HILASSOUN A. ROLAND SANOU

Ingénieur R&D Cybersécurité — Détection et réponse sur les postes | Analyse de menaces | Sécurité par apprentissage automatique

Mersin, Turquie · +90 536 992 12 17 · rolandS01@outlook.fr

linkedin.com/in/hilassoun-a-roland-sanou · github.com/rolandsanou

RÉSUMÉ PROFESSIONNEL

Ingénieur R&D en cybersécurité avec plus de 3 ans d'expérience chez C-Prot, le principal éditeur turc de sécurité des postes de travail, au service de plus de 5 millions d'utilisateurs dans le monde. Spécialiste des systèmes de détection et de remédiation des menaces, fondés sur l'apprentissage automatique et sur des heuristiques, pour les plateformes EDR et de sécurité mobile. Construit actuellement des solutions EDR Windows atteignant 99 % de précision de détection pour des clients des secteurs bancaire, énergétique et de la défense. En Master d'Intelligence Artificielle afin d'approfondir le ML adverse et le renseignement sur les menaces de nouvelle génération.

EXPÉRIENCE PROFESSIONNELLE

Ingénieur R&D — EDR & Sécurité des postes Windows

C-Prot Siber Guvenlik Teknolojileri A.S. · Mersin, Turquie · *Janvier 2025 — Présent*

- Conception et développement de solutions EDR (Endpoint Detection and Response) pour Windows, intégrant des moteurs de détection par apprentissage automatique et par heuristiques pour identifier les menaces persistantes avancées (APT), les rançongiciels et les exploits zero-day.
- Architecture de pipelines de détection temps réel atteignant 99 % de précision sur diverses familles de malwares, réduisant significativement le taux de faux positifs pour les clients entreprises des secteurs bancaire et énergétique.
- Développement de workflows de remédiation automatisés qui mettent en quarantaine, restaurent et neutralisent les menaces avec un impact minimal pour l'utilisateur, réduisant le délai de réponse aux incidents.
- Collaboration au sein d'une équipe R&D de 10 ingénieurs pour livrer des solutions de sécurité déployées auprès de plus de 5 millions d'utilisateurs dans le monde (entreprises et particuliers).
- Travaux de renseignement sur les vecteurs d'attaque Windows émergents : malwares sans fichier, binaires détournés du système (LOLBins) et techniques d'injection de processus.
- Développement de règles YARA et de signatures comportementales pour la chasse proactive aux menaces et les chaînes d'analyse statique et dynamique.

Ingénieur R&D — Sécurité Android & Recherche de menaces

C-Prot Siber Guvenlik Teknolojileri A.S. · Mersin, Turquie · *Septembre 2024 — Janvier 2025*

- Étude et classification des différents types d'attaques visant les appareils Android : hameçonnage, injection de code malveillant, abus de permissions et attaques par superposition.
- Conception et entraînement de modèles d'apprentissage automatique (classification, détection d'anomalies) pour détecter avec une haute précision les URL d'hameçonnage et les APK malveillants, intégrés au produit de sécurité mobile de C-Prot.
- Développement de méthodes de détection heuristiques combinant analyse comportementale et inspection statique du code afin d'identifier des menaces inédites.
- Réalisation d'exploits de démonstration sur les surfaces d'attaque Android pour valider les capacités de détection et en étendre la couverture.
- Rédaction de la documentation technique des travaux de recherche et des mesures de performance des modèles pour l'équipe R&D.

Ingénieur stagiaire — Développement Android

C-Prot Siber Guvenlik Teknolojileri A.S. · Mersin, Turquie · *Février 2023 — Août 2024*

- Contribution au développement et à la maintenance de l'antivirus Android et de l'application de sécurité mobile de C-Prot.
- Implémentation de fonctionnalités de sécurité : analyse en temps réel, alertes de menaces et mise en quarantaine des malwares.
- Participation aux revues de code, à la planification des sprints et aux processus de développement agile de l'équipe mobile.
- Optimisation des performances de l'application et de sa consommation de batterie tout en maintenant une couverture complète des menaces.

COMPÉTENCES TECHNIQUES

Domaine	Technologies
Outils de sécurité	Wireshark, Metasploit, Burp Suite, YARA, IDA Pro, Ghidra, Frida, SIEM (Splunk, ELK), Nmap, OWASP ZAP
EDR / Postes de travail	Moteurs de détection, analyse comportementale, analyse statique et dynamique, bac à sable, réponse à incident, chasse aux menaces
ML pour la sécurité	scikit-learn, TensorFlow, PyTorch, détection d'anomalies, classification de malwares, NLP pour l'hameçonnage
Langages de programmation	Python, C/C++, Java, Kotlin, C#, Bash, SQL, Go, JavaScript
Plateformes	Windows (débogage noyau, analyse PE), Linux, Android (AOSP, rétro-ingénierie d'APK)
Cloud / DevOps	AWS, GCP, Azure, Docker, Kubernetes, CI/CD (Jenkins, GitHub Actions), Git
Rétro-ingénierie	Analyse de fichiers PE, désassemblage (IDA Pro, Ghidra), instrumentation dynamique (Frida), décompilation d'APK Android
Réseaux	TCP/IP, DNS, analyse HTTP/TLS, capture de paquets, règles de pare-feu, VPN, investigation réseau

FORMATION

M.Sc. Informatique — Intelligence Artificielle

Université de Mersin, Mersin, Turquie · *2025 — 2027 (en cours)*

Recherche : apprentissage automatique adverse, détection de menaces pilotée par l'IA, applications des LLM en cybersécurité.

Licence en Ingénierie Informatique

Université de Mersin, Mersin, Turquie · *2020 — 2024*

CERTIFICATIONS

- Tests de pénétration — Coursera (certifié)
- Spécialisation Machine Learning — Coursera (certifié)

PROJETS NOTABLES

Moteur de détection d'hameçonnage et de malwares par ML — C-Prot R&D

Conception de modèles de classification détectant les URL d'hameçonnage et les APK Android malveillants, avec 99 % de précision. Intégré à un produit de sécurité mobile en production servant des millions d'utilisateurs.

Chaîne de détection et de remédiation EDR Windows — C-Prot R&D

Construction d'un moteur de détection temps réel combinant modèles d'apprentissage automatique et règles heuristiques pour les rançongiciels, les malwares sans fichier et les APT sur postes Windows. Déployé chez des clients entreprises des secteurs bancaire et énergétique.

Application mobile de détection d'émotions

Développement d'un modèle d'apprentissage profond de reconnaissance des émotions faciales déployé sur Android, architecture CNN et inférence embarquée via TensorFlow Lite.

Contrôleur de robot nettoyeur de panneaux solaires

Développement d'une application Android pour le pilotage à distance en temps réel d'un robot industriel de nettoyage de panneaux solaires via Bluetooth/WiFi, avec tableau de bord télémétrique et plannings de nettoyage automatisés.

LANGUES

Français : langue maternelle · **Dioula** : langue maternelle · **Anglais** : C1 (avancé) · **Turc** : courant

CENTRES D'INTÉRÊT

Compétitions CTF, renseignement sur les menaces, outils de sécurité open source, IA/ML appliqués à la cybersécurité, sécurité de l'IoT.