YONEL TOUSSAY

CONSULTANT CYBERSÉCURITÉ

avec compétences Admin et Dev

PROFIL

Plus de 12 ans d'expériences en IT (systèmes/réseaux et développement), j'ai renforcé mes compétences en Cybersécurité.

LANGUES

Anglais : Courant
Français: Bilingue
Créoles: Bilingue

COORDONNÉES

07 69 51 13 44

yonel.toussay@gmail.com

93100, Montreuil

/yonel-toussay

yonel-toussay.fr

FORMATIONS

2021 : Attestation Cybersécurité à l'ANSSI

2021: Certifications Cybersécurité (Inforensic et Pentesting) chez M2i Formation

2014: BAC+4 Administrateur Systèmes et Réseaux à l'ENI

2012: Certification MCITP Server Administrator chez Microsoft

2011: BTS Informatique de Gestion au Lycée Joseph Gaillard

2009: BAC STI Électronique au Lycée Joseph Gaillard

AUTRES

Permis B

Microsoft CERTIFIED IT Professional

COMPÉTENCES

- Concevoir et déployer des architectures réseau sécurisées, incluant le ZTNA (Fortinet) pour un accès réseau continu et protégé
- Réaliser des états des lieux techniques et fonctionnels, analyser les réseaux pour identifier et exploiter leurs vulnérabilités
- Élaborer des matrices de flux et de sécurité (SSI) adaptées aux risques identifiés et proposer des recommandations pour réduire la surface d'attaque
- Sécuriser les flux réseau avec des certificats conformes aux standards de l'ANSSI et revoir les habilitations, identités et accès (applications web, AD, OS)
- Intégrer et sécuriser des solutions telles que SSO (Keycloak), ITSM (GLPI) et outils de supervision
- Virtualiser et containeriser les serveurs, tout en assurant la gestion du cycle de vie des actifs et le maintien en condition opérationnelle et de sécurité (MCO/MCS)
- Investiguer les alertes, résoudre les incidents et fournir des rapports et indicateurs sur l'état global de la SSI
- Développer des applications web en Java et PHP, avec maîtrise des technologies front-end (HTML/CSS, JavaScript, Angular, React)
- Automatiser les tâches et administrer des environnements centralisés (GPO)

COMPÉTENCES TECHNIQUES

Cybersécurité :
ZTNA, 802.1X, Radius, infrastructures PKI, Bitlocker, gestions des clés de chiffrement, des certificats numériques, cryptographie, certbot, Keepass, Microsoft 365 Defender, UTM Stormshield, UTM Sophos, OSINT Framework, Google dorking, ingénierie sociale, outils d'analyse de logs, SIEM, serveur NPS, SSL, MetaSploit, LogPoint Hydra, Nmap, TheHarvester, Nessus, OpenVAs, Burp Suite, SQLMap, Bettercap, MSFVenom, Fail2Ban, Headers de sécurité, Splunk, Wallix Bastion, Nmap, CA Identity Manager, Citrix Netscaler VPN, Citrix Workspace, LockSelf, QRadar, One Identity, Office365, GPOAdmin, QAS, Rapid7, ISE Cisco, CyberArk etc.

Développement :
HTML, CSS, C++, JavaScript, PHP, Python, Java EE, jQuery, Bootstrap, Symfony, Doctrine, Angular, Hibernate, Spring, Docker, Jenkins, Maven, JUnit, TDD, Git, GitHub, CMS, JDBC, Agile etc.

Systèmes et Réseaux :
Azure, Cloud OVH, Active Directory, Microsoft 365, 802.1x, GPO, ADFS, SCCM, DNS, DHCP, VMWare ESXi, Hyper-V, Firewall, Apache, Tomcat, Payara Glassfish, IIS, Powershell, Batch, Bash, Shell, IPMI, iDRAC 9, NIS, Samba, Squid, Pfsense, NTP, VPN, Stockage, Impression, Nagios, Centreon, Tcpdump, Wireshark, EyesOfNetwork, EdgeLink, Exchange, IIS, Apache, DFS, mstsc.exe, Cisco Catalyst, WLC, AP 1141, Netgear, Juniper, Enterasys, Dell, IBM, Lenovo, Outils de ticketing et gestion de parc, GLPI, HP Asset Manager, GNS3, RoyalTS, ServiceNow etc.

Télécoms :
IPBX Alcatel 4760, SFR Business, Hp 6460/6470/6470b, Samsung, Huawei, Redmi, Iphones etc.

