



UserGate

uFactor

Продукты, сервисы и услуги
в области обеспечения
информационной безопасности



- Иммуниетет продуктов экосистемы UserGate
- SOC as a Service
- Аудит и консалтинг

uFactor



Защита ИТ-инфраструктуры и обеспечение информационной безопасности —

обязательная часть бизнес-стратегии любой компании. Чтобы самостоятельно решить эту задачу в условиях кадрового дефицита и постоянно усложняющегося ландшафта киберугроз, потребуются масштабные временные, финансовые и человеческие ресурсы.

UserGate —

одна из ведущих компаний на российском рынке информационной безопасности — аккумулирует глубокую экспертизу в области киберзащиты и предлагает набор эффективных продуктов, сервисов и услуг для обеспечения устойчивости критически важных бизнес-процессов и предотвращения киберинцидентов.

uFactor —

специализированное подразделение высококвалифицированных экспертов UserGate, которые в режиме 24/7 ищут, исследуют и нейтрализуют актуальные киберугрозы.



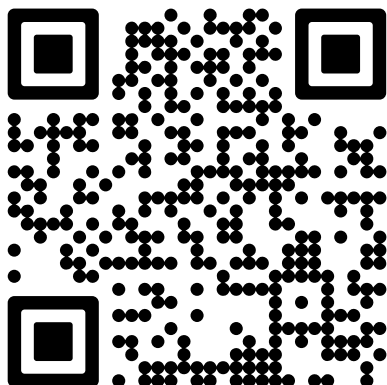
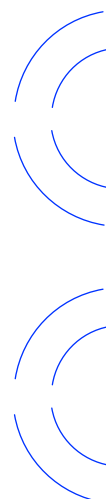
uFactor предоставляет широкий спектр услуг

по выстраиванию архитектуры и процессов информационной безопасности: от SOC as a Service до анализа вредоносного кода. Помимо оказания услуг в области ИБ, uFactor непрерывно повышает экспертизу решений UserGate, помогая разработчикам интегрировать в продукты средства защиты от актуальных угроз.

Сотрудничество с uFactor обеспечит гибкий подход к ИБ и позволит выстроить надежную систему цифровой защиты с учетом особенностей вашей инфраструктуры и потребностей бизнеса.

Векторы работы uFactor:

- Иммунитет продуктов экосистемы UserGate
- SOC as a Service
- Аудит и консалтинг по информационной безопасности



Новости
uFactor
об актуальных
угрозах
и уязвимостях

Иммунитет продуктов экосистемы UserGate

Специалисты uFactor помогают разработчикам компании UserGate реализовывать механизмы защиты в продуктовой линейке, насыщая экспертизой экосистему решений UserGate.

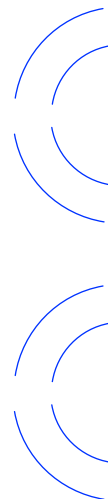
Команда uFactor анализирует информацию из различных источников:

- Полученных экземпляров вредоносного ПО
- Публичных и собственных honeypots
- Российских (FinCERT, GovCERT и др.) и международных баз уязвимостей
- Данных, полученных от партнеров и пользователей
- Публикаций и выступлений исследователей информационной безопасности

Непрерывный мониторинг и исследование киберсферы позволяют uFactor эффективно защищать информационные ресурсы, реализуя широкий спектр действий.

Среди них:

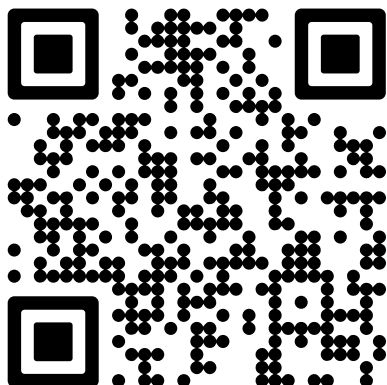
- Выработка механизмов противодействия злоумышленникам
- Внедрение технологий поведенческого анализа
- Разработка и обновление сигнатур
- Создание правил корреляции



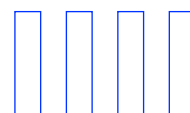
Ценность поддержания иммунитета продуктов UserGate для бизнеса:



- Постоянное увеличение защищенности продуктов экосистемы UserGate и предотвращение актуальных угроз информационной безопасности (при наличии у заказчика действующих подписок)



Подробнее
о моделях
лицензирования



uFactor

SOC as a Service

Security Operations Center as a Service (SOC как услуга, SOCaaS) —

это сервис круглосуточного мониторинга, анализа и защиты ИТ-инфраструктуры от киберугроз. SOC as a Service не требует развертывания и поддержки собственной инфраструктуры. Вместо этого используется внешний поставщик услуг для непрерывного отслеживания и реагирования на инциденты безопасности.

Специалисты SOCaaS UserGate при помощи современных инструментов ИБ предоставляют клиентам проактивную защиту и экспертизу для обнаружения и предотвращения киберугроз.

Доверяя управление событиями информационной безопасности SOCaaS UserGate, вы получаете возможность выявлять инциденты, отражать атаки на ранних стадиях, а также использовать профессиональные рекомендации, позволяющие не допустить повторения инцидентов в будущем.

Ценность SOCaaS UserGate для бизнеса:

- Выявление до 100% инцидентов любой сложности
- Экономия до 90% затрат по сравнению с формированием собственной команды
- Оповещение об инцидентах в течение нескольких минут
- Перевод расходов из CAPEX в OPEX
- Быстрое подключение услуги
- Гибкий подход к потребностям вашего бизнеса
- Работа с инфраструктурой любого размера и нетиповыми источниками событий

Что входит в услуги SOCaaS UserGate:

- Круглосуточный мониторинг и регистрация инцидентов
- Подключение и настройка источников событий
- Разработка и настройка правил выявления инцидентов
- Выработка мер реагирования и координация действий команды
- Формирование оперативной отчетности
- Анализ инцидентов и создание рекомендаций по их недопущению в будущем



uFactor

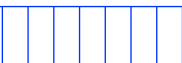


Аудит информационной безопасности и консалтинг от uFactor

Доверьте опытным специалистам uFactor организацию и сопровождение процессов информационной безопасности вашего бизнеса.

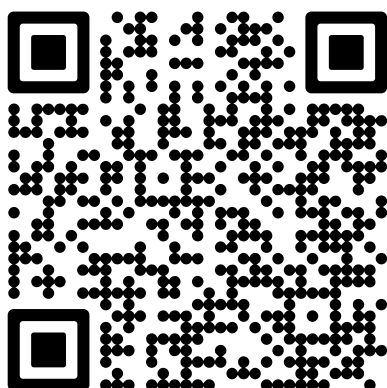
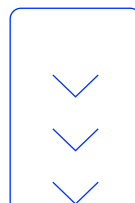
Мы поможем реализовать структурный подход к обеспечению конфиденциальности, целостности и доступности информации, найти и устранить уязвимости ИТ-инфраструктуры и процессов ИБ в компании, защитить бизнес от простоя, финансовых и репутационных потерь.

Используя консалтинг от uFactor, вы сможете комплексно повысить уровень защищенности вашей компании — провести аудит ИБ, улучшить уровень осведомленности сотрудников и оптимизировать ресурсы, затрачиваемые на ИБ.

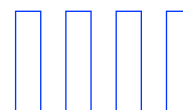


Арсенал услуг uFactor:

- Анализ защищенности
- Разработка архитектуры и процессов ИБ
- Расследование инцидентов
- Анализ вредоносного кода
- Virtual CISO



Подробнее
об услугах



Анализ защищенности

Сканирование уязвимостей в инфраструктуре заказчика

Сканирование уязвимостей — один из необходимых шагов для построения полноценного процесса Vulnerability Management (VM) в компании. Частота проведения сканирования напрямую влияет на актуальность и полноту знаний о потенциальных рисках в ваших информационных системах. Оценка уязвимостей и риск-менеджмент позволяют осознанно подойти к выбору стратегии информационной безопасности и предотвратить атаки злоумышленников.

Ценность услуги для бизнеса:

- выявление недостатков в защите инфраструктуры компании и предотвращение инцидентов
- предоставление рекомендаций по устранению уязвимостей

Контроль защищенности

Для поддержания киберустойчивости компании необходим регулярный аудит ИТ-архитектуры и инфраструктуры. Это позволяет оценить корректность построения процессов с учетом требований ИБ и принять необходимые технические и организационные меры для обеспечения эффективной защиты ресурсов и соответствия требованиям регуляторов.

Ценность услуги для бизнеса:

- интеграция отсутствующих процессов ИБ и улучшение действующих
- построение или актуализация модели угроз, создание реестра активов
- корректная настройка используемых в компании средств защиты информации
- определение актуальной модели угроз и предоставление рекомендаций по внедрению необходимых классов решений для более полной защиты информационных систем

Поиск признаков компрометации

Поиск признаков компрометации дает возможность обнаружить злоумышленника в инфраструктуре до того, как он нанесет ущерб компании. Заблаговременное выявление нелегитимных пользователей или процессов в информационных системах позволяет предотвратить серьезные инциденты и минимизировать риски.

Ценность услуги для бизнеса:

- обнаружение действий злоумышленника на ранней стадии атаки
- возможность принять превентивные меры и устранить угрозу



Разработка архитектуры и процессов ИБ

С ростом бизнеса масштабируются информационные системы компании и усложняются внутренние процессы. Это приводит к появлению новых уязвимостей в ИТ-инфраструктуре и высоким рискам потери данных.

Комплексная оценка построения инфраструктуры и уровня ИБ, проведенная командой uFactor, позволит актуализировать данные об информационных активах компании и применимых к ним угрозах.

По результатам аудита и выявленных рисков предоставляются рекомендации по корректировке текущих бизнес-процессов, изменению архитектуры ИТ и ИБ, а также процессов резервного копирования и аварийного восстановления.

