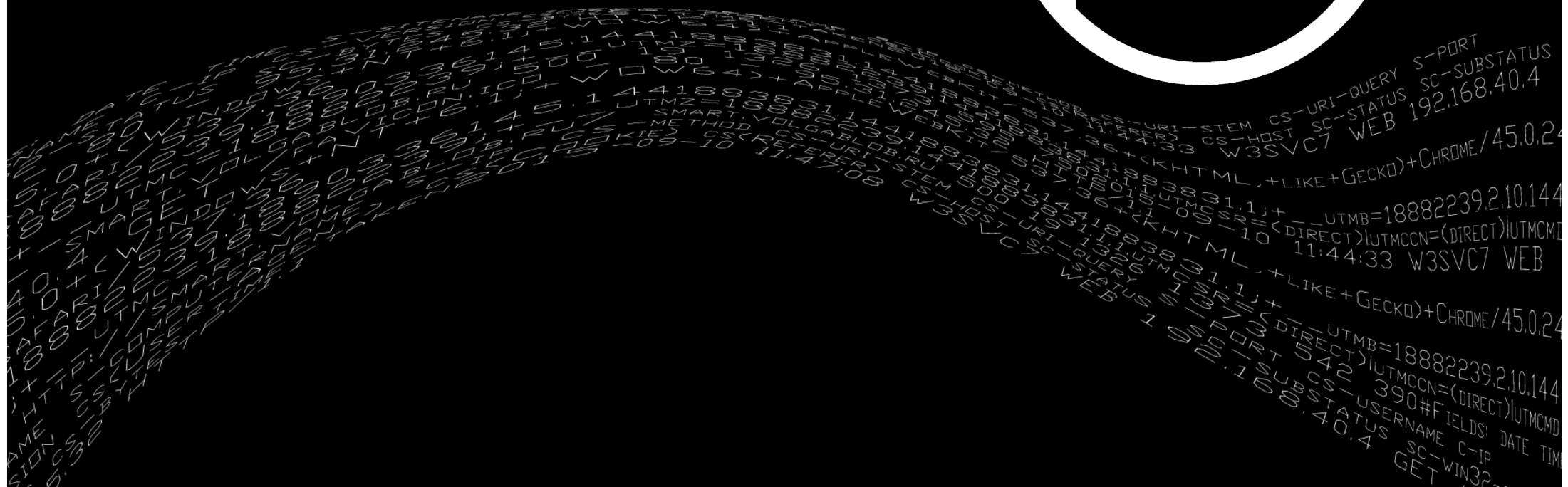


Автоматизация SOC: управление инцидентами

Новые возможности Smart Monitor



Функциональные возможности

Автоматизированное и ручное создание инцидентов

Интеграция
с профилированием

Оповещение о произошедших инцидентах

Отчетность о произошедших инцидентах

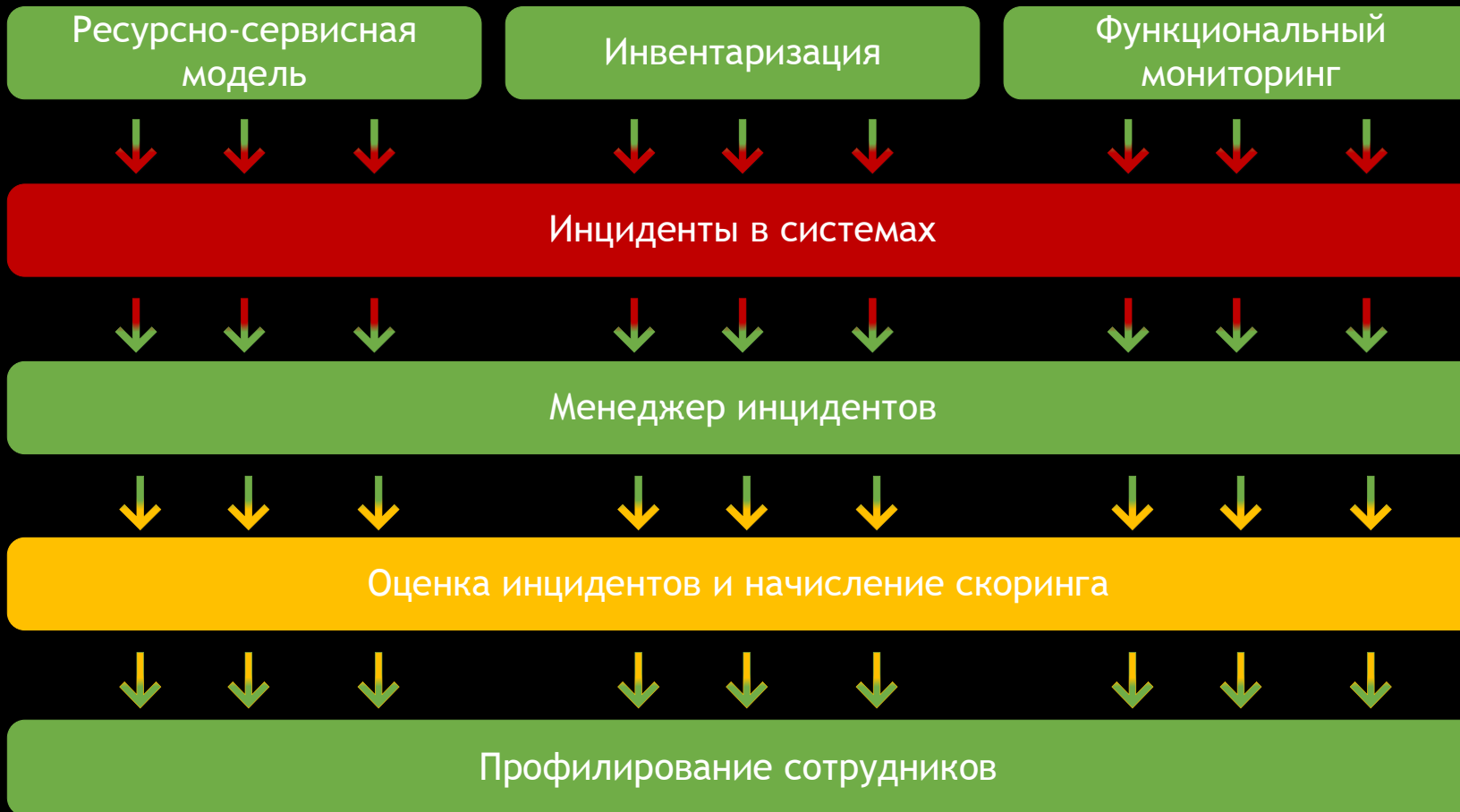


Оповещение об изменении и назначении инцидентов



Поддержка линий
обработки инцидентов
(SOC)

Управление
инцидентами

Интеграция с модулями Smart Monitor



Оповещение об инцидентах

IncidentManager@volgablob.ru  Входящие - VolgaBlob 0:04 

[SM][INCIDENT] Кража учетных данных (INC-294921)
Кому: chernigin.y@volgablob.ru, melnikov.t@volgablob.ru, Максим Кириенко

Обновлена информация об инциденте [Кража учетных данных \(INC-294921\)](#)

