Engineer Платформа

Портфоліо

Інженерні послуги з прикладами виконаних робіт.

Engineer ApS зареєстровано у 2025 році. Більшість показаних тут робіт виконано до того нашою засновницею у складі команд клієнтів; частину виконала сама компанія, а частину — згодом, працюючи за наймом. Ті самі руки й ті самі стандарти — і ми прямо кажемо, що є що, а не розмиваємо межу.

Знайдіть досвід, вартий застосування

Використайте перелік, щоб знайти досвід, доречний для вашого проєкту.

Переглянути наші послуги Зв'язатися з нами →

Прочитайте про рішення, що стоять за роботами

Приклади описують виконані роботи за різними послугами. Прочитайте огляд ситуації та рішень.

Кейси Зв'язатися з нами →

Перегляд за категоріями

РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Backend-розробка · Frontend-розробка · Full-Stack-розробка · API та інтеграції · Веброзробка · Тестування та QA · Оптимізація продуктивності · Python · Інтернаціоналізація

ДАНІ ТА БАЗИ ДАНИХ

Бази даних · PostgreSQL · SQL · Інженерія даних · Пайплайни даних (ETL/ELT) · Аналітика даних · Управління даними · GIS / геопросторові дані

ХМАРА, ІНФРАСТРУКТУРА ТА DEVOPS

Хмарні технології · Контейнери (Docker/Kubernetes) · DevOps · Автоматизація та CI/CD

Інфраструктура
Linux та сервери
Системне адміністрування
Мережі та VPN
Моніторинг і спостережуваність
Надійність і резервне копіювання
Безпека
Архітектура платформи
Міграції та модернізація

КОНСАЛТИНГ ТА ЛІДЕРСТВО

Технічне лідерство
Керівництво командою
Agile та Scrum
Управління проєктами
Продукт і вимоги
Зацікавлені сторони та звітність
Документація
Архітектура рішень
Бренд і маркетинг

Усе, що нижче, **вже зроблено** — не запропоновано й не заплановано.

Кожен запис називає, що робота змінила, і веде до послуг, які вона підтверджує.

Що ми пропонуємо Скільки це коштує →

{ Хмара, інфраструктура та DevOps }

Хмарна інфраструктура та міграція

Там, де працює програма

Сервери під те навантаження, яке у вас справді є, перенесені в хмару чи назад, із порахованим наперед місячним рахунком.

Підготувала другий сервер із коду

Автоматизувала підготовку (provisioning) другого сервера в другого хмарного провайдера, створюючи фаєрвол раніше за машину, щоб вона від самого початку була за ним, а фаєрволи обох провайдерів налаштовуються безпосередньо через їхні REST API, без сторонньої колекції.

Запустила контейнери на Podman і Quadlet

Розгорнула контейнерну платформу на Podman і Quadlet під systemd, а не на Docker, бо типове публікування портів Docker у мережі bridge може обходити правила UFW, — а для розгортань виділила непривілейованого користувача з однією фіксованою командою замість root.

Публічні служби на невеликому сервері

Розмістила публічні служби компанії на одноядерному хості з 512 МБ — git-сервер, вебсервер для семи доменів, Tor, два сервери альтернативних протоколів і блокування вторгнень, — використовуючи 464 МБ доступної пам'яті як проєктне обмеження; автоматизація резервування є окремою реалізацією.

Інфраструктура, описана в репозиторії

Побудувала власну інфраструктуру компанії у вигляді 19 плейбуків Ansible і 34 ролей обсягом 12 065 рядків YAML, які приводять робочий хост до задекларованого стану, причому кожен play ідемпотентний.

Побудувала всю базову інфраструктуру з нуля

Як одна з перших співробітниць, спроєктувала та побудувала всю базову інфраструктуру та супутні процеси з нуля для SaaS-стартапу в зеленій енергетиці, заклавши фундамент для швидкого зростання.

Відповідала за розгортання платформи в Azure

Відповідала за наскрізне розгортання платформи в Azure, керуючи релізами в середовищах development, staging і production.

Розгорнула інфраструктуру Azure як код

Розгорнула інфраструктуру Azure як код за допомогою Bicep — Container Apps, PostgreSQL Flexible Server, Front Door/WAF та мережу — у середовищах development, staging і production.

