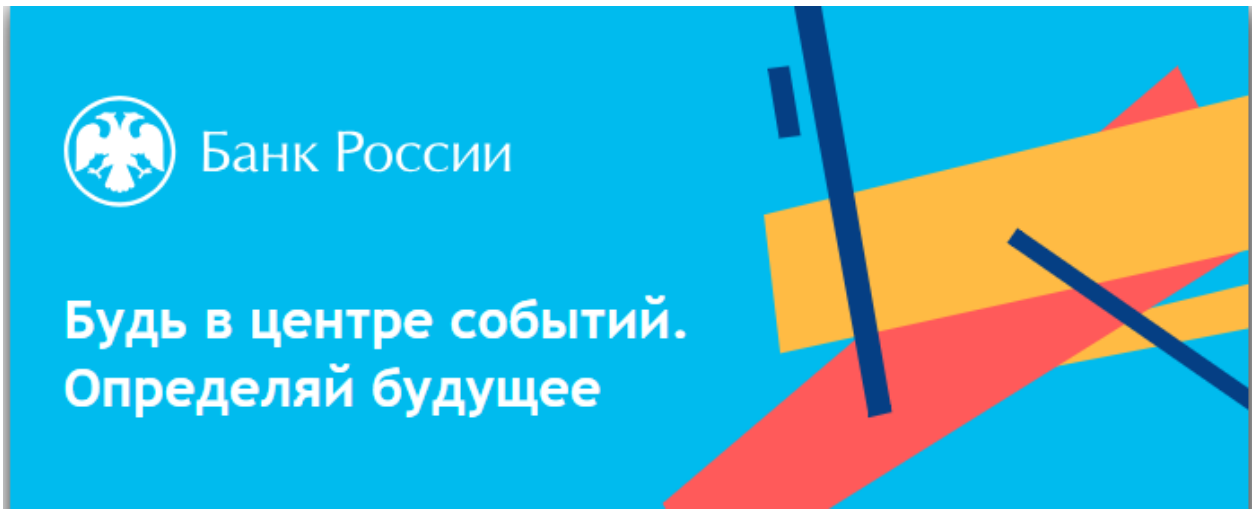

Ведущий инженер по информационной безопасности (SOC)

Центр управления и мониторинга ИБ Департамента безопасности Банка России приглашает в команду Инженеров SOC в области мониторинга и реагирования на инциденты ИБ.
Центр решает широкий спектр задач, направленных на обеспечение кибербезопасности Банка России: мониторинг и реагирование на инциденты кибербезопасности, тестирования на проникновение, управление уязвимостями, эксплуатация решений по обеспечению ИБ, проведение проверок и внутренних аудитов информационной безопасности.
Мы ищем коллегу - единомышленника, который примет участие в повышении зрелости процесса расследования и реагирования на инциденты ИБ в Банке России.

Задачи:

- оперативный мониторинг состояния информационной безопасности в ИТ-инфраструктуре;
- обнаружение, реагирование и расследование инцидентов информационной безопасности;
- контроль выполнения требований нормативных и регламентирующих документов по информационной безопасности эксплуатирующими подразделениями информатизации;
- участие во внедрении программных комплексов автоматизированных банковских систем в части обеспечения информационной безопасности;
- контроль за обеспечением информационной безопасности при выполнении плановых и внеплановых работ в ИТ-инфраструктуре, контроль устранения инцидентов ИБ и высокоприоритетных инцидентов IT;
- рассмотрение документации техно-рабочих проектов в части соответствия требованиям по информационной безопасности.

Наши ожидания от кандидатов:

- высшее профильное образование, по направлениям подготовки ИТ или ИБ;
- умение анализировать журналы событий от различных источников IT-инфраструктуры;
- понимание принципов компьютерной и сетевой безопасности, встроенных механизмов обеспечения ИБ операционных систем (Windows, Linux), баз данных (Oracle, MS SQL, PostgreSQL) и активного сетевого оборудования (Cisco, Alcatel, Huawei);
- понимание принципов работы SIEM, IDS и IPS систем;
- опыт работы с системами защиты от НСД (ПАК Аккорд, SecretNet) и корпоративными антивирусными решениями (KES, Dr.Web);

- приветствуется опыт работы с программными продуктами Splunk, Elastic Search, vGate, DLP InfoWatch, MaxPatrol, Cisco ASDM, Wallix Bastion, Гарда БД, АПКШ Континент.
- приветствуется наличие сертификатов о прохождении сертифицированных курсов по вопросам информационной безопасности.

