Security Operation Center (SOC)

Как специалист по SOC может спасти вашу компанию от кибератак, чего не сможет сделать ИТ-специалист

МегаФон

Станислав Погоржельский

Специалист технологической поддержки

Предпосылки

- Указ Президента РФ от 01.05.2022 № 250
- Необходимость в организации SOC
- Персональная ответственность за инциденты ИБ
- Сложность с наймом ИБ специалиста для SOC
- «Навесить» задачи для Системного Администратора

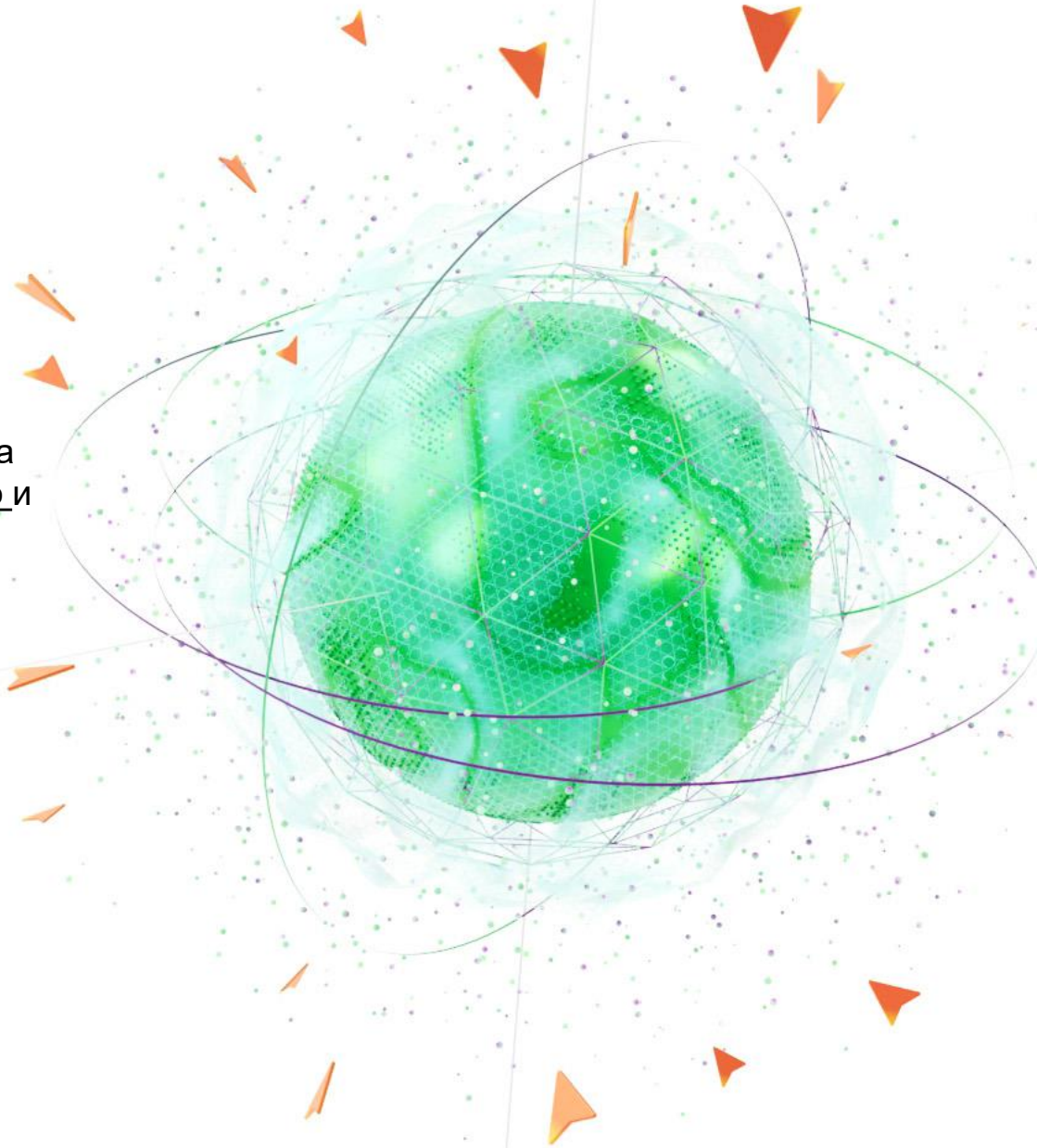
МегаФон

Киберриски

Государственные структуры часто сталкиваются со сложностями в области кибербезопасности. Но дело не только в росте количества и сложности кибератак

На организацию, которую атакуют, повлияет отсутствие квалифицированных кадров в штате, недостаток ресурсов на анализ всех происходящих событий информационной безопасности, а также нехватка времени. А как известно, на инциденты информационной безопасности (ИБ) надо реагировать мгновенно и правильным способом, пока они не причинили значительный ущерб.

