Что такое новый Dozor?

Игорь Ляпунов
Генеральный директор

Solar Security

Основные факты

- Компания Solar Security выделилась как независимая компания-разработчик из ведущего ИБ-интегратора – компании «Инфосистемы Джет»
- Наша команда создала JSOC – первого российского MSSP-провайдера и выпустила первый российский продукт класса Security Intelligence – Solar inView;
- Мы стали пионерами в разработке нового класса решений, выпустив 15 лет назад первую российскую DLP-систему – «Дозор-Джет»;
- Решения Solar Security работают более чем в 30% компаниях из ТОП 100 российского бизнеса;
- Исследовательская лаборатория Solar CyberSecurity Team анализирует более 150 тысяч внутренних и внешних инцидентов информационной безопасности в год.

Что мы делаем для клиентов

SOLAR SECURITY
software&services

Solar Security – удобные продукты и сервисы для целевого мониторинга и оперативного управления безопасностью

Solar Security – это продукты и сервисы, удобные в использовании и простые в восприятии. Мы делаем технологии доступными руководителям и сотрудникам подразделений информационной безопасности, позволяя им выбрать удобный канал доставки в виде сервиса, приложения и комплексной системы.

Продукты и сервисы

Dozor

inView

inRights

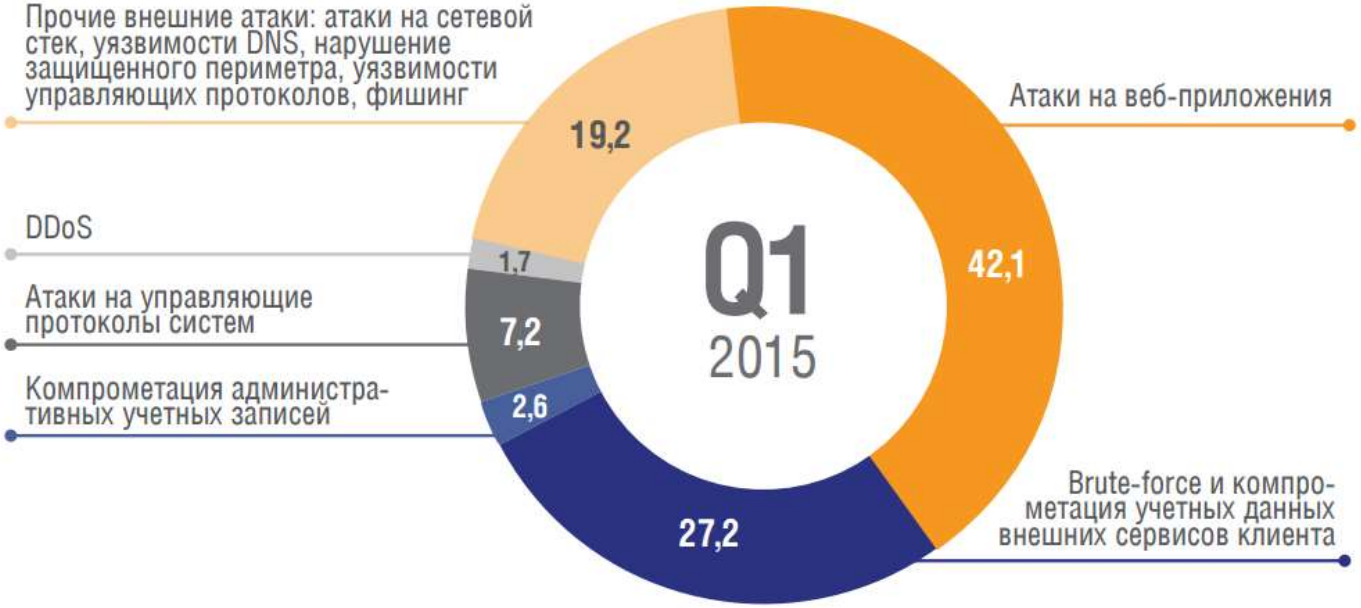
JSOC

Что угрожает? Снаружи или изнутри?