EXPÉRIENCES PROFESSIONNELLES

L'Oréal, Consultant Cybersécurité
Septembre 2024 - Aujourd'hui

o Assurer le Maintien en Condition de Sécurité (MCS) des environnements de développement, de qualification et de production, avec un rôle technico-fonctionnel

- Mettre en place le SSO pour les applications web via Azure AD, suivi du pilotage jusqu'à la mise en production
- Déployer et maintenir les applications web métier en conditions de sécurité, incluant la mise à jour des frameworks, bibliothèques, composants Java, archives Web (war), ainsi que des serveurs d'applications (Tomcat, Payara)
- Superviser la migration d'Oracle APEX et d'ORDS (Oracle REST Data Services)
- Piloter les mises à jour des systèmes d'exploitation des serveurs et accompagner la migration des applications web
- Intégrer des applications lourdes dans SCCM et assurer leur suivi

MOSS, Consultant Cybersécurité
Mai 2023 - Août 2024

o Projet spatial : suivre l'avancement de la sécurisation de l'architecture (rôle technico-fonctionnel) en conformité avec les recommandations de l'ANSSI

- Réaliser un état des lieux des systèmes, proposer des solutions pour réduire les risques, et piloter les travaux de sécurité informatique
- Analyser le réseau pour établir le schéma réseau, la matrice des flux (rétro-ingénierie) et la matrice SSI
- Automatiser des tâches avec des scripts Bash (extraction des habilitations utilisateurs dans SQL et Microsoft Access)
- Gérer la sécurisation : fermeture des ports non utilisés, flux persistants, et tokens d'authentification
- Générer des certificats sécurisés selon les standards ANSSI et intégrer les comptes et applications web dans le SSO
- Surveiller l'intégrité des fichiers sensibles et configurer des outils de supervision
- Administrer les environnements virtuels : gestion des images Docker/Docker-Compose et des VM
- Déployer un serveur de messagerie sous Debian 12 et mettre en place un Zero Trust Network Access (ZTNA) avec Fortinet
- Rédiger des procédures, rapports et fournir des indicateurs d'avancement en matière de SSI

Bouygues Telecom, Consultant Cybersécurité
Août 2022 - Janvier 2023

o Projet Cyberboost visant à accélérer l'identification et la remédiation des vulnérabilités du SI

- Gestion des tickets et alertes de sécurité avec ServiceNow
- Configuration et gestion des coffres CyberArk (rotation des mots de passe des comptes à privilèges, investigation des incidents)

Systèmes d'exploitation :
Windows (toutes versions), Linux (Debian, CentOs, RedHat RHEL, Ubuntu, BackTrack, Kali), MacOs, Android, iOs

Bases de données :
Oracle, MySQL, Microsoft SQL Server, PostgreSQL

- Revue des habilitations des comptes utilisateurs et gestion de l'Active Directory, incluant l'ajout/modification des GPO avec GPOAdmin
- Déploiement de l'EDR Crowdstrike en remplacement de l'EDR Symantec
- Fourniture hebdomadaire des KPI sur l'état de la sécurité
- Identification et réduction des flux permissifs, bridage SSH (fermeture des ports ouverts non autorisés)
- VPN avec Citrix Netscaler
- Provisioning des comptes AD via CAIM (via l'interface et/ou directement sur les tables SQL)
- Migration et décommissionnement de serveurs et flux existants :
  - ► NAS X7 (serveur de transfert de fichiers)
  - ► ACE et serveurs web (migration des flux Squid et Apache)
  - ► NIS (migration des comptes NIS vers LDAP)
- Suivi de la redirection des flux vers une nouvelle architecture

Kalis Consulting, Consultant Cybersécurité

Novembre 2021 - Avril 2022

- Accompagnement dans l'amélioration de la sécurité des systèmes d'information (SMSI) selon les normes ISO 27001, ISO 27005 et EBIOS
- Réalisation de tests d'intrusion et audits de code (pentests internes et externes en boîte noire et grise), suivi par des plans d'action pour remédier aux vulnérabilités identifiées
- Conception d'architectures sécurisées et durcissement des serveurs Linux et Windows
- Déploiement, configuration et monitoring des solutions de sécurité
- Analyse des logs et investigation avancée avec Splunk
- Supervision des identités et des accès privilégiés (IAM/PAM) via Wallix Bastion
- Sensibilisation et formation des collaborateurs à la sécurité informatique

