Захист облікових записів

з CrowdStrike Falcon Identity Protection

Модуль платформи CrowdStrike дозволяє запобігти кібератакам, які здійснюються з використанням вкрадених ідентифікаційних даних.

Кібератаки на облікові записи стають дедалі більш поширеними. Понад 80% кіберінцидентів відбуваються через зловмисне використання облікових даних для отримання доступу до корпоративних мереж. Нещодавня кібератака на одного з найбільших телекомунікаційних операторів країни показала, що навіть найпрогресивніші компанії не мають імунітету до кіберзагроз. А той факт, що кібератака відбулася через скомпрометований обліковий запис одного зі співробітників, підкреслює критичну важливість захисту облікових записів компаній.

Атаки з використанням ідентифікаційних даних часто важко виявити, особливо якщо зловмисник діє обережно. Традиційні системи безпеки можуть не помітити неавторизовану діяльність, коли вона мімікрує під звичну поведінку користувачів.

Водночас, Microsoft Active Directory (AD) стає все більш привабливою мішенню для зловмисників. Ця технологія з'єднує користувачів з кінцевими точками та надає доступ до систем, додатків і ресурсів. Вразливості AD стають все більшим ризиком для організацій через популярність використання облікових записів для атак.

Про це свідчать аналітичні дані: згідно зі звітом про глобальні загрози CrowdStrike за 2023 рік, у 80% атак використовуються викрадені ідентифікаційні дані, а кількість реклами послуг брокерів доступу на підпільних форумах у 2022 році підскочила на 112%.

З огляду на те, що зловмисники вдосконалюють свою тактику, засоби кіберзахисту також повинні розвиватися. Ефективний спосіб протистояти сучасним кіберзагрозам – рішення безпеки, орієнтоване на протидію зловмиснику. Такі рішення поєднують захист світового класу для кінцевих точок з захистом ідентифікаційних даних у режимі реального часу. Це дозволяє охопити всі аспекти інструментарію зловмисника – від експлуатації вразливостей та доставки шкідливого ПЗ до безфайлових атак і використання викрадених облікових даних.

Провідна у світі платформа для виявлення загроз та захисту облікових записів

CrowdStrike Falcon Identity Threat Protection, модуль платформи CrowdStrike Falcon, виявляє і зупиняє порушення, пов'язані з ідентифікаційними даними, в режимі реального часу в складному гібридному ландшафті облікових записів за допомогою єдиного агента і уніфікованого інтерфейсу загроз з кореляцією атак на кінцеві точки, робочі навантаження, облікові записи та дані.

Ось деякі з переваг використання CrowdStrike Identity Protection:

1. Інвентаризація та гігієна AD: CrowdStrike Identity Protection надає багату інформацію про облікові записи AD, зокрема про їхні привілеї, статус, паролі та інші атрибути. Це допомагає організаціям виявляти потенційні проблеми безпеки, такі як:

- приховані або надмірні привілеї;
- застарілі, приховані та загальні облікові записи;
- погано захищені облікові записи;
- користувачі з високим ризиком;
- користувачі, які найчастіше роблять помилки під час вході в систему;
- скомпрометовані паролі та паролі з необмеженим строком дії;
- відкриті паролі GPO;
- привілейовані користувачі, які мають некеровані кінцеві пристрої.

2. Ідентифікація та запобігання специфічним атакам: CrowdStrike Identity Protection використовує низку технологій для виявлення та зупинення специфічних методів кібератак, що включають *Kerberoasting*, *SharpHound*, *BloodHound*, а також різні тактики, зокрема *Pass the Ticket*, *Pass the Hash*, *Golden Ticket* тощо.

3. Виявлення аномалій в поведінці (UEBA): Falcon Identity Protection виконує аналіз поведінки користувачів на основі трафіку та шаблонів поведінки, виявляючи складні для ідентифікації загрози, такі як програми-здирники, латеральне переміщення, RDP в контролері домену (DC), інтерактивні входи в службові облікові записи та інші.

4. Умовний доступ: CrowdStrike Identity Protection дозволяє організаціям застосовувати політику умовного доступу до облікових записів AD. Це допомагає забезпечити, щоб користувачі мали доступ лише до тих ресурсів, які їм потрібні, і лише за певних умов.

Falcon Identity Protection – це просте та зрозуміле рішення, яке вимагає встановлення лише невибагливого агента на контролерах домену. Агенти CrowdStrike Falcon синхронізуються з CrowdStrike Security Cloud, забезпечуючи безперебійний обмін даними та виконання складних аналітичних завдань у хмарі, що знімає навантаження з локальних систем.

Пам'ятайте, що зловмисники не чекатимуть зручного для вас моменту, щоб розпочати свою атаку. Тому не зволікайте з захистом облікових записів. Протестуйте можливості Falcon Identity Threat Protection вже сьогодні, щоб вчасно зупинити витік ідентифікаційних даних та забезпечити надійний захист вашої корпоративної мережі.

Отримати детальну інформацію та протестувати функціонал рішень від **CrowdStrike** *ви можете у офіційного дистриб'ютора компанії на території України –* **iIT Distribution**

Контакти: +38 (044) 339 91 16; cs@iitd.io

Офіційний сайт: www.iitd.com.ua