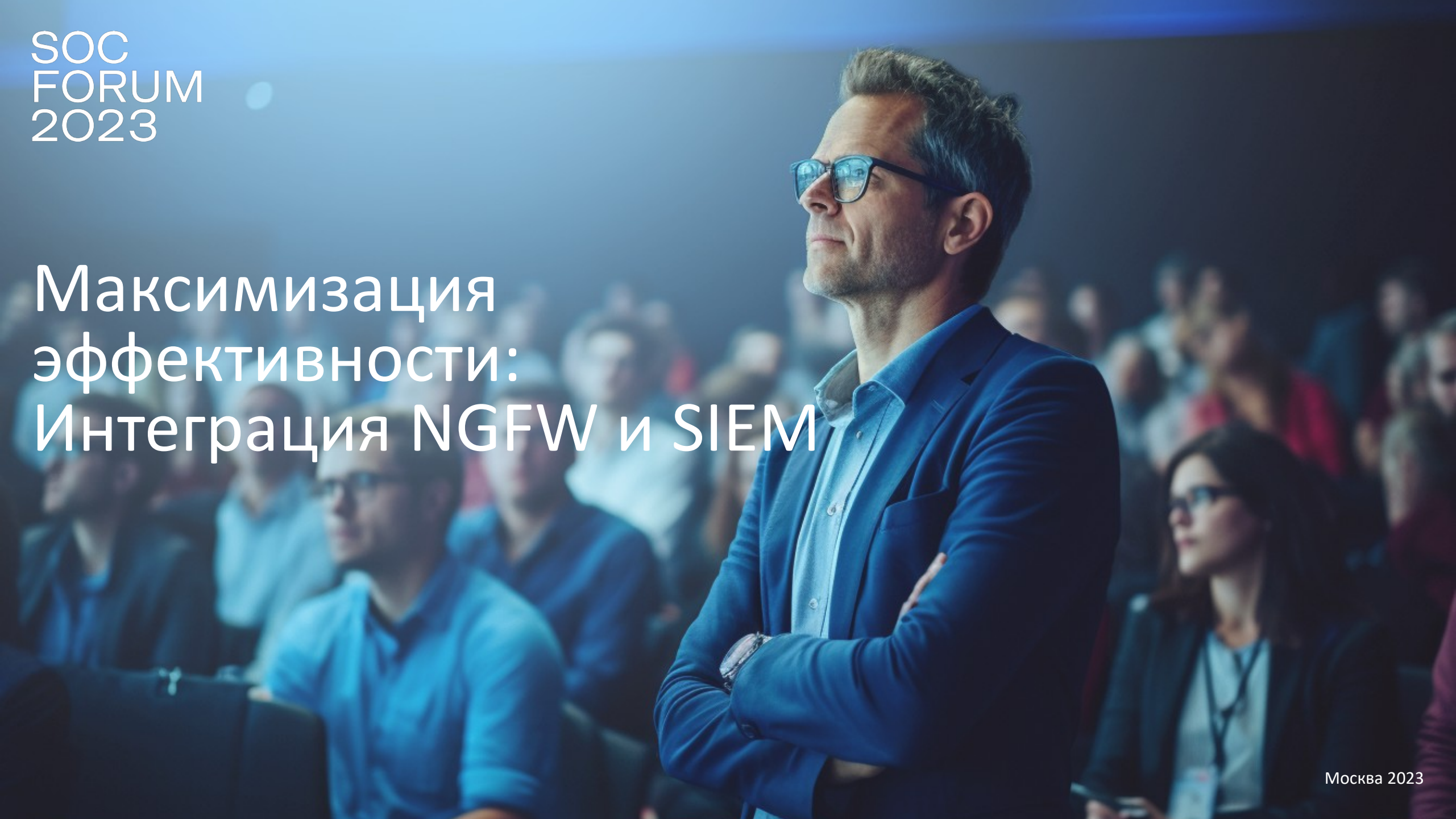
SOC
FORUM
2023

Максимизация эффективности: Интеграция NGFW и SIEM



Москва 2023

SOC
FORUM
2023

Гальченко Данил

Код
Безопасности

Ключевые вопросы

SOC FORUM 2023

- Какие данные надо передавать из NGFW для повышения эффективности SOC?
- Как эти данные надо обработать для повышения эффективности SOC?
- Какие данные имеет смысл оставить внутри системы мониторинга NGFW ?

Какие данные надо передавать и обрабатывать для повышения эффективности SOC?

SOC FORUM 2023

- Заблокированные соединения и трафик
- Успешные и неудачные попытки входа
- Атаки и вредоносные действия
- События изменения конфигурации и обновления ПО
- События безопасности приложений

Заблокированные соединения и трафик

SOC FORUM 2023

Какие данные надо передавать из NGFW для повышения эффективности SOC?