Спрощена інфраструктура поза AWS

Перебудувала інфраструктуру міжнародного клієнта, вилучивши невикористані служби, скоригувавши потужність і перенісши навантаження з AWS. За свідченням засновниці, витрати на хмару скоротилися у 10 разів без втрати продуктивності.

Вела 20 застосунків Docker у Google Cloud і AWS

Розгорнула та підтримувала 20 контейнеризованих застосунків Docker, усуваючи несправності за допомогою Podman і Kubernetes, а також керувала застосунками на R у Google Cloud та AWS.

{ Хмара, інфраструктура та DevOps }

Infrastructure as Code

Сервери, які можна відтворити з версійованої конфігурації

Уся конфігурація записана у файлах, тож її можна відтворити точно, і вона не живе лише в чиїйсь голові.

Опублікувала читабельне onion-дзеркало в Tor

Опублікувала сайт як onion-дзеркало в Tor за читабельною адресою, що починається з engineer, з ключем, згенерованим поза хостом, тож він ніколи не потрапив ні до цього репозиторію, ні на ноутбук, і залишила цей вхід єдиним із чотирьох, відвідування якого ніколи не рахуються.

Перевірила CI-хук git-сервера, знайшла 2 дефекти

Відрепетирувала CI-хук на боці git-сервера й знайшла два дефекти, яких не виявити читанням файлу: запасний варіант, що передавав на вхід хука аргумент, який неможливо розв'язати, і власну змінну середовища git, яка потрапляла слідом за гейтом у checkout і робила 19 тестів червоними.

Розділила всі операційні секрети за хостами

Розділила чотири операційні секрети так, щоб кожен хост мав власні, з'ясувавши, що два хости зі спільним dead man's switch сповіщають про збої рідше, ніж два окремі перемикачі, а не частіше, і що спільна парольна фраза резервних копій може відкрити доступ до копій обох хостів навіть в окремих репозиторіях, якщо хтось отримає її та зможе прочитати зашифровані дані й файли ключів обох репозиторіїв.

Ваш код на вашому власному сервері

Розгорнула власний git-сервер компанії на Soft Serve, приватний за замовчуванням і без вебпанелі, з портом SSH, прив'язаним до loopback за проміжним хостом (jump host), і зробила цільову сторінку перед ним артефактом збірки основного сайту, а не копією, яку підтримують вручну.

Посилила ізоляцію systemd для кожного юніта

Знизила оцінку відкритості (exposure) у пісочниці systemd для кожного юніта, який встановлює платформа: служба dead man's switch — з 9,6 UNSAFE до 1,5, відкритий в інтернет git-сервер — з 8,3 EXPOSED до 1,5, — і додала перевірку парсером під час converge, після того як знайшла у трьох шаблонах юнітів директиву з орфографічною помилкою, яку systemd мовчки ігнорував.

Описала зону DNS із 20 записів як код

Налаштувала декларативне узгодження зони DNS із 20 записів з API Cloudflare, з окремими точками входу для аудиту та експорту в BIND, а побудувавши проксі CDN, знову вимкнула його з міркувань приватності.

Додала секундну попередню перевірку секретів

Додала попередній плей (preflight), який приблизно за секунду проганяє той самий код, що й converge, на локальних секретах оператора, — після того як продакшн-запуск обірвався на дев'ятому завданні, застосувавшись лише наполовину, а налаштування swap уже було записано на робочий хост.

Домоглася, щоб check mode в Ansible казав правду

Домоглася, щоб check mode показував правду на всій платформі, після того як знайшла шість перевірок, що ухвалювали рішення за значенням, якого хост ніколи не повертав: модуль command в Ansible у режимі --check звітує про успіх, узагалі не виконуючи команду.

Побудувала моніторинг хоста з dead man's switch

Побудувала моніторинг за принципом dead man's switch, який надсилає пінг, лише поки пам'ять і диск у нормі, тож хост у погіршеному стані здіймає тривогу своїм мовчанням, — і виявила шість імен змінних зі словом «free» там, де перевірка правильно вимірювала «available»: на машині з 464 МБ ці значення різняться на порядок.

Автоматизація резервування з явним способом відновлення

Реалізувала автоматизацію резервування restic з політикою зберігання, перевіркою цілісності та щомісячним тестом відновлення; задокументувала активацію сховища й перевірку справжнього відновлення як окремі операційні кроки.

