VALENTIN SPORER

Ingénieur Logiciel

Poitiers, FRANCE
+33 6 22 95 39 20
v@sporer.fr
30 ans
github.com/demonoidv

QUI SUIS-JE ?

Principalement développeur back-end mais avec un attrait pour le front-end, je suis pragmatique et polyvalent.
J'adore apprendre et je m'adapte facilement à de nouveaux langages et technologies comme le montrent mes dernières expériences.
J'aime le travail en équipe mais je suis également à l'aise en totale autonomie.

Je recherche aujourd'hui un nouveau challenge au travers de projets ayant un impact concret et bénéfique sur la vie des gens, comme la protection de la vie privée et des données personnelles, le domaine de la santé, les outils pour developpeur ou le domaine de l'IA.

FORMATIONS

2016 – 2021 — **Titre d'Expert informatique et système d'information (RNCP 7)** — **Ecole 42 Paris**
Formation dans divers domaines de l'informatique: algorithmie, graphisme, système UNIX, sécurité, jeux vidéos, web...
J'y ai appris à développer presque depuis zéro, d'abord en C puis en Rust et en Assembleur, me specialisant dans le développement d'application bas niveau et la sécurité.

2013 – 2015 — **BTS ERO** — **Lycee Val de Garonne**
BTS en étude et réalisation d'outillages de mise en forme des matériaux.
Conception 3D et réalisation, par l'usinage de bloc d'acier, de moules pour l'injection plastique en série.

2010 - 2013 — **Bac pro Technicien Modeleur** — **Lycee professionnel Mas Jambost**
Baccalauréat professionnel en conception et réalisation de maquettes, prototypes et modèles pour moule de fonderie.

CERTIFICATIONS

2022 — **Microsoft Certified: Security, Compliance, and Identity Fundamentals**
Voir la certification sur Credly

EXPERIENCES

2021 – Octobre 2024 — **Ingénieur logiciel** — **Tenable**
3 ans

Société : Tenable est une société américaine spécialisée dans l'édition de logiciels de cybersécurité destinés aux entreprises de toutes tailles. Son activité est vaste et inclut notamment des solutions de sécurité pour le Cloud, l'IoT, les machines virtuelles (VMs), et l'Active Directory (depuis l'acquisition d'Alsid), entre autres.

Contexte : Pendant plus de trois ans, j'ai travaillé sur plusieurs projets, tels que Tenable Identity Exposure (anciennement Alsid for AD), dédié à la sécurité des identités numériques, et Tenable ONE, une plateforme conçue pour unifier toutes les solutions proposées par Tenable en un produit unique.

J'ai eu l'opportunité de contribuer à différents aspects de ces produits : la collecte de données, les moteurs d'analyse de sécurité, les services d'APIs, ainsi que l'interface utilisateur.

Missions :

- Conception, lead et développement d'un projet visant à simplifier et accélérer la configuration des capacités de détection d'attaques :
  - Amélioration de l'agent Rust s'executant sur les Controleurs de Domaines de l'Active Directory des clients (rechargement dynamique des configurations).
  - Refonte de la page de configuration utilisateur pour une modification simplifiée.
- Conception, lead et développement d'une solution permettant la désactivation et la réactivation automatique de capacités de détection d'attaques, afin de maintenir les performances du reste de la stack sous très forte charge.
- Étude et développement du scaling horizontal pour les services de détection d'attaques :

  - Création de deux services en C# pour le traitement et la gestion des données des événements Windows.
  - Implémentation d'un système de cache inspiré de Redis pour améliorer les performances.
- Intégration dans Tenable ONE des données collectées dans par les autres solution de Tenable (Identity Exposure, Cloud Security, VM, IoT, WAS, ...) :
  - Développement en Kotlin d'un service back-end servant les APIs (approche OpenAPI first) pour le front-end, requêtes SQL performantes (Snowflake et PostgreSQL).
  - Développement de composants front-end en React (TypeScript).
  - Intégration des composants dans les pages web client de Tenable ONE.
- Refonte et intégration de l'interface utilisateur de Tenable Identity Exposure via iframe en Typescript/React.
- Maintien et développement de nouvelles APIs et requêtes SQL (MSSQL) pour le service back-end de Tenable Identity Exposure (TypeScript/Node.js).
- Maintien et développement de nouvelles fonctionnalités (mots-clés, syntaxe, etc.) pour le SEL (Security Engine Language), permettant aux clients d'implémenter eux-mêmes de nouvelles capacités de détection de vulnérabilités ou d'attaques grâce à un langage (SEL) simple et concis.
- Développement et mise à jour des tests unitaires, des tests d'intégration et des tests systèmes pour chaque nouvelle fonctionnalité ou modification de fonctionnalités existantes.
- Mise à jour régulière de la documentation interne et externe.
- Ajout de nouvelles metriques pour le monitoring lorsque pertinant.
- Développement de tableaux de bord et d'alertes Datadog pour le monitoring des services déployés en production.

