



VERINT®

INTELLIGENCE POWERED SECURITY

Situational Intelligence Solutions

От традиционных ситуационных центров к интеллектуальным с помощью решений Verint Systems

Вячеслав Безман

Пресейл-менеджер
Verint Systems

Решения в области безопасности построенные на мощной основе



Веринт (Verint): Интеллектуальные и комплексные решения безопасности



Решения по
Взаимодействию с
Клиентами



Verint CES

Решения по
Киберразведке

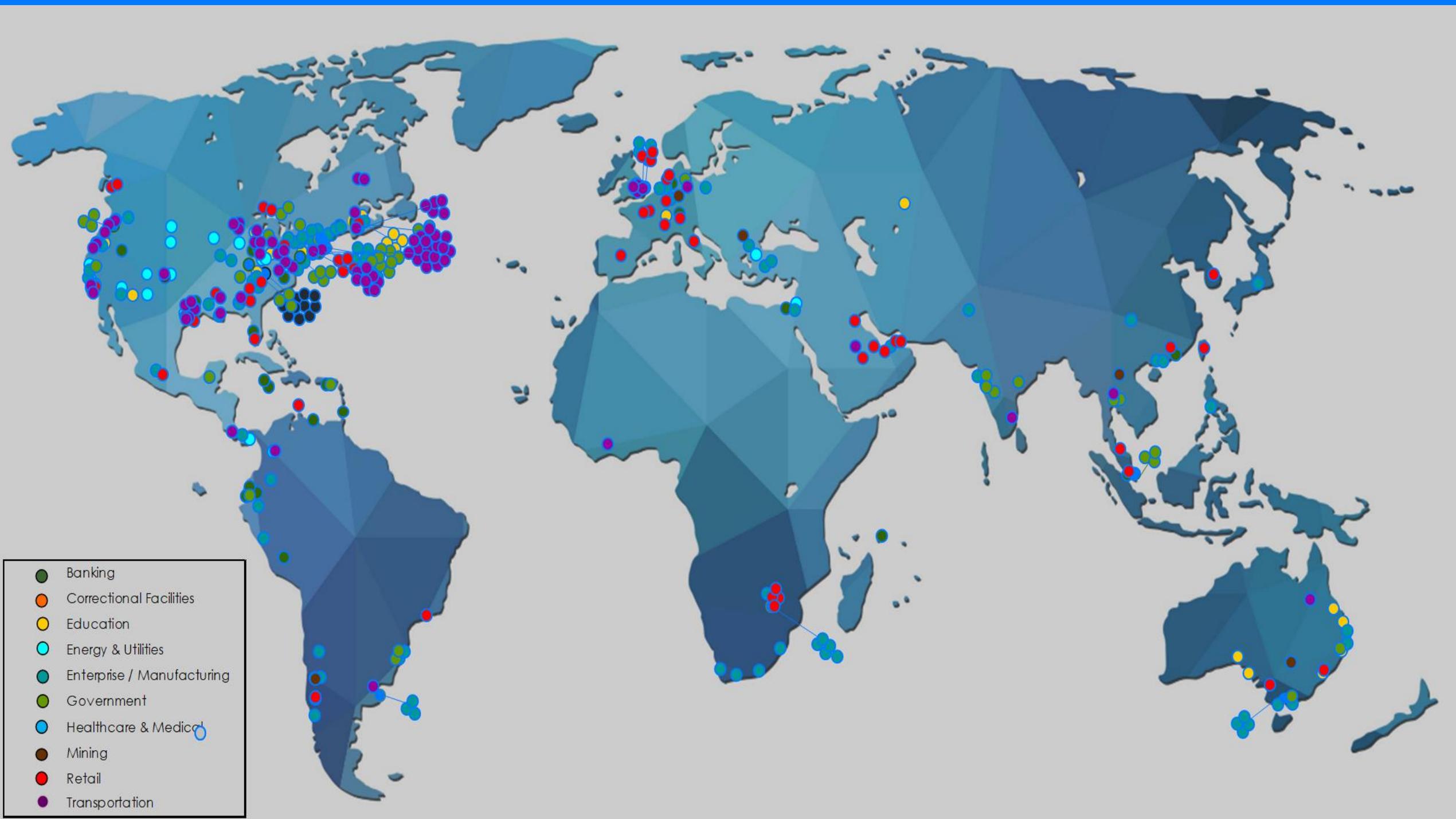


Verint CIS

Ситуационно
разведывательные
решения



Verint SIS



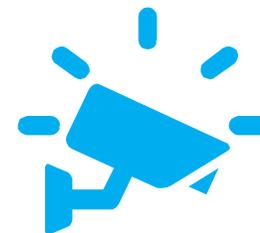
Что требует рынок безопасности сегодня?



