INNOSTAGE

ЦЕНТР РАЗРАБОТОК

Ваш проводник на пути к киберустойчивости

INNOSTAGE ЦЕНТР РАЗРАБОТОК

Разработчик продуктов, решений и сервисов по управлению цифровыми рисками

Наша цель – обеспечение киберустойчивости наших клиентов

В нашем фокусе комплексная защита, охватывающая все ключевые сегменты: от физической безопасности до надежной охраны цифровых данных и инфраструктуры

Наш портфель технологических решений позволяет не только выявлять потенциальные угрозы, но и активно предотвращать их, не давая развиться в серьёзные инциденты, способные нанести вред вашему бизнесу

ПРИНЦИПЫ

Мы ориентированы на сотрудничество с компаниями, которые стремятся занять лидирующие позиции на рынке, ценят глубокую специализацию и экспертный подход в обеспечении безопасности своих данных и процессов

Innostage Центр Разработок активно работает с ведущими секторами экономики, в том числе с КИИ, АСУ ТП, ТЭК / Энергетикой, Финансовым сектором и Государственными организациями

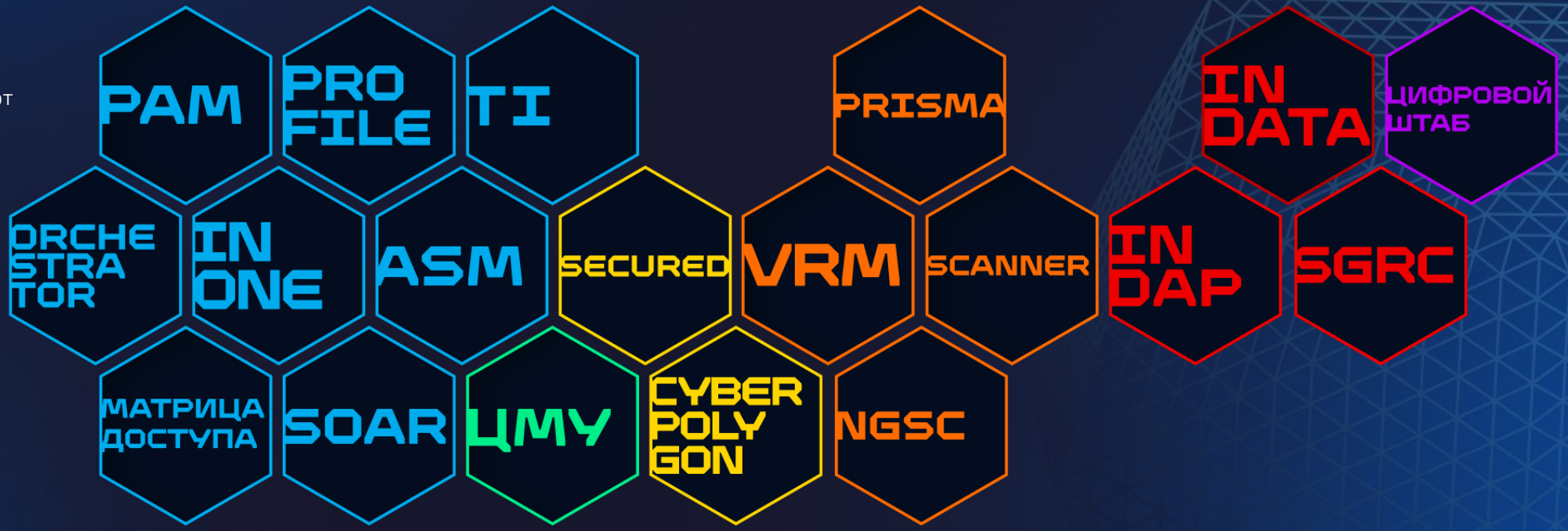
Мы открыты для работы с компаниями из любых сфер деятельности и готовы предложить решения, которые будут соответствовать уникальным потребностям каждой отрасли

