ГАРДА

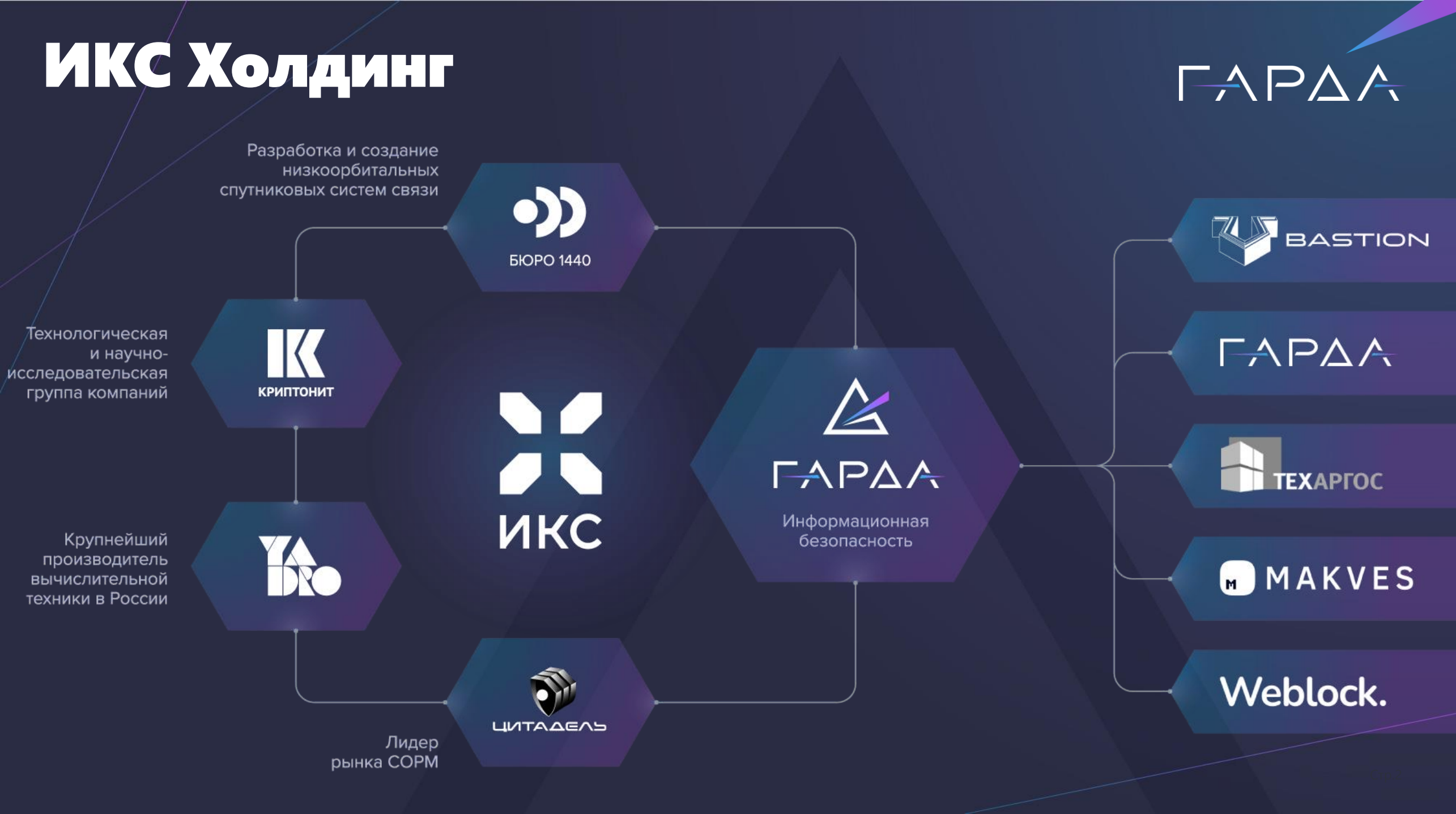
14 стратегий кибербезопасности Data Lake:

от периметра до ядра

Денис Батранков

Директор по продуктам информационной безопасности ИКС Холдинг, bdv@x-holding.ru

ИКС Холдинг


ГАРДА
Разработка и создание низкоорбитальных спутниковых систем связи
БЮРО 1440
Технологическая и научно-исследовательская группа компаний
КРИПТОНИТ
ИКС
Крупнейший производитель вычислительной техники в России
YADRO
ЦИТАДЕЛЬ
Лидер рынка СОРМ
ГАРДА
Информационная безопасность
BASTION
ГАРДА
ТЕХАРГОС
MAKVES
Weblock.