Кем изменено: Чернигин Юрий Юрьевич ([chernigin.y@volgablob.ru](#)).

Статус: **Новый В работе**
Критичность: Тревога
Линия: Л1
Ответственный: **Не назначен** Мельников Тимофей Алексеевич ([melnikov.i.local](#))

Спасибо за обращение! Принято в работу.

Спасибо за обращение! Принято в работу.

Ответственный: **Не назначен** Мельников Тимофей Алексеевич ([melnikov.i.local](#))
Линия: Л1
Критичность: Тревога
Статус: **Новый В работе**

Кем изменено: Чернигин Юрий Юрьевич ([chernigin.y@volgablob.ru](#)).

Статус: **Новый В работе**
Критичность: Тревога
Линия: Л1
Ответственный: **Не назначен** Мельников Тимофей Алексеевич ([melnikov.i.local](#))

Спасибо за обращение! Принято в работу.

Спасибо за обращение! Принято в работу.

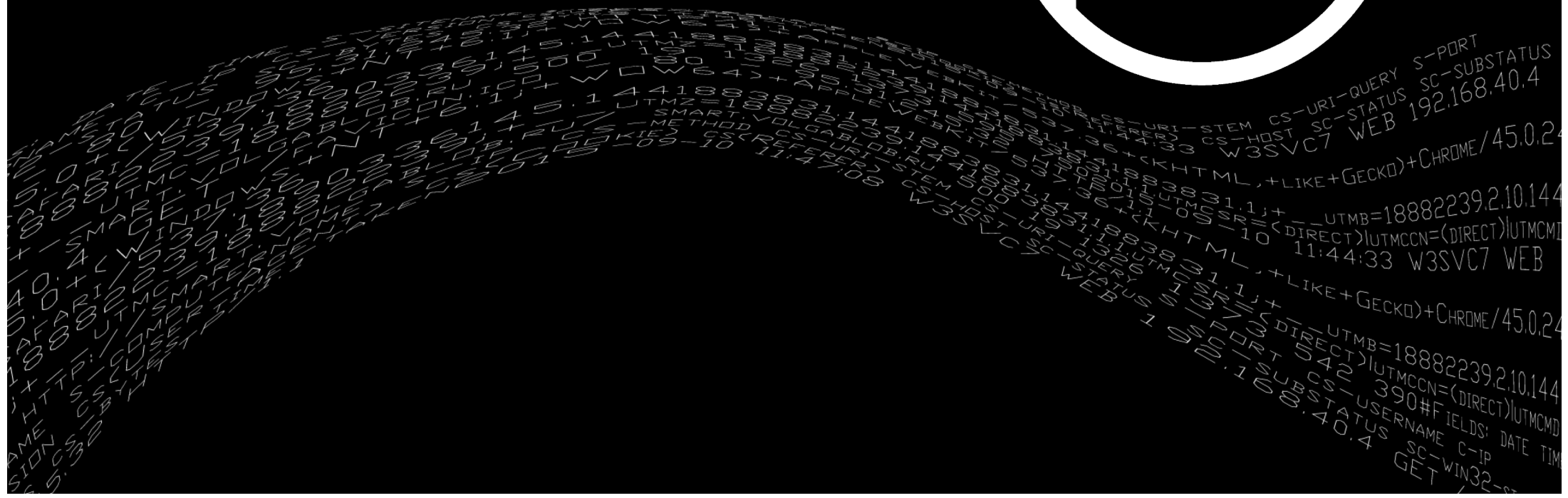
(melnikov.i.local)