Crous de Créteil, Administrateur Systèmes et Réseaux

Juin 2021 - Septembre 2021

- Configuration d'OpenVPN pour sécuriser les connexions réseau
- Mise en place et gestion d'une infrastructure RDS (Remote Desktop Services)
- Scripting Shell pour gérer le trafic réseau, incluant le routage et les règles Iptables
- Migration de l'Active Directory de Windows Server 2008 R2 vers Windows Server 2019
- Supervision et monitoring des systèmes avec Nagios et Centreon
- Virtualisation d'infrastructures avec VMware ESXi
- Réalisation de schémas réseaux complexes pour optimiser l'architecture et les flux

Mimina Cakes, Développeur Java Fullstack

Juillet 2020 - Octobre 2020

- Analyser les besoins métiers
- Participer à la conception de l'architecture logicielle
- Réaliser et héberger le site vitrine et son design
- Créer un progiciel de gestion (prestations, commandes, clients, factures, recettes)
- Développer de nouvelles applications et fonctionnalités en TDD
- Effectuer les tests et corrections de l'application

Dawan, Stagiaire Développeur Java EE

Avril 2019 - Janvier 2020

- Développement d'applications web Java:
  - ► pour la gestion des alertes dans les transports en commun
  - ► pour les véhicules d'entreprise (location, état, géolocalisation, renouvellement)
- Participation aux réunions et sprints Agile SCRUM
- Conception et développement des fonctionnalités

British American Tobacco, Responsable Informatique

Janvier 2018 - Mars 2019

- Suivi des projets/demandes informatiques
- Management d'une équipe de 3 personnes et coordination des interventions des prestataires
- Intégration de serveurs physiques et virtuels, et mise en place d'un serveur CEGID pour la fiscalité (avec gestion des bases SQL Express)
- Gestion des profils dans l'Active Directory (création/suppression, activation/désactivation des services)
- Gestion des droits NTFS, des partages et des connexions des lecteurs réseaux
- Administration des comptes Juniper Junos Pulse Secure, RSA SecurID, Azure, Active Directory et Office 365
- Scripting Batch et PowerShell pour l'automatisation des tâches
- Gestion des attributions et restitutions de matériels

EFS, Superviseur Réseaux

Décembre 2016 - Novembre 2017

- Gestion proactive des incidents réseau, serveurs et services informatiques
- Déclenchement et coordination des alertes en temps réel
- Analyse des remontées d'informations des différentes solutions
- Rédaction de rapports et mise à jour des outils internes
- Support Helpdesk

RTE, Administrateur Systèmes Réseaux et Sécurité

Novembre 2012 - Septembre 2014

- Mise en place d'une infrastructure PKI avec serveur Radius et Autorité de Certification pour sécuriser le Wifi (8021x)
- Maintien en Condition Opérationnelle des applications métiers et des systèmes
- Support incidents et demandes de niveau 2, en présentiel ou à distance, avec suivi des tickets auprès des services support
- Gestion du parc informatique et de l'Active Directory
- Création des profils TOIP dans l'IPBX Alcatel 4760 et attribution des IP phones
- Gestion de projets (déploiement, migration Windows XP vers 7, renouvellement, TOIP, 8021x) et communication des avancées avec le client
- Gestion des supports de données sensibles (sauvegarde, externalisation, restauration, destruction)

YONEL TOUSSAY

CYBERSECURITY CONSULTANT

with skills of Admin and Dev

PROFILE

With over 12 years of experience in IT (systems/networks and development), I have strengthened my skills in cybersecurity.

LANGUAGUES

English : Fluent
French: Bilingual
Creole: Bilingual

CONTACT INFORMATION

+33 7 69 51 13 44

yonel.toussay@gmail.com

Paris, FRANCE

/yonel-toussay

yonel-toussay.fr

TRAININGS

2021 : Cybersecurity Certificate from ANSSI

2021: Cybersecurity Certifications (Inforensic and Pentesting) from M2i Formation

2014: Master's degree Systems and Network Administrator at ENI

2012: MCITP Server Administrator Certification from Microsoft

2011: Associate's Degree Computer Science and Management from high school Joseph Gaillard

