SOLAR

Охотник за ботами: как UEBA помогает компаниям бороться с ботнетами и DDoS

Артём Избаенков

Заместитель директора по продуктовому развитию ГК "Солар"

Член правления АРСИБ

Член РОЦИТ

SOLAR

Почему это важно?

1. Ботнеты - серьезная опасность.
2. Обнаружение критично важно.
3. Организации с множеством пользователей под угрозой.
4. Раннее обнаружение - ключевой момент.
5. Необходим всесторонний подход.

SOLAR

Что такое боты и как они вредят вашему бизнесу?

Хорошие боты

Автоматизируют рутинную работу, разные бизнес-процессы, применяются в поисковых системах, инструментах аналитики.

Плохие боты

Создаются злоумышленниками из взломанных устройств, используются для разных кибератак.

Бот – программа, которая автоматически выполняет заданные действия.

Создать вредоносный ботнет из тысяч и миллионов взломанных устройств становится всё легче из-за растущего количества IoT-устройств с плохой защитой.

Самые распространённые бот-атаки

DoS- и DDoS-атаки

Боты генерируют огромное количество запросов, чтобы сделать ресурсы недоступными.

Поиск уязвимостей

С помощью ботов злоумышленники ищут уязвимости приложений и эксплуатируют zero-day уязвимости.

Кардинг

Боты могут использовать украденные данные карт, чтобы покупать товары без участия владельцев карт.

Брутфорс

Боты взламывают аккаунты с помощью автоматического перебора паролей.

Рекламный фрод

Боты могут кликать на платную рекламу. В итоге компания платит за трафик, который не конвертируется в покупки, ухудшаются позиции сайта в поисковой выдаче.

Искажённая аналитика

Бот-трафик искажает реальную картину поведения пользователей. Компании не получают достоверных данных и не могут оптимизировать конверсии.

Скрейпинг

Боты собирают данные с сайтов и могут, например, передать их конкурентам или использовать для спам-рассылок и т.п.