Посилила SSH до 24 перевірених директив

Посилила захист SSH: 24 директиви, кожну з яких перевіряє assert, і триетапна валідація — файл-кандидат, зібрана конфігурація, а потім зворотне зчитування самим демоном, — після того як таке зчитування виявило, що запущений сервер мовчки перевизначав дві з двадцяти чотирьох.

Налаштувала резервні копії та відновлення як код

Налаштувала зберігання резервних копій бази даних у вигляді інфраструктури як коду (infrastructure-as-code), провела аудит готовності до відновлення й задокументувала процедуру відновлення — чітко назвавши наявні прогалини, а не залишивши їх на час інциденту.

Написала 1 000 правил RBAC для Linux-серверів

Посилила безпеку даних, впровадивши 1 000 правил RBAC для розробників, інстансів застосунків, PostgreSQL, MS SQL та інших Linux-серверів, запобігши несанкціонованому доступу; задокументувала їх як автоматизацію в Ansible.

Цю послугу застосовано в роботах, наведених деінде на цій сторінці:

Підготувала другий сервер із коду · Публічні служби на невеликому сервері · Інфраструктура, описана в репозиторії · Розгорнула інфраструктуру Azure як код

{ Хмара, інфраструктура та DevOps }

DevOps та автоматизація CI/CD

Випускати зміни без нервів

Перевірено, випущено і з можливістю відкату, тож зміни доходять до клієнтів у вівторок удень, а не пізно в п'ятницю.

Привела 4 репозиторії до одного стандарту історії

Привела чотири репозиторії до одного стандарту історії — conventional-коміти, без емодзі, без рядків атрибуції, з контролем через хук повідомлень комітів, — поряд із 48 документами інструкцій, що визначають, як виконується робота.

Знайте ліцензію всього, що випускаєте

Запровадила перевірку сумісності ліцензій 644 крейтів Rust під час кожної збірки й довела, що вона спрацьовує, переписавши ліцензію одного крейта та змістивши зафіксовану ревізію ядра без перегенерації.

Задіяла невикористану половину ядра

Задіяла ту половину ядра обміну повідомленнями, якою застосунок ніколи не користувався, — передавання резервної копії, зникомі повідомлення, редагування та повторне надсилання, підтверджені запрошення, проксі та політику шифрування, — проганяючи кожен тест на справжній бібліотеці без заглушок.

Пришвидшила набір тестів до 8,9 секунди

Скоротила набір тестів від шести тестів, що перевищували ліміт у шістдесят секунд, до 135 успішних за 8,9 секунди, профілюючи головний потік і прибравши два виклики, у яких він перебував 3 989 із 4 017 вибірок.

Написала парсер, що перевіряє кожен виклик FFI

Написала парсер, який читає справжній C-заголовок на 7 308 рядків і перевіряє кожне місце виклику, кожну константу переліку й те, що кожен клас-власник вказівника є final, після того як через написаний вручну заголовок-заглушку виклики трьох вилучених функцій компілювалися, лінкувалися й аварійно завершувалися.

Виявила розбіжність між хуками й гейтом якості

Виявила, що хуки комітів і гейт якості виконують різні перевірки, хоча документ обіцяв, що вони однакові, порівнявши два переліки в тесті, — п'ять перевірок, які запускалися лише вручну, були саме тими, що читали текст CV.

Написала тести для самих перевірок

Написала тести для самих перевірок, з'ясувавши, що перевірка, яка отримує лише чисті вхідні дані, одного дня звітуватиме про чистоту, бо нічого не прочитала: підклала помилку правопису, щоб підтвердити, що перевірка орфографії її знаходить, і взяла діапазон ідентифікаторів із бази даних, а не з числа в тесті.

Увімкнула всі правила лінтера Python як помилки

Увімкнула всі правила лінтера Python як помилки й довела 1 815 зауважень до нуля; кожен із небагатьох винятків має письмове обґрунтування, а два з них підкріплені перевіркою, а не коментарем.

Забезпечила генератору 981 тест і 92% покриття

Покрила генератор 981 тестовим випадком із мінімальним порогом покриття гілок 92%, де попередження вважаються помилками, і перевірила ідемпотентність, двічі запустивши весь пайплайн збірки з порожнього файлу та вимагаючи, щоб другий прохід нічого не змінював.

