YÜNA SUZUKI

INGÉNIEUR CYBERSÉCURITÉ
30 ANS

COMPÉTENCES

Exploitation Web
CSRF, CRLF, SQLi, LFI/RFI, Code Execution, XSS, Spidering

Exploitation Logicielle
Debug, Shellcode, Buffer overflow, Heap overflow, String format exploit, Metasploit, Fuzzing

Outils
QRadar, Splunk, Netwitness, Elastic, Wireshark, Tcpdump, Hexedit, Sqlmap, Nmap, Sys-Internals, Volatility

ExpIoitation réseau
Mitm (Spoofing), DoS IP, DoS Ethernet, Spoofing SMTP

Reverse Engineering
CheatEngine, IDA/Ollydbg, Windbg

Scanners de vulnérabilité
Metasploit, Nmap, Qualys, Acunetix, Nessus

Programmation
C, C++, C#, Python, OCaml, Java

Web
XHTML, CSS, Javascript, PHP

Base de données
MySQL, PostgreSQL

Logiciels
Visual Studio, Photoshop, MS Project, Office suite

Scripting
Shell, Python, PowerShell

Versionnement
Git, Subversion

Typographie
LATEX

CONTACT

LINKEDIN.COM/IN/YUNA-SUZUKI-A38974183

FORMATION

Dec 2019 SANS - GIAC Certified Forensic Examiner - FOR 500
Avr 2019 ELASTIC - Elasticsearch Engineer I and II
Fev 2018 RSA - Security Analytics Netwitness and Endpoint training
2015 - 2016 EPITA - Cycle Ingénieur Spécialité SRS - Systèmes Réseaux et Sécurité
2013 - 2014 EPITA - Cycle Ingénieur Tronc Commun
2010 - 2013 EPITA - Classe Préparatoire

EXPÉRIENCES

Sept 2018-2021

CSIRT BNP
(Systemis)

Analyste CSIRT N3 - Consultant CyberSécurité
Développement de scénario de détection (usecases) (ETL - Ansible/ Java/Javascript/SQL/Python)
Développement et amélioration du système de corrélation du SIEM
Amélioration et support de l'infrastructure du SIEM pour APAC/AMER/MEA
Investigation / Threat Hunting / Forensic Incident Response (DFIR)

Sept 2016 - 2018

SOC EDF
(Sopra Steria)

Analyste SOC N2/N3 - Consultant CyberSécurité
Amélioration de la surveillance SIEM (Tuning/Mise en place de règle de corrélation)
Développement et amélioration d'outils d'analyse de malware - Sandboxing
Automatisation et gestion des sources de Threat Intelligence
Analyse et monitoring d'équipements de sécurité (Proxy/IPS/FW/Sandbox)
Veille stratégique : Surveillance Deep Web/Dark Web (Leaks, Shadow IT, Risks)
Gestion de crises et réaction sur incident - Analyse forensique

Mars - Août 2016

SOC EDF
(Sopra Steria)

Mise en place d'une sandbox forensique améliorée
Stage de fin d'études d'une durée 6 mois dans l'entreprise Sopra Steria
Mettre en place une sandbox forensique correspondant aux besoins d'une équipe
d'analystes. Améliorer la sandbox forensique contre les techniques d'évasion (Hardening).
Tâches : Recherche et Dévéloppement et Intégration à l'équipe d'analystes