022 à Avril 2023

Systèmes embarqués

- Conception et intégration de solutions technique respectant les recommandations de l'ANSSI
 - Conception de solutions techniques en réponse des exigences du clients
- Développement d'applications de sécurité sur AOSP
 - Intégration d'une solution VPN-IPSec le Noyau/Linux d'AOSP avec une architecture AARCH64/ARM 2/6
 - Modification du framework AOSP
 - Recherche de vulnérabilités ou backdoor sur le mobile utilisé
 - Développement d'un noyau dédié à la gestion des périphériques utilisés
- Mise en place de serveurs VPN et firewall sur ESXi8

Société :

Lulubuy, Lexfo, SG-Markets, Airliquid, OCD MGAS

- Test d'intrusion WEB
- Test d'intrusion REST API
- Test d'intrusion Mobile Android
- Test d'intrusion Infrastructures Windows
- Test d'intrusion Infrastructures Linux
- Test d'intrusion Active Directory
- Campagne de Phishing

Analyste SOC : Technip Energies Octobre 2021- Décembre 2022

- Gestion d'incidents de sécurité N2 et N3
- Analyse de malwares et de vulnérabilités
- Forensic et investigation
- Investigation Avancée avec Windows Defender
- Surveillance des emails/spams sur Office 365
- Filtrage des domaines indésirables sur le proxy ZScaler
- Automatisation de la gestion d'incidents avec Phantom SOAR
- Développement de playbook sur Phantom SOAR
- Détection et whitelisting des faux positifs
- Création de règles de détection sur Splunk
- Création de dashboards sur Splunk

Société :

Analyste SOC- Client

Orange Cyberdéfense (Juin 2021- Novembre 2022)

- Gestion d'incidents de sécurité N2 et N3
- Analyse de malwares et de vulnérabilités
- Revue de playbooks sur le SOAR Cotex
- Détection et whitelisting des faux positifs
- Création de règles de détection sur Splunk
- Création de dashboards sur Splunk
- Vérification journalière des dashboards Cortex et Splunk
- Nettoyage des alertes en backlog
- Responsable de comités techniques hebdomadaires
- Préparation des comités techniques avec les remontées de KPI
- Préparation des comités de pilotage mensuels
- Présentation des cas les plus pertinents et critiques (avec les détails technique) aux clients lors du comité opérationnel

Décembre 2020 Sécurité systèmes embarqués et mobiles, Atos, Paris (6 mois).

- Intégration les outils et solutions de sécurité sur les systèmes embarqués
 - Intégration deux VPN simultanément (TLS et IPSec) dans différentes couches de l'environnement Android
 - Sécurisation l'environnement du noyau Linux
 - Reverse engineering sur environnement ARM/AARCH64
 - Attaques hardware sur le SoC MediaTek
 - Développement des programmes sur ARM TrustZone OS
 - Développement de Trusted Applications sur Prove&Core OS en utilisant le langage C — Analyse de code statique sécurisé sur des applications C
 - Fuzzing des programmes binaires, développés en C sur des architectures ARM
 - Exploitation de différentes vulnérabilités Overflow sur la Stack et sur la Heap
- 3/6
- Pentest sur les cartes RFID
 - Audit de sécurité des infrastructures et architectures

Mars 2020 Analyste SOC, SCRT, Genève (6 Mois).

- Mise en place d'un SIEM
- Mise en place d'une infrastructure SPLUNK
- Installation de WEC/WEF
- Déploiement de WinlogBeat, Sysmon et différentes applications SPLUNK — Gestion d'incidents de sécurité (SOC)

- Mission purple et détection d'attaques en temps réels
- Étude de nouveaux usecases et intégration des règles SIGMA dans les alertes de SPLUNK

Mars 2019 Analyste en Sécurité Web, Genève (9 Mois).