Перевірила лінтером 10 242 рядки перевірки якості

Охопила форматувальником і лінтером 10 242 рядки JavaScript у перевірках якості, з'ясувавши, що це найбільший обсяг коду в репозиторії і єдиний, який ніщо не перевіряло, — виправила 13 зауважень і не вимкнула жодного.

Виправила мапу сайту з однією позначкою часу

Виправила мапу сайту, де 172 з 176 URL мали одну позначку часу зміни, взявши дату з історії git, після того як з'ясувала, що експорт переписує кожен файл під час кожного запуску.

Віддзеркалила сайт у Gemini та Gopher

Побудувала вихідні формати Gemini та Gopher з того самого джерела сайту; запис досягнення фіксує по 777 документів на тому етапі та нуль змінених байтів HTML від додавання форматів.

Страховка, що більше не забирає пів години

Скоротила браузерну перевірку якості сайту з 1 636 секунд до 615, запускаючи перевірки від найдовших до найкоротших через пул воркерів із максимум чотирма одночасними перевірками, після того як виміряла, що алфавітний порядок коштував 320 секунд проти 224.

Побудувала перевірку комітів із 22 лінтерів

Побудувала перевірку перед комітом із 22 лінтерів, кожен з яких описується одним рядком, і ще п'ятьох, що заслуговують окремого абзацу, без рівня попереджень і без дозволу на вбудоване вимкнення правил, яка охоплює HTML, CSS, JavaScript, Python, YAML, Markdown, shell, посилання, орфографію, секрети й типографіку.

Запровадила безперервне сканування безпеки

Запровадила безперервну програму безпеки — сканування коду, DAST, перевірки залежностей і вразливостей, генерацію SBOM, пошук секретів та actions, закріплені за SHA, — поряд із 21 письмовим аудитом безпеки.

Тримала схему узгодженою впродовж 1 022 міграцій

Тримала схему узгодженою впродовж 1 022 міграцій за допомогою перевірки CI, яка збирає базу даних обома шляхами — чиста інсталяція та інсталяція плюс усі міграції — і падає, коли вони розходяться.

Побудувала власні моніторинг помилок і трасування

Побудувала власний моніторинг помилок і трасування OpenTelemetry, а не купила готові — очищення payload, виявлення сплесків і регресій, символікацію та синтетичний heartbeat — за 11 операторськими поданнями.

Побудувала механізм із 268 перевірок репозиторію

Побудувала механізм перевірок репозиторію — 268 зареєстрованих перевірок коміту, 277 правил лінтингу та 15 власних правил ESLint — а також 146 тестів самих перевірок, щоб стандарт тримала збірка, а не код-рев'ю.

Побудувала тести для Go, SQL і браузера

Побудувала багаторівневий набір автоматизованих тестів — 981 тест Go, 543 фронтендні та браузерні специфікації, 494 поведінкові тести SQL — з мутаційним тестуванням, property-based тестами та обов'язковою перевіркою доступності.

Автоматизувала командну співпрацю

Автоматизувала командну співпрацю, керування паролями, управління завданнями та часом, а також створила напівавтоматичну систему демонстрації проєктів, підвищивши продуктивність команди.

Запровадила нуль попереджень у шести мовах

Встановила стандарт якості без жодних попереджень для шести мов — Go, TypeScript, SQL, Python, Shell і Markdown — дотримання якого забезпечували pre-commit hooks.

Написала 578 цілей автоматизації go-task

Написала 578 цілей автоматизації go-task, що охоплюють нативний, Docker- та HTTPS-режими розробки, лінтинг, тестування, базу даних та розгортання.

Побудувала пайплайни CI/CD на GitHub Actions

Побудувала пайплайни CI/CD на GitHub Actions з distroless-образом продакшн-фронтенду та просуванням релізів між кількома середовищами.

Згенерувала контракт API із самої бази даних

Згенерувала контракт API з бази даних назовні — OpenAPI, типізований TypeScript-клієнт на 44 076 рядків, 61 mock-обробник та обмеження, які застосовує UI, — з перевіркою на кожній ланці, що падає в разі розбіжностей.

Автоматизувала обробку даних на Python і PL/pgSQL

Автоматизувала завдання обробки даних за допомогою shell-скриптів, PL/pgSQL, Python та Transact-SQL, підвищивши продуктивність і ефективність.

Заощадила 4 000 годин з CI/CD на GitHub і GitLab

Оптимізувала процеси аналізу даних та розробки програмного забезпечення, заощадивши 4 000 годин завдяки впровадженню практик CI/CD на базі GitHub, GitLab, Bash та Python.