Проводить анализ
ситуации в реальном
времени



Использовать открытые
платформы с
возможностями интеграции



Сделать видео
“умнее”



Автоматизировать
процессы



Улучшить
сотрудничество
подразделений



Сделать
расследование более
продуктивным

Как выглядит традиционный Ситуационный Центр (iSOC)?

Множество больших экранов,
видео-ориентированная работа

Ограниченная реакция оператора -
слишком большой набор видео-окон, под
постоянным наблюдением

Ограниченное количество и тип данных,
которые можно принять и обработать

Ограниченная возможность корреляции
различных данных

Ограниченная возможность выявлять
угрозы заблаговременно



Когда нам стоит задуматься о **Интеллектуальном Ситуационном центре (iSOC)**?



Когда не хватает **общей картины ситуации**, в реальном времени и **на географической карте**



Когда **действия** оператора должны **выполняться быстрее**, на основе большого потока вводимых данных, из множества подсистем



Когда требуется **снизить человеческий фактор**, используя встроенные процедуры или благодаря автоматическим действиям системы



Когда требуется **взаимодействие со службами безопасности** и силами реагирования



Когда требуется **реконструкция инцидентов**, с пониманием когда и кем были сделаны определенные действия

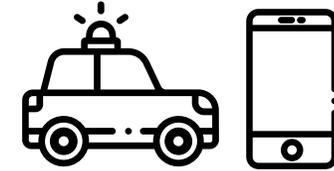
Принятие правильного и своевременного решения...



Обнаружение угрозы
(первоначальное оповещение)



Анализ угрозы



Ответные действия и
диспетчеризация

- Подлинная ли угроза, и требуются ли ответные действия?
- Нужно ли далее продолжать расследование угрозы?
- Какие устройства/датчики вовлечены, и на что может повлиять эта угроза?
- Требуется ли моментальная реакция? Можно ли отложить расследование в зависимости от приоритетности?

Цели и задачи Интеллектуального Ситуационного центра (iSOC)?



Как выглядит Интеллектуальный Ситуационный Центр?

Переход от видео-ориентированной среды в интеллектуальную

Улучшения возможностей анализа угроз и своевременного реагирования

Сбор и анализ данных в реальном времени, оценка рисков и рекомендации по реагированию

Сведение к минимуму количества ложных срабатываний, при обработке потока информации с датчиков



Комплексный подход в технологиях и решениях компании Verint



Ситуационная Платформа (SA PLATFORM™) от Verint



Работа с видео
источниками



Управление
инцидентами



Диспетчер



KPI - Панель
Менеджера

Что произошло?...Где произошло?...Как реагировать?

Панель мониторинга Активы Оповещения Ответные действия Инциденты Найти

Сост...	Источник	Подсистема	Тип сигнала	Подтип сигнала	Описание	Метка времени
🔔	Door #36	Simulator	Отказано в доступе	Недействительный PIN	Event - A Door was fon	18.11.2019 13:07:57
🔔	TSA checkpoint Facial I Simulator		Лицо распознано	Не разрешено	Employee Terminated	18.11.2019 13:07:37
🔔	Fiber Optic Intrusion St Simulator		Сигнализация вторже		Event - Intruder Alarm	18.11.2019 13:06:37
🔔	Airport Data Center Eni Simulator		Отказано в доступе	Доступ прекращен	Employee Terminated	18.11.2019 13:05:12
🔔	TSA Checkpoint Bypass Simulator		Отказано в доступе	Доступ прекращен	Employee Terminated	18.11.2019 13:04:18
🔔	North Perimeter Fence Master Recorder		Сигнализация VMS		Person crossing line de	18.11.2019 13:03:53
🔔	Emergency Exit EAST Simulator		Двери принудительнс		DoorforcedOpen force	18.11.2019 13:03:37
🔔	Hold up Alarm Bank Ac Simulator		Сигнализация вторже		Event - Intruder Alarm	18.11.2019 13:03:37
🔔	N Pecos S Master Recorder		Сигнализация VMS		Vehicle crossing line de	18.11.2019 13:02:40
🔔	Fiber Optic Intrusion Sc Simulator		Сигнализация вторже		Event - Intruder Alarm	18.11.2019 13:02:38
🔔	Door #37 Simulator		Отказано в доступе	Недействительный PIN	Event - An access has b	18.11.2019 13:02:37
🔔	Door #38 Simulator		Отказано в доступе	Недействительный PIN	Access Denied	18.11.2019 13:01:27
🔔	TSA checkpoint Facial Re Simulator		Лицо распознано	Не разрешено	Event - An unauthorized fa	18.11.2019 13:00:57
🔔	Lobby - V5620 Master Recorder		Сигнализация VMS		Device Stalled Lobby - V	18.11.2019 13:00:15