INNOSTAGE

ПРОДУКТОВЫЙ ПОРТФЕЛЬ

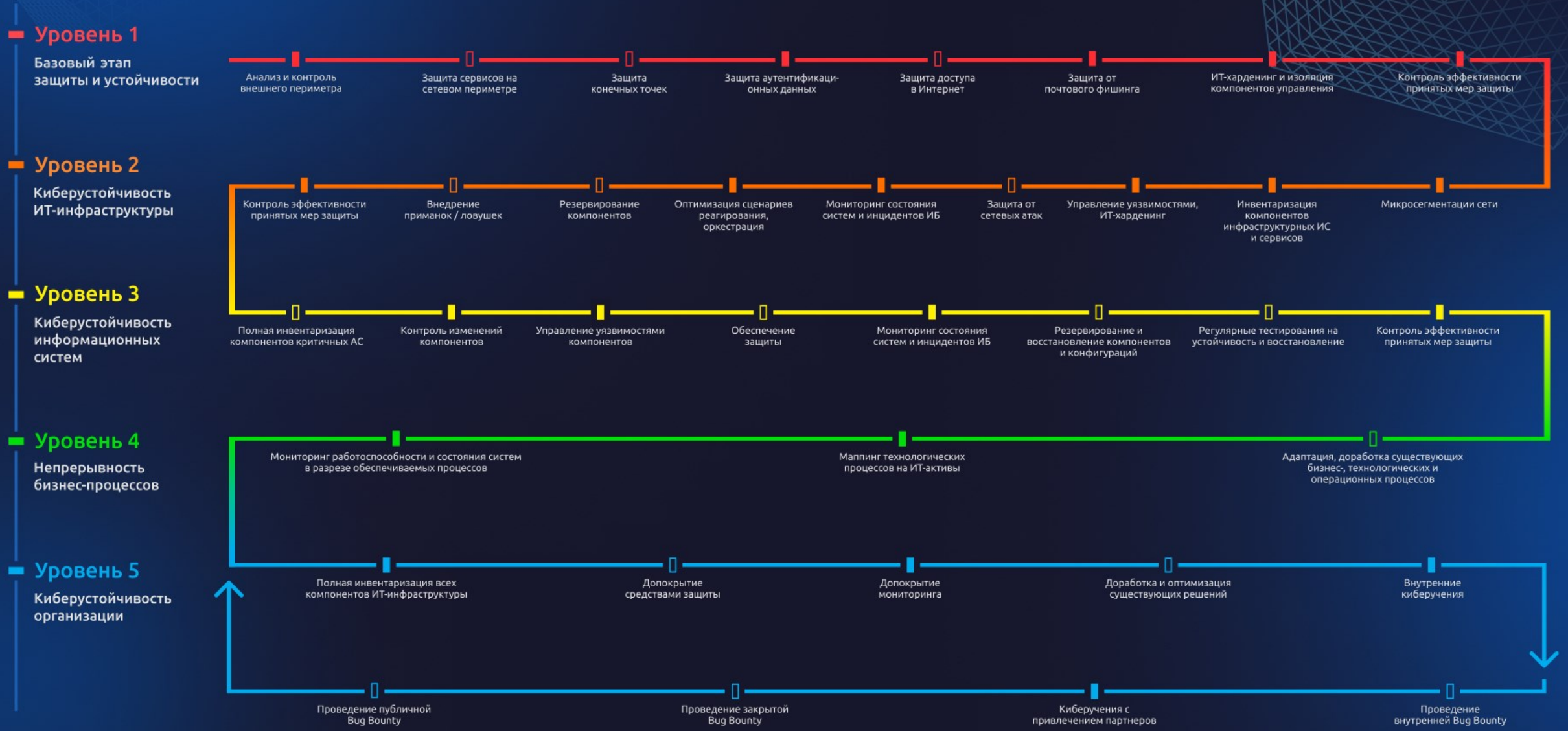
Мы объединяем новейшие разработки в сфере информационных технологий и передовые подходы в области защиты корпоративных данных, чтобы помочь вашему бизнесу эффективно расти в защищенной среде

- ИБ
- ИБ: документооборот
- ИБ: обучение
- ИТ для ИБ
- Решения
- ФизБез



INNOSTAGE

ФРЕЙМВОРК



НАПРАВЛЕНИЯ

Используя многолетнюю экспертизу Innostage, мы оптимизируем ИТ-инфраструктуру и обеспечиваем полный цикл защиты организации за счет комплекса сервисов и продуктов компании

Распознавание угроз

Отслеживание и выявление угроз, анализ полученных данных и разработка комплекса мер по предотвращению повторных атак

Оптимизация процессов

Повышение эффективности и продуктивности бизнес-процессов, повышение защищенности инфраструктуры