Оптимізувала CI/CD, заощадивши 4 000 годин

Оптимізувала процеси CI/CD, заощадивши 4 000 годин завдяки впровадженню автоматизації в пайплайнах розробки програмного забезпечення.

Автоматизувала SSL/TLS для 100 застосунків Docker

Автоматизувала створення сертифікатів SSL/TLS для 100 застосунків Docker, забезпечивши безпечні з'єднання на хостах Ubuntu Linux.

Реорганізувала процеси, заощадивши 8 000 годин

Реорганізувала внутрішні процеси, заощадивши 8 000 годин завдяки вдосконаленню архітектури програмного забезпечення, систем та ефективності планування.

Знизила операційні ризики з Grafana і Prometheus

Знизила операційні ризики, впровадивши дашборд моніторингу на базі Grafana та Prometheus, підвищивши надійність системи.

Автоматизувала 100 критичних резервних копій

Автоматизувала 100 критично важливих резервних копій даних за допомогою Barman, Google Cloud, Bash та Python, забезпечивши цілісність даних в усіх базах.

Автоматизувала розгортання 20 GIS-пайплайнів

Автоматизувала розгортання 20 пайплайнів GIS-даних та ETL-процесів даних застосунку, оптимізувавши автоматизацію інфраструктури та звітність.

Автоматизувала розгортання GIS SaaS через CI/CD

Автоматизувала розгортання GIS SaaS-застосунку, обробку даних та систему звітності за допомогою GitHub Actions CI/CD, Python, Bash та SQL.

Цю послугу застосовано в роботах, наведених деінде на цій сторінці:

Перевірила CI-хук git-сервера, знайшла 2 дефекти · Запустила контейнери на Podman і Quadlet · Ваш код на вашому власному сервері · Додала секундну попередню перевірку секретів · Домоглася, щоб check mode в Ansible казав правду · Інфраструктура, описана в репозиторії · Побудувала всю базову інфраструктуру з нуля · Відповідала за розгортання платформи в Azure · Спрощена інфраструктура поза AWS · Вела 20 застосунків Docker у Google Cloud і AWS

{ Хмара, інфраструктура та DevOps }

Контейнеризація та оркестрація

Програма, що всюди працює однаково

Запакована так, що поводиться однаково на ноутбуці, на тестовому сервері й у продакшні, і масштабується, коли настає напружений тиждень.

Цю послугу застосовано в роботах, наведених деінде на цій сторінці:

Запустила контейнери на Podman і Quadlet · Посилила ізоляцію systemd для кожного юніта · Побудувала пайплайни CI/CD на GitHub Actions · Автоматизувала SSL/TLS для 100 застосунків Docker · Вела 20 застосунків Docker у Google Cloud і AWS

{ Хмара, інфраструктура та DevOps }

Надійність та моніторинг (SRE)

Дізнаватися раніше за клієнтів

Моніторинг і сповіщення, які попереджають, поки збій ще малий, і цифри, що показують, як часто так і залишається.

Змусила шість збирачів звітувати про пропущене

Змусила шість збирачів звітів повідомляти ту частину свого входу, яку вони так і не прочитали, — файли, що лишилися закритими, невстановлені зонди, нерозпізнані рядки журналу, — і підігнала пороги до 116 виміряних зразків, з'ясувавши, що сліпий збір і справний хост дають однакову сторінку.

Виміряла 13 адрес без трекінгу

Виміряла тринадцять адрес лише за власним журналом доступу вебсервера — без кукі, без трекерів і без сторонніх сервісів — маскуючи мережу клієнта в момент запису рядка та згортаючи результат у постійний архів із 21 денного показника та 20 місячних фасетів.

Обмежений потік подій у застосунку macOS

Обмежила буфери подій і журналювання після зафіксованого інциденту macOS зі зростанням на 41 МБ за секунду й 111 ГБ стиснених сторінок на машині з 36 ГБ; зафіксований повний тестовий запуск зменшив журнал ядра з 610 996 до 1 411 рядків.

Побудувала 7 ролей звітності лише для читання

Побудувала сім ролей звітності лише для читання, які описують робочий хост у Markdown — факти, доступ, git, метрики, трафік, безпека та інвентар провайдера, — за правилом: не виводиться жодне число, якого запуск не виміряв.

