Партнерский кейс

«Контроль авторизации входа»

Контекст / описание проблемы:

Поставщики услуг бурения нефтяной и газовой отраслей предоставляют своим клиентам возможность в режиме реального времени контролировать и получать данные о бурении и геологии с удаленных буровых установок с использованием так называемой системы обработки данных в реальном времени. Этот веб-сервис с расположенными в Москве серверами является важным инструментом для информированного и быстрого принятия клиентом решения непосредственно в своем офисе, без необходимости ждать, пока геологические данные или данные о бурении с буровой площадки будут отправлены по электронной почте или переданы иными способами. Система обработки данных в реальном времени работает с крайне важными и конфиденциальными данными клиента, поэтому используется система контроля авторизации входа и управление доступом к специальной клиентской папке. Каждому зарегистрировавшемуся пользователю доступ к клиентским данных предоставляется только после того, как уполномоченный представитель клиента дает ему разрешение на это. После того как пользователь получает разрешение на доступ к клиентской папке в системе обработки данных в реальном времени, поставщик услуг уже не может контролировать, вошел ли в систему именно этот конкретный пользователь, или кто-то другой заполучил его логин/пароль и использует его для работы в системе. Есть два фактора, которые следует учитывать: 1) система обработки данных в реальном времени предоставляет клиенту возможность пользоваться услугой как с персонального ноутбука, так и с мобильного устройства (например, планшета или смартфона), и это означает, что пользователь может использовать свой логин/пароль для входа в систему обработки данных одновременно и на ноутбуке, и мобильном устройстве; 2) если в офисе клиента работают несколько пользователей системы обработки данных в реальном времени, все ПК часто распознаются под одним статическим IP-адресом, потому что в качестве моста все они используют то же устройство.

Задача:

Основная цