ACA

CONSULTANT SSI (SOC N3)

DOMAINES DE COMPÉTENCES

Savoir-faire	• Analyse et remédiation d'incidents de sécurité et investigation
	  ○ Incidents de sécurité de niveau 1, 2 et 3.
	  ○ Analyse forensic sur les endpoints et systèmes critiques.
	  ○ Investigation des incidents complexes et identification des indicateurs de compromission (IOC).
	• Gestion des vulnérabilités
	  ○ Identification, qualification et suivi des vulnérabilités en fonction des contextes métiers.
	  ○ Amélioration des procédures de gestion des vulnérabilités et rédaction des politiques associées.
	  ○ Gestion des campagnes de scans de vulnérabilités
	• Supervision et monitoring
	  ○ Monitoring de la sécurité via des solutions SIEM
	  ○ Création et gestion de règles d'alerting basées sur des référentiels tels que MITRE ATT&CK.
	• Gestion de projets et amélioration continue
	  ○ Migration de solutions de sécurité
	  ○ Documentation et optimisation des processus
	  ○ Animation de workshops (DevOps et IT)
	  ○ Participation à des exercices de cellule de crise.
	• Analyse des risques et audits

Outils	• RSA, RSA Analytics, Gralyog, Splunk, Kibana,Fortigate, FireEye, SourceFire, TheHive, VadeSecure, Outscan/Netscan (Outpost24), Harbor, SentinelOne, Azure AD, Kubernetes, Vectra, Intune, Harbor, Cortex, Jira, SIEM, Logpoint, ELK, Wireshark
Framework	• NIST CSF, MITRE ATTACK

DIPLÔMES

- **2018 :** Master 2 Sécurité des réseaux - Itescia
- **2015 :** DUT Réseaux et Télécommunications – IUT de Villetaneuse

FORMATIONS PROFESSIONNELLES & CERTIFICATIONS

- **2024 :** Comptia Security+ Certified
- **2023 :** Google Cybersecurity Certified

LANGUES

- **Anglais :** Courant

EXPÉRIENCES PROFESSIONNELLES

Consultant SSI Transverse I RATP Smart System

- Juin 2024 à Septembre 2024

Contexte : Au sein de l'équipe Sécurité Opérationnelle, j'interviens pour accompagner les projets, renforcer les équipes, et améliorer les services, notamment dans le cadre des JO 2024.

Missions principales :

Réponse aux alertes (SOC) : J'assurais la gestion des alertes de sécurité, en analysant et en corrélant les alertes via SentinelOne, Vectra, et EntraID. Les investigations impliquaient des interactions avec les utilisateurs, le croisement d'informations provenant de différentes sources d'exploitation (firewall, équipements réseau, l'active directory, NDR/XDR) et la collaboration avec les équipes DevOps pour les environnements Kubernetes et AWS.
Exemples notable :

- Gestion d'une suspicion d'usurpation d'identité depuis un pays non autorisé (Confidentialité)
- Supervision et gestion des alertes liées à l'installation de logiciels non autorisés (Intégrité)
- Gestion d'une tentative d'accès/intrusion non autorisé (Confidentialité)

Gestion des vulnérabilités (VOC) : En utilisant Cyberwatch et Jira, j'identifiais et qualifiais les vulnérabilités selon leur impact métier. En collaboration avec le CERT RATP, je traitais les IoCs et CVEs liés au périmètre à surveiller en les blacklistant ou en y remédiant.
Chaque lot de vulnérabilités était discuté en atelier avec les référents applicatifs pour évaluer les solutions de remédiation, les risques acceptables ou les contournements.
Exemples notables :

- Test d'exploitation de la vulnérabilité CVE-2024-30078, campagne de vulnerability assessment sur le parc RATP Smart System, et suivi de remédiation.

Gestion des incidents (CISRT) : Réponse efficace aux menaces en mettant en œuvre des solutions de remédiation immédiates :

- Blocage de processus malveillants
- Mise en quarantaine de machines infectées
- Suspension de comptes utilisateur compromis
- Mise en œuvre de blocages réseau ;

Bien qu'il n'y ait pas eu d'équipe dédiée CSIRT pour la gestion des crises, j'ai eu l'opportunité de participer à un exercice de simulation de crise avec un prestataire externe spécialisé, en collaboration directe avec le DSI.

Conformité et normalisation : J'ai assuré la mise en conformité des outils de cybersécurité avec les normes du groupe RATP, notamment en réalisant des opérations de hardening, en rédigeant la documentation d'exploitation, et en définissant les processus.

Environnement technique : SentinelOne, Cyberwatch, Vectra, Intune, Jamf, Automox, Azure AD (EntraID), AWS – Kubernetes, Slack, Grafana (Prometheus et Loki).

Consultant SSI I CLS (Collection Localisation Satellite)

- D'août 2021 à Décembre 2023

Contexte : Il s'agit d'accompagner les projets SSI et l'amélioration continue des problématiques de cybersécurité sur le département Sécurité (3-4 personnes) de CLS

Missions principales :

Gestion des alertes (SOC Détection & Réaction) : J'assurais le monitoring sur nos différents outils, Cortex, Logpoint, Azure cloud Security et d'autres solutions maisons et je répondais aux différentes menaces détectées en investiguant les contextes et/ou interrogeant les utilisateurs ou parties IT impliqués. Des workshops étaient organisés avec les équipes IT pour l'éradication ou le confinement de la menace.

