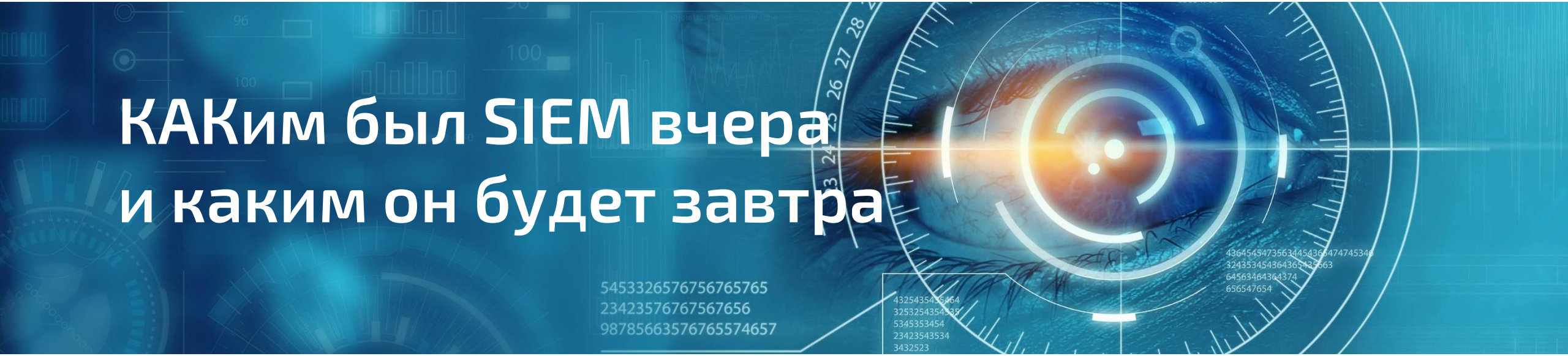
Rusiem
ВСЁ ПОД КОНТРОЛЕМ

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ



КАКим был SIEM вчера и каким он будет завтра

Максим Степченков
RUSIEM

КАКим был SIEM вчера и каким он будет завтра

1 ОСНОВНЫЕ ДРАЙВЕРЫ РАЗВИТИЯ SIEM В 2019 ГОДУ

2 ГДЕ И КАК СЕГОДНЯ ПРИМЕНЯЕТСЯ SIEM?

3 2019 КАКИМ ОН БЫЛ ДЛЯ RuSIEM, ДОСТИЖЕНИЯ И ТОЧКИ РОСТА

4 ПЕРСПЕКТИВЫ РАЗВИТИЯ РЕШЕНИЙ КЛАССА SIEM

Но что является основным драйвером?

1. ЗАКОНЫ И ТРЕБОВАНИЯ РЕГУЛЯТОРОВ?
2. НЕВОЗМОЖНОСТЬ ИСПОЛЬЗОВАНИЯ ТЕКУЩИХ ТЕХНОЛОГИЙ?
3. МАЛЫЕ КОМПАНИИ КАК ТОЧКА РОСТА?
4. КЛАССИЧЕСКАЯ BIG DATA?

ГДЕ И КАК СЕГОДНЯ ПРИМЕНЯЕТСЯ SIEM?

Везде, где из журналов событий можно извлечь полезную информацию

ПРИМЕРЫ СОБЫТИЙ

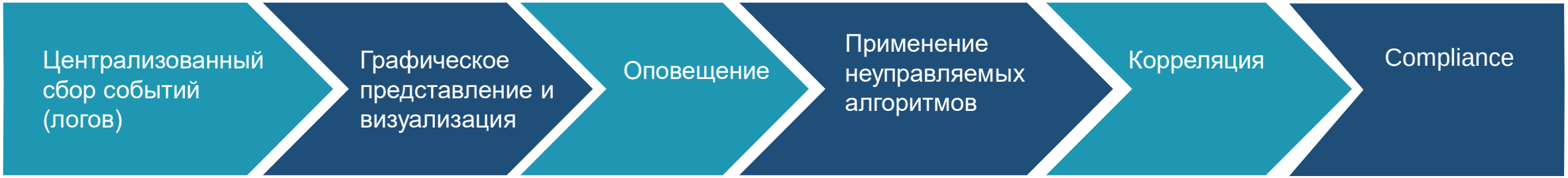
- Сетевые атаки
- Фрод и мошенничество
- Откуда и когда блокировались учетные записи
- Изменение конфигураций «не админами»
- Повышение привилегий
- Выявление несанкционированных сервисов
- Обнаружение НСД (вход под учетной записью уволенного сотрудника)
- Отсутствие антивирусной защиты на новом установленном компьютере
- Изменение критичных конфигураций с VPN подключений
- Контроль выполняемых команд на серверах и сетевом оборудовании
- Аудит изменений конфигураций (сетевых устройств, приложений, ОС)
- Выполнение требований Законодательства и регуляторов (PCI DSS, СТО БР, ISO 27xx)
- Аномальная активность пользователя (массовое удаление/копирование)
- Обнаружение вирусной эпидемии
- Обнаружение уязвимости по событию об установке софта
- Оповещение об активной уязвимости по запуску ранее отключенной службы
- Обнаружение распределенных по времени атаках
- Влияние отказа в инфраструктуре на бизнес-процессы

ВЧЕРА СЕГОДНЯ

SIEM

Какова причина роста функционала SIEM систем?