ГАРДА

- 50% всего российского интернета защищены Гарда Anti-DDoS
- Отраслевой стандарт в защите баз данных
- Полностью российские решения

400+ клиентов

5 офисов в городах России

700+ сотрудников

20+ продуктов

- Безопасность **данных**
- Безопасность **сети**
- Безопасность **рабочих станций**
- Безопасность **экономическая**

Комплексная стратегия защиты Data Lake:

От шифрования до непрерывной оценки безопасности

ГАРДА

Передовые методы шифрования данных в Data Lake

- Непроницаемая защита покоящихся данных: Технология At-rest encryption
- Безопасность в движении: In-transit encryption и протоколы SSL/TLS

Инновационные подходы к контролю доступа в экосистеме Data Lake

- RBAC: Революция в управлении доступом на основе ролей
- ABAC: Новый уровень гибкости в контроле доступа к данным
- MFA: Многофакторная аутентификация как щит от несанкционированного доступа

Передовые технологии мониторинга и обнаружения угроз для Data Lake

- NDR: Интеллектуальное обнаружение сетевых аномалий
- SIEM: Комплексный анализ событий безопасности в реальном времени
- PAM: Контроль привилегированного доступа

DAM и DLP: Стражи целостности данных в Data Lake

- DAM: Всевидящее око мониторинга доступа к данным
- DLP: Предотвращение утечек данных на новом уровне

Tokenization и Masking: Искусство сокрытия данных в Data Lake

- Tokenization: Трансформация конфиденциальных данных в безопасные токены
- Data Masking: Маскировка данных для безопасного использования

Соответствие нормативам и аудит в мире Data Lake

- Compliance: Навигация в море регуляторных требований
- Аудит: Прозрачность и контроль каждой операции с данными

Сегментация сети: Архитектура безопасности Data Lake

- Зоны безопасности: Стратегическое разделение для максимальной защиты

Защита периметра Data Lake: API и веб-приложения

- WAF: Щит для API и веб-интерфейсов
- API Gateway: Централизованное управление безопасностью API

Проактивное управление уязвимостями в Data Lake

- Сканирование уязвимостей: Постоянная бдительность
- Patch Management: Своевременное устранение уязвимостей

Борьба с инсайдерскими угрозами в Data Lake

- UEBA: Поведенческая аналитика на страже безопасности
- Аналитика и OSINT: корреляция баз данных из различных источников

Инновации в безопасности обработки данных

- Homomorphic Encryption: Будущее конфиденциальных вычислений
- Secure Multi-party Computation: Коллаборация без компромиссов

Непрерывная оценка безопасности Data Lake

- Penetration Testing: Испытание на прочность
- Red Team Exercises: Симуляция реальных атак

Метаданные: Скрытый фронт безопасности Data Lake

- Metadata Security: Защита фундамента Data Lake

Устойчивость Data Lake: Backup и Disaster Recovery

- Стратегии резервного копирования и восстановления: Гарантия непрерывности бизнеса

Комплексная стратегия защиты Data Lake

ГАРДА

Для защиты data lake (озера данных) рекомендуется использовать комплексный подход, который включает несколько уровней безопасности. Вот основные методы и инструменты:

Шифрование данных

- **Шифрование на уровне хранения (at-rest encryption)**

  Защита данных в состоянии покоя, используя методы шифрования, такие как AES-256 или ГОСТ.

- **Шифрование данных при передаче (in-transit encryption)**

  Шифрование данных при передаче между узлами сети с использованием протоколов SSL/TLS.

Контроль доступа и управление правами

- **Role-Based Access Control (RBAC)**
  Управление доступом на основе ролей пользователей, чтобы ограничить доступ к данным в зависимости от ролей и привилегий.
- **Attribute-Based Access Control (ABAC)**
  Более гибкий контроль доступа, который учитывает атрибуты пользователей и ресурсов для принятия решений о доступе.
- **Multi-Factor Authentication (MFA)**
  Использование нескольких факторов аутентификации для обеспечения безопасного доступа.
- **Privileged Access Management (PAM)**
  Внедрение решений для управления привилегированным доступом.

Комплексная стратегия защиты Data Lake

ГАРДА

Мониторинг и обнаружение угроз

- **Network Detection and Response (NDR)**

  Использование систем обнаружения и ответа на угрозы в сети для мониторинга аномальной активности и возможных нарушений безопасности.

- **Security Information and Event Management (SIEM)**

  Интеграция с SIEM-системами для анализа логов и событий безопасности с целью выявления и реагирования на инциденты.

Data Access Monitoring (DAM) и Data Loss Prevention (DLP)

- **DAM**

  Мониторинг доступа к данным и их использование, чтобы выявить несанкционированные действия или подозрительные запросы.

- **DLP**

  Предотвращение утечек данных путем выявления и блокировки передачи конфиденциальной информации за пределы организации.

Tokenization и Masking данных

- **Tokenization**

  Замена конфиденциальных данных на уникальные токены, которые могут использоваться в системах без раскрытия исходных данных.

- **Data Masking**

  Маскирование чувствительных данных в целях защиты при использовании в тестовых или аналитических средах.

Комплексная стратегия защиты Data Lake

ГАРДА

Обеспечение соответствия и аудит

- **Compliance**

  Внедрение и поддержание соответствия нормативным требованиям (например,ФЗ-152, КИИ, PCI DSS) с использованием соответствующих политик и процедур.

- **Аудит и журналирование**

  Ведение подробных журналов доступа и операций с данными для последующего анализа и аудита.

Сегментация сети и зон безопасности

Разделение data lake на изолированные зоны с разными уровнями доступа и защиты, что ограничивает возможность распространения угроз.

Защита API и веб-приложений

- **Web Application Firewall (WAF)**

  Использование WAF для защиты API и веб-интерфейсов, связанных с data lake, от атак на уровне приложений.

- **API Gateway**

  Внедрение API Gateway для централизованного управления, мониторинга и защиты API-интерфейсов.

Комплексная стратегия защиты Data Lake

ГАРДА

Управление уязвимостями

- **Регулярное сканирование уязвимостей**

  Проведение регулярных проверок инфраструктуры data lake на наличие уязвимостей.

- **Patch Management**

  Своевременное обновление или виртуальные патчи всех компонентов data lake.

Защита от инсайдерских угроз

- **User and Entity Behavior Analytics (UEBA)**

  Использование UEBA для выявления аномального поведения пользователей и сущностей.

Безопасность данных в процессе их обработки

- **Homomorphic Encryption**

  Использование гомоморфного шифрования для обработки зашифрованных данных без их расшифровки.

- **Secure Multi-party Computation**

  Применение методов безопасных многосторонних вычислений для обработки данных из разных источников.

Комплексная стратегия защиты Data Lake

ГАРДА

Непрерывная оценка безопасности

- **Penetration Testing**

  Регулярное проведение тестов на проникновение для выявления слабых мест в защите data lake.

- **Red Team Exercises**

  Организация учений с имитацией реальных атак для проверки эффективности мер безопасности.

Управление метаданными:

- **Metadata Security**

  Обеспечение безопасности и целостности метаданных, которые критичны для правильного функционирования data lake.

Резервное копирование и восстановление

- **Backup and Disaster Recovery**

  Реализация надежных стратегий резервного копирования и восстановления данных в случае инцидентов безопасности или сбоев.

Безопасность данных

ГАРДА

Анализ рисков доступа: выявляет и предотвращает аномальные попытки доступа к данным

Выявляет и предотвращает попытки внешнего вторжения в СУБД

Выявляет инсайдеров и инциденты утечек данных через коммуникации

Обнаруживает конфиденциальные данные в общем доступе в сетевых хранилищах.

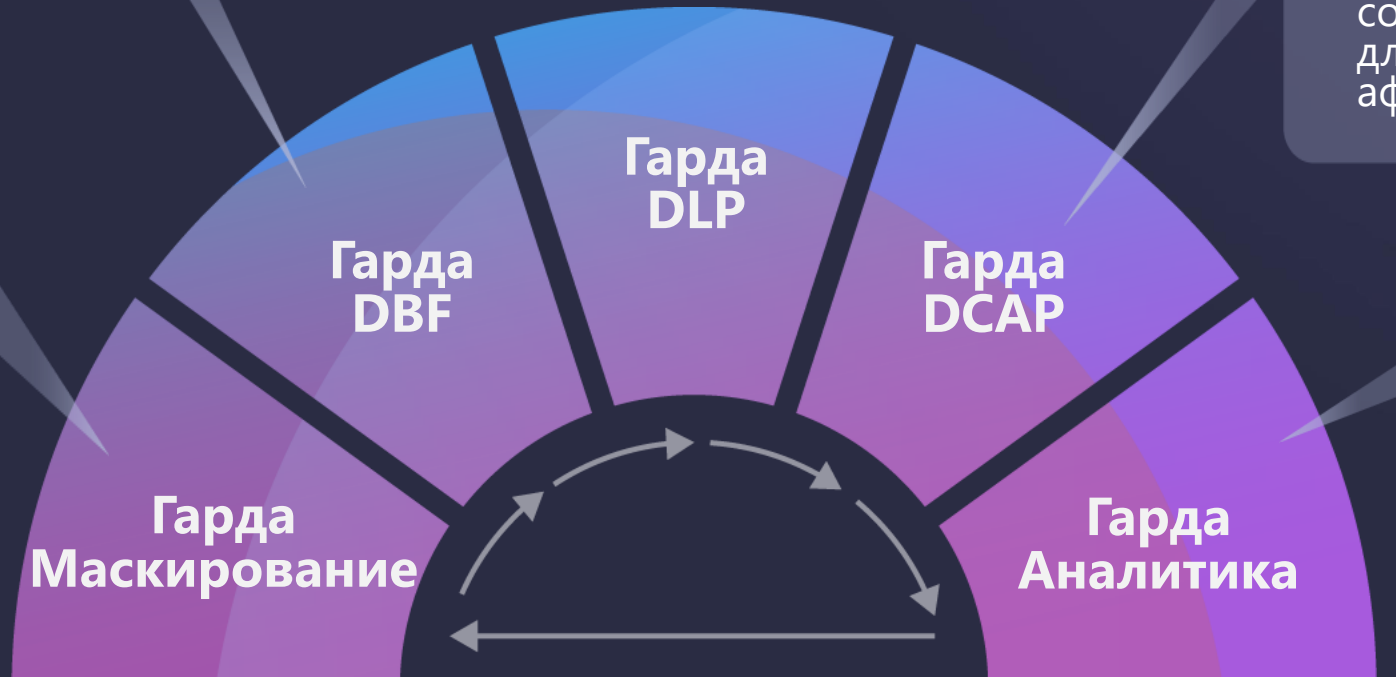
Выявляет взаимосвязи между сотрудниками для контроля аффилированности.

Предотвращает утечки баз данных и аномальное поведение пользователей

Находит все базы данных и их неучтенные копии в структуре организации

Создает обезличенные копии баз данных

Экономическая безопасность: автоматизация массовых проверок сотрудников



Сетевая безопасность

ГАРДА

Выявить и заблокировать атаки на веб-приложения.

Защитить веб-приложения от несанкционированного доступа.

Защитить сеть от таргетированных атак

Защитить сеть от проникновения

Получить экспертизу по киберугрозам

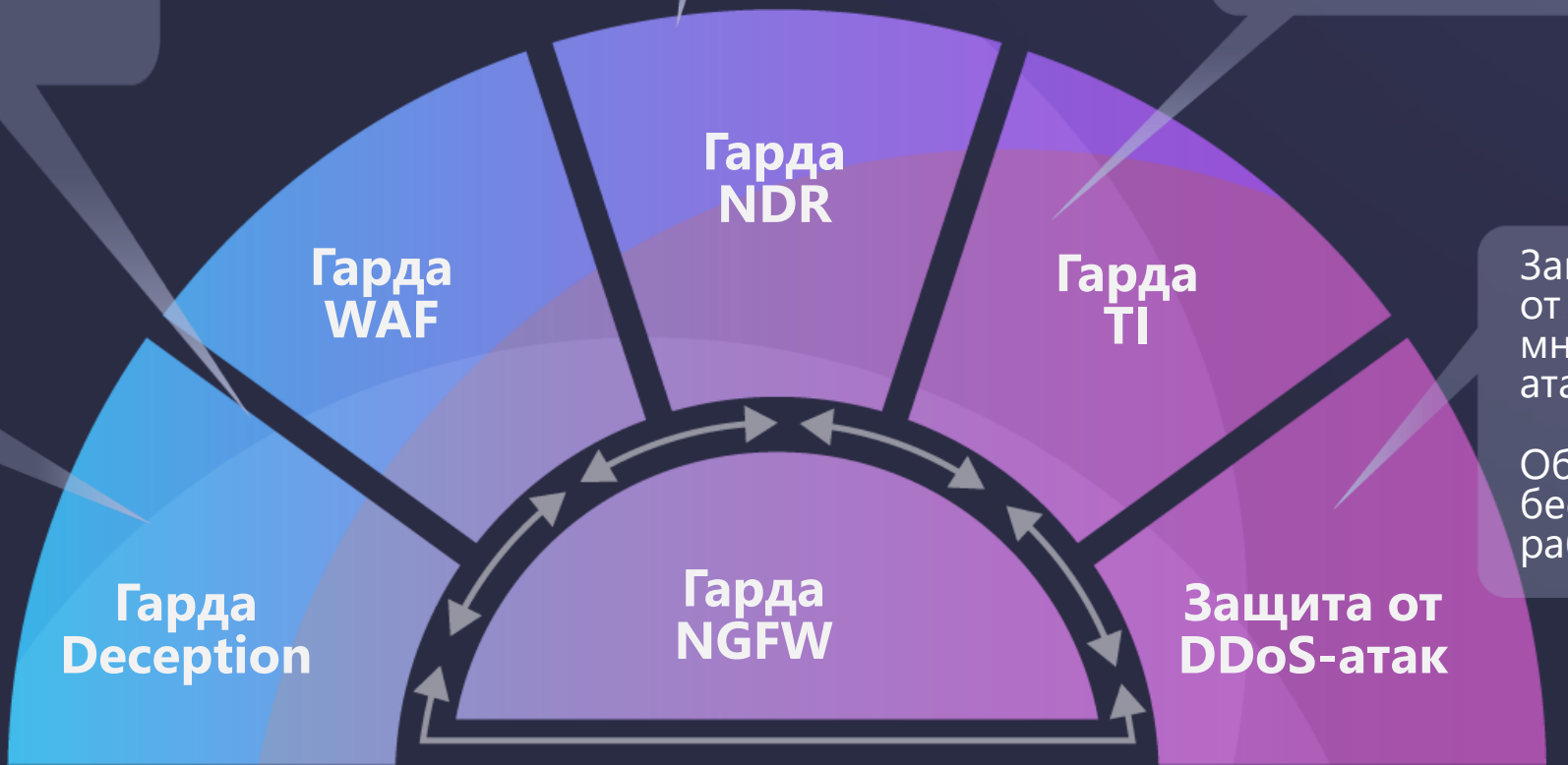
Определить индивидуальный перечень угроз ИБ

Заманить злоумышленника в ловушку

Распознать методы и техники киберпреступника

Защитить сеть даже от сложных многовекторных атак

Обеспечить бесперебойную работу сервисов



Область применения решений

ГАРДА

СУБД	**DBF** *А чем защищаете данные в БД от инсайдеров?*
SIEM	**NDR+TI** *Откуда берете сетевой трафик? Чьи сигнатуры используете? Есть ли фиды?*
Терминальные сервера	**NDR+TI, DLP** *Есть ли необходимость контролировать действия пользователей?*
Любые сетевые СЗИ	**TI** *Чем обогащены эти СЗИ?*
Среда разработки	**Маскирование** *А в среде разработки используются базы из ПРОД сегмента?*
Файловые хранилища	**DCAP** *Аудит доступа пользователей и выявление критической информации*

Эксперты компании

ГАРДА

Исследования и анализ киберугроз, — поставляют экспертный сервис

Исследование актуальных угроз, тактик, техник злоумышленников, разработка методов их обнаружения

Консультирование специалистов заказчика по вопросам работы комплексов «Гарда» в соответствии с требованиями законодательства

Помощь в настройке комплексов «Гарда» и формирование отчетов

Адаптация политик и настроек под нужды заказчика

ГАРДА

Уникальные компетенции вендора

- Гарда DBF
- Гарда DLP
- Гарда Маскирование
- Града Deception
- Гарда NDR
- Гарда Threat Intelligence


Москва, конгресс-центр Soluxe
Конференция 24 октября 2024
СОХРАНИТЬ ВСЁ БЕЗОПАСНОСТЬ ИНФОРМАЦИИ
Регистрируйтесь
partner@gardatech.ru
отдел по работе с партнерами
sk.partner@gardatech.ru
координатор партнерского канала
ГАРДА
ОРГАНИЗАТОР
Группа компаний «Гарда»
МАНИФЕСТ
ОПЕРАТОР МЕРОПРИЯТИЯ
Агентство Продающий Событий
ПРИ ПОДДЕРЖКЕ
ФСТЭК России
Минцифры России
ПРИ ПОДДЕРЖКЕ
Минцифры России

ГАРДА

Обращайтесь!

Офис в Москве
улица Новодмитровская, дом 2Б

8 800 770 70 60
garda.ai
info@garda.ai

Подписывайтесь
на телеграм-канал **garda.ai**