UserGate

В здоровом SOC здоровое реагирование

Дмитрий Чеботарев
менеджер по развитию продукта

Дмитрий Шулинин
SOC Lead

Задача

- **Дано:**
  - определены границы объекта защиты (инвентаризация);
  - определены риски ИБ, а на их основе то, что необходимо мониторить SOC;
  - набор технических средств;
  - аналитики необходимой квалификации.

- **Требуется:**
  - максимально эффективно построить процесс реагирования на инциденты ИБ.

Коротко о главном

- документирование;
- взаимодействие;
- инструментарий;
- проверка и улучшение.

Документирование

UserGate

- общий процесс реагирования на инциденты ИБ;
- плейбуки (хорошо, но не обязательно);
- инструкции по работе с инструментарием (как снять дамп, как проверить PDF, как анализировать IOC и т.п.).

Взаимодействие или «кто есть who?»

UserGate

- внутри SOC – между разными группами аналитиков, командой форензики;
- с владельцами защищаемых активов;
- с внешними подрядчиками и партнерами;
- с юридическим отделом;
- с PR.

Инструментарий

UserGate

- SIEM или лог-менеджмент система, позволяющая гибко работать с данными;
- сырые логи напрямую из IT-систем,
- SOAR/IRP для упрощения и автоматизации процесса реагирования;
- песок;
- Threat Hunting, анализ дампов и т.п:
  - ❑ THOR lite;
  - ❑ Hayabusa;
  - ❑ Chainsaw;
  - ❑ Zircolite.

Этапы развития SIEM

UserGate

Log Manager

- сбор логов;
- дашборды и виджеты;
- отчеты.

Классический SIEM

- правила корреляции;
- инциденты
- анализ.

Экосистемный SIEM

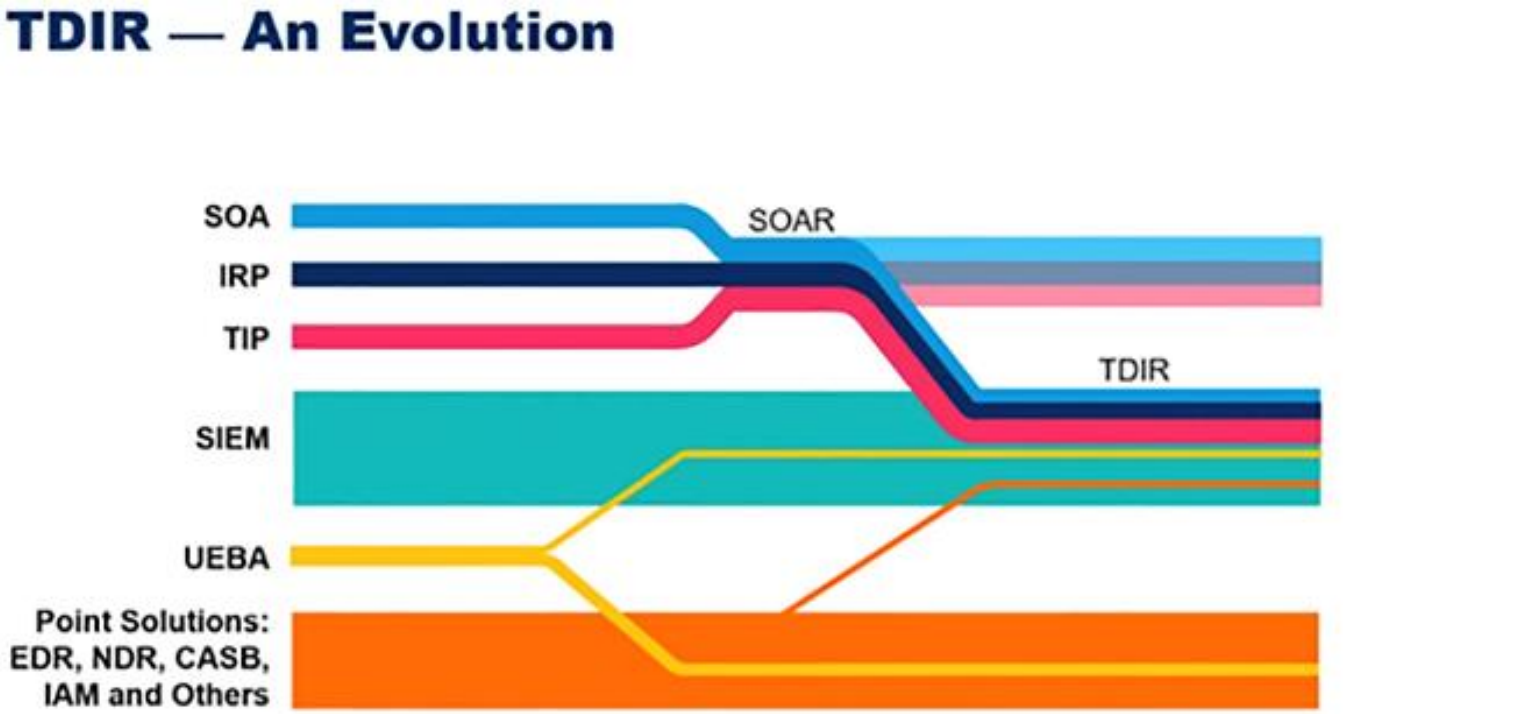
- улучшение логирования за счет экосистемных продуктов;
- увеличенный функционал системы.