Ценность услуги для бизнеса:

- комплексная оценка процессов и архитектуры в соответствии с требованиями стандартов и best practices
- актуализация активов и построение модели угроз
- встраивание процессов информационной безопасности в текущую деятельность компании
- применение лучших практик по резервному копированию и аварийному восстановлению
- выработка мер по устранению уязвимостей

Расследование инцидентов

Инцидент информационной безопасности — это событие, которое может нарушить целостность и доступность данных и привести к утечке конфиденциальной информации.

Последствия инцидента грозят серьезными финансовыми рисками и оборотными штрафами для компании.

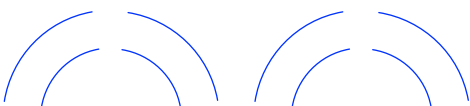
Чтобы минимизировать риск повторения инцидента, необходимо проанализировать, какие события к нему привели и какие активы компании были затронуты.

При расследовании инцидента команда uFactor:

- соберет все необходимые данные, связанные с инцидентом
- определит, завершена атака или еще продолжается
- изучит произошедшие события
- проанализирует скомпрометированные активы
- предоставит рекомендации по устранению уязвимостей, которые привели к инциденту

Ценность услуги для бизнеса:

- минимизация рисков информационной безопасности
- предотвращение повторения инцидентов



Анализ вредоносного кода

Внедрение и активация вредоносного программного обеспечения — один из наиболее популярных видов атак злоумышленников.

Антивирусные программы не гарантируют стопроцентную защиту от заражения информационных систем. Чтобы понять, как работает потенциально опасное ПО, требуется провести реверс-инжиниринг.

Команда uFactor реконструирует логику вредоноса и проанализирует его жизненный цикл и возможные последствия.

Ценность услуги для бизнеса:

- локализация и устранение последствий действия вредоносного ПО

Virtual CISO

Ежегодно дефицит кадров в области информационной безопасности увеличивается на несколько десятков тысяч человек. С нехваткой квалифицированных специалистов сталкивается большинство российских компаний, а поиск опытного директора по информационной безопасности (CISO) в среднем занимает от 6 месяцев до года.

При этом большинство претендентов, выбирая новое место работы, отдадут предпочтение организациям со сложной инфраструктурой, в которых они смогут столкнуться с новыми профессиональными вызовами.

Быстро решить кадровую проблему поможет привлечение vCISO — эксперта топ-уровня из команды uFactor.

Его основная задача — формирование стратегии ИБ и построение комплексной системы защиты инфраструктуры вашего бизнеса вне зависимости от ее размера и индивидуальных особенностей.

vCISO uFactor имеют реальный опыт построения процессов информационной безопасности, в том числе с нуля. Они разработают оптимальный план внедрения процессов ИБ и помогут грамотно реализовать его внутри инфраструктуры.

Схемы привлечения vCISO uFactor:

- консультации с экспертами топ-уровня — помогут свериться с заданным курсом ИБ в компании
- выделенный сотрудник с ролью директора по ИБ — vCISO непрерывно на связи с внутренней командой в качестве руководителя
- управление внутренней ИБ-командой и процессами на постоянной основе — погружение во все процессы и нюансы вашего бизнеса и обеспечение эффективной защиты от угроз.

Ценность услуги для бизнеса:

- преодоление кадрового дефицита в компании
- гибкий подход к потребностям бизнеса

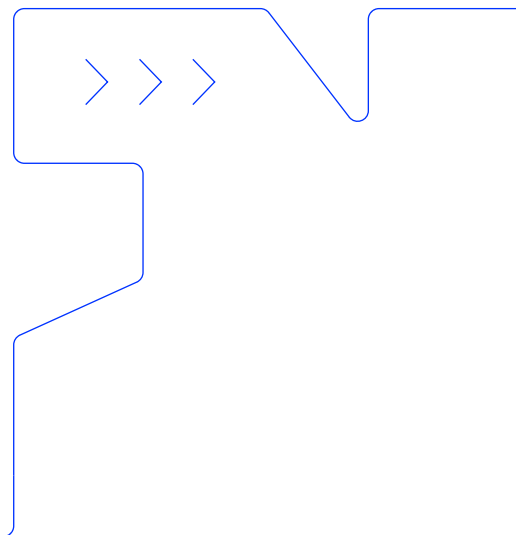
Как начать работать с uFactor

- Шаг 1** Отправьте письмо с запросом требуемой услуги на sales@usergate.com и получите опросный лист
- Шаг 2** Заполните и передайте опросный лист вашему менеджеру в UserGate
- Шаг 3** При необходимости ответьте на уточняющие вопросы от команды uFactor
- Шаг 4** Встретьтесь с командой uFactor в онлайн-формате для определения ваших потребностей и условий реализации проекта
- Шаг 5** Согласуйте техническое задание
- Шаг 6** Получите коммерческое предложение
- Шаг 7** Заключите договор и получите услугу

Запрос на SOCaas



Запрос на услуги ИБ



Контактная информация:

Телефон: 8 800 500-40-32
Клиентам: sales@usergate.com
Партнерам: partner@usergate.com
Маркетинг: marketing@usergate.com

Полезные ресурсы UserGate:



© ООО «Юзергейт», 2026.
Все права защищены