Александр Киричук
Эксперт команды Резбез

Методология Результативной кибербезопасности (РКБ)

Недопустимое событие

Событие, возникшее в результате кибератаки, которое делает невозможным достижение операционных и (или) стратегических целей организации или приводит к значительному нарушению ее основной деятельности.

Цель РКБ

Сделать реализацию недопустимого события невозможной

Примеры недопустимых событий

- Остановка производства
  (более 3 суток)
- Кража денежных средств
  со счетов организации
  (более 20% от оборота)
- Вывод из строя ГИС
  (более 4 часов простоя)

Порог ущерба

- допустимый ущерб

- значительный ущерб

- недопустимый ущерб

Руководство

Знает, что действительно недопустимо для организации

→

Перечень

недопустимых для организации событий

Операционные руководители

Помогут понять, как НС может быть реализовано

→

Сценарий

реализации НС

Специалисты по ИТ, ИБ

Помогут обозначить системы в которых может быть реализовано НС

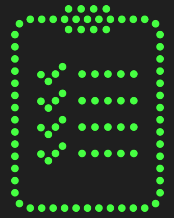
→

Системы

взлом которых повлечет НС

Перечень недопустимых событий

- недопустимые события;
- возможные негативные последствия в случае реализации недопустимых событий;
- сценарии реализации недопустимых событий;
- целевые информационные системы;
- критерии реализации недопустимых событий.



Приземление НС на ИТ-инфраструктуру

Ключевая система

Объект в информационной инфраструктуре, несанкционированный доступ к которому или воздействие на который необходимы нарушителю, чтобы развить атаку на целевую систему, или система, взлом которой существенно упростит сценарий атаки или повысит ее эффективность

Точка проникновения

Объект в информационной инфраструктуре, несанкционированный доступ к которому или воздействие на который позволяют внешнему нарушителю получить доступ к внутренней IT-инфраструктуре

Соотнесение бизнес-процессов и целевых систем

Соотнесения целевых систем и бизнес-процессов могут использоваться для изменения бизнес-процессов или разделения систем по отдельным видам деятельности, чтобы уменьшить поверхность атаки и снизить затраты на обеспечение защиты

Блоки РКБ

Блок 1:
Целеполагание

1. Определение недопустимых событий
2. «Приземление» недопустимых событий на IT-инфраструктуру

