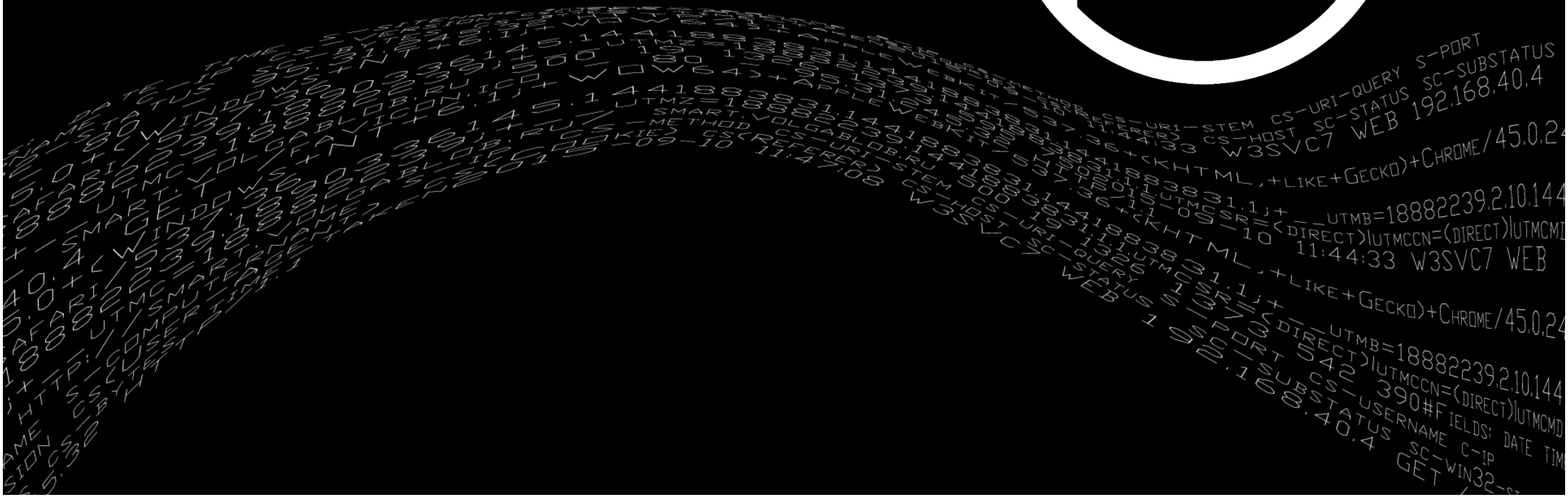
Автоматизация SOC: управление инцидентами

