WGU

Ingénieur en Cyber Sécurité senior

9 ans d'expériences

DIPLÔMES

Mastère En Technologie de L'informatique spécialité Réseaux et Sécurité.

COMPÉTENCES TECHNIQUES

Securité	**Splunk** Entreprise, **Splunk** Cloud, Entreprise Security, Azure Sientinel (**SIEM & SOAR**), QRADAR, Cloud Watch, Cloud Trail, AlienVault, ATA (Advanced Threat Analytics), ATP (Advanced Threat Protection), MDI (Microsoft Defender pour Identity), Microsoft 365 Defender, DLP (Data Loss Prevention), MCAS (Microsoft Cloud App Security), CyberReady,CybelAngel, Rapid**7 InsightVM, Rapid7 Nexpose**, Kaspersky EDR CrowdStrike Falcon, ProofPoint, SecretServer,LanGuard,Nessus,Qualys,NMAP, Metasploit Framework & Console, ZAP Owasp Console, Maltego, Dirb, Hydra, SQLMAP, WPScan, Trend Micro XDR, Netskope.
Outils de sécurité EndPoint.	**McAfee** ePolicy Orchestrator (ePO), **Symantec** End Point Protection, **ESET** End Point Protection, **Kaspersky** End Point Protection.
Système D'Exploitation	Windows Server 2012/2016/2019, Windows 7, 8.0, 8.1, 10, RedHat, CentOS, KaliLinux.
Virtualisation	VMWare, VCenter, VSphere.
Backup	NAS, QNAP, Syncovery.
Automatisation	Phantom SOAR, Azure Sentinel.
Outils de Supervision	Zabbix, Centreon, PRTG, Nagios, Cacti.

Langages de script	CLI, PowerShell, CloudShell.
Outils de Ticketing	Service-Now, Easy-Vista, Jira, ZenDesk, ITOP, GLPI ITSM

Formations, certifications et récompenses d'honneur.

03/2022	Certified Cyber Security Analyst **Ec-Council University**
10/2020	Certified C)SA1 *(13291-160-339-8306)* **Mile2**
02/2020	Certified Azure Administrator - AZ103 **VertiLearn**
11/2019	Certified Ethical Hacker V10 *(ECC7042398156)* **Ec-Council University**
10/2019	Certified Secure Computer User V2 *(ECC1534902786)* **EC-Council University**
PRIX D'HONNEUR	Meilleur interprète pour le 4e trimestre de l'année 2018 – HELPLINE.
	Certificat de gentillesse de l'année 2018 - HELPLINE.

Formation (2022)	Formation Cyber Security Analyst (CSA EC Council Program) **Numeryx University**
Formation (2021)	Formation Docker (Online Training Session) **Numeryx University**
	Splunk Fundamentals 7.X P2

Formation (2020)	**Splunk**
Formation (2020)	Splunk Fundamentals 7.X P1 **Splunk**
Formation (2020)	SC 200 (Microsoft Security Operations Analyst) **Microsoft/Pluralsight**
Formation (2020)	AZ 500 (Microsoft Azure Security Technologies) **Microsoft/Pluralsight**
Formation (2020)	MS 500 (Security Administrator Associate) **Microsoft/Pluralsight**

Compétences générales

Attitude positive, Communication, Esprit d'équipe, Capacité à accepter des commentaires constructifs, Pensée critique et résolution de problèmes, Compétences en gestion du temps, Autonome.

01/2025 - PRESENT	INGENICO
Rôle	SOC Analyst Expert L3 / SecOps Engineer
Environnement Technique	• Windows, Microsoft Azure, Microsoft End Point Protection, Solutions Securité SaaS.
Activité Réalisé	• Analyser les incidents remontés par le SOC, identifier les causes et les impacts, assurer leurs suivis jusqu'à résolution, et proposer des améliorations ou plans de remédiation pour optimiser les processus tout en enrichissant la base de connaissances. • Analyser les données de flux réseau et détecter les activités malveillantes et les anomalies.