Довела, що блокування вторгнень працює щоразу

Довела працездатність усього ланцюжка блокування вторгнень під час кожного запуску посилення захисту: блокувала зарезервовану тестову адресу, зчитувала створене правило ядра й знімала блокування в гарантованому блоці очищення, тож jail, який перестав працювати, обриває запуск помилкою, а не звітує про справність.

Три замки на дверях, і жоден не замкнений

Знайшла й виправила три механізми захисту SSH від перебору паролів, які ніколи не працювали: jail блокування, що стежив за портом 22, тоді як демон слухав порт 1986; обмеження частоти, яке перекривало ширше правило, розташоване вище; і дію блокування, бінарний файл якої так і не знаходився, тож жодне блокування жодного разу не спрацювало.

Побудувала ліміти запитів і захист від зловживань

Побудувала засоби протидії зловживанням за принципом fail-closed — 22 обмежувачі частоти на Redis, Cloudflare Turnstile, ідемпотентність запитів та прив'язку до origin — щоб платформа відсікала ботів і напливи, а не довіряла тим, хто її викликає.

Перенесла повільні операції в чергу завдань River

Перенесла повільну роботу зі шляху запиту в чергу завдань River — 15 модулів воркерів, 8 запланованих задач та 20 завдань pg_cron — щоб запит повертався, поки робота за ним триває.

Побудувала інфраструктуру, що працює роками

Планувала та впроваджувала нову функціональність інфраструктури для внутрішніх і зовнішніх систем, створюючи рішення, достатньо довговічні, щоб працювати роками з мінімальними змінами.

Забезпечувала безперебійну передачу сигналів IPTV

Забезпечувала безперебійну передачу сигналів IPTV-стрімінгу між постачальниками та клієнтами, цілодобово відстежуючи та підтримуючи стрімінгову мережу й IP-телефонію.

Підтримувала 24/7 близько 1 000 серверів IPTV/OTT

Забезпечувала підтримку інфраструктури в режимі 24/7 для IPTV/OTT-стрімінгової платформи, адмініструючи ~1 000 серверів та системи клієнтів для глобальних замовників у Китаї, США та Німеччині.

Побудувала пошту з failover і журналом доставки

Побудувала електронну пошту як можливість платформи — три провайдери з резервним перемиканням, webhooks доставки, логування надсилання й доставки, шаблонізацію та кампанії — з перевіркою під час запуску, яка не дасть застосунку стартувати без жодного налаштованого поштового провайдера.

Картографічний продукт від початку до кінця

Спроєктувала, розробила й підтримувала інфраструктуру, обробку даних і картографічний застосунок протягом 2 років, охопивши розробку та операційне обслуговування.

Адмініструвала 40 вебсайтів на Apache і Nginx

Адмініструвала 40 вебсайтів на хостинг-серверах Ubuntu Linux з Apache та Nginx, забезпечивши високу доступність і продуктивність.

Підтримувала 10 серверів PostgreSQL і MS SQL

Спроєктувала, розгорнула та підтримувала 10 серверів PostgreSQL і MS SQL на Ubuntu Linux VPS, забезпечивши оптимальну продуктивність і надійність серверів.

Запустила перший дашборд спостережуваності

Розробила та запустила перший у компанії дашборд спостережуваності, що забезпечував аналітику продуктивності системи в реальному часі та візуалізацію даних на великому офісному телевізорі.

Цю послугу застосовано в роботах, наведених деінде на цій сторінці:

Розділила всі операційні секрети за хостами · Домоглася, щоб check mode в Ansible казав правду · Побудувала моніторинг хоста з dead man's switch · Автоматизація резервування з явним способом відновлення · Побудувала власні моніторинг помилок і трасування · Відповідала за розгортання платформи в Azure · Знизила операційні ризики з Grafana і Prometheus

{ Хмара, інфраструктура та DevOps }

Резервне копіювання та відновлення

Повернути все після поганого дня

Резервні копії, які перевірено, а не просто вважають робочими, і записаний план на той ранок, коли сервер не ввімкнеться.

Керувала 30 інстансами Ubuntu Linux VPS

Керувала 30 інстансами Ubuntu Linux VPS, впровадивши стратегії аварійного відновлення та забезпечивши оптимальні конфігурації мережі.

