ПРОЦЕССЫ И СРЕДСТВА ВЕДОМСТВЕННЫХ/КОРПОРАТИВНЫХ ЦЕНТРОВ, НЕОБХОДИМЫЕ ДЛЯ РЕШЕНИЯ ЗАДАЧ ГОССОПКА

Новиков А.О. – 8 Центр ФСБ России

Ведомственный/корпоративный центр ГосСОПКА

CERT

CSIRT

SIEM

SOC

MSSP

MDR

CERT - Computer Emergency Response Team
CSIRT - Computer Security Incident Response Team
SIEM - Security Information and Event Management

SOC - Security Operations Center
MSSP - Managed Security Services Providers
MDR - Managed Detection and Response

Ведомственный/корпоративный центр ГосСОПКА

CERT

CSIRT

SIEM

SOC

MDR

MSSP

CERT - Computer Emergency Response Team
CSIRT - Computer Security Incident Response Team
SIEM - Security Information and Event Management

SOC - Security Operations Center
MSSP - Managed Security Services Providers
MDR - Managed Detection and Response

“Портфель" классического SOC

- централизованный сбор и управление событиями информационной безопасности
- мониторинг/выявление массовых компьютерных атак на защищаемые информационные ресурсы (корреляционные правила, сигнатуры)
- выявление компьютерных инцидентов
- управление и долгосрочное хранение информации об инцидентах
- содействие в реагировании на типовые инциденты, вызванные массовыми компьютерными атаками
- администрирование средств защиты информации
- инвентаризация активов, паспортизация информационных систем
- поиск уязвимостей в сетевых сервисах и ПО, выявление ошибок в конфигурациях и архитектуре
- документирование процедур и результатов мониторинга, а также результатов реагирования

SOC - Security Operations Center

“Портфель" современного SOC

- централизованный сбор и управление событиями информационной безопасности
- мониторинг/выявление массовых компьютерных атак на защищаемые информационные ресурсы (корреляционные правила, сигнатуры)
- выявление компьютерных инцидентов
- управление и долгосрочное хранение информации об инцидентах
- содействие в реагировании на типовые инциденты, вызванные массовыми компьютерными атаками
- администрирование средств защиты информации
- инвентаризация активов, паспортизация информационных систем
- поиск уязвимостей в сетевых сервисах и ПО, выявление ошибок в конфигурациях и архитектуре
- документирование процедур и результатов мониторинга, а также результатов реагирования

- углубленная аналитика по результатам мониторинга, написание сигнатур и корреляционных правил
- работа с дополнительными источниками информации об угрозах по подписке
- локальное реагирование на компьютерные инциденты, работа с артефактами атаки, NetFlow и т.п.
- локализация последствий компьютерного инцидента
- защита бренда
- профилирование системы обеспечения информационной безопасности под политику организации, внедрение best practice

SOC - Security Operations Center

Ведомственный/корпоративный центр ГосСОПКА

CERT

CSIRT

SIEM

SOC

MSSP

MDR

CERT - Computer Emergency Response Team
CSIRT - Computer Security Incident Response Team
SIEM - Security Information and Event Management

SOC - Security Operations Center
MSSP - Managed Security Services Providers
MDR - Managed Detection and Response

Side note: Outsource Selectively?

SOC/MSSP hybrid models:

1. MSSP for Level 1/in-house for triage.
2. MSSP at night, SOC for daytime/workdays.
3. MSSP for basic monitoring, advanced — in-house.
4. MSSP for DMZ alerts, SOC for inside
5. MSSP helps manage SIEM
6. Partner helps with serious incident IR

"MSSP's business is … business,
not your security"

Gartner

“Портфель" современного SOC

- централизованный сбор и управление событиями информационной безопасности
- мониторинг/выявление массовых компьютерных атак на защищаемые информационные ресурсы (корреляционные правила, сигнатуры)
- выявление компьютерных инцидентов
- управление и долгосрочное хранение информации об инцидентах
- содействие в реагировании на типовые инциденты, вызванные массовыми компьютерными атаками
- администрирование средств защиты информации
- инвентаризация активов, паспортизация информационных систем
- поиск уязвимостей в сетевых сервисах и ПО, выявление ошибок в конфигурациях и архитектуре
- документирование процедур и результатов мониторинга, а также результатов реагирования

- углубленная аналитика по результатам мониторинга, написание сигнатур и корреляционных правил
- работа с дополнительными источниками информации об угрозах по подписке
- локальное реагирование на компьютерные инциденты, работа с артефактами атаки, NetFlow и т.п.
- локализация последствий компьютерного инцидента
- защита бренда
- профилирование системы обеспечения информационной безопасности под политику организации, внедрение best practice

SOC - Security Operations Center

Ведомственный/корпоративный центр ГосСОПКА

CERT

CSIRT

SIEM

SOC

MSSP

MDR

CERT - Computer Emergency Response Team
CSIRT - Computer Security Incident Response Team
SIEM - Security Information and Event Management

SOC - Security Operations Center
MSSP - Managed Security Services Providers
MDR - Managed Detection and Response

“Портфель" современного SOC

- централизованный сбор и управление событиями информационной безопасности
- мониторинг/выявление массовых компьютерных атак на защищаемые информационные ресурсы (корреляционные правила, сигнатуры)
- выявление компьютерных инцидентов
- управление и долгосрочное хранение информации об инцидентах
- содействие в реагировании на типовые инциденты, вызванные массовыми компьютерными атаками
- администрирование средств защиты информации
- инвентаризация активов, паспортизация информационных систем
- поиск уязвимостей в сетевых сервисах и ПО, выявление ошибок в конфигурациях и архитектуре
- документирование процедур и результатов мониторинга, а также результатов реагирования