Environnement technique : Rust, Kotlin, SQL (Snowflake, PostgreSQL, MSSQL), React, Typescript, C#, .NET, Node.JS, Xunit, Nunit, Moq, Jest, Bouchon, Mockito, Junit, REST, Flyway, Swagger, OpenAPI, Jenkins, AWS, NeoVim (Rust), IntelliJ (Kotlin, Typescript), Rider (C#), Dbeaver, Git, GitHub, Prometheus, Datadog, RabbitMQ, Kafka, Redpanda, Docker, Kubernetes, Postman, cURL, Windows, Linux.

2020 – 2021 (1 ans et 10 mois) **Ingénieur logiciel - Apprenti** **Alsid / Tenable**

Société : Alsid est une société de type start-up spécialisée dans l'édition de logiciels de cybersécurité, destinée aux entreprises de taille moyenne, aux grandes entreprises et aux grands groupes.
Son activité se concentre sur la détection des vulnérabilités dans la configuration de l'Active Directory, ainsi que sur la détection des attaques en temps réel.

Alsid a été rachetée par Tenable en 2021.

Tenable est une société américaine spécialisée dans l'édition de logiciels de cybersécurité destinés aux entreprises de toutes tailles. Son activité est vaste et inclut notamment des solutions de sécurité pour le Cloud, l'IoT, les machines virtuelles (VMs), et l'Active Directory (depuis l'acquisition d'Alsid), entre autres.

Contexte : En contrat d'apprentissage en alternance pendant un peu moins de deux ans avec Alsid, puis avec Tenable suite au rachat du premier par le second, j'ai eu l'opportunité de contribuer à différents aspects de la solution de cybersécurité Alsid for AD (renommée Tenable.AD après le rachat).

Mes contributions ont porté sur divers éléments : la collecte de données, les moteurs d'analyse de sécurité, les services d'APIs, ainsi que, plus rarement, l'interface utilisateur.

Missions :

- Développement en Typescript (NodeJS) de nouvelles APIs REST pour interagir avec la base de donnée.
- Lead et réécriture en C# des crawlers (programmes en C et C++ que j'ai optimisés lors de mon stage et maintenus depuis) pour les intégrer à un service unifié de collecte de données.
- Maintenance des crawlers en C# (correction de bugs, collecte de nouvelles données développement de nouveaux parsers).
- Conception et développement en Rust d'un agent d'agrégation d'événements systèmes (event logs Windows) pour la détection d'attaques en temps réel.
- Amélioration du moteur d'analyse de sécurité en C#, permettant l'exploitation en temps réel des événements Windows pour la détection d'attaques.
- Développement de nouvelles capacités de détection de failles de sécurité et attaques en C#.
- Maintien et implémentation de nouvelles APIs et requêtes SQL (MSSQL) pour le service backend de Tenable Identity Exposure (TypeScript/Node.js).
- Maintenance des crawlers en C et C++ (correction de bugs).
- Développement et mise à jour des tests unitaires, des tests d'intégration et des tests systèmes pour chaque nouvelle fonctionnalité ou modification de fonctionnalités existantes.
- Mise à jour régulière de la documentation interne et externe.

- Ajout de nouvelles metriques pour le monitoring lorsque pertinant.
- Développement de tableaux de bord et d'alertes Grafana pour le monitoring des services déployés en production.