- Попытки НСД
- Заблокированные правилами соединения
- Аномальная активность в трафике
- Ошибки конфигурации инфраструктуры

Как эти данные надо обработать для повышения эффективности SOC?

- Проверка информации о соединениях на наличие совпадений IP/URL в актуальных базах IoC
- Корреляция с другими событиями для выявления целенаправленных атак

Какие данные имеет смысл оставить внутри системы мониторинга NGFW?

- Разрешенные соединения
- Данные с определенными MIME-типами содержимого

Успешные и неудачные попытки входа

SOC FORUM 2023

Какие данные надо передавать из NGFW для повышения эффективности SOC?

- Попытки входа
- Атаки типа «перебор пароля»
- Аномальная активность, связанная с использованием учетных данных
- Методы и сценарии авторизации и аутентификации

Как эти данные надо обработать для повышения эффективности SOC?

- Создание правил/пользовательских сигнатур и механизмов определения аномальных попыток входа
- Необходимо учитывать метод входа, разделить реагирование по типам попыток

Какие данные имеет смысл оставить внутри системы мониторинга NGFW?

- События, явно определенные как False Positive

Атаки и вредоносные действия

SOC FORUM 2023

Какие данные надо передавать из NGFW для повышения эффективности SOC?

- Попытки эксплуатации уязвимостей
- Попытки DoS – атак
- Попытки внедрения ВПО
- Подозрительная сетевая активность
- Несвойственные действия со стороны УЗ

Как эти данные надо обработать для повышения эффективности SOC?

- Создание пользовательских сигнатур, основанных на активности в инфраструктуре
- Внедрение механизмов корреляции и агрегации

Какие данные имеет смысл оставить внутри системы мониторинга NGFW?

- Сработки сигнатур, дающих False positive результат

События изменения конфигурации и обновления ПО

SOC FORUM 2023

Какие данные надо передавать из NGFW для повышения эффективности SOC?

- Изменения конфигураций оборудования
- Контроль обновления ПО
- Изменения политик безопасности ключевых устройств и модулей NGFW

Как эти данные надо обработать для повышения эффективности SOC?

- Документирование всех изменений в конфигурации сетевых устройств
- Проверка изменений на соответствие политикам безопасности и выявление аномалий

Какие данные имеет смысл оставить внутри системы мониторинга NGFW?

- События обновлений ПО и конфигурации с устройств, не имеющих влияния на функционирование и управление инфраструктурой в целом

События безопасности приложений

SOC FORUM 2023

Какие данные надо передавать из NGFW для повышения эффективности SOC?

- Попытки использования запрещенных приложений
- Сбор полных данных об активности «опасных» приложений
- События, указывающие на потенциальные угрозы нарушения политик безопасности

Как эти данные надо обработать для повышения эффективности SOC?

- Необходимо ввести классификацию приложений
- Создание правил для фиксации нарушения политики безопасности

Какие данные имеет смысл оставить внутри системы мониторинга NGFW?

- Статистика использования приложений
- Доступ к разрешенным приложениям

SOC FORUM 2023

На что еще надо обратить внимание для максимизации эффективности

На что еще надо обратить внимание для максимизации эффективности

SOC FORUM 2023

Приоритезация событий

Мониторинг производительности системы

Внедрение передовых технологий

Агрегация и анализ

Ошибки, которые приводят к повышенной нагрузке

SOC FORUM 2023

- Недостаточная фильтрация событий
- Неоптимизированные запросы
- Неоднородные форматы логов
- Отсутствие кеширования данных

Ошибки, которых следует избегать при совместной настройке NGFW и SIEM

SOC FORUM 2023

- Неправильная конфигурация правил МЭ
- Недостаточная детализация логирования
- Несовместимость форматов логов
- Отсутствие регулярного мониторинга и аудита
- Недостаточное обновление и мониторинг угроз
- Неправильная конфигурация режимов работы
- Неправильная интеграция с другими системами безопасности

С какими угрозами у NGFW могут возникнуть трудности, и как с ними справиться?

SOC FORUM 2023

- Атаки “Zero-day”
- Социальная инженерия и фишинг
- Утечки данных через нестандартные каналы
- Внутренние угрозы
- Атаки на уровне WEB-приложений
- DDoS атаки

Общие выводы

SOC FORUM 2023

- Оптимизация взаимодействия на протяжении всего жизненного цикла проекта
- Важно уделять внимание специфике инфраструктуры
- Важно оставлять возможность для масштабирования систем защиты
- Необходимо вести процесс мониторинга ресурсов средств защиты
- Необходимо резервирование архивных данных SIEM для оптимизации ресурсов
- Важно определить события, требующие предварительной обработки перед попаданием в SIEM

SOC FORUM 2023

+7 (495) 982-30-20
info@securitycode.ru

Москва, 1-й Нагатинский проезд, д.10, стр.1