Віртуальний аналітик з кібербезпеки

від CrowdStrike: зустрічайте Charlotte AI

CrowdStrike розробила віртуального «помічника», який підвищує ефективність кібербезпеки і дозволяє навіть недосвідченим фахівцям швидко реагувати на загрози.

В еру цифрової трансформації, коли кожен аспект нашого життя все більше залежить від Інтернет-підключення, питання кібербезпеки набуває критичної важливості. Світ постійно стикається з новими видами загроз, що можуть паралізувати цілі організації або навіть державну інфраструктуру. У цьому непередбачуваному середовищі інструменти кібербезпеки повинні постійно еволюціонувати, аби залишатися на крок попереду потенційних загроз.

Штучний інтелект (ШІ) відіграє дедалі більшу роль в індустрії кібербезпеки. Він використовується для автоматизації рутинного аналізу та виявлення загроз, а також для створення нових методів захисту від кібератак. За останні місяці кілька компаній, зокрема Microsoft і Google, включили помічників зі штучним інтелектом у свої платформи безпеки. Ці асистенти дають змогу аналітикам запитувати великі обсяги даних про безпеку, використовуючи живу мову, і встановлювати кореляції між різними джерелами даних.

На конференції Fal.Con 2023, яка нещодавно відбулася в Лас-Вегасі, компанія CrowdStrike представила **Charlotte AI** — передову генеративну модель штучного інтелекту, створену для ролі «віртуального аналітика з безпеки». Призначенням цієї технології є автоматизація завдань, що їх виконують аналітики операційних центрів безпеки (SOC), задля оптимізації їхнього робочого навантаження і підвищення ефективності.

Підхід до інновацій в стилі CrowdStrike

Компанія CrowdStrike була заснована з метою переосмислення підходів до кібербезпеки та завжди відзначалася своїм акцентом на інноваціях. Керуючись своєю місією — зупиняти порушення, — CrowdStrike розробляє продукти, які не просто відповідають сучасним викликам, але й здатні протистояти майбутнім загрозам. Ця філософія допомогла успішно створити низку революційних для галузі інструментів.

Основні технології й продукти CrowdStrike, такі як Falcon Prevent (антивірус нового покоління) та Falcon OverWatch (розвідка загроз), вже стали синонімами надійності та інноваційного підходу. Ці продукти з самого початку розроблялись з використанням технологій штучного інтелекту та автоматизації для проактивного виявлення загроз, що дозволяє CrowdStrike надавати комплексний аналіз безпеки та допомагати експертам швидко реагувати на інциденти.

Це прагнення до інновацій також відображається у відносинах компанії з клієнтами та партнерами. CrowdStrike працює з організаціями різних масштабів, від малого бізнесу до великих корпорацій, надаючи інструменти для захисту їхніх цифрових активів. Підхід CrowdStrike ґрунтується на поєднанні технічних знань з глибоким розумінням специфіки бізнесу кожного клієнта, що дозволяє надавати персоналізовані, інтелектуальні та продумані рішення.

CrowdStrike продовжує бути на передовій інновацій, випереджаючи виклики завтрашнього дня. З впровадженням Charlotte AI компанія знову підтвердила свою репутацію лідера, який формує майбутнє кібербезпеки.

Charlotte AI – новий рівень кібербезпеки

Charlotte AI — не просто черговий продукт у світі кібербезпеки; це втілення передових технологій та багатьох років експертного досвіду CrowdStrike.

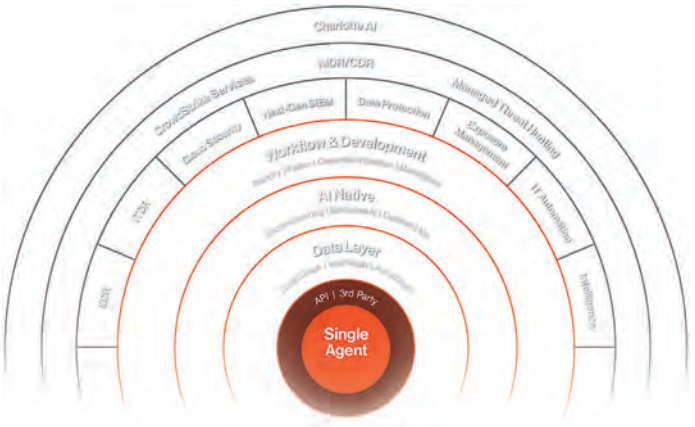

Рис. Структура платформи Crowdstrike Falcon. Charlote AI живиться даними з її компонентів

За словами Джорджа Курца, генерального директора CrowdStrike, *«ця технологія інтегрує колективний досвід, накопичений компанією за понад дванадцять років її існування, і містить знання про незліченні загрози й атаки, яким вдалося запобігти за цей час».*

Charlotte AI використовує найточніші у світі дані про безпеку, які включають трильйони подій, зафіксованих в CrowdStrike Threat Graph, телеметрію від різних користувачів, пристроїв, ідентифікаційних даних, хмарних робочих навантажень і провідну в галузі аналітику загроз від CrowdStrike.