- углубленная аналитика по результатам мониторинга, написание сигнатур и корреляционных правил
- работа с дополнительными источниками информации об угрозах по подписке
- локальное реагирование на компьютерные инциденты, работа с артефактами атаки, NetFlow и т.п.
- локализация последствий компьютерного инцидента
- защита бренда
- профилирование системы обеспечения информационной безопасности под политику организации, внедрение best practice

SOC - Security Operations Center

Ведомственный/корпоративный центр ГосСОПКА

CERT

CSIRT

SIEM

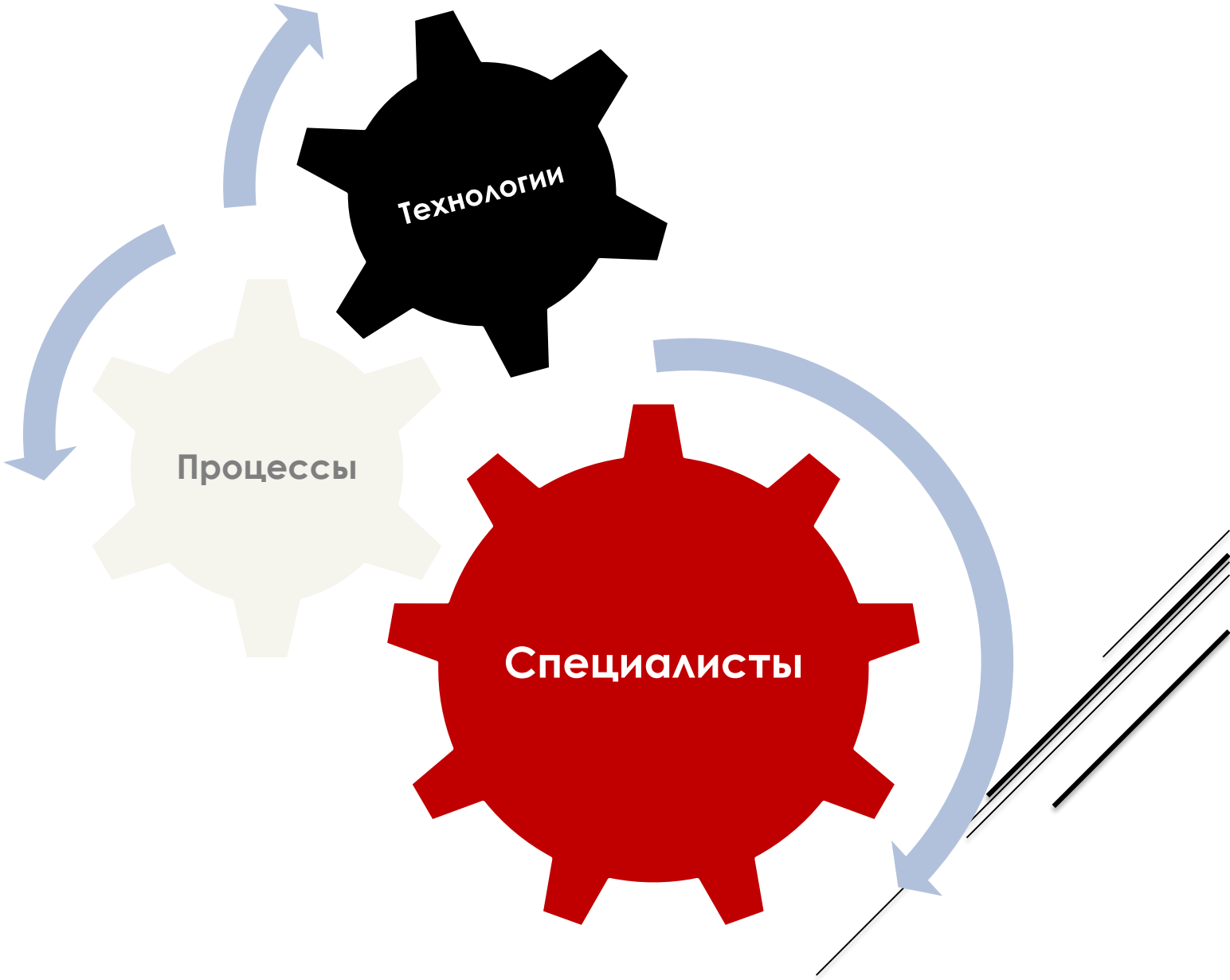
SOC

MSSP

MDR

CERT - Computer Emergency Response Team
CSIRT - Computer Security Incident Response Team
SIEM - Security Information and Event Management

SOC - Security Operations Center
MSSP - Managed Security Services Providers
MDR - Managed Detection and Response


Технологии
Процессы
Специалисты

“Портфель" современного SOC

- централизованный сбор и управление событиями информационной безопасности
- мониторинг/выявление массовых компьютерных атак на защищаемые информационные ресурсы (корреляционные правила, сигнатуры)
- выявление компьютерных инцидентов
- управление и долгосрочное хранение информации об инцидентах
- содействие в реагировании на типовые инциденты, вызванные массовыми компьютерными атаками
- администрирование средств защиты информации
- инвентаризация активов, паспортизация информационных систем
- поиск уязвимостей в сетевых сервисах и ПО, выявление ошибок в конфигурациях и архитектуре
- документирование процедур и результатов мониторинга, а также результатов реагирования

- углубленная аналитика по результатам мониторинга, написание сигнатур и корреляционных правил
- работа с дополнительными источниками информации об угрозах по подписке
- локальное реагирование на компьютерные инциденты, работа с артефактами атаки, NetFlow и т.п.
- локализация последствий компьютерного инцидента
- защита бренда
- профилирование системы обеспечения информационной безопасности под политику организации, внедрение best practice

SOC - Security Operations Center

Спасибо за внимание