Усилить защиту от кибератак и компенсировать нехватку ресурсов поможет Security Operation Center — выделенный центр мониторинга и реагирования на инциденты ИБ, который работает в режиме 24/7 и объединяет в себе опыт тысяч компаний и государственных учреждений.



МегаФон

SOC

Security Operation Center — центр мониторинга и реагирования на инциденты информационной безопасности в режиме 24/7

Анализ событий
и инцидентов

Агрегация событий
ИБ из разных источников

Реагирование
на инциденты

Отчетность
и визуализация данных

МегаФон

Из чего состоит SOC

Команда экспертов ИБ

SIEM

Security Information and Event Management

Платформа для сбора и анализа информации о событиях ИБ

IRP

Incident Response Platform

Платформа для автоматизации реагирования на киберинциденты

МегаФон

Указ Президента РФ от 01.05.2022 № 250

«О дополнительных мерах по обеспечению информационной безопасности Российской Федерации».

Персональная ответственность!

«2. Возложить на руководителей органов (организаций) персональную ответственность за обеспечение информационной безопасности соответствующих органов (организаций).»
П. 2 Указа

Возложить данные функции на существующее структурное подразделение

а) возложить на заместителя руководителя полномочия по обеспечению ИБ, в том числе по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты; б) создать структурное подразделение, осуществляющее функции по обеспечению информационной безопасности, в том числе по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты, либо возложить данные функции на существующее структурное подразделение;
Пп.а) б) п.1 Указа

МегаФон

Сравним Системного Администратора и специалиста SOC

Компетенции системного администратора:
1. Установка и настройка серверного и клиентского ПО.
2. Администрирование сетевой инфраструктуры.
3. Конфигурирование и настройка оборудования и сетевых устройств.
4. Управление доступом пользователей к ресурсам сети.
5. Резервное копирование и восстановление данных.
6. Обеспечение безопасности сети и защита от внешних угроз.
7. Мониторинг состояния сети и устранение возникающих проблем.
8. Участие в проектах по развитию и совершенствованию сети.

Компетенции специалиста SOC:
1. Мониторинг ИБ предприятия.
2. Анализ и обработка информации о возможных угрозах.
3. Разработка и внедрение мер по обеспечению ИБ.
4. Организация системы реагирования на инциденты в ИБ.
5. Координация работы с другими службами предприятия по вопросам безопасности.
6. Разработка и внедрение планов аварийного восстановления в случае атаки.
7. Анализ и сбор статистических данных по безопасности информации.
8. Обучение пользователей основам безопасности информации.

Команда экспертов 24/7

1-я линия

Мониторинг и аналитика событий и инцидентов ИБ — работа по одному готовому сценарию действий: проверка ложноположительных инцидентов ИБ, обогащение инцидента данными, необходимыми для дальнейшего расследования

2-я линия

Техническое реагирование и расследование инцидентов ИБ — работа по нескольким готовым сценариям действий: сдерживание и/или ликвидация последствий инцидента ИБ, выявление первопричины инцидента (например, поиск злоумышленника)

3-я линия

Работа без готовых сценариев действий. Кроме участия в аналитике, реагировании и расследовании, эта линия занимается новых сценариев, правил корреляции, «парсеров» и «коннекторов»

Методолог

Оформление разработанных сценариев в унифицированный вид для дальнейшего использования линиями при помощи инструментов платформы SOAR — Security Orchestration, Automation and Response (в SOC возможны тысячи сценариев)

Сервис-менеджер

Менеджер, ответственный за проект на этапе эксплуатации

МегаФон

Компетенции специалиста SOC

- Знание технологий информационной безопасности;
- Умение работать с защитной антивирусной техникой;
- Опыт работы с **системами детекции инцидентов**;
- **Умение анализировать и оценивать инциденты**;
- Опыт работы с технологиями мониторинга сети;
- Умение использовать **методы анализа данных** для обнаружения атак;
- Знание технологий реакции на угрозы и их противодействие;
- Умение использовать технологии **анализа лог-файлов**;
- Опыт проведения аудита безопасности;
- **Знание законодательства** по безопасности информации;
- Умение разрабатывать и реализовывать политики безопасности;
- Умение проводить обучение работников организации по теме безопасности;
- Умение работать с различными **инструментами анализа и мониторинга безопасности**;
- Умение поддерживать и обновлять систему безопасности организации;
- Опыт работы с технологиями криптографии;
- Опыт работы с системами бизнес континуума.

В каких системах работает специалист SOC

Каждая из этих систем выполняет определенные функции в области безопасности информационных технологий. Специалист SOC использует эти системы для мониторинга, обнаружения и предотвращения угроз безопасности, а также для обработки инцидентов и решения проблем в области безопасности.

