

Ingénieur Poste de Travail & Sécurité

Points forts

Ingénieur poste de travail et sécurité diplômé d'un Mastère Cybersécurité RNCP 7, avec 2 ans d'expérience en environnement bancaire critique (Ayvens - Société Générale, 2 000+ endpoints).

Expert du cycle de vie complet du poste de travail Windows : ingénierie des masters MDT/PXE, déploiement applicatif SCCM, automatisation PowerShell avancée, gestion des vulnérabilités Tanium et sécurisation des endpoints. Initiateur de la collaboration production/SSI ayant permis d'atteindre l'objectif 0% Very High CVE.

Chef de projet du renouvellement de 56 postes sur 11 sites suite à faille RCE critique.

Double compétence systèmes/sécurité consolidée par des projets SOC (Splunk, Wazuh, Suricata, forensique, Sigma rules). Disponible immédiatement.

Expérience professionnelles

AYVENS (Filiale SG) Septembre 2023 à ce jour

Ingénieur Poste de Travail & Sécurité

Environnement bancaire critique | 2 000+ endpoints | SCCM (MECM), MDT, Tanium, Active Directory, PowerShell, O365

- ✓ Ingénierie masters Windows (MDT / PXE) : création et maintenance des images Windows 10/11 Entreprise via MDT, injection dynamique des pilotes par modèle, boot PXE réseau, séquences de tâches multi-plateformes.
- ✓ Déploiement applicatif SCCM (MECM) : création et gestion des collections statiques et dynamiques WQL, déploiement par vagues, suivi granulaire, 1869 postes migrés (CVE critiques)
- ✓ Automatisation PowerShell avancée : scripts de remédiation industrialisée : connexion distante silencieuse sur postes utilisateurs, extraction GUID MSI via registre, désinstallation/installation silencieuse, mise à jour EDR
- ✓ Symantec sans collection, nettoyage du poste, script réutilisable - documentés et versionnés
- ✓ Remédiation agents Tanium mal configurés : diagnostic via TaniumClient.log, activation Registre à distance, correction des clés ServerName/LastGoodServer (HKLM\WOW6432Node\Tanium), redémarrage service, vérification reconnexion, procédure documentée et automatisée PowerShell
- ✓ Recensement Java - remédiation & conformité : inventaire via Tanium Interact + SCCM (filtres Computer Name, Installed Applications, Silent Uninstall String), croisement avec les usages métier, désinstallation sur 38% du parc - réduction de la surface d'attaque CVE et conformité licences Oracle
- ✓ GPO & conformité Windows : déploiement et gestion des politiques de sécurité, hardening système

- ✓ (BitLocker, Secure Boot, TPM 2.0, EDR), analyse d'impact, résolution des conflits de stratégies, contrôle des configurations PSSI sur l'ensemble du parc
- ✓ Gestion des vulnérabilités - cycle complet (Tanium / SCCM) : qualification CVE via Tanium Comply
- ✓ (rapports Medium/High/Very High, CVSS v3, EPSS, CISA KEV, framework NIST SP 800-40 bancaire SG), priorisation par impact métier et probabilité d'exploitation, remédiation multi-méthodes (collections SCCM, PowerShell silencieux, registre à distance) - objectifs atteints : 0% Very High, <10% High
- ✓ Analyse des événements de sécurité & détection : surveillance continue via Event Viewer et Sysmon (EventID 4688 - création processus, 4624/4625 - connexions, 7045 - services), détection de comportements anormaux sur les endpoints, qualification des alertes et remontée aux équipes SSI avec contexte complet
- ✓ Veille CVE/CTI & amélioration continue : suivi NVD, CISA KEV, CVE/CERT, MITRE ATT&CK - intégration des nouvelles menaces pour adapter les configurations Windows et les priorités de remédiation, contribution aux playbooks de réponse
- ✓ Reporting sécurité & pilotage : KPI vulnérabilités, taux de remédiation, conformité PSSI - tableaux de bord
- ✓ hebdomadaires pour les équipes SSI et le management lors des comités sécurité, matrice RACI sur les projets

IMERYS **Septembre 2022 à Septembre 2023**

Technicien Support Informatique N2 au siège EMEA d'Imerys en environnement international

- ✓ Support N2 & déploiement postes (ServiceNow) : diagnostic et résolution des incidents,
- ✓ installation/configuration des postes de travail, gestion des tickets SLA, support remote et on-site en environnement EMEA
- ✓ Administration systèmes Windows/Linux : supervision serveurs virtualisés, monitoring proactif, maintien de la disponibilité des services
- ✓ Infrastructure réseau : configuration switches Cisco, VLAN, TCP/IP, dépannage connectivité multi-sites IAM (Active Directory) : comptes, groupes de sécurité, droits d'accès, cycle de vie des identités
- ✓ Documentation : procédures techniques et sensibilisation cybersécurité des utilisateurs