Exemples notables :

- L'activité d'un compte fantôme a amené à la détection d'un attaquant sur notre périmètre. Une revue immédiate des comptes et un verrouillage du dit compte ont eu lieu pour endiguer la menace. Des analyses ont eu lieu pour identifier d'autres compromission (confidentialité)

J'avais à charge des **activités de RUN** comme :

- L'accompagnement des utilisateurs et leur sensibilisation sur la menace des mails
- La MCO et le maintien de la documentation techniques de nos outils de sécurité
- Le monitoring du phénomène de Sideloading afin limiter un maximum, l'installation supplémentaire de surface d'attaques ou l'utilisation illégale de logiciel.

Gestion des vulnérabilités (VOC) : En utilisant les outils d'Outpost24 et Jira, j'identifiais et qualifiais les vulnérabilités selon leur impact métier. J'effectuais l'amélioration continue des processus de vulnerability assessment via des scripts NMAP.
Chaque lot de vulnérabilités était discuté en atelier avec les référents applicatifs pour évaluer les solutions de remédiation, les risques acceptables ou les contournements.
Exemples notables :

- Campagne de vulnerability assessment sur le parc CLS, suite à la découverte de la vulnérabilité log4J.

Je m'occupais aussi du processus de gestion et de scan d'artefacts (image docker) via Harbor avant leur mise en production.

Projets SSI :

- J'étais en charge de la migration des utilisateurs vers une nouvel solution de VPN, en recensant les compte utilisateurs. J'étais responsable d'accompagner les utilisateurs dans l'initiation de leur token ainsi que de la prise en charge de la MCO de l'outil RSA SECUREID.
- Un autre de mes projets consistait à proposer une politique/procédure de gestion de vulnérabilité. Le but était de normaliser les processus de scan de vulnérabilité et de responsabiliser les parties IT engagés, dans la résolution des vulnérabilités remontées.

Environnement technique : SentinelOne, Cyberwatch, Vectra, Intune, Jamf, Automox, Azure AD (EntraID), AWS – Kubernetes, Slack, Grafana (Prometheus et Loki).

Consultant SSI, CDG33 (Conseil départementale de la Gironde)

- Septembre 2020 à Avril 2021

Contexte : Intégration aux équipes de la DSIN (3 personnes) - Analyser et évaluer des menaces liées aux mails et aux alertes Trend Micro - Analyser et répondre à des incidents de sécurité - MCO des serveurs Windows du SI

Missions principales :

Analyse et évaluation des menaces (Detect & Response)

- J'dentifiais les menaces liées aux courriers électroniques et aux alertes via TrendMicro (Apex, Encyclopedia) et VadeSecure.
- Je menais des analyses approfondies des emails suspects via des pièces jointe, des liens hypertexte et l'en-tête pour détecter les éléments malveillants ou tout simplement via les contextes respectifs des mails.
- Je monitorais et répondais aux alertes remontées par les solutions de sécurité pour prévenir les incidents.
- Je participais à la sensibilisation des utilisateurs sur les bonnes pratiques lors de réception de mails en communiquant directement avec ces derniers ou via des ateliers.

Maintien en condition opérationnelle (MCO) :

- Je m'occupais de la mise à jour des systèmes et applications pour corriger les vulnérabilités et améliorer la résilience du SI et de la documentation des procédures liées aux opérations de MCO pour assurer une traçabilité optimale.

Environnement Technique : Windows, Trendmicro

Consultant SSI (SOC N2), Itrust

- Avril 2019 Juin 2020

Contexte : Intégration de l'équipe SOC (7 personnes)

- Supervision des SI des différents clients, y compris celui d'Itrust
- Analyser et répondre à des incidents de sécurité
- Apporter des préconisations sur les process, documentations et fiches de réponses à incidences.

Missions principales :

Detect and Response (SOC) :

- Analyse et parsing des logs à l'aide d'outils tels que Graylog et Logstash pour identifier des anomalies ou comportements suspects.
- Monitoring des en temps réel des signaux faibles ou des infrastructures clients via le SIEM ITRUST.
- Investigation des incidents détectés, incluant :
    - Corrélation d'événements complexes issus de diverses sources (Firewall, Antivirus, Windows).
    - Identification des indicateurs de compromission (IOC) pour détecter des menaces.
    - Qualification de l'alerte et escalade au niveau 3 si nécessaire.
    - Collaboration avec les équipes clients pour fournir des recommandations et résoudre les incidents.

Gestion des vulnérabilités (VOC)

- Gestion des procédures de vulnerability assessment, en configurant les scans et en respectant le calendrier de disponibilité client.
- Rédaction de documentations techniques et de rapports clients détaillant les mesures correctives et les recommandations pour réduire les risques.
- J'accompagnais aussi les clients (Référents technique) dans la remédiation des vulnérabilités détectés en les conseillant sur les bonnes pratiques à mettre en place.