1. SIEM (Security Information and Event Management)
2. IDS/IPS (Intrusion Detection/Prevention System)
3. DLP (Data Loss Prevention)
4. EDR (Endpoint Detection and Response)
5. UEBA (User and Entity Behavior Analytics)
6. WAF (Web Application Firewall)
7. PAM (Privileged Access Management)
8. NAC (Network Access Control)
9. VA/VM (Vulnerability Assessment/Vulnerability Management)
10. SOAR (Security Orchestration, Automation and Response)
11. FIM (File Integrity Monitoring)
12. IAM (Identity and Access Management)
13. MDM (Mobile Device Management)
14. EMM (Enterprise Mobility Management)
15. DRM (Digital Rights Management)
16. ATP (Advanced Threat Protection)
17. TIP (Threat Intelligence Platform)
18. MFA (Multi-Factor Authentication)
19. CASB (Cloud Access Security Broker)
20. SWG (Secure Web Gateway)

МегаФон

SIEM

Security Information and Event Management

— **система, которая используется для сбора, анализа и управления событиями безопасности. Она позволяет собирать данные из различных источников, включая системы брандмауэров, системы обнаружения вторжений и системы управления угрозами.**

- **Сбор и агрегация данных:** SIEM получает данные из различных источников, включая логи, события, потоки данных, устройства и приложения.
- **Анализ и корреляция:** SIEM анализирует данные, используя различные методы, такие как машинное обучение, статистические анализы и правила, чтобы выявлять угрозы и аномалии.
- **Реагирование и уведомление:** SIEM может отправлять уведомления о событиях безопасности, генерировать предупреждения и автоматически принимать меры по блокированию или заблокированию угроз.
- **Хранение и архивирование:** SIEM сохраняет данные о событиях безопасности и может предоставлять возможность поиска и доступа к этим данным для анализа и расследования происшествий.
- **Управление рисками:** SIEM помогает оценить риски и улучшить безопасность за счет выявления и устранения уязвимостей в системе.
- **Соответствие нормативным требованиям:** SIEM помогает организациям следить за соблюдением нормативных требований в области безопасности.

МегаФон

IRP

Incident Response Platform

— это специализированное программное обеспечение, которое разработано для обработки инцидентов безопасности. IRP является дополнительным инструментом, который может быть использован вместе с SIEM для обеспечения защиты информации на высоком уровне. Вот несколько функций IRP, которых нет в SIEM:

- **Обнаружение и классификация инцидентов:** IRP может обнаруживать и классифицировать инциденты безопасности в режиме реального времени, используя различные методы, такие как машинное обучение, анализ поведения и т. д.
- **Автоматизация и оркестрация:** IRP может автоматизировать процессы реагирования на инциденты, что позволяет сократить время ответа и уменьшить вероятность ошибок.
- **Коллаборация и координация:** IRP позволяет различным командам безопасности работать вместе и координировать свои действия для эффективного реагирования на инциденты.
- **Документирование и аудит:** IRP предоставляет возможность документировать все действия, связанные с инцидентами, и сохранять их для аудита и последующей аналитики.
- **Управление угрозами:** IRP может интегрироваться с различными системами управления угрозами (Threat Intelligence Platforms), что позволяет быстро определять и реагировать на новые угрозы.

Это не полный список функций IRP, но он демонстрирует, как IRP может дополнить SIEM и усилить общую защиту информации.

МегаФон

Как рассчитать стоимость «своего» SOC

Для расчета стоимости SOC (Security Operations Center) по затратам необходимо учесть следующие факторы:

- **Оборудование и программное обеспечение.** Это включает в себя закупку и настройку серверов, сетевого оборудования, систем мониторинга и управления безопасностью, а также лицензии на программное обеспечение.
- **Персонал.** Необходимо определить количество сотрудников, которые будут работать в SOC, и их зарплаты. Это могут быть аналитики безопасности, инженеры безопасности, администраторы систем и т.д.
- **Обучение и сертификация.** Сотрудники SOC должны иметь соответствующую квалификацию и сертификаты, что требует дополнительных затрат на обучение и сертификацию.
- **Расходы на электроэнергию и коммунальные услуги.** Необходимо учитывать затраты на электричество, охлаждение оборудования и интернет-соединение.
- **Расходы на обслуживание и поддержку.** SOC требует постоянного обслуживания и поддержки, включая техническую поддержку оборудования и программного обеспечения.
- **Расходы на аренду помещения.** Если SOC находится в отдельном помещении, то необходимо учитывать расходы на аренду помещения и его обустройство.

Выводы

Важно обеспечивать **выделенного специалиста SOC**, так как он специализируется на обеспечении безопасности информационных систем, а именно на **обнаружении и предотвращении кибератак** и других угроз. И знаком со специфическими инструментами и методами, необходимыми для этой работы.

IT-специалист (Системный Администратор) ≠ **Выделенный Специалист SOC**

Технологии включают бизнес

Погоржельский Станислав
Специалист технологической поддержке по облачным и инфраструктурным решениям МегаФона