- Réponse aux incidents de sécurité sur le périmètre Digital
- Gestion d'incidents de sécurité (Failles WEB, Phishing, DOS)
- Investigation/forensic en utilisant Kibana
- Coordination et pilotage des audits de pentest
- Revue et correction des rapports de pentest, confirmation des vulnérabilités reportées — Conseils et expertises dans plusieurs projets de développement de plate-forme e-commerce
- Gestion des solutions PKI (Symantec PKI, Digicert PKI et Richemont PKI)
- Gestion des demandes de certificats SSL
- Automatisation du processus de génération de certificat
- Automatisation de la gestion des tickets Jira
- Automatisation du processus d'audit de code source
- Gestion de la solution Checkmarx
- Intégration de Checkmarx avec l'ADFS et l'utilisation de l'authentification SAML
- Développement de scripts (Groovy) qui relie Checkmarx et Bitbucket afin de lancer les scans de code ressource à chaque PULL Request
- Audits de code source sur les sites d'e-commerce (PHP, Java EE, Javascript)
- Test d'intrusion et scan de vulnérabilité sur des site web e-commerce
- Accompagnement des développeurs à corriger les vulnérabilités
- Formation et sensibilisation des développeurs aux attaques WEB (OWASP)
- Développement de scripts python pour la gestion automatiques des incidents, en se basant sur les API de Jira
- Développement de scripts python pour la gestions des projets dans Sonarqube
- Développement de différents jobs Jenkins en langage Java/Groovy
- Gestion et validation des demandes VPN IPSec et SSL en respectant le politique de sécurité Richemont.
- Maintenance des accès VPN SSL et troubleshooting des problèmes liés au VPN IPSec

Décembre 2017 Consultant en Cybersécurité (1 ans et 3 MOIS).

- Mise en place de nouvelles procédures pour la gestion d'incidents
 - Rédaction de rapport d'analyse d'incidents avec préconisation d'amélioration de procédures
 - Présentation des actions des méthodes suivies lors de la réponse d'incidents
 - Élaboration de processus d'industrialisation de tests d'intrusion
 - Audit de sécurité applicatif (.NET, C, PHP, Oracle), Methodologies : OWASP
 - Audit de sécurité infrastructure (Active Directory, Compromission de serveurs, MITM, mouvement latéral, pivoting)
 - Élaboration de modèle de rapports de tests d'intrusion
 - Participation aux missions RED TEAMING
 - Conception et élaboration d'attaques via le vecteur d'ingénierie sociale, OSINT, PHISHING, Phone 4/6 Freaking, clé USB vérolée
 - Conception d'un C2 en langage Python pour contourner les nouvelles protections d'antivirus — Recherche d'information impactant le business de l'entreprise (Fiches de paies, documents de projets confidentiels)
- Novembre 2016 Ingénieur en sécurité SI,

Pentesteur, SFR (1 an).

- Réalisation d'audits de sécurité suivant différentes méthodologies : PTES STANDARD, OWASP

- Étude des normes PASSI

- Réalisation de tests d'intrusion de tout type : boîte noire, boîte blanche, boîte grise.

- Test d'intrusion WEB (SQL injection, LFI, RFI, Attaques d'authentification , XSS, CSRF)

- Test d'intrusion VOIP (Déni service, interception, usurpation d'identité)

- Test d'intrusion sur Active Directory (Compromission de serveur, vol de session, mouvement latéral, pivoting)

- Test d'intrusion sur poste de travail sur Windows 10 (Injection de backdoor, Robber Ducky, Dump mémoire, dump mots de passes, élévation de privilèges)

Avril 2015- Ingénieur Sécurité Réseaux et Systèmes, ELIT, Sonelgaz, Alger (1 an et 6 mois).

- Mise en place d'un système de routage statique et dynamique.

- Configuration de plusieurs services : HTTP/S, PHP, DNS, Mail (SMTP, IMAP, POP), FTP/S, SSH, VPN, BackUp, Impression, Samba (CIFS, NTFS), Gestionnaire de quota.

- Recherche de différentes vulnérabilités dans les applications Web réalisées par les filiales du groupe de SONELGAZ.

- Recherche de différentes vulnérabilités dans les serveurs mis en service.

- Gestion de la plate-forme réseau informatique du groupe SONELGAZ en exploitant les différents équipements de supervisions et de sécurité (PRTG, E-mail gateway, SIEM).

- Test des performances et de la robustesse de l'antivirus Endpoint Protection mis en place.

- Étude et compréhension des systèmes S.C.A.D.A avec leurs différents domaines d'application.

- Étude des protocoles spécifiques au S.C.A.D.A appliqué aux systèmes électriques.

- Conception et réalisation d'un prototype de communication entre les postes de surveillance et le réseaux électrique avec une IHM simplifiée.

- Développement en C++ et en Java

- Etude du protocole IEC-62-443 qui est la référence de la sécurisation des systèmes S.C.A.D.A

- Installation et administration de serveurs et clients SVN — Gestion des commits et conflits de code source

- Gestions des incidents via la plate-forme HelpDesk

- Rédaction de rapports détaillés des vulnérabilités détectées et les correctifs à appliquer

- Gestion des cas d'exceptions des restrictions des droits d'accès Proxy et Active Directory