- Потребность?
- Отсутствие персонала?
- Рост уровня угроз?



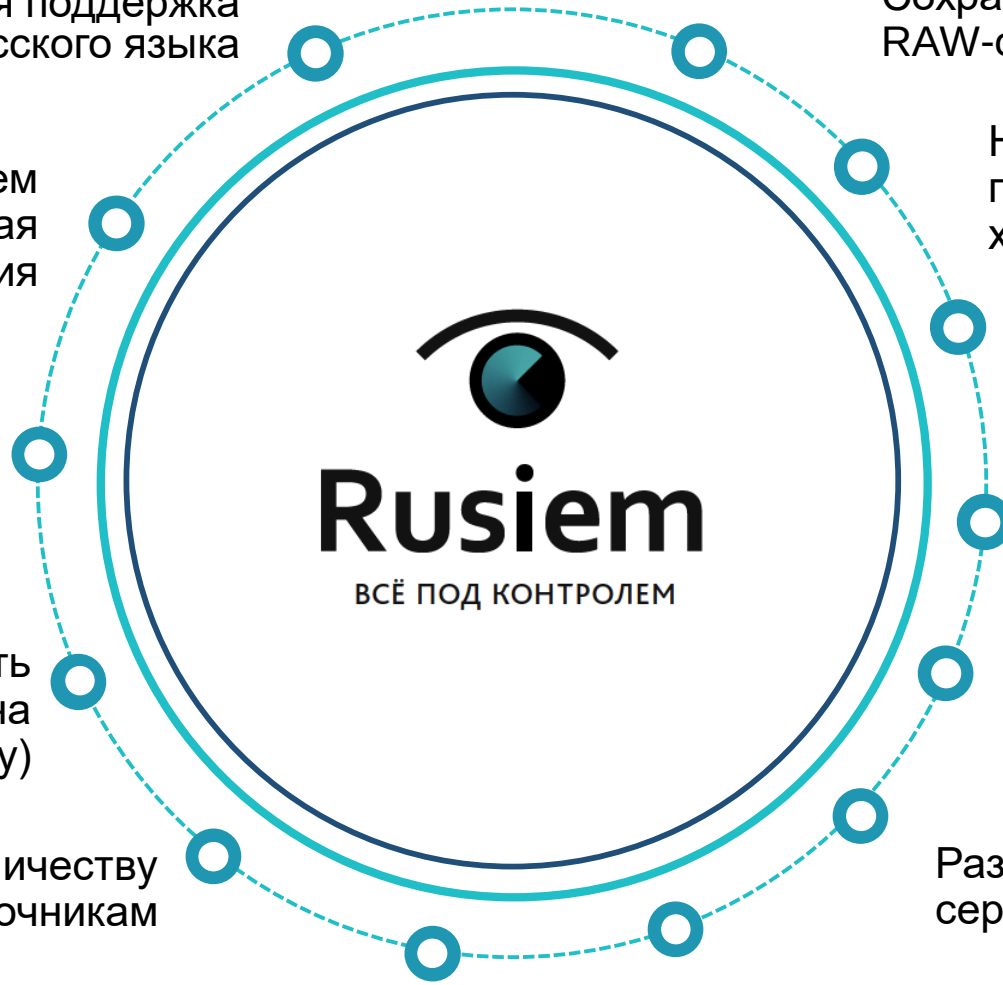
СЕГОДНЯ ЗАВТРА

SIEM

Направление развития SIEM систем очень обширно и выбор остается за Вами, что необходимо именно Вам.

Нормализация	Asset Management	SOC	Threat Intelligence	UBA
Симптоматика	Vulnerability management	GRC	DL/ML/AI	SOAR

КОНКУРЕНТНЫЕ ПРЕИМУЩЕСТВА



Полная поддержка русского языка

Сохранение исходных RAW-событий

Приведенная к общем формату объектная нормализация

Нет ограничений по размеру архивного хранилища

Коннекторы от производителя

Встроенная управляемая и редактируемая корреляция

Real-time и историческая корреляция

Высокая производительность (Свыше 90000 событий на одну ноду)

Наличие собственных модульных агентов

Нет ограничений по количеству событий и источникам

Разделение нагрузки на несколько серверов или виртуальных машин

Легкая вертикальная масштабируемость

#CODEIB

СПАСИБО
ЗА ВНИМАНИЕ

m.stepchenkov@rusiem.com