2009: Bachelor Technical Electronics program in high school Joseph Gaillard

OTHERS

Driver's license

Microsoft CERTIFIED IT Professional

SKILLS

- Design and deploy secure network architectures, including ZTNA (Fortinet) for continuous and protected network access
- Conduct technical and functional assessments, analyze networks to identify and exploit vulnerabilities
- Develop flow and security matrices (SSI) tailored to identified risks and provide recommendations to reduce the attack surface
- Secure network flows using certificates compliant with ANSSI* standards, and review permissions, identities, and access (web applications, AD, OS)
- Integrate and secure solutions such as SSO (Keycloak), ITSM (GLPI), and monitoring tools
- Virtualize and containerize servers while managing asset lifecycles and ensuring operational and security maintenance
- Investigate alerts, resolve incidents, and deliver reports and indicators on the overall state of information security (SSI)
- Develop web applications in Java and PHP, with proficiency in front-end technologies (HTML/CSS, JavaScript, Angular, React)
- Automate tasks and administer centralized environments (GPO)

**ANSSI: the french CISA*

TECHNICAL SKILLS

Cybersecurity :
ZTNA, 802.1X, Radius,PKI infrastructures, Bitlocker, Encryption key management, digital certificates, cryptography, certbot, Keepass, Microsoft 365 Defender, UTM Stormshield, UTM Sophos, OSINT Framework, Google dorking, Social engineering, log analysis tools, SIEM, NPS server, SSL, MetaSploit, LogPoint, Hydra, Nmap, TheHarvester, Nessus, OpenVAS, Burp Suite, SQLMap, Bettercap, MSFVenom, Fail2Ban, security headers, Splunk, Wallix Bastion, Nmap, CA Identity Manager, Citrix Netscaler VPN, Citrix Workspace, LockSelf, QRadar, One Identity, Office365, GPOAdmin, QAS, Rapid7, Cisco ISE, CyberArk, etc.

Development :
HTML, CSS, C++, JavaScript, PHP, Python, Java EE, jQuery, Bootstrap, Symfony, Doctrine, Angular, Hibernate, Spring, Docker, Jenkins, Maven, JUnit, TDD, Git, GitHub, CMS, JDBC, Agile etc.

Systèmes et Réseaux :
Azure, OVH Cloud, Active Directory, Microsoft 365, 802.1x, GPO, ADFS, SCCM, DNS, DHCP, VMware ESXi, Hyper-V, Firewall, Apache, Tomcat, Payara Glassfish, IIS, PowerShell, Batch, Bash, Shell, IPMI, iDRAC 9, NIS, Samba, Squid, Pfsense, NTP, VPN, Storage, Printing, Nagios, Centreon, Tcpdump, Wireshark, EyesOfNetwork, EdgeLink, Exchange, IIS, Apache, DFS, mstsc.exe, Cisco Catalyst, WLC, AP 1141, Netgear, Juniper, Enterasys, Dell, IBM, Lenovo, ITSM, GLPI, HP Asset Manager, GNS3, RoyalTS, ServiceNow, etc.

Telecoms :
IPBX Alcatel 4760, SFR Business, Hp 6460/6470/6470b, Samsung, Huawei, Redmi, Iphones etc.

WORK EXPERIENCE

L'Oréal, Cybersecurity Consultant
September 2024 - Today

o Ensure Security Maintenance for development, testing, and production environments, with a techno-functional role

- Implement SSO for web applications via Azure AD, overseeing the process through to production deployment
- Deploy and maintain business web applications in secure conditions, including updating frameworks, libraries, Java components, web archives (WAR), and application servers (Tomcat, Payara)
- Oversee the migration of Oracle APEX and ORDS (Oracle REST Data Services)
- Manage server OS updates and support the migration of web applications
- Integrate and monitor heavy applications in SCCM

MOSS, Cybersecurity Consultant
May 2023 - August 2024

o Space project: monitor the progress of securing the architecture in compliance with ANSSI recommendations (technical-functional role).

- Conduct system assessments, propose risk mitigation solutions, and oversee IT security initiatives
- Analyze the network to create the network diagram, flow matrix (reverse engineering), and SSI matrix
- Automate tasks using Bash scripts (eg, extracting user permissions from SQL and Microsoft Access)
- Manage security by closing unused ports, securing persistent flows, and safeguarding authentication tokens
- Generate secure certificates aligned with ANSSI standards and integrate accounts and web applications into SSO
- Monitor the integrity of sensitive files and configure supervision tools
- Administer virtual environments, including managing Docker/Docker-Compose images and VMs
- Deploy a mail server on Debian 12 and implement Zero Trust Network Access (ZTNA) with Fortinet
- Draft procedures, reports, and provide progress indicators for information systems security (ISS)