Распределение инцидентов по внешним и внутренним[1] в %-ном соотношении от общего числа:

Внешние инциденты

Направления атак в %-ном соотношении от общего числа:



Внутренние инциденты

Направления атак в %-ном соотношении от общего числа:

Изменение вектора работы служб безопасности

Предпосылки:

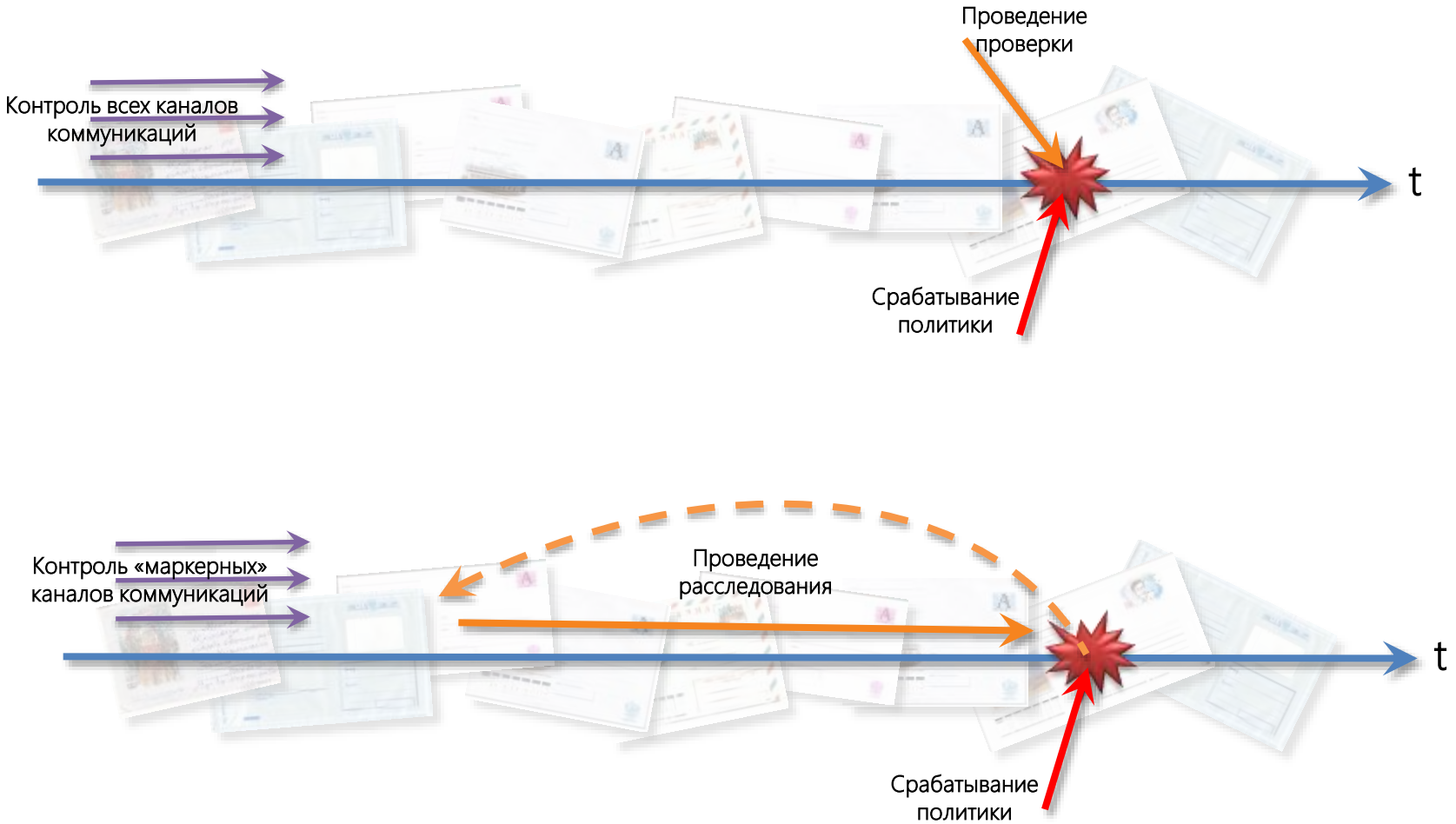
- Рост зрелости служб безопасности: ориентир на бизнес-цели компании и защиту денег
- Кризисные явления: максимальное фокусирование только на реальных задачах и контроле «точек монетизации»
- Кризисные явления: обострение нелояльности сотрудников и их поиски «дополнительных доходов»

Переход от задач «чистой ИБ» к задачам реальной безопасности и борьбе с внутренним мошенничеством.

Что же такое внутренний фрод?