Сведения о сигнализации

Дополнительная информация

Идентификатор эмблемы: 1455426

Персональный идентификатор: 2665344

Код отказа: Forced Door

Описание отказа: Door forced o...

Связанные устройства

Связанные инциденты

Подробности отправки

- Door #36
- Break Room - North
- Lobby - V5620

Вложения



Изображение

World Map



Break Room—North



18.11.2019 13:07:50

Что произошло?...Где произошло?...Как реагировать?

The screenshot displays a security monitoring interface with the following components:

- Navigation Bar:** Панель мониторинга, Активы, Оповещения, Ответные действия, **Инциденты**, Найдти
- Left Panel:**
 - Упорядочить по: Метка времени
 - Подозрительное лицо:** Отказано в доступе-Недействительный PIN из Door #36 : Event - A Door was forced open. 13:07:57. Принято Bezman, Slava #9919.
 - Закрытые инциденты:** Недавно закрытые инциденты отсутствуют.
- Center Panel:**
 - Процедура реагирования:** Attach Video, Collaborate, Add Map Location, Take Snapshot of Video FOV, Add Additional Video, Close Incident.
 - World Map:** Aerial view of a building complex with a red location pin and a green arrow pointing to the incident location.
 - Данные об инциденте:**
 - Журнал:** System: 18.11.2019 13:11:18 [Bezman, Slava] Инцидент был принят; System: 18.11.2019 13:11:00 [Bezman, Slava] Был создан инцидент с уровнем важности Normal.
 - Устройства:** Door #36, Break Room - North.
 - Связанные устройства - Doo...:** Break Room - North, Lobby - V5620.
- Right Panel:** Video feed titled "Break Room - North" showing an interior view of a kitchen area with a timestamp of 18.11.2019 13:08:07.

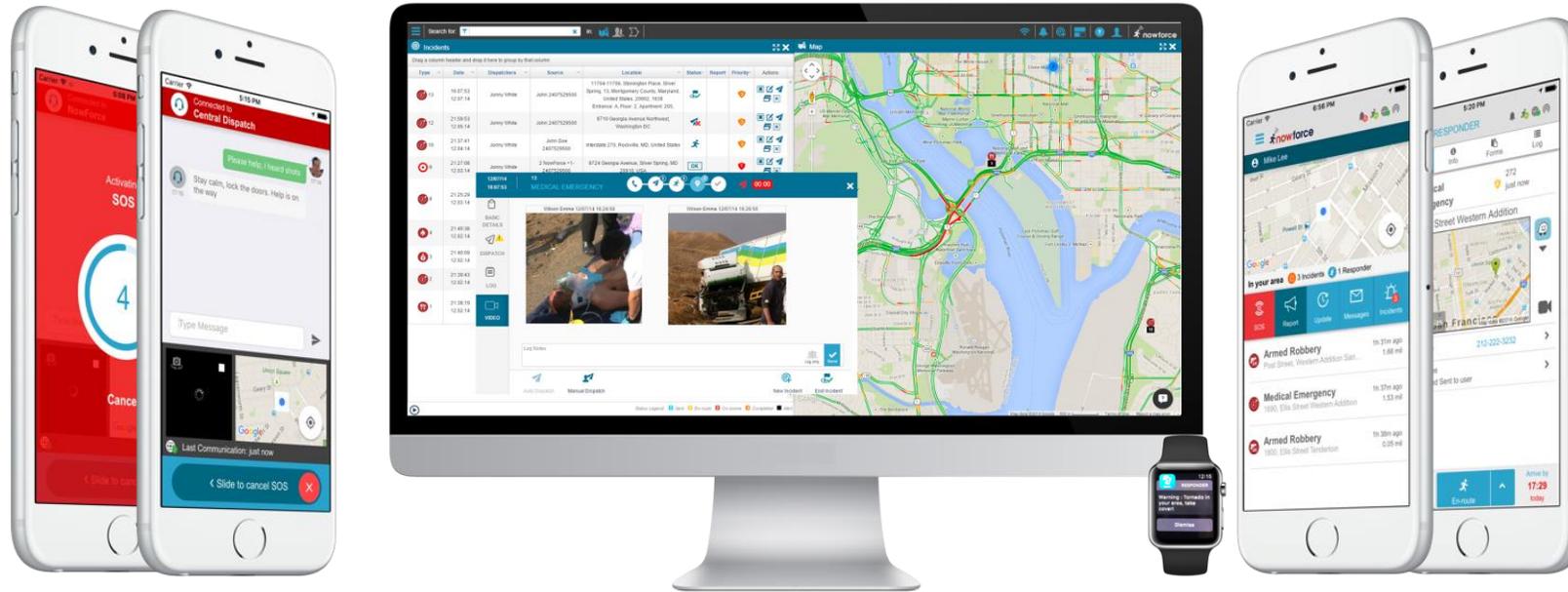
Управление силами и службами реагирования