Новые возможности Smart Monitor

VB-Trend 2019 plan>b VolgaBlob



Функциональные возможности

VB-Trend 2019 plan>b VolgaBlob

Автоматизированное и ручное создание инцидентов

Интеграция с профилированием

Оповещение о произошедших инцидентах

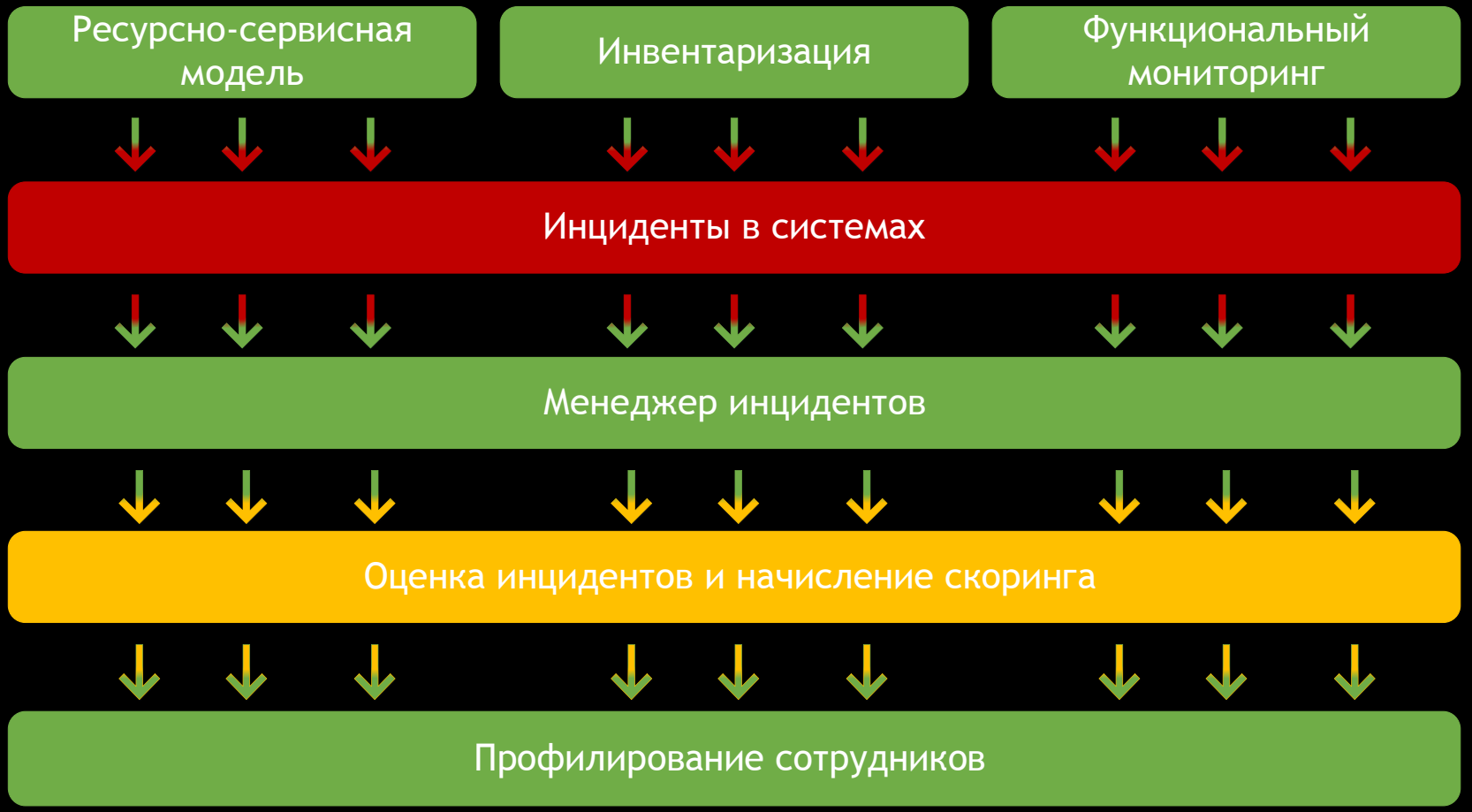
Отчетность о произошедших инцидентах

Оповещение об изменении и назначении инцидентов

Поддержка линий обработки инцидентов (SOC)