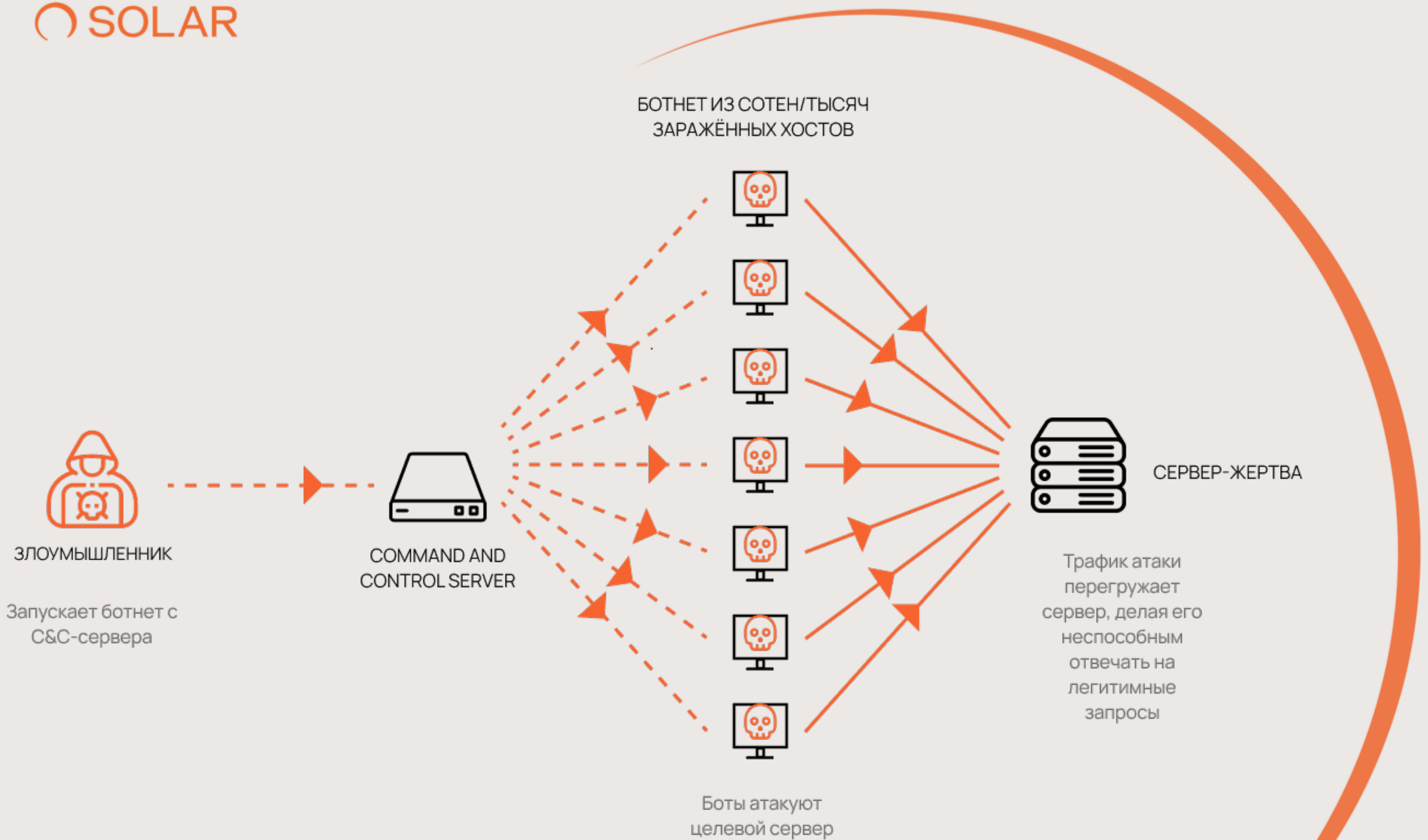
Скальперские покупки

Злоумышленники автоматически скупают ограниченный товар, чтобы перепродать его дороже.

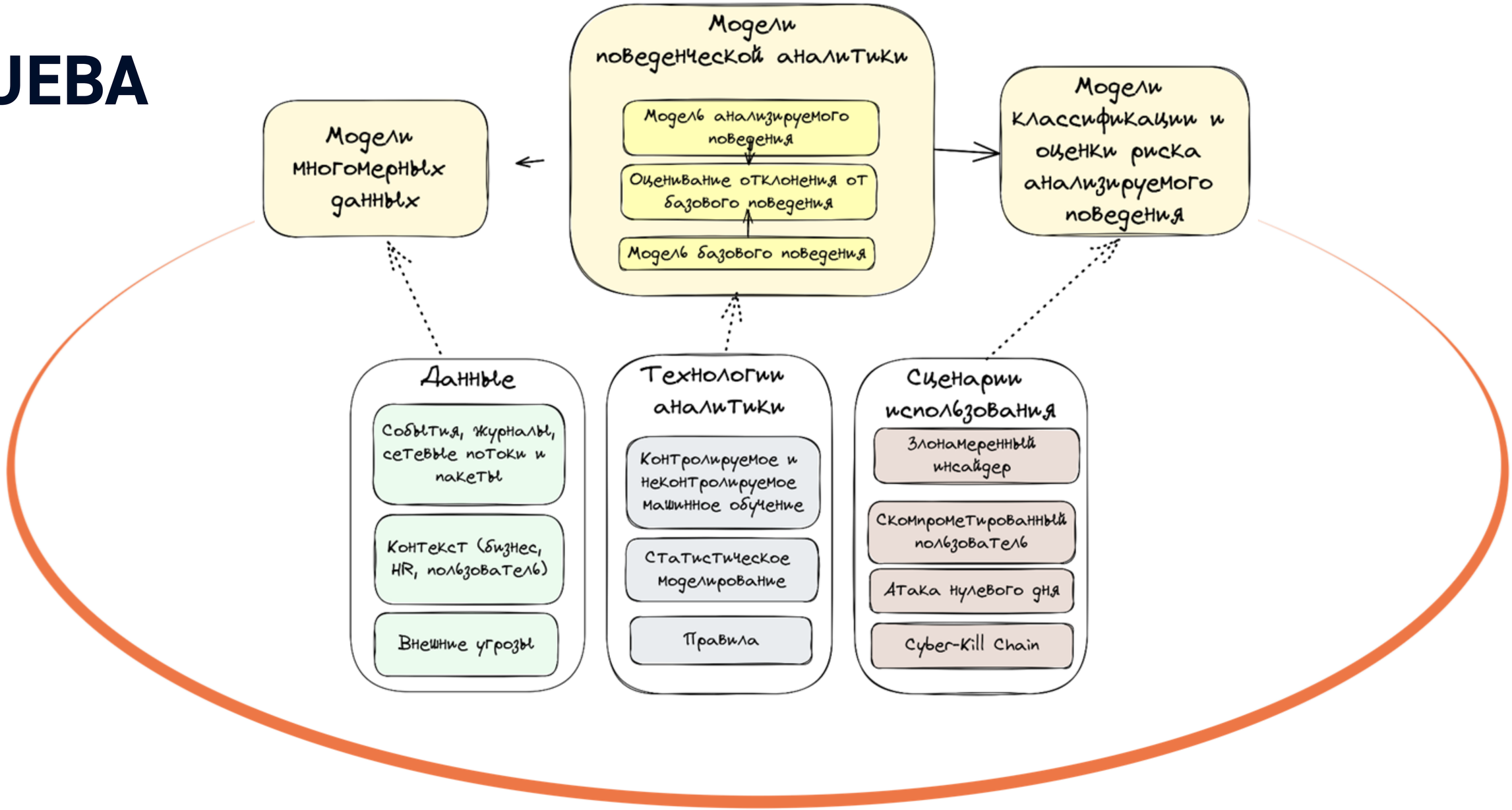
Исчерпание товаров (Denial of Inventory)