Противодействие кибератакам

Обеспечение комплекса мер: защита внутренних ресурсов компании, сетевого контура и повышение устойчивости систем

Теория и практика кибербезопасности

Повышение осведомленности для рядовых сотрудников и специалистов ИБ, обучение на базе реального «красного» трафика

INNOSTAGE

РАСПОЗНАВАНИЕ УГРОЗ

01 Мониторинг и реагирование на инциденты кибербезопасности

Ускорение времени реагирования на инциденты

02 Кибераналитика и киберразведка

Возможность превентивного реагирования на угрозы

03 Сетевая аналитика

Увеличение эффективности обнаружения сетевых атак

04 Разработка аналитического контента

Увеличение эффективности выявления кибератаки

INNOSTAGE

ПРОТИВОДЕЙСТВИЕ КИБЕРАТАКАМ

01 **Защита от фишинговых атак**
Повышение устойчивости систем к фишинговым атакам

02 **Защита внешнего сетевого периметра**
Контролируемый и безопасный внешний сетевой периметр

03 **Защищенный удаленный доступ**
Повышение безопасности удаленного подключения на 50%

04 **Сервис противодействия DDoS-атакам**
Обеспечение бесперебойной работы сетевой инфраструктуры

INNOSTAGE

ОПТИМИЗАЦИЯ ПРОЦЕССОВ

01 Защита конфиденциальных данных

Снижение риска утечки и защита чувствительной информации

02 WEB-аналитика
(на базе решений класса WAF)

Повышение защищенности веб-ресурсов

03 Администрирование и эксплуатация компонентов SOC

Оптимизация ресурсов и повышение продуктивности в процессах работы

04 Защита критичных информационных систем

Снижение рисков успешных атак на КИС

INNOSTAGE

ТЕОРИЯ И ПРАКТИКА КИБЕРБЕЗОПАСНОСТИ

01 Purple Teaming
Итеративный подход к эффективному и быстрому повышению уровня защищенности

02 Повышение осведомленности
Для не-технических специалистов: уменьшение вероятности атаки через человеческий фактор

03 Технико-тактическая программа
Повышение уровня компетенции инженеров: оперативное реагирование и принципы работы СЗИ

04 Белые хакеры: точка входа
Подготовка этичных хакеров из начинающих специалистов

05 Кибербитва
Интерактивная тренировка ИБ-команд в модуляции реальных условий

КАК ЭТО РАБОТАЕТ

1. Определяем текущий уровень киберустойчивости
2. Выделяем уязвимости и точки роста для развития ИБ инфраструктуры компании
3. Предоставляем перечень понятных и простых шагов к обеспечению киберустойчивости
4. Фокусируемся на максимально эффективном использовании уже имеющихся инструментов и защитных механизмов
5. Формируем перечень дополнительных мер защиты, необходимых компании
6. Внедряем сервисы и продукты

ПУТЬ К КИБЕРУСТОЙЧИВОСТИ ПРОЙДЕН НАШЕЙ КОМПАНИЕЙ ОТ НАЧАЛА ДО КОНЦА, БЛАГОДАРЯ ЧЕМУ МЫ УВЕРЕНЫ В ЭФФЕКТИВНОСТИ И РАБОТОСПОСОБНОСТИ НАШЕЙ МЕТОДОЛОГИИ

РЕЗУЛЬТАТ РАБОТЫ

Innostage не только поставляет сервисы, услуги и продукты, но и на своем опыте доказывает их эффективность

30% → 2%

Сокращение эффективных фишинговых атак

15 МИНУТ → ∞ МИНУТ

Увеличение времени захвата домена: пытаться захватить контроль над инфраструктурой можно бесконечно долго

~В 5 РАЗ

Сокращение времени реагирования на угрозы

0% ШАНС

Остаться незамеченным при реализации недопустимых событий

BUG BOUNTY – СМЕЛЫЙ ШАГ ДЛЯ ЛЮБОЙ КОМПАНИИ. МЫ ВЫШЛИ НА ПУБЛИЧНОЕ ТЕСТИРОВАНИЕ, НЕ СОМНЕВАЯСЬ В СВОЕЙ ЗАЩИЩЕННОСТИ.
В ОСНОВЕ НАШЕЙ БЕЗОПАСНОСТИ ЛЕЖАТ НАШИ СОБСТВЕННЫЕ СЕРВИСЫ И ПРОДУКТЫ