- Analyser & Traiter les mails de Phishing et SPAM.
- Suivi des campagnes de sensibilisation de phishing.
- Sensibiliser les utilisateurs qui ne respectent pas les règles de sécurité.
- Identifiez les menaces et les vulnérabilités potentielles.
- Assurer une veille permanente sur les cybermenaces, vulnérabilités.
- Configuration des politiques de sécurité et des règles de détection personnalisées pour les endpoints, serveurs, e-mails.
- Intégration de sources de données multiples (SIEM, Active Directory, EDR, etc.) pour un enrichissement des événements de sécurité.
- Réalisation de recherches avancées (Search & Threat Hunting) via la console (recherche IOC, activités suspectes, etc.).
- Définition et application de politiques d'élévation des privilèges basées sur les rôles, les groupes, et les applications autorisées.
- Supervision des demandes d'accès administrateur via la console centrale ; approbation ou refus selon les règles de sécurité établies.
- Conception et optimisation de workflows ITSM pour la gestion des incidents, des demandes de service et des changements.
- Proposition et mise en œuvre de processus structurés alignés sur les SLA contractuels pour assurer un suivi rigoureux des incidents et demandes.
- Contribution à la mise en place de tableaux de bord de suivi (reporting opérationnel et stratégique) pour améliorer la visibilité sur les KPI.
- Participer au développement des fonctionnalités du SOC et à l'amélioration continue des processus.
- Participer à élaboration les règles de détection adaptées et renforcer les capacités de réponse aux incidents en se basant sur la matrice MITRE ATT&CK et MITRE D3FEND, tout en assurant une coordination efficace pour améliorer la posture globale de sécurité de l'organisation.
- Participation active aux cellules de crise et réaliser des analyses forensique.
- Assurer l'intégration, la formation et la montée en compétence des nouveaux arrivants dans l'équipe SOC.
- Coordination avec les équipes IT pour le traitement des incidents et la mise en place de plans correctifs.
- Collaboration avec les équipes de sécurité pour améliorer le cyber score et renforcer la réputation numérique de l'entreprise.

- Rédiger des rapports d'incidents à destination de la Management.
- Rédaction et mise à jour des Procédures techniques.

Technologies Utilisés

Microsoft Azure, Office 365, Microsoft Security Center, ELK , MDE, Qulays, XDR Trend Micro, ProofPoint.

2022 - 2024 GROUPE TF1

Rôle

Consultant en cybersécurité N2/N3

Environnement Technique

- Windows, Microsoft Azure, Microsoft End Point Protection, Solutions SaaS.

Activité Réalisé

- Analyser les menaces et développer des plans de blocage. (Enquête, Recommandations, Plans de remédiation...)
- Analyser les données de flux réseau et détecter les activités malveillantes et les anomalies par Vectra.
- Analyser les alertes remontés par le SOC Advens (N2/N3).
- Suivi sur les incidents.
- Analyser & Traiter les alertes MDE.
- Analyser & Traiter les mails de Phishing et SPAM.
- Suivi des campagnes de phishing menées par Cyber Ready.
- Identifiez les menaces et les vulnérabilités potentielles.
- Faire des sensibilisations aux utilisateurs qui ne respectent pas les règles de sécurité chez TF1.
- Référent sur la gestion des incidents de sécurité SOC.
- Back-Up sur la gestion des incidents CTI.
- Back-Up sur la gestion des scanners de vulnérabilités.
- Participer sur les process de améliorations continu au sein de la BlueTeam.
- Développement de Fonctionnalités Autour du SOC.
- Rédaction et mise à jour des Procédures techniques.

Technologies Utilisés

Microsoft Azure, Office 365, Microsoft Security Center, ELK , MDE, Tenable Nessus, CrowdStrike, CyberReady, CyberAngel, Jamf, Panorama PaloAlto, Vectra, ProofPoint.