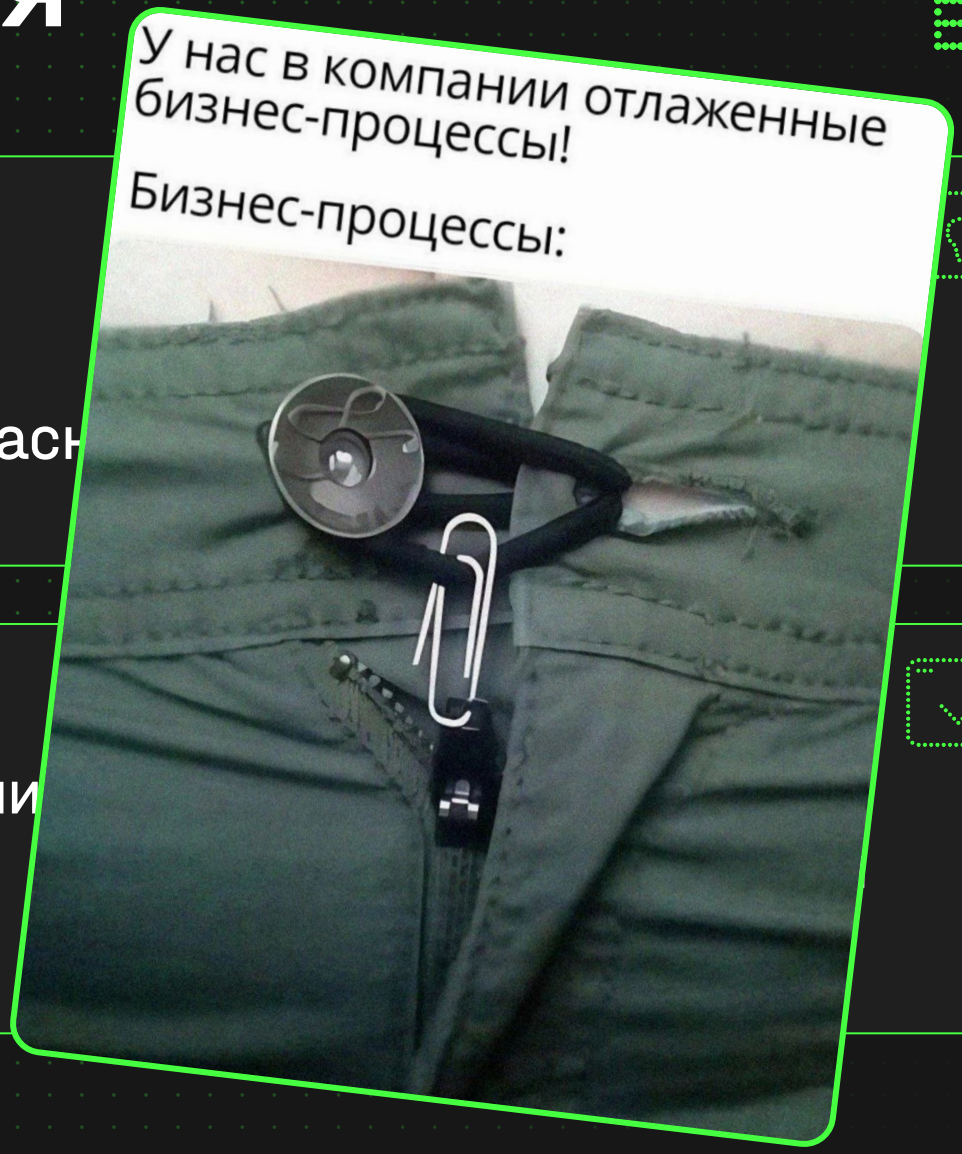
Кибертрансформация

Харденинг ИТ-инфраструктуры

Обучение практикам кибербезопасн

Проверка защищенности

Выстраивани процессов



Блоки РКБ

Блок 1:
Целеполагание

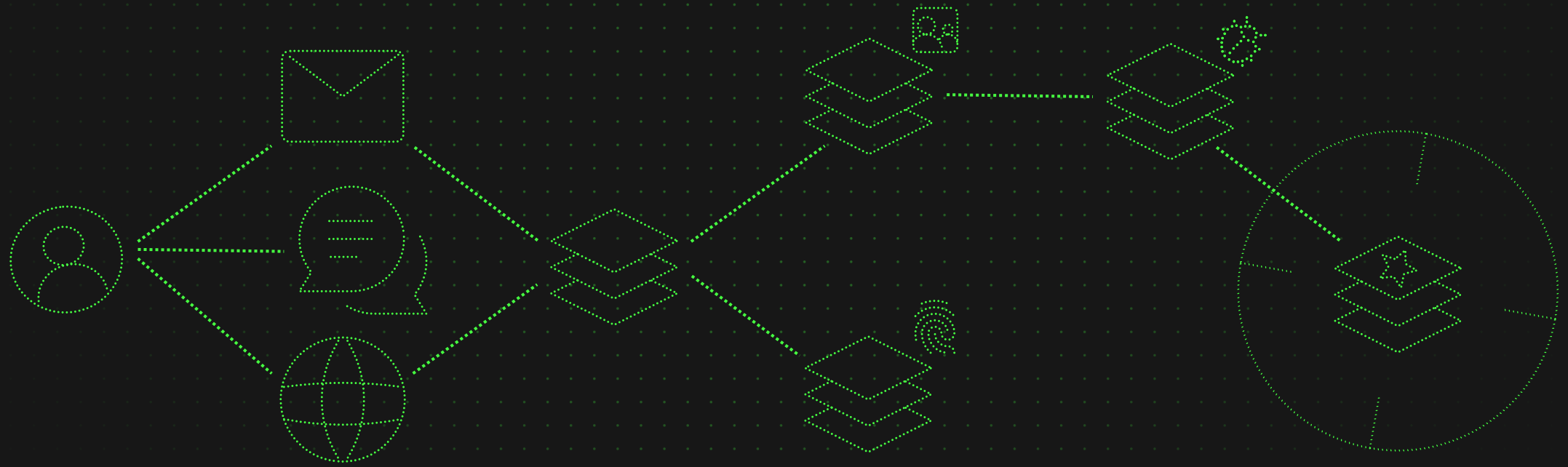
1. Определение недопустимых событий
2. «Приземление» недопустимых событий на IT-инфраструктуру

Блок 2:
Кибертрансформация

1. Харденинг IT-инфраструктуры
2. Обучение практикам кибербезопасности
3. Мониторинг и реагирование на инциденты
4. Проверка защищенности
5. Выстраивание процессов
6. Оценка эффективности

APT Bug Bounty

финальный этап работ со всеми доменами результативной кибербезопасности, так как непрерывная и разносторонняя оценка защищенности существенно повышает уровень киберустойчивости организации.