Преимуществом будут:

- опыт администрирования ОС Windows / Linux;
- опыт администрирования СУБД;
- опыт администрирования активного сетевого оборудования (Cisco, Alcatel, Huawei);
- опыт внедрения SIEM систем или других решений по мониторингу ИТ-безопасности.

Мы предлагаем:

- инновационные проекты, в настоящее время это проект Цифровой рубль;
- профессиональную среду, которая дает возможности расти экспертно, прокачивает, побуждает к новым достижениям;
- широкий социальный пакет (дополнительные дни к отпуску, возможности для отдыха по льготным ценам, активную спортивную жизнь внутри Банка России, пенсионную программу и многое другое);
- график работы сменный: 1/3 (сутки через трое);
- место работы: г. Нижний Новгород ул. Большая Покровская 26, формат работы только из офиса.

Контактное лицо: Поляшова Алена, PolyashovaAA@cbr.ru

Аналитик ИБ

Центр управления и мониторинга ИБ Департамента безопасности Банка России приглашает в команду Аналитика ИБ.
Центр решает широкий спектр задач, направленных на обеспечение кибербезопасности Банка России: мониторинг и реагирование на инциденты кибербезопасности, тестирования на проникновение, управление уязвимостями, эксплуатация решений по обеспечению ИБ, проведение проверок и внутренних аудитов информационной безопасности.
Мы ищем коллегу - единомышленника, который примет участие в повышении зрелости процесса расследования и реагирования на инциденты ИБ в Банке России.

Задачи:

- анализ состояния информационной безопасности в ИТ-инфраструктуре, выявление уязвимостей;
- расследование инцидентов информационной безопасности (2-3 линия);
- разработка сценариев реагирования на инциденты ИБ;
- разработка методов мониторинга событий и реагирования на инциденты с применением SIEM;
- настройка правил и политик SIEM;
- участие в проверках соответствия фактического уровня информационной безопасности требованиям нормативно-методических документов;
- подготовка рекомендаций по усилению мер защиты;
- участие при внедрении программных комплексов и автоматизированных банковских систем в части обеспечения информационной безопасности;

- рассмотрение документации техно-рабочих проектов в части соответствия требованиям по информационной безопасности.

Наши ожидания от кандидатов:

- высшее профильное образование, по направлениям подготовки ИТ или ИБ;
- умение анализировать журналы событий от различных источников IT-инфраструктуры;
- понимание принципов компьютерной и сетевой безопасности, встроенных механизмов обеспечения ИБ операционных систем (Windows, Linux), баз данных (Oracle, MS SQL, PostgreSQL) и активного сетевого оборудования (Cisco, Alcatel, Huawei);
- опыт работы с SIEM, IDS и IPS системами;
- опыт работы с системами защиты от НСД (ПАК Аккорд, SecretNet) и корпоративными антивирусными решениями (KES, Dr.Web);
- приветствуется опыт работы с программными продуктами Splunk, Elastic Search, Smart Monitor, vGate, DLP InfoWatch, MaxPatrol, Cisco ASDM, Wallix Bastion, Гарда БД, АПКШ Континент.

Преимуществом будут:

- опыт администрирования ОС Windows и Linux;
- опыт внедрения/администрирования SIEM-систем или других решений по мониторингу IT-безопасности;
- опыт администрирования СУБД;

Мы предлагаем:

- инновационные проекты, в настоящее время это проект Цифровой рубль;
- профессиональную среду, которая дает возможности расти экспертно, прокачивает, побуждает к новым достижениям;
- широкий социальный пакет (дополнительные дни к отпуску, возможности для отдыха по льготным ценам, активную спортивную жизнь внутри Банка России, пенсионную программу и многое другое);
- график работы: пятидневная рабочая неделя 08-17 часов;
- место работы: г. Нижний Новгород ул. Большая Покровская 26, формат работы только из офиса.

Контактное лицо: Поляшова Алена, PolyashovaAA@cbr.ru