Цю послугу застосовано в роботах, наведених деінде на цій сторінці:

Розділила всі операційні секрети за хостами · Автоматизація резервування з явним способом відновлення · Налаштувала резервні копії та відновлення як код · Автоматизувала 100 критичних резервних копій

{ Хмара, інфраструктура та DevOps }

Системне адміністрування

Щоб усе просто працювало

Щоденний догляд за серверами, поштою, обліковими записами й оновленнями, щоб те, на що всі покладаються, працювало тихо й без сюрпризів.

Перевірила правила фаєрвола за позицією

Перевірила правила фаєрвола за позицією, а не лише за наявністю, зчитуючи пронумерований перелік правил і чинний ланцюжок фільтрації пакетів, бо наявне правило ще не означає, що до нього доходить хоч один пакет.

Впровадила корпоративний менеджер паролів

Інтегрувала загальнокорпоративну систему керування паролями, посиливши безпеку та оптимізувавши керування доступом.

Адмініструвала 100 серверів Bare Bone

Адмініструвала 100 серверів Bare Bone, фізичні мережі та системи IP-телефонії, забезпечивши надійну інфраструктуру для зростання компанії.

Налаштувала та встановила 1 000 Wi-Fi-роутерів

Налаштувала та встановила 1 000 Wi-Fi-роутерів, покращивши доступність і продуктивність мережі для клієнтів.

Адмініструвала мережеву інфраструктуру

Адмініструвала мережеву інфраструктуру для понад 1 000 серверів, забезпечивши оптимальне розгортання систем, безпеку та усунення несправностей.

Керувала 8 з'єднаннями WireGuard VPN та IPsec VPN

Керувала 8 з'єднаннями WireGuard VPN та IPsec VPN й усувала в них несправності, забезпечивши безпечний зв'язок між системами Google Cloud та Linux.

Керувала доступом у M365 і SSO

Запобігла порушенням безпеки, очоливши ініціативи з керування доступом, використовуючи M365, 1Password, Red Hat SSO та OKTA SSO.

Цю послугу застосовано в роботах, наведених деінде на цій сторінці:

Опублікувала читабельне onion-дзеркало в Tor ·

Змусила шість збирачів звітувати про пропущене ·

Перевірила CI-хук git-сервера, знайшла 2 дефекти · Ваш код на вашому власному сервері ·

Побудувала 7 ролей звітності лише для читання · Посилила ізоляцію systemd для кожного юніта · Описала зону DNS із 20 записів як код · Побудувала моніторинг хоста з dead man's switch ·

Автоматизація резервування з явним способом відновлення ·

Довела, що блокування вторгнень працює щоразу · Посилила SSH до 24 перевірених директив · Публічні служби на невеликому сервері · Інфраструктура, описана в репозиторії · Побудувала всю базову інфраструктуру з нуля · Побудувала інфраструктуру, що працює роками · Забезпечувала безперебійну передачу сигналів IPTV · Підтримувала 24/7 близько 1 000 серверів IPTV/OTT · Адмініструвала 40 вебсайтів на Apache і Nginx · Керувала 30 інстансами Ubuntu Linux VPS · Написала 1 000 правил RBAC для Linux-серверів · Підтримувала 10 серверів PostgreSQL і MS SQL

{ Хмара, інфраструктура та DevOps }

Налаштування мереж та VPN

З'єднати ваші офіси і ваших людей

Wi-Fi, фаєрволи і віддалений доступ налаштовані так, щоб працювати можна було звідусіль, а заходити — лише своїм.

Цю послугу застосовано в роботах, наведених деінде на цій сторінці:

Підготувала другий сервер із коду · Описала зону DNS із 20 записів як код · Перевірила правила фаєрвола за позицією · Три замки на дверях, і жоден не замкнений · Забезпечувала безперебійну передачу сигналів IPTV · Розгорнула інфраструктуру Azure як код · Адмініструвала 100 серверів Bare Bone · Налаштувала та встановила 1 000 Wi-Fi-роутерів · Адмініструвала мережеву інфраструктуру · Керувала 8 з'єднаннями WireGuard VPN та IPsec VPN · Керувала 30 інстансами Ubuntu Linux VPS

{ Хмара, інфраструктура та DevOps }

Безпека та керування доступом

Визначити, хто до чого має доступ

Облікові записи, паролі й права налаштовані так, щоб доступ відповідав роботі, а звільнені втрачали його того ж дня.