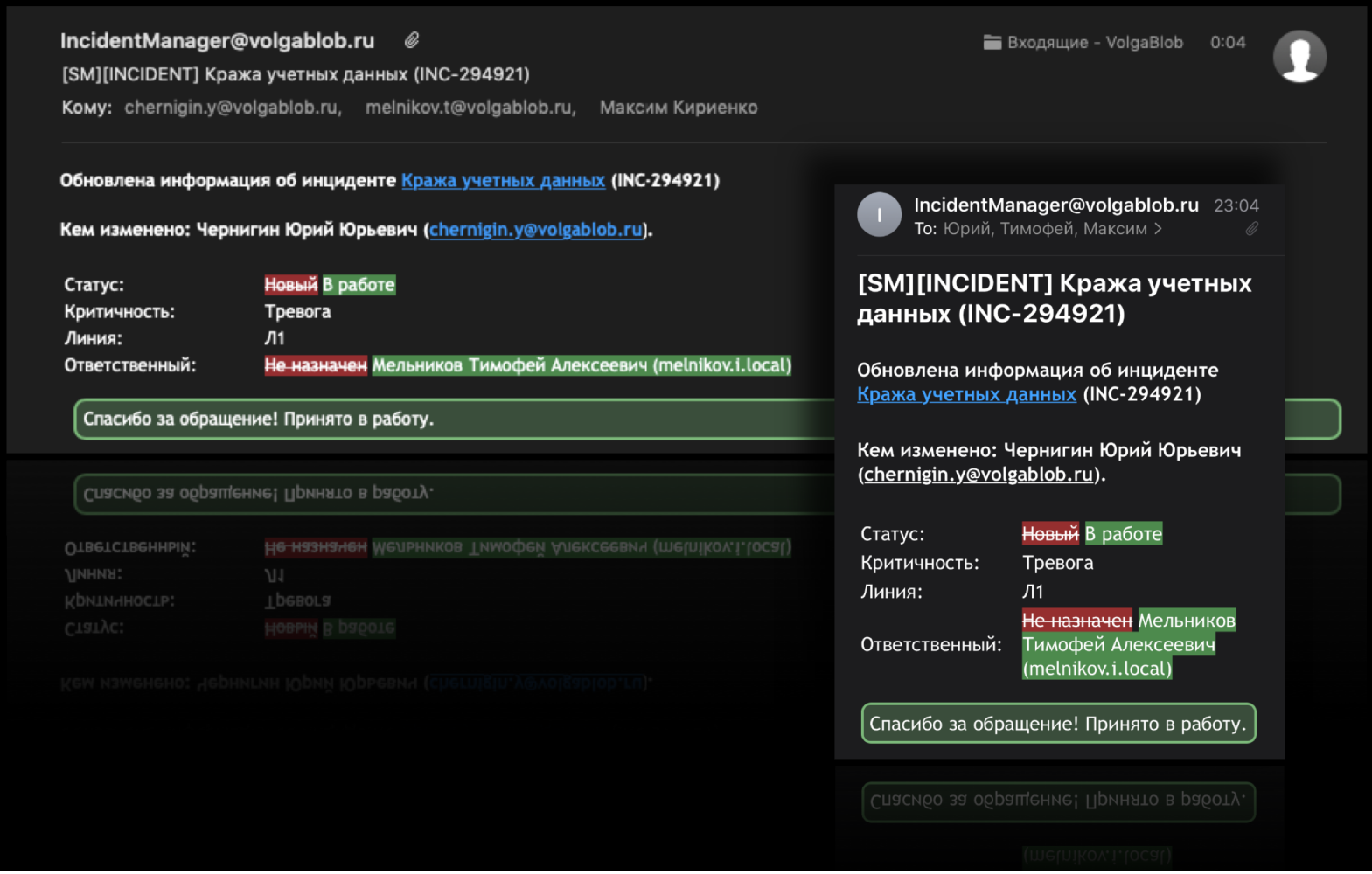
Управление инцидентами

Интеграция с модулями Smart Monitor



Оповещение об инцидентах

VB-Trend 2019 plan>b VolgaBlob

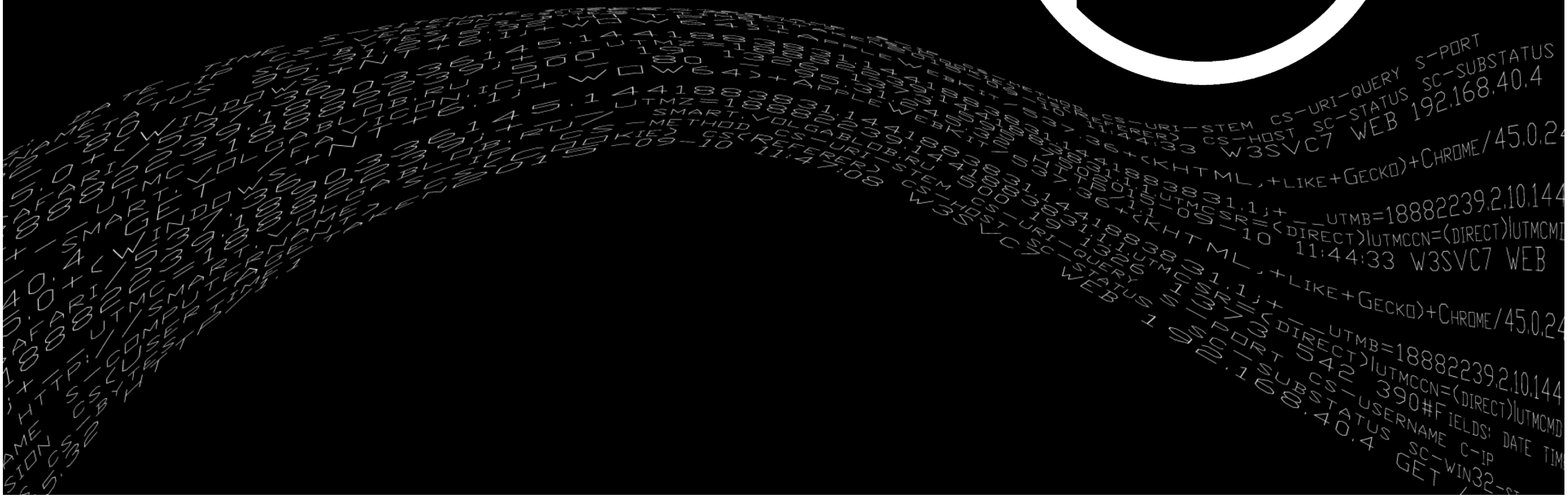


Профилирование сотрудников

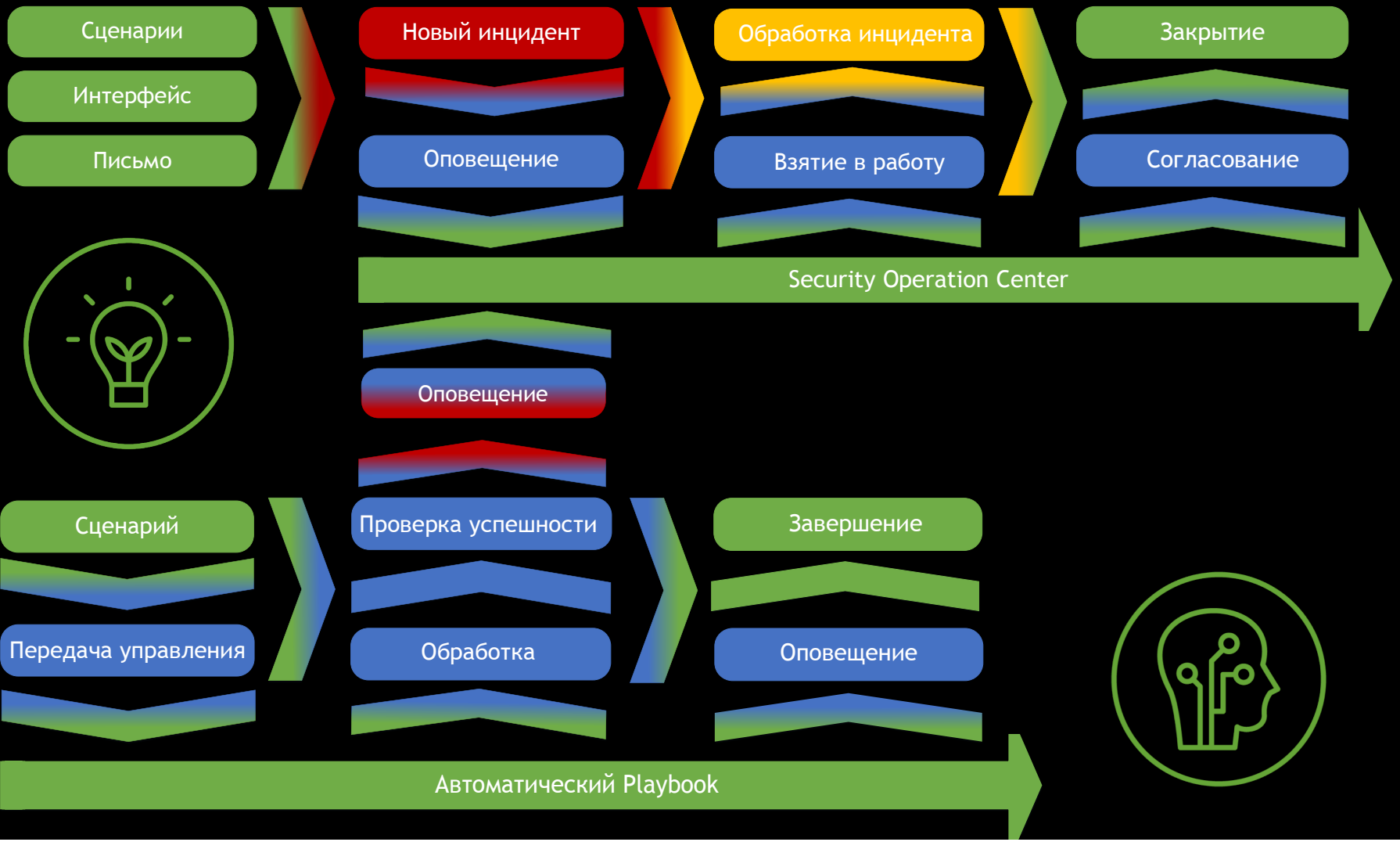
VB-Trend 2019 plan>b VolgaBlob

- Начисление скоринг-балла на основе произошедших инцидентов.