Товары: например, заполнить корзины или забронировать весь товар. Реальные пользователи не смогут его купить, но товар так и не будет продан.

SOLAR


БОТНЕТ ИЗ СОТЕН/ТЫСЯЧ ЗАРАЖЁННЫХ ХОСТОВ
ЗЛОУМЫШЛЕННИК
Запускает ботнет с C&C-сервера
COMMAND AND CONTROL SERVER
Боты атакуют целевой сервер
СЕРВЕР-ЖЕРТВА
Трафик атаки перегружает сервер, делая его неспособным отвечать на легитимные запросы

UEBA


Модели поведенческой аналитики
Модель анализируемого поведения
Оценивание отклонения от базового поведения
Модель базового поведения
Модели многомерных данных
Модели классификации и оценки риска анализируемого поведения
Данные
События, журналы, сетевые потоки и пакеты
Контекст (бизнес, HR, пользователь)
Внешние угрозы
Технологии аналитики
Контролируемое и неконтролируемое машинное обучение
Статистическое моделирование
Правила
Сценарии использования
Злонамеренный инсайдер
Скомпрометированный пользователь
Атака нулевого дня
Cyber-Kill Chain

Инцидент 1

Федеральный оператор связи

Проблема: Крупный оператор связи столкнулся с серией DDoS атак, которые вызывали недоступность сети для абонентов. Атаки происходили периодически и имели различные формы, что затрудняло их обнаружение и предотвращение. Команда безопасности оператора была в затруднительном положении из-за необходимости оперативно реагировать на атаки и защищать инфраструктуру от новых угроз.

Результаты: В ходе мониторинга система UEBA обнаружила аномалии в поведении некоторых устройств внутри инфраструктуры оператора связи. Анализ данных показал, что эти устройства были заражены вредоносным программным обеспечением и использовались для участия в DDoS ботнете. Благодаря обнаружению ботнета с помощью UEBA, команда безопасности оператора смогла принять меры по изоляции зараженных устройств, блокировке вредоносного трафика и предотвращению дальнейших атак.

Инцидент 2

Финансовый брокер

Проблема: Крупный банк с региональными офисами столкнулся с серией DDoS атак, которые приводили к недоступности онлайн-банкинга и сервисов для клиентов. Атаки были направлены как на центральный офис, так и на региональные филиалы, что сильно затрудняло управление и реагирование на угрозу.

Результаты: Система UEBA обнаружила необычные паттерны трафика и поведения в сети банка, характерные для DDoS атак. Анализ данных выявил, что региональные офисы были использованы для распространения вредоносных программ и участия в ботнете, направленном на атаку на центральный офис банка. Благодаря обнаружению атаки с помощью UEBA, банк смог оперативно принять меры по блокировке вредоносного трафика и защите своей инфраструктуры.

Инцидент 3

Розничная сеть супермаркетов

Проблема: Крупная розничная сеть супермаркетов столкнулась с серией DDoS атак, которые вызывали недоступность онлайн-магазина и систем управления запасами. Атаки были направлены на серверы, обрабатывающие онлайн-заказы и данные о товарах, что приводило к простоям в работе и ущербу бизнесу.

Результаты: Система UEBA обнаружила аномалии в поведении клиентов и необычные паттерны трафика, характерные для DDoS атак. Анализ данных выявил, что атаки были организованы через ботнеты, использующие уязвимости в онлайн-магазине. Благодаря UEBA, супермаркеты смогли своевременно заблокировать атаки и предпринять меры по усилению защиты.

SOLAR

Артём Избаенков

Заместитель директора по продуктовому развитию ГК "Солар"

Член правления АРСИБ

Член РОЦИТ