Administration et maintenance du SIEM (MCO)

- Gestion et maintien en condition opérationnelle d'un SIEM sous Docker pour assurer une collecte efficace des événements.
- Supervision des mises à jour et des optimisations pour garantir la stabilité et la performance des outils SOC.

Conception et amélioration des processus (BUILD)

- Développement et implémentation de règles d'alerting basées sur le référentiel MITRE ATT&CK pour améliorer la détection des menaces.
- Préconisations sur l'amélioration des processus SOC, rédaction et mise à jour des fiches de réponse aux incidents sous excel.

Environnement Technique : ELK, VirusTotal, Wireshark, Graylog,Graphana, IA, TheHive, MitreAttack,Docker.

Adjoint Architecte SSI, Airbus GEO

- De Janvier 2019 à Avril 2019

Contexte : Modéliser et Challenger les aspects de sécurité liés aux sous-systèmes et applications métiers

Missions principales :

- Modélisation du fonctionnement des services ITs et de leurs interactions par zone (NIP) via Microsoft Visio. Je schématise les différentes connections entre systèmes, segment réseaux et les différentes zones de sécurité de l'architecture projet
- Identification des problématiques de sécurité, en prenant des réunions avec les référents IT correspondants. Je questionne les référents IT de chaque projet sur les bonnes pratiques et mesures de sécurité mise en place.
    - Exemple : Mise en place d'outil type DAST/SAST dans la chaîne CI/CD.
- Challenge des modélisations existantes et évaluations des sujets IT en questionnant les mesures des sécurités mise en place ou pas.
- Participation au workshop (comité d'architecture) de définition et d'identification du zoning des services applicatifs, des services métiers, des problématiques SIIV, et des sujets IT.

Environnement Technique : Visio, Linux

Consultant SSI (SOC N2), Airbus

- D'août 2018 à décembre 2018

Contexte : Intégration de l'équipe SOC (10 personnes)

Missions principales :

Analyse de domaines suspects : J'investiguais les domaines signalés comme « suspects » par les outils de protection (FireEye, SourceFire, RSA Analytics) en utilisant des plateformes spécialisées telles que VirusTotal, Whois, et UrlScan.io. Le blacklisting des éventuels domaines suspects était aussi une tâche dont j'étais responsable via les systèmes Bluecoats.

Detect & Response & Recovery : Dans le cadre d'escalade d'alerte au niveau 2 ou tout simplement via l'alerting de nos outils de sécurité, je qualifiais les menaces en investiguant les informations remontées dans l'alerte.) Je corrélais les informations de nos outils de sécurité (RSA, FireEye, Bluecoats, etc) et des parties impliquées. Dans certains cas, je procédais à l'isolement d'actifs suspects détectés grâce aux solutions EDR pour limiter les risques de propagation.
Une analyse approfondie des endpoints(postes de travail et serveurs) pouvais avoir lieu afin d'en récupérer des artefacts comme la modification de registres ou des lancements de processus inhabituels.

Investigation des courriels : J'étais également en charge d'analyser les courriels et pièces jointes signalés par les utilisateurs ou détectés par les outils de protection, afin d'identifier les URL ou fichiers binaires malveillants.

Détection des contournements de sécurité : Mes responsabilités incluaient l'identification des tentatives de contournement des mesures de sécurité.

Exemple : Détections de connexions suspectes vers des serveurs de commande et contrôle (C&C) depuis des postes compromis.

Documentation et amélioration continue :

- Je rédigeais, maintenais et améliorais la documentation des processus SOC ainsi que les fiches techniques de prise en main des outils.
- Mon objectif était de garantir une utilisation optimale des outils techniques et de renforcer l'efficacité des opérations de sécurité.

Environnement Technique : ELK, VirusTotal, Wireshark, Graylog,Graphana, IA, TheHive, MitreAttack,Docker.

Ingénieur Sécurité Système et Réseaux, Alcatel & Nokia [1]

- De mai 2015 à août 2018

Contexte : Automatisation de tests de sécurité unitaire et Implémentation de framework de tests de sécurité

Missions principales :

- Mise en place de Tests de vulnérabilités système sur produits réseaux en utilisant des outils comme CRON/Jenkins-Détection et analyse de cores (erreurs systèmes)
- Automatisation de tests de sécurité avec Shell/Python/Ansible
- Développement d'un Framework de test de sécurité (Botnet as a Security Test Framework)
- Intégration de solution open source (OpenVAS, OpenScap, Nessus, etc.) à un Framework de test et automatisation de tests de sécurité systèmes et réseaux
- Installation de maquettes pour différents produits réseaux.
- Proposition d'un PoC (Proof of concept) avec les technologies Radware et Deepfield Nokia
- Rédaction de documents sur les différents scripts et outils utilisés/implémentés

Environnement Technique: Radware, Deepfield, JackTheRipper, Scapy, Vsphere, Openstack, Shell, Python, Linux, Windows, OpenVAS, Lynis

[1] Stage