Записала правило меж після витоку облікових даних

Записала в репозиторій правило про межі його вмісту після того, як під час реструктуризації туди потрапили інвентар, дозволи фаєрвола та тексти іншої компанії, — і залишила відокремлений у карантин залишок під наглядом сканера секретів, а не виключила його.

Побудувала процес заявок на володіння компанією

Побудувала наскрізний процес заявок на володіння компанією — користувач заявляє права на компанію, адміністратор ухвалює рішення, а схвалення переписує граф авторизації, який визначає, кому що дозволено редагувати.

Доступ через Stripe та покупки в застосунку

Побудувала рівень платежів і прав доступу — Stripe поряд із внутрішньозастосунковими покупками Apple і Google — обмеживши каталог, пошук та експорт моделлю доступу з 11 таблиць, яку перевіряє сервер.

Посилила захист застосунку CSP на основі nonce

Посилила захист застосунку за допомогою CSP на основі nonce, HSTS, cookie SameSite, ролей бази даних за принципом найменших привілеїв та серверних повторних перевірок прав доступу.

Побудувала перемикання контексту організації

Спроєктувала систему перемикання контексту організації з клієнтським localStorage та серверним дзеркалюванням cookie, що дала змогу користувачам діяти від імені керованих організацій, забезпечуючи авторизацію за принципом найменших привілеїв.

Покращила комунікацію та співпрацю в команді

Покращила комунікацію та співпрацю в команді, впровадивши Slack, Mattermost, 1Password та Jira, заощадивши 8 000 людино-годин.

Цю послугу застосовано в роботах, наведених деінде на цій сторінці:

Опублікувала читабельне onion-дзеркало в Tor · Виміряла 13 адрес без трекінгу · Знайте ліцензію всього, що випускаєте · Задіяла невикористану половину ядра · Розділила всі операційні секрети за хостами · Підготувала другий сервер із коду · Запустила контейнери на Podman і Quadlet · Посилила ізоляцію systemd для кожного юніта · Описала зону DNS із 20 записів як код · Додала секундну попередню перевірку секретів · Перевірила правила фаєрвола за позицією · Довела, що блокування вторгнень працює щоразу · Посилила SSH до 24 перевірених директив · Три замки на дверях, і жоден не замкнений · Запровадила безперервне сканування безпеки ·

Побудувала ліміти запитів і захист від зловживань ·
Впровадила корпоративний менеджер паролів · Автоматизувала командну співпрацю ·
Розгорнула інфраструктуру Azure як код · Побудувала пошту з failover і журналом доставки ·
Автоматизувала SSL/TLS для 100 застосунків Docker · Адмініструвала мережеву інфраструктуру ·
Керувала 8 з'єднаннями WireGuard VPN та IPsec VPN · Керувала доступом у M365 і SSO ·
Написала 1 000 правил RBAC для Linux-серверів

{ Хмара, інфраструктура та DevOps }

Безпека ШІ-агентів

Щоб ШІ не чіпав того, чого не слід

Доступ кожного агента описано й обмежено необхідним,
кожну дію записано в журнал, якого агент не може змінити,
і кожен захист перевірено на ділі, а не взято на віру.

Цю послугу застосовано в роботах, наведених деінде на цій сторінці:

Розділила всі операційні секрети за хостами ·
Записала правило меж після витоку облікових даних ·
Додала секундну попередню перевірку секретів ·
Довела, що блокування вторгнень працює щоразу · Три замки на дверях, і жоден не замкнений ·
Запровадила безперервне сканування безпеки ·
Побудувала ліміти запитів і захист від зловживань · Керувала доступом у M365 і SSO ·
Написала 1 000 правил RBAC для Linux-серверів

Порівняйте початкові умови

Оберіть схожу роботу й визначте відмінності вашої ситуації.

Дивитися, скільки це коштує Зв'язатися з нами →

Обговоріть доречний підхід

Попросіть перетворити відповідний досвід на підхід, який ви зможете оцінити.

Переглянути наші послуги

welcome@engineer.company +45 50 10 61 84 Копенгаген, Данія

Візьміть цю сторінку із собою

Візитівка

Дбайливо зроблено з любов'ю — D.

CVR 45969703 · Tagensvej 105C, 3. th, 2200 København N

Авторське право © 2025 – дотепер · Engineer ApS · Усі права захищено.

Надруковано з https://platform.engineer.company/uk/portfolio/