Projets techniques

- ✓ Renouvellement du parc Windows 11, faille RCE critique : pilotage complet du remplacement de 56 postes sur 11 sites, conception d'un master sécurisé (TPM 2.0, Secure Boot, BitLocker, EDR, GPO), déploiement via MDT/PXE avec injection de pilotes, sauvegarde et restauration OneDrive, mise en place de checklists post migration et PV utilisateurs signés, 100 % du périmètre traité dans les délais avec zéro poste vulnérable restant
- ✓ Remédiation PDFCreator (SCCM) : remplacement PDFCreator (CVE critiques) par PDFSam sur 1 869 postes, phase pilote, collections SCCM install/désinstall, déploiement par vagues, documentation complète
- ✓ Blue Team C2 Detection Lab - 2026 (lab perso) : 2 VMs (endpoint Windows + serveur SOC Ubuntu) - Sysmon
- ✓ SwiftOnSecurity (EventID 1/3/11/12/13/22), Splunk, beacon simulator Python avec jitter (Cobalt Strike/Silver),
- ✓ Flask C2, détection SPL (timing analysis, User-Agent, connexions répétées), dashboards Splunk, Sigma rules, MITRE ATT&CK T1071/T1059,
- ✓ SOC Cloud Hybride : Wazuh (10+ sources, règles de corrélation), TheHive SOAR (playbooks), Suricata IDS, MISP CTI via Cortex/VirusTotal etc - Docker, Bash, Python

- ✓ **Analyse Forensique** : investigation système compromis : Volatility (dump RAM), Autopsy/FTK Imager (disque), persistance (clés Run, services, tâches planifiées), reconstruction kill chain MITRE ATT&CK

Compétences techniques

- ✓ **Déploiement / SCCM (MECM) / MDT** : Collections WQL statiques/dynamiques, Task Sequences, Distribution Points, images master Windows, PXE, injection pilotes %Model% (Dell/HP/Lenovo), déploiement Required/Available par vagues, WSUS, Monitoring > Deployments
- ✓ **Automatisation PowerShell** : Remédiation automatisée (registre à distance HKLM, GUID MSI, msixexec /qn /norestart), connexion distante silencieuse, gestion des services (Net start/stop), reporting conformité - scripts documentés et industrialisés
- ✓ **Tanium** : Comply (CVE Medium/High/Very High), Interact (requêtes live Computer Name/Applications/Uninstall), Asset, Patch, Deploy - remédiation, conformité, reconfiguration agents
- ✓ **Systèmes Windows** : Windows 10/11 Entreprise, Windows Server 2016/2019/2022, registre (HKLM/HKCU), Event Viewer, Sysmon (EventID 4688/4624/4625/7045), GPO, WMI, Task Scheduler, troubleshooting avancé
- ✓ **Sécurité & Vulnérabilités** : CVE/CVSS v3, EPSS, CISA KEV, NVD, NIST, MITRE ATT&CK, BitLocker, EDR/XDR
- ✓ **Microsoft 365 / IAM** : Entra ID, Active Directory, OKTA, MFA, Conditional Access, RBAC, Kerberos, LDAP
- ✓ **SIEM & Détection** : Splunk (SPL, streamstats, dashboards, Field Extractions), Wazuh, ELK, Sigma rules
- ✓ **SOC / CTI** : TheHive (SOAR), MISP (CTI), Suricata, Cortex/VirusTotal - gestion incidents, playbooks, IOC
- ✓ **Forensique** : Volatility, Autopsy, FTK Imager - analyse RAM/disque, persistance, timeline
- ✓ **Scripting** : PowerShell (avancé), Python (beacon simulator, Flask, automatisation), Bash
- ✓ **Virtualisation / Réseau** : VMware ESXi (vCenter, vMotion), Hyper-V, Proxmox, TCP/IP, Cisco (VLAN, switches), DNS, DHCP, Wireshark (analyse de trames), pfSense, VPN (IPsec, OpenVPN), load balancing, supervision réseau
- ✓ **Référentiels** : MITRE ATT&CK, ISO 27001, NIST, NIS 2, RGPD, OWASP

Formation

- **Mastère Cybersécurité** - RNCP Niveau 7 Expert en systèmes d'information, spécialisation Cybersécurité Sup de Vinci, La Défense
- **Bachelor AIS** - RNCP Niveau 6 Administrateur d'Infrastructures Sécurisées Webitech, Paris

Certifications

- **CTF Tanium 2024** | CompTIA Security+ en cours de préparation | Pratique régulière TryHackMe / HackTheBox
- **Langues** : Français (natif) | Anglais (B2) | Hindi (natif)
- **Projets en cours** : Blue Team C2 Detection Lab (Splunk/Sysmon/Sigma), serveur de tests Active Directory (attaque/défense), IA locale cybersécurité, Reverse engineering

- **Veille : CVE/CERT, WSUS/SCCM bulletins Microsoft, MITRE ATT&CK updates, actualité cyber - Finance, économie, littérature**
- **Formation : Udemy, IBM cybersécurité, CISCO Analyste junior en cybersécurité**