2021 - 2022	GRTgaz
Rôle	**Consultant en cybersécurité N2/N3**
Environnement Technique	• Windows Server 2019, Active Directory, Microsoft Azure, Office 365, Amazon Web Services (AWS).
Activité Réalisé	• Analyser les menaces et développer des plans de blocage. (Enquête, Recommandations, Plans de remédiation...) • Analyser les données de flux réseau et détecter les activités malveillantes et les anomalies. • Bosser sur l'activité PDIS en collaboration avec Orange Cyber Défense (OCD). • Analyser les alertes remontés par le SOC PDIS (N2/N3). • Suivi sur les incidents et préparation des KPI. • Analyser & Traiter les alertes ATP/CASB/MDI/MDE. • Analyser & Traiter les mails de Phishing et SPAM. • Identifiez les menaces et les vulnérabilités potentielles. • Assurer le suivi d'installation des correctifs de sécurité. • Bloquer les Menaces. • Bosser sur les sujets de Compromission des Fournisseurs dans le cas de crise ou attaque informatique. • Traitement des incidents de sécurité N2/N3. • Participer sur les process de améliorations continu au sein de la CSIRT. • Développement de Fonctionnalités Autour du SOC. • Collaborer avec toutes les différentes équipes pour satisfaire le client.
Technologies Utilisés	Microsoft Azure, Office 365, Microsoft Security Center, Amazon Web Services (AWS), ATP, MDI, MDE, CASB, QRADAR, BitSight, Nessus, Symantec End Point Protection.

2020 - 2021	VERMEG for Banking & Insurance Software
Rôle	**Ingénieur en cybersécurité / Référent technique SOC**
Environnement Technique	• Windows Server 2016/2019, Active Directory, VMWare, VCenter, RedHat 7/8, CentOS 7/8, Microsoft Azure, Amazon Web Services (AWS).

Activité Réalisé

- Administration des outils SIEM (Splunk, Azure Sentinel).
- Préparation des architectures. (Splunk)
- Implémentation et installation des solutions SIEM (Splunk, Azure Sentinel)
- Gestion des licences des SIEM (Splunk, Azure Sentinel).
- Gestion des instances et des index des solutions SIEM. (Splunk, Azure Sentinel).
- Gestion des applications et addons SIEM. (Splunk, Azure Sentinel).
- Création des classeurs et tableaux de bord, Gestion des cahiers de chasse (Hunting notebooks). (Splunk, Azure Sentinel).
- Gestion et configuration des agents des SIEM. (Splunk, Azure Sentinel).
- Création/Affectation des Rôles SIEM, Gestion des utilisateurs SIEM. (Splunk, Azure Sentinel).
- Lecture, Contrôle et Investigation sur le journal corrélé…). (Splunk, Azure Sentinel).
- Analyser les menaces et développer des plans de blocage. (Enquête, Recommandations, Plans de remédiation...)
- Enquête avancée sur les attaques détectées, les CVE, les failles de sécurité en utilisant Splunk, Azure Sentinel, ATA, CVE Details, NIST, ExploitDB …
- Analyser les données de flux réseau et détecter les activités malveillantes et les anomalies (Enquête avancée suite aux tickets ou incidents signalés par l'équipe SOC / Gestion de crise informatique).
- Identifiez les menaces et les vulnérabilités potentielles.
- Installation, configuration et administration des solutions Endpoint Protection.
- Création de politique de Sécurité via les solutions Endpoint.
- Bloquer les Menaces, les Trojans, les Ransomwares…
- Enquêtez sur les Attaques Détectées et Appliquez les plans de correction Nécessaires pour Éviter Une nouvelle Attaque.
- Traitement des alertes DLP Office 365.
- Création des politiques de sécurité anti-phishing et anti-spam.
- Traitement des incidents de sécurité N2/N3.
- Rédaction des rapports après la résolution des incident ou la mise en place d'un plan de remédiation.
- Créer et Maintenir des rapports Opérationnels pour les KPI Hebdomadaires et Mensuels. (KPI).
- Rechercher et tester de nouveaux Outils / Produits de Sécurité et faire des Recommandations pour les Outils à Mettre En Œuvre dans L'environnement SOC. (POC).
- Développement de Fonctionnalités Autour du SOC.
- Référent technique. (SIEM et Endpoint Protection).
- Rédaction et mise à jour des Procédures techniques.
- Former les nouveaux collaborateurs.