Verint Dispatch Manager™ -

Управление **мобильными силами** реагирования, повышая **всестороннюю ситуационную осведомленность**, а так же **эффективность коммуникации**, в повседневной жизни и в кризисных ситуациях

Управление силами и службами реагирования



**Verint Dispatch
Manager™**

Осведомление
о ситуации

Эскалация
инцидентов

Анализ
событий

Отслеживание
перемещения
сотрудников

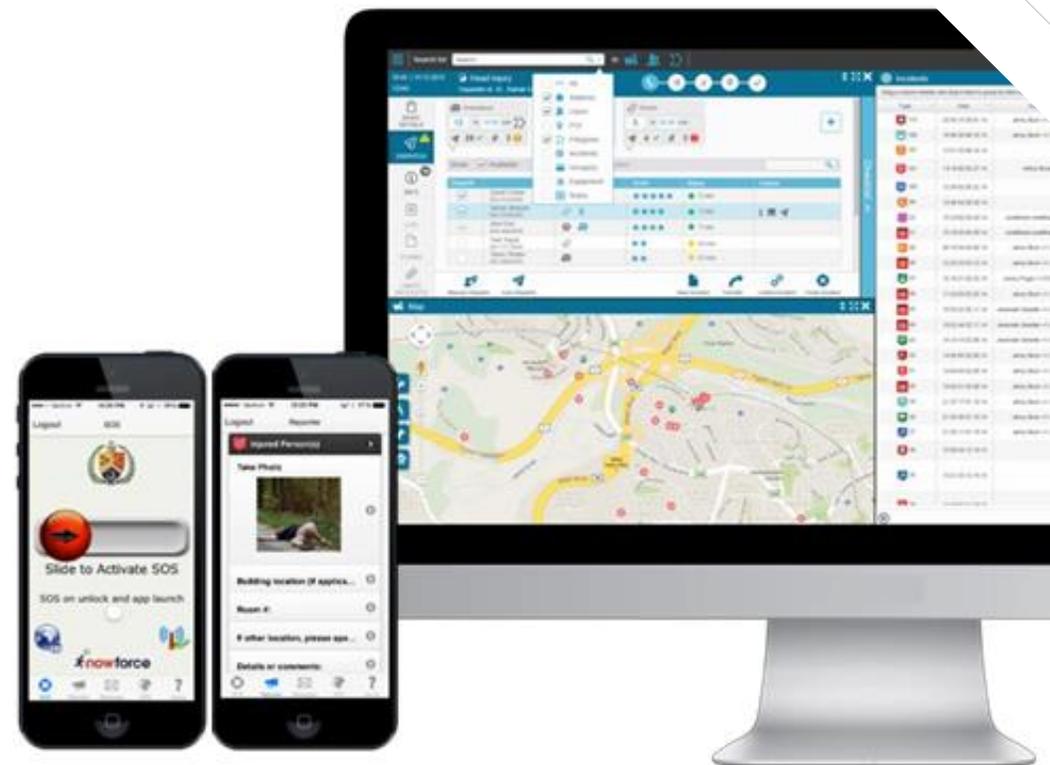
Персональная
Безопасность

Двухсторонняя
связь

Массовое
уведомление

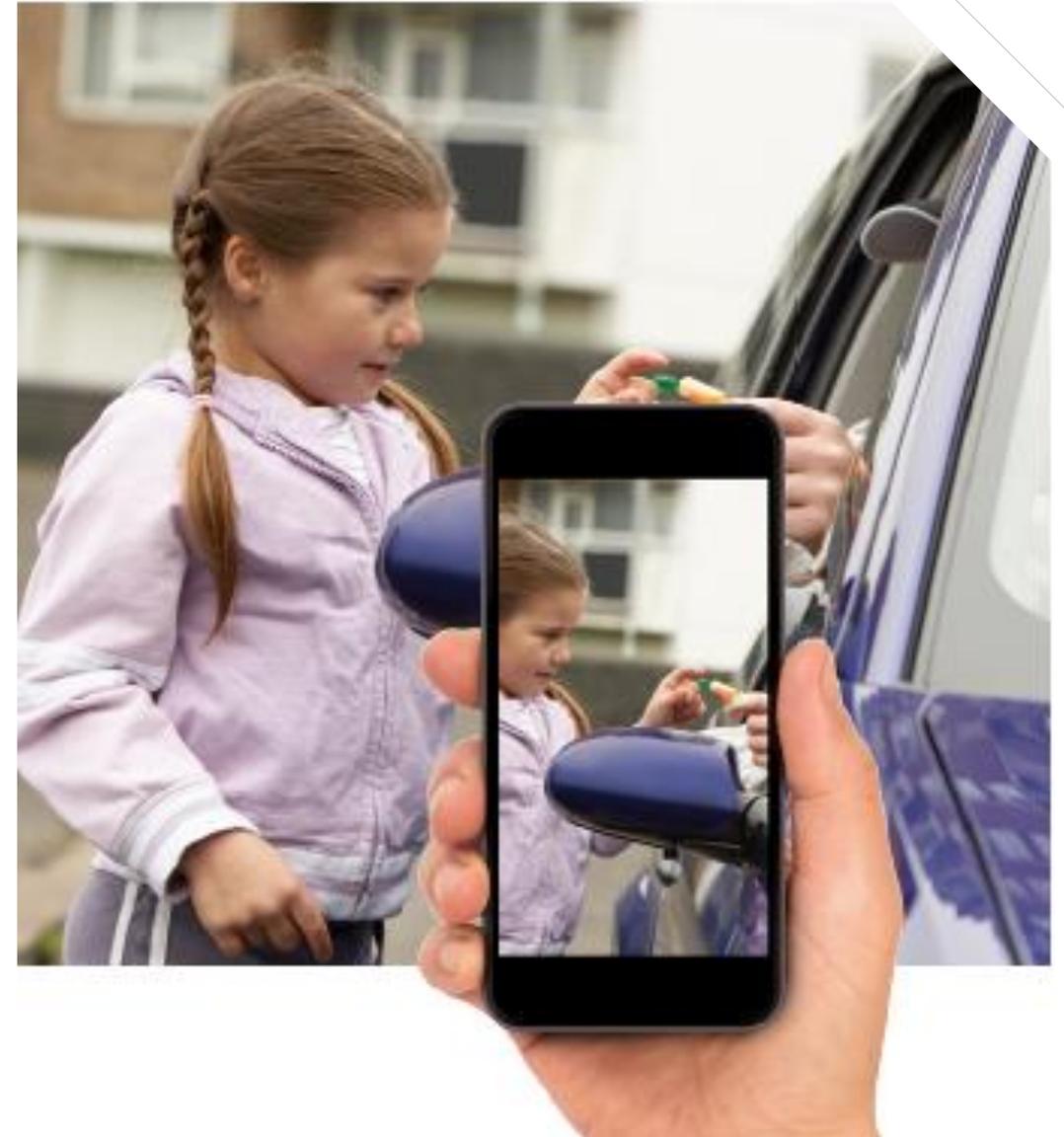
Краудсорсинг в действии – Verint Dispatch Manager™

- + Личная безопасность (кнопка SOS, активный трекинг, геофенсинг)
- + “Видел что-нибудь – расскажи”. Передача информации, видео, аудио и фотографий, о любых происшествиях
- + Передача оповещений от незарегистрированных пользователей (анонимно)
- + Массовые оповещения пользователям в зависимости от месторасположения
- + Сбор информации для отчета и анализа происшествий



Жители города – источник важной информации

- + Технологии мобильной связи уже достаточно развиты, чтобы поддерживать передачу информации, потоковое видео и изображения от пользователей, непосредственно в ситуационный центр
- + **Краудсорсинг** – возможность получать от граждан информацию об инцидентах и происшествиях
- + Легкий и удобный способ передачи информации - позволяет увеличить количество "глаз" на улице



Комплексный подход – от аналитики на камере до реакции охраны на происшествие



VERINT.

Q&A

Verint Situational Intelligence Solutions



VERINT®

Protect What Matters Most