Где взяли экспертизу?

Где взяли экспертизу?

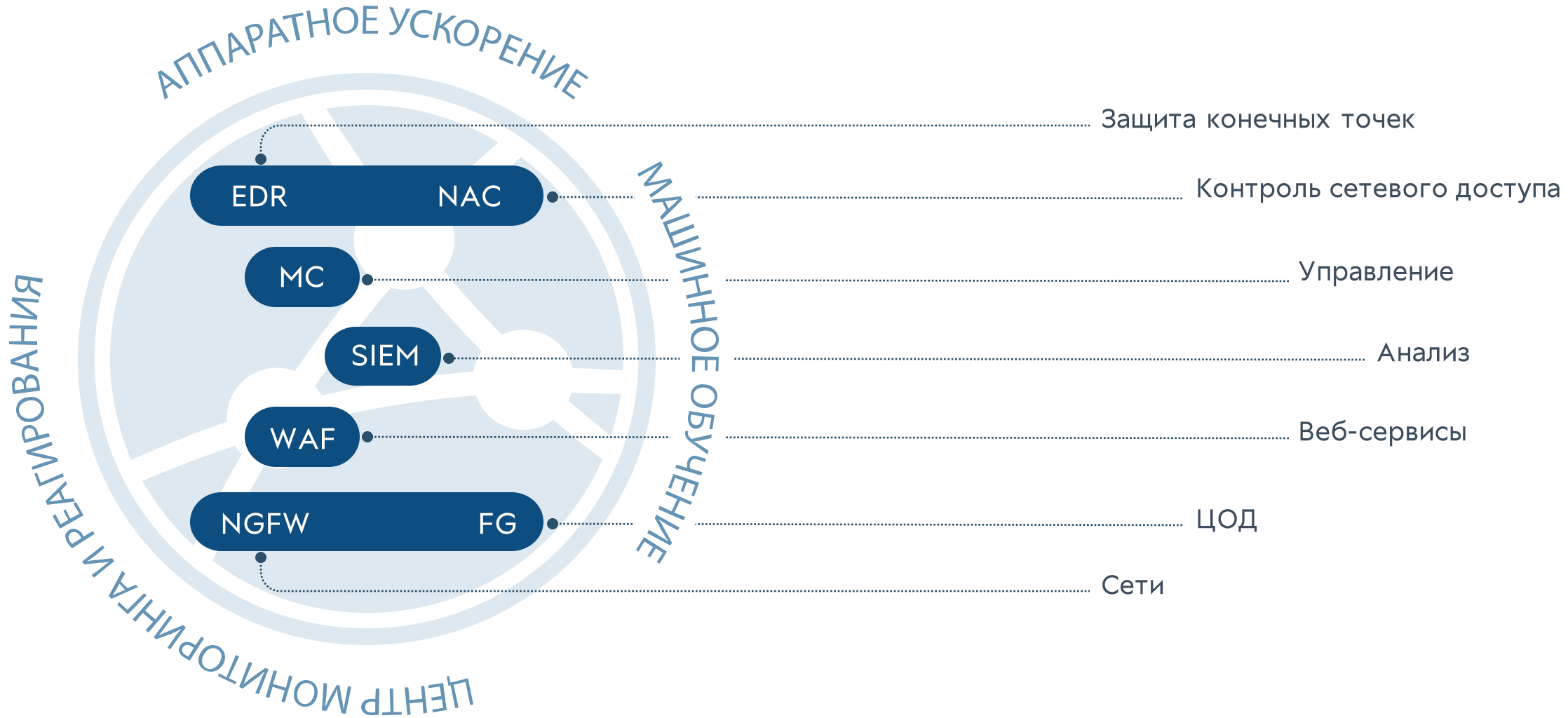
Сами написали

SIEM-системы должны эволюционировать!



UserGate SUMMA

100% видимость событий безопасности



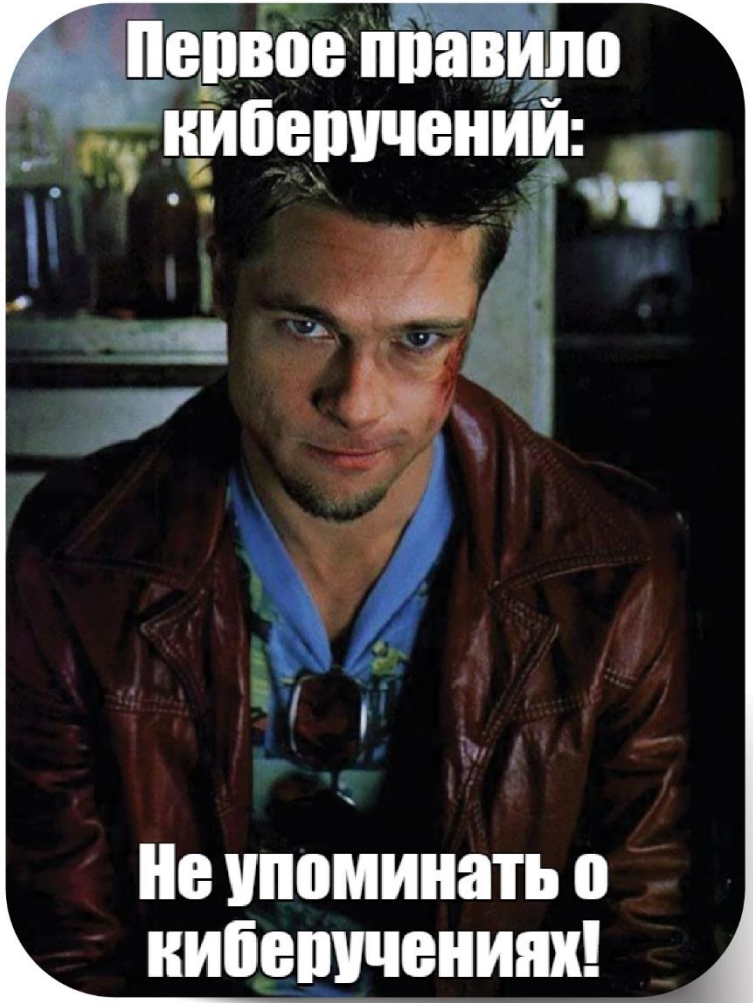
Преимущества

- готовое решение «из коробки»;
- простая настройка и внедрение;
- готовая экспертиза от специалистов Центра мониторинга и реагирования UserGate;
- подключаемые источники данных для обогащения событий и расследования инцидентов;
- интеграция с ГосСОПКА;
- широкий спектр поддерживаемых платформ и протоколов для интеграции;
- автоматизация реагирования;
- возможность расширения функциональности лицензией UserGate Log Analyzer.

Проверка и улучшение

- **Пентесты:**
  - выстроить взаимодействие и полномочия по реагированию.

- **Киберучения:**
  - желательно иметь свой RedTeam;
  - никому не говорить о киберучениях.



Тестирование UserGate SIEM

Отправьте заявку на тестирование решений UserGate

sales@usergate.ru

8 (800) 500-40-32

UserGate

Спасибо за внимание!

Вопросы?

Дмитрий Чеботарев
менеджер по развитию продукта

Дмитрий Шулинин
SOC Lead