- Расчет индекса соответствия сотрудников показателям:
  - Трудовая дисциплина.
  - Информационная безопасность.
  - Бизнес процессы.
- Создании инцидентов и оповещение при понижении индекса соответствия контролируемых единиц:
  - Филиал.
  - Департамент.
  - Сотрудник.

Демонстрация!



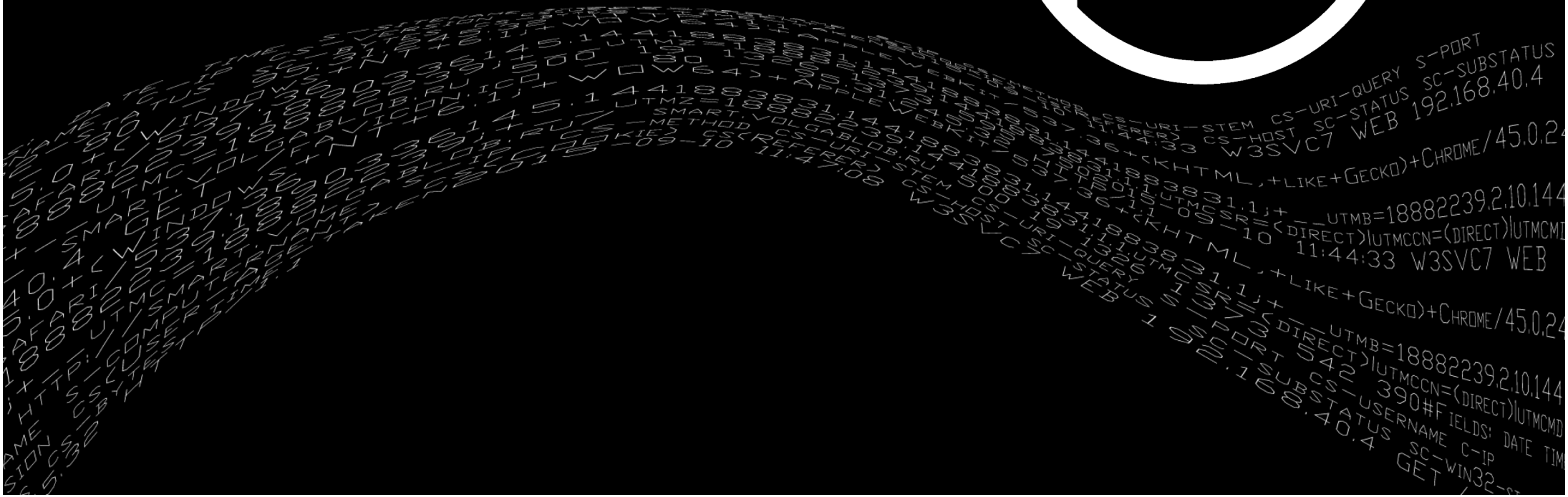
Workflow обработки инцидентов



Спасибо за внимание!

… какие тут могут быть вопросы? :)

VB-Trend 2019
plan>b
VolgaBlob



Опрос

VB-Trend 2019 plan>b VolgaBlob

На чем следует делать основной акцент при расследовании инцидентов в SOC?

- ❑ Объекты мониторинга (компоненты инфраструктуры)
- ❑ Субъекты мониторинга (сотрудники или внешние пользователи)
- ❑ Процессы/сервисы (метрики KPI/SLA)
- ❑ Другое

Поделитесь мнением, пожалуйста!