Профилирование сотрудников

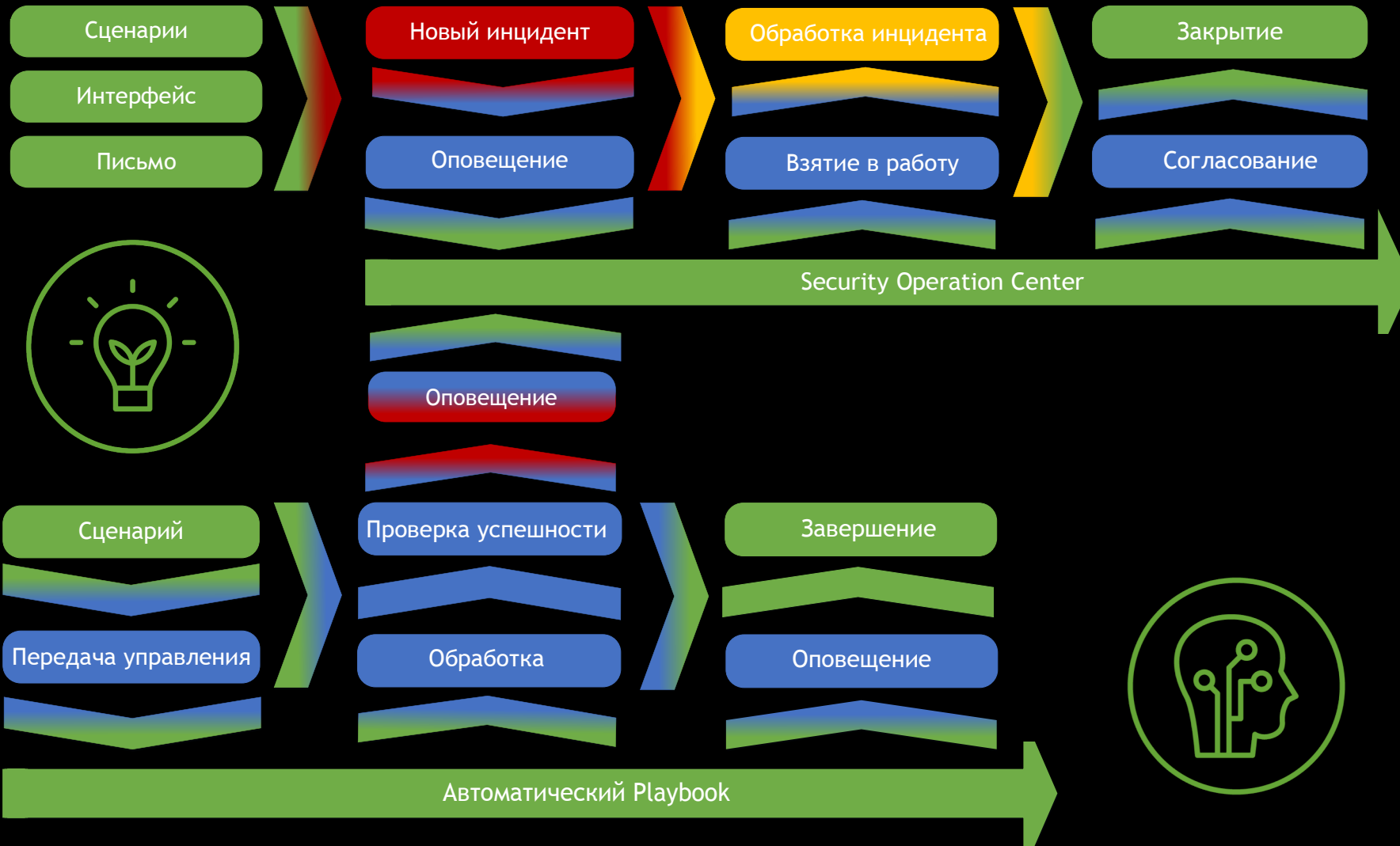
- Начисление **скоринг-балла** на основе произошедших инцидентов.
- Расчет **индекса соответствия** сотрудников показателям:
 - Трудовая дисциплина.
 - Информационная безопасность.
 - Бизнес процессы.
- Создании **инцидентов** и оповещение при понижении индекса соответствия контролируемых единиц:
 -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



Демонстрация!



Workflow обработки инцидентов



Спасибо за внимание!
... какие тут могут быть вопросы? :)



Опрос

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!