Bouygues Telecom, Consultant Cybersécurité
August 2022 - January 2023

o Cyberboost Project: Accelerating the Identification and Remediation of IT System Vulnerabilities

- Manage security tickets and alerts via ServiceNow
- Configure and administer CyberArk vaults (password rotation for privileged accounts, incident investigations)

Operating Systems :

Windows (all versions), Linux (Debian, CentOS, RedHat RHEL, Ubuntu, BackTrack, Kali), macOS, Android, iOS

Databases :

Oracle, MySQL, Microsoft SQL Server, PostgreSQL

- Review user account permissions and manage Active Directory, including adding/modifying GPOs with GPOAdmin
- Deploy CrowdStrike EDR to replace Symantec EDR
- Provide weekly KPI reports on security status
- Identify and reduce permissive flows, including SSH hardening (closing unauthorized open ports)
- Troubleshoot VPN issues with Citrix Netscaler
- Handle AD account provisioning via CAIM (through the interface or directly on SQL tables)
- Decommission servers and migrate flows, including:
  - ► NAS X7 (file transfer server)
  - ► ACE and web servers (migrate flows from Squid and Apache)
  - ► NIS accounts to LDAP
- Monitor flow redirection to the new architecture

Kalis Consulting, Cybersecurity Consultant

November 2021 - April 2022

- Support in improving information system security (ISMS) in compliance with ISO 27001, ISO 27005, and EBIOS standards
- Conduct penetration tests and code audits (internal and external, black-box and gray-box), followed by action plans to address identified vulnerabilities
- Design secure architectures and harden Linux and Windows servers
- Deploy, configure, and monitor security solutions
- Perform log analysis and advanced investigations using Splunk
- Manage privileged identities and access (IAM/PAM) with Wallix Bastion
- Provide security awareness and training for employees

Crous de Créteil, Systems and Network Administrator

June 2021 - September 2021

- Configure OpenVPN to secure network connections
- Set up and manage a Remote Desktop Services (RDS) infrastructure
- Create Shell scripts for network traffic management, including routing and Iptables rules
- Migrate Active Directory from Windows Server 2008 R2 to Windows Server 2019
- Monitor and supervise systems using Nagios and Centreon
- Virtualize infrastructures with VMware ESXi
- Design complex network diagrams to optimize architecture and flows

Mimina Cakes, Fullstack Java Developer

July 2020 - October 2020

- Analyze business requirements
- Contribute to software architecture design
- Develop and host the showcase website, including its design
- Create a management software suite (services, orders, clients, invoices, revenue)
- Develop new applications and features using TDD
- Perform application testing and debugging

Dawan, Java EE Developer Intern

April 2019 - January 2020

- Develop Java web applications for:
  - ► Managing alerts in public transportation
  - ► Managing company vehicles (rental, status, geolocation, renewal)
- Participate in Agile SCRUM meetings and sprints
- Design and develop application features

British American Tobacco, IT Manager

January 2018 - March 2019

- Oversee IT projects and requests
- Manage a team of three and coordinate vendor interventions
- Integrate physical and virtual servers, including setting up a CEGID server for fiscal management (SQL Express database administration)
- Handle Active Directory profile management (creation/deletion, service activation/deactivation)
- Manage NTFS permissions, shared folders, and network drive connections
- Administer accounts for Juniper Junos Pulse Secure, RSA SecurID, Azure, Active Directory, and Office 365
- Automate tasks using Batch and PowerShell scripting
- Manage hardware assignments and returns

EFS, Network Supervisor

December 2016 - November 2017

- Proactive management of network, server, and IT service incidents
- Trigger and coordinate real-time alerts
- Analyze data from various monitoring solutions
- Draft reports and update internal tools
- Provide Helpdesk support

RTE, Systems, Network, and Security Administrator

November 2012 - September 2014

- Deployment of a PKI infrastructure with a Radius server and Certification Authority to secure Wi-Fi (8021x)
- Operational maintenance of business applications and systems
- Level 2 incident and request support, on-site or remote, with ticket follow-up with support teams
- Management of the IT inventory and users accounts in Active Directory
- Creation of TOIP profiles in IPBX Alcatel 4760 and assignment of IP phones
- Project management (deployment, Windows XP to 7 migration, renewal, TOIP, 8021x) and progress updates to clients
- Management of sensitive data storage (backup, externalization, restoration, destruction)