Environnement technique : C, C++, Win32, Rust, SQL (MSSQL), Typescript, C#, .NET, Xunit, Nunit, Moq, Jest, Bouchon, Node.JS, REST, Swagger, Azure DevOps, Azure Pipelines, NeoVim (Rust), VS Code (Typescript et Rust), Rider (C#), Visual Studio (C#), Microsoft SQL Management Studio, Git, GitHub, Prometheus, Grafana, RabbitMQ, Docker, Kubernetes, Postman, cURL, Windows, Active Directory, HyperV, SMB, LDAP.

2018 – 2020 (13 mois) **Ingénieur logiciel junior** **Alsid**

Société : Alsid est une société de type start-up spécialisée dans l'édition de logiciels de cybersécurité, destinée aux entreprises de taille moyenne, aux grandes entreprises et aux grands groupes.
Son activité se concentre sur la détection des vulnérabilités dans la configuration de l'Active Directory, ainsi que sur la détection des attaques en temps réel.

Contexte : En CDI à mi-temps, afin de me permettre de poursuivre mes études à l'École 42 en parallèle, j'ai contribué pendant un peu plus d'un an à des projets majeurs liés au produit Alsid for AD, développé par Alsid.

Missions :

- Développement de nouvelles capacités de détection de vulnérabilités en C#.
- Développement du moteur d'analyse de sécurité, identifiant les vulnérabilités à partir des données collectées, en C#/.NET :
  - Réécriture complète du moteur d'analyse en C#/.NET à partir de l'ancien code en PowerShell.
  - Gestion des événements liés aux modifications Active Directory en temps réel.
- Maintenance des crawlers, en C et C++, optimisés lors de mon stage :
  - Correction de bugs et ajout de fonctionnalités (collecte de nouvelles données LDAP, ouveaux fichiers de configuration).
- Mise à jour régulière de la documentation interne et externe.
- Ajout de nouvelles metriques pour le monitoring lorsque pertinant.
- Développement de tableaux de bord et d'alertes Grafana pour le monitoring des services déployés en production.

Environnement technique : C, C++, Win32, C#, .NET, Xunit, Nunit, Moq, PowerShell, Azure DevOps, Azure Pipelines, Visual Studio (C, C++ et C#), Rider (C#), Git, GitHub, RabbitMQ, Docker, Kubernetes, Grafana, Windows, Active Directory, HyperV, SMB, LDAP.

2018 (6 mois *stage*) **Developpeur système - Stagiaire** **Alsid**

Société : Alsid est une société de type start-up fondée en 2016 comptant une dizaine de collaborateurs au moment du stage.
Elle est spécialisée dans l'édition de logiciels de cybersécurité, destinée aux entreprises de taille moyenne, aux grandes entreprises et aux grands groupes.
Son activité se concentre sur la détection des vulnérabilités dans la configuration de l'Active Directory.

Contexte : En tant que stagiaire chez Alsid, mon rôle a été de drastiquement améliorer les performances des deux programmes, écrits en C et C++, responsables de la collecte de données sur l'Active Directory des clients.

La nécessité d'améliorer les performances découlait de l'objectif, pour la version 2.0 de la solution, de gérer en temps réel les événements de changement de configuration.

Missions :

- Integration au sein des crawlers de RabbitMQ et TLS pour la communication entre les services.
- Optimisation des crawlers, deux programmes écrits en C et C++ orientés Windows (Win32 API), utilisés pour collecter les données de configuration Active Directory des clients.
  - Ajout du multithreading et de la bufferisation pour détecter et parser les modifications de la configuration de l'Active Directory en temps réel.
- Développement d'outils de test en Python et PowerShell pour vérifier les modifications des crawlers (tests de non regression) et évaluer les gains de performance.
- Création d'environnements de tests via des machines virtuelles (Windows Server 2000 à 2016 R2) sur HyperV

Environnement technique : C, C++, Python, Powershell, Win32 API, SMB, LDAP, Active Directory, HyperV, Visual Studio, Git, GitHub, RabbitMQ, Windows.

LANGUES

Français - Natif
Anglais - Avancé

LOISIRS

J'aime configurer mes NAS et mon réseau domestique. Monter et entretenir mes machines. Je pratique le tir à l'arc ainsi que la conception et l'impression 3D.

OUTILS

Git, Docker, OpenAPI, Vim, IntelliJ, Visual Studio, VS Code, Rider, Rust Rover, Grafana, Datadog, Sentry, Kafka, RabbitMQ, Snowflake, PostgreSQL, ...