Основою Charlotte AI є унікальний набір даних, підтверджений експертами CrowdStrike. «Вона» користується безперервним циклом зворотного зв'язку від фахівців CrowdStrike® Falcon OverWatch™ (полювання на загрози), CrowdStrike Falcon® Complete (кероване виявлення та реагування), CrowdStrike Services та CrowdStrike Intelligence (розвідка кіберзагроз). Цей величезний масив інтелектуальних даних, який використовується для зупинки порушень в реальному світі, є повністю унікальним: тільки CrowdStrike створює таку потужну комбінацію телеметрії безпеки, розвідки загроз і перевіреного людиною контенту в найпотужнішу інформаційну систему в кібербезпеці.

Це розумний аналітик з безпеки, який буде доступний для всіх користувачів платформи Falcon та допомагатиме їм краще розуміти загрози та ризики, з якими стикається їхня організація в повсякденній діяльності. Користувачі можуть ставити запитання англійською та десятками інших мов, отримуючи зрозумілі відповіді. Наприклад, Charlotte AI з легкістю відповість на запити на кшталт: *«Чи є у нас проблеми, пов'язані з Microsoft Outlook?»* або: *«Чи захищені ми від вразливості Log4j?»*.

Charlotte AI також дозволить менш досвідченим фахівцям з IT та безпеки швидше приймати правильні рішення, сприятиме автоматизації повторюваних завдань, таких як збір даних, вилучення та базовий пошук і виявлення загроз, а також спростить виконання складніших дій.

Моделі, на яких працюють чат-боти, ко-пілоти і робочі станції, що з'являються на ринку кібербезпеки, завжди будуть настільки хорошими, наскільки якісні дані вони використовують. Великі мовні моделі (LLM) побудовані таким чином, щоб використовувати знання з зовнішніх сховищ даних, а також дані, отримані за допомогою таких технологій, як платформа Falcon (**рис.**). CrowdStrike має найкращі і найточніші в галузі дані про безпеку і людський досвід для використання в LLM і для забезпечення роботи майбутнього генеративного ШІ у сфері безпеки.

Приклади реального застосування Charlotte AI

Демократизація кібербезпеки – кожен користувач стає експертом: завдяки Charlotte AI будь-хто — CISO, IT-директори, працівники служб підтримки IT, — можуть швидко отримати інформацію про профіль ризиків організації, зокрема про ландшафт загроз, рівень ризику, що його становлять критичні вразливості, поточну систему безпеки, відповідність нормативним вимогам, показники ефективності кібербезпеки та багато іншого.

Підвищення продуктивності аналітиків безпеки завдяки полюванню на загрози: Charlotte AI дозволить менш досвідченим IT-фахівцям і спеціалістам з безпеки швидше приймати кращі рішення, тим самим закриваючи прогалину в навичках і скорочуючи час реагування на критичні інциденти. Малодосвідчені члени команди тепер зможуть працювати з платформою CrowdStrike Falcon як більш просунуті аналітики SOC.

Посилення ефективності роботи фахівців з безпеки: Charlotte AI дозволяє найдосвідченішим фахівцям з безпеки автоматизувати повторювані завдання, такі як збір і вилучення даних, пошук і виявлення базових загроз, полегшуючи при цьому виконання більш складних дій. Також це прискорить використання XDR на рівні підприємства для кожної поверхні атаки, так само як і сторонніх продуктів безпосередньо з платформи CrowdStrike Falcon. Полювання на загрози та їх усунення у всій організації стане швидшим і простішим завдяки можливості робити запити рідною мовою.

Впровадження штучного інтелекту невпинно зростає, сьогодні кожен постачальник у галузі кіберзахисту вважає своїм обов'язком збільшувати використання ШІ-технологій у своїх рішеннях. Але, як і в будь-якій справі, важливо підходити до цього питання з відповідальністю та розумом, як це робить CrowdStrike. Місія компанії полягає не лише у відповіді на вже відомі загрози, але й у передбаченні нових викликів, а зусилля спрямовані на забезпечення цифрової безпеки на глобальному рівні. Ця мета зумовила створення технологій, які задають тренди галузі, та надихають на дослідження та розроблення рішень, які ще вчора здавалися фантастикою.