Technologies Utilisés	Splunk Enterprise, Splunk Cloud, Enterprise Security, Microsoft Azure, Azure Sentinel, Office 365, Microsoft Security Center, Intune, Amazon Web Services (AWS), CloudWatch, CloudTrail, Advanced Threat Analytics (ATA), Advanced Threat Protection (ATP), Microsoft Cloud App Security (MCAS), Data Loss Prevention (DLP) Office 365, Rapid7 (Insight VM & NexPose), Secret Server, Kaspersky End Point Protection.
2019 à 2020	Helpline (Neurones IT Groupe)
Role	**Systèmes et Securité Administrateur Consultant**
Environnement Technique	Windows Server 2012/2016, Active Directory, Microsoft Azure, Amazon Web Services (AWS), NAS/QNAP, Syncovery.
Activités Réalisés	• Monitoring des Serveurs / Systèmes clients. • Gérer les Différentes infrastructures Informatiques des clients. (Patch Management, gestion des Agents SCCM, Déploiement des Packages, Suivi sur les installations, Dépannage technique sur les Erreurs des installations/Dépannage et proposition des solutions de Contournement …) • Installation, configuration et administration des solutions Endpoint Protection. • Installation des correctifs et patch de sécurité et assurer le fonctionnement des patches dans les environnements de Test et Prod ainsi que le suivi sur les installations réussi, échoué … • Bloquer les Menaces, les Trojans, les Ransomwares… • Enquêtez sur les Attaques Détectées et Appliquez les plans de correction Nécessaires/Proposition des solutions pour Éviter Une nouvelle Attaque. • Résolution des incidents N2 - N3. • Créer et Maintenir des rapports Opérationnels pour les KPI Hebdomadaires et Mensuels. (KPI). • Formalisation et Transfert expertise Vers le support Help Desk. • Rédaction et mise à jour des Procédures techniques.

Technologies Utilisés	Zabbix, Centreon, PRTG, Microsoft Azure, Office365, SCCM, Altiris, Symantec End Point Protection, McAfee ePolicy Orchestrator (ePO), ESET End Point Protection.
2018 à 2019	Helpline (Neurones IT Groupe)
Role	**IT Support Consultant**
Environnement Technique	Windows Server 2012/2016, Active Directory, Microsoft Azure.
Activités Réalisés	• Surveillance des Serveurs/Systèmes clients. • Résolution des incidents N0 - N1 - N2. • Controller les Agents Antivirus et les Agents SIEM au niveaux des Terminaux et Faire le troubleshooting dans le cas de besoin selon le périmètre de chaque client. • Rédaction et mise à jour des Procédures techniques. • Créer et Maintenir des rapports Opérationnels pour les KPI Hebdomadaires et Mensuels. (KPI).
Technologies Utilisés	Zabbix, Centreon, PRTG, Microsoft Azure, Office365, AirWatch, MobileIron.
2016 à 2018	BITS Informatique
Role	**IT Support/Proximity Support**
Environnement Technique	Windows Server 2012/2016, Windows XP, 7, 8.0, 8.1, 10.
Activités Réalisés	• Préparation de Windows Masters pour les clients. • Réparation D'ordinateurs. • Installation & Configuration des Solutions EndPoint auprès de nos clients. • Résoudre les incidents Liés aux Terminaux, à L'infrastructure, aux Systèmes, aux applications et aux Réseaux pour les Entreprises Clientes. • Rédaction et mise à jour des Procédures techniques.

- Créer et Maintenir des rapports Opérationnels pour les KPI Hebdomadaires et Mensuels. (KPI).

Technologies Utilisés

Windows Server 2012/2016, Windows XP, 7, 8.0, 8.1, 10.