- Сговор или аффилированность с клиентами или с поставщиками
- Передача клиентов другим компаниям
- Искусственное завышение цен
- Использование подставных поставщиков или посредников
- Проведение сделок с подконтрольными компаниями
- «Откаты»
- Подделка или фальсификация документов
- Использование сотрудников, оборудования, материалов или ресурсов компании в личных целях
- Оплата счетов за невыполненные работы или непоставленные товары

Изменение требований к DLP-системе



Функции Solar Dozor 6.0 для борьбы с внутренним мошенничеством:

- Эффективный масштабируемый архив
- Средства выявления косвенных признаков мошенничества
- Аналитика для проведения расследований
- Автоматизация деятельности службы безопасности

Ситуационный центр по внутренним угрозам:

Новые поисковые возможности:

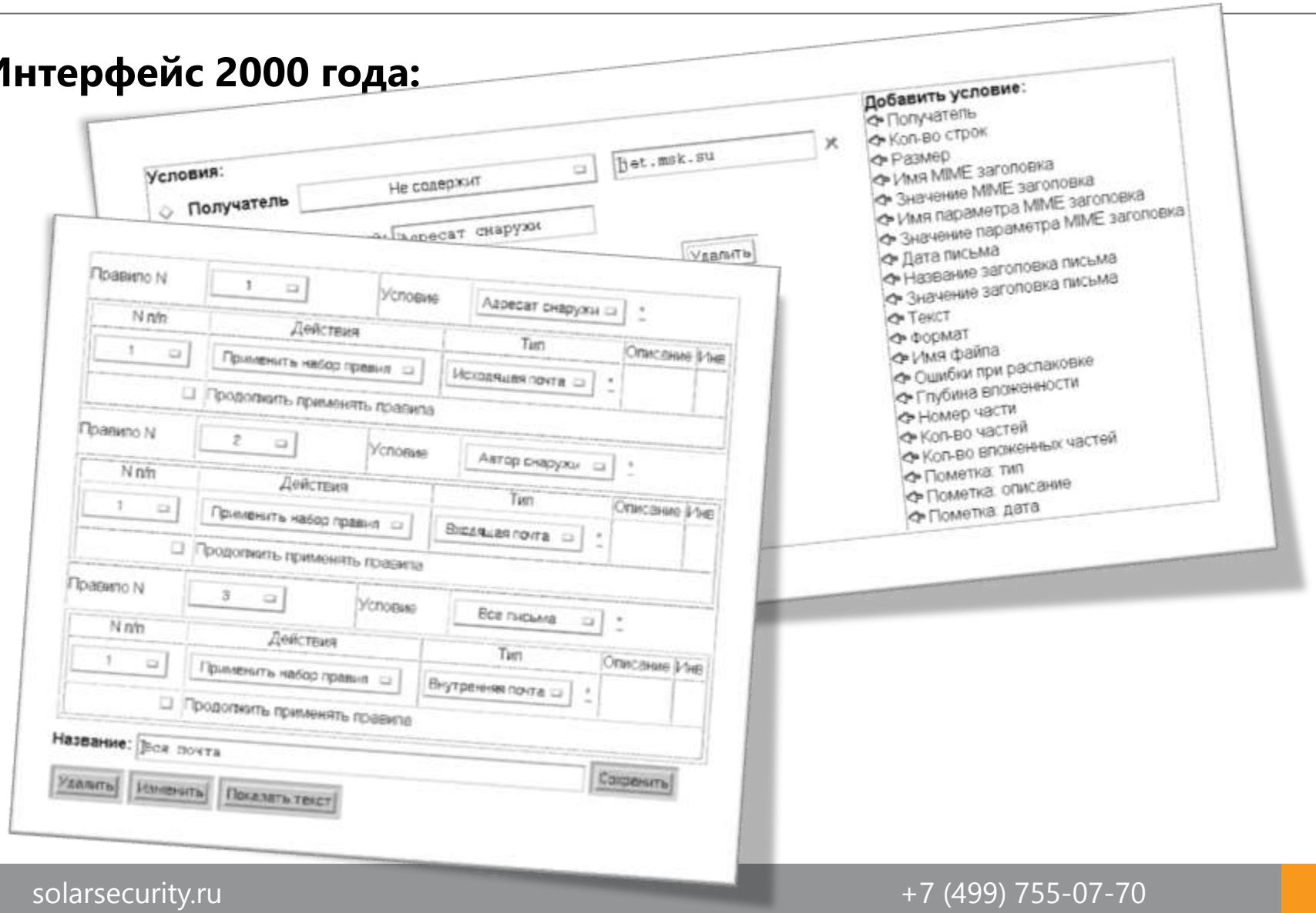
- Простой интерфейс в стиле популярных интернет-поисковых систем
- Большая библиотека готовых поисковых запросов с задаваемыми пользователем параметрами
- Углубленный поиск с широкими возможностями детализации поискового запроса
- Действительно быстрый поиск. Используемые технологии фасетного поиска позволяют достичь скорости поиска < 1 сек в архиве из 17 млн сообщений

Новые аналитические возможности:

- Технологии выявления аномалий в коммуникациях сотрудников
- Обновленная технология построения уровня доверия сотрудника.
- Досье с возможностью обогащения из кадровой системы или внешних систем проверки контрагентов
- Подсказка следующих шагов при проведении расследований
- Анализ данных на основе OLAP и BI-технологий с возможностью мгновенной детализации в формате drill-down
- Каталог выявляемых мошеннических схем и их ранних признаков с отраслевой спецификой

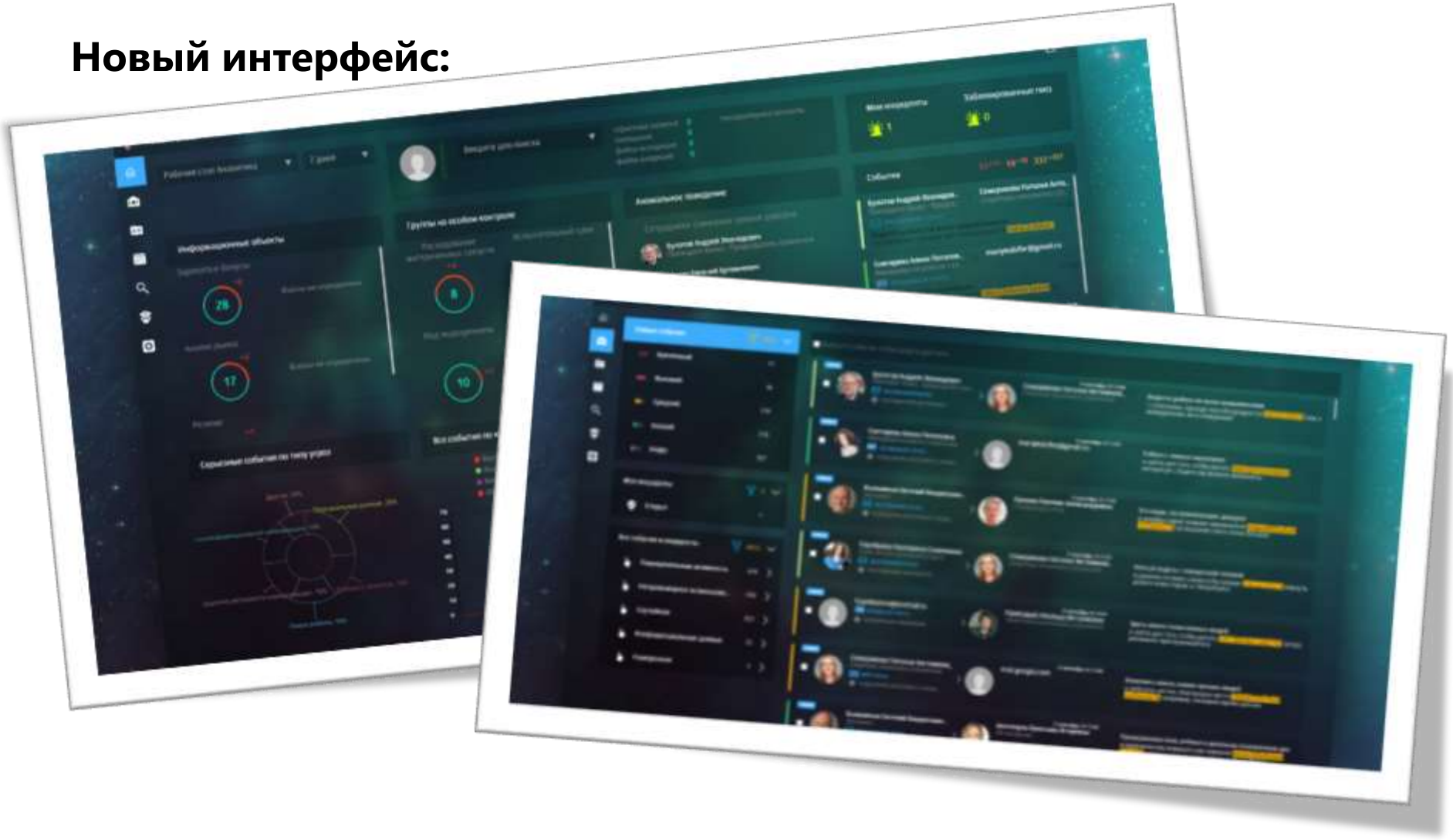
Solar Dozor 6.0. Что нового

Интерфейс 2000 года:



Solar Dozor 6.0. Что нового

Новый интерфейс:



Спасибо за внимание!

Игорь Ляпунов
+7 499 755 0770
i.liapunov@solarsecurity.ru