Блоки РКБ

Блок 1: Целеполагание

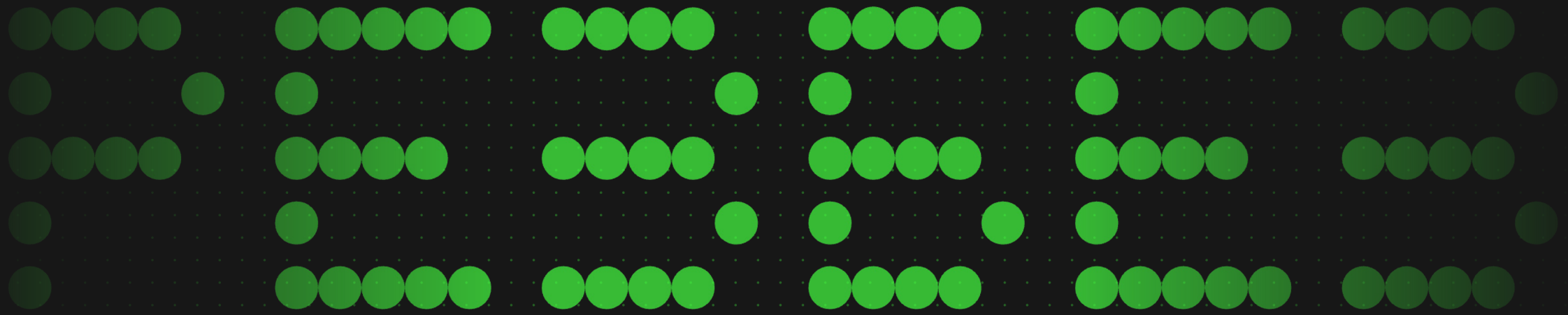
1. Определение недопустимых событий
2. «Приземление» недопустимых событий на IT-инфраструктуру

Блок 2: Кибертрансформация

1. Харденинг IT-инфраструктуры
2. Обучение практикам кибербезопасности
3. Мониторинг и реагирование на инциденты
4. Проверка защищенности
5. Выстраивание процессов
6. Оценка эффективности

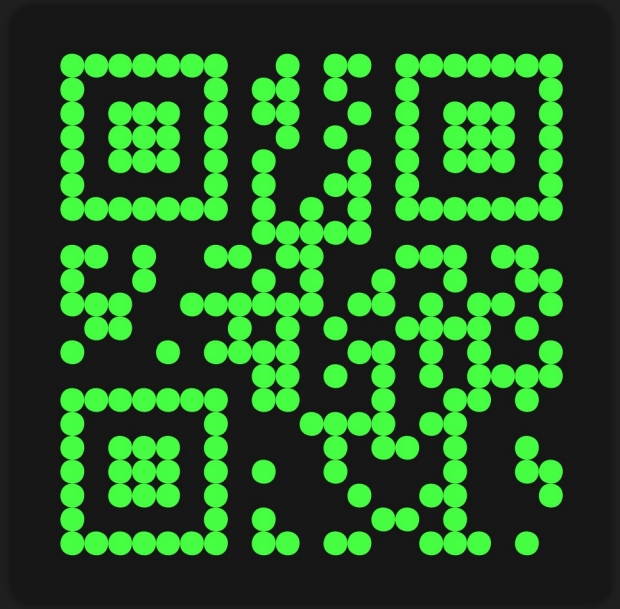
Блок 3: Подтверждение киберустойчивости

1. Запуск программы APT Bug Bounty



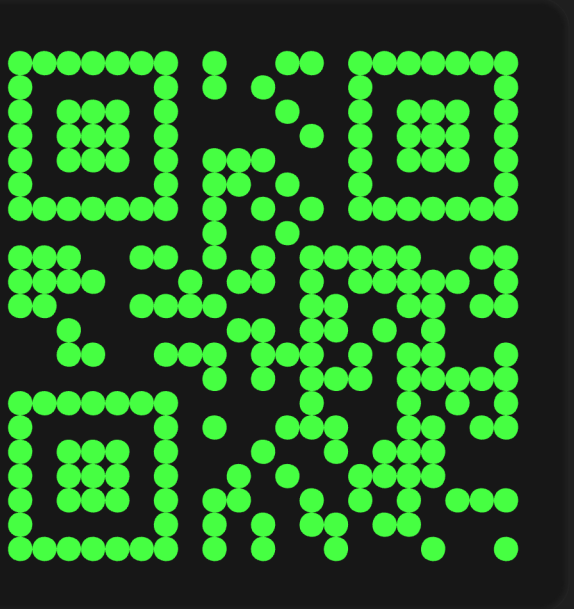
Наши ресурсы

Открытый портал Резбез



rezberz.ru

Телеграм аккаунт Резбез



@Rez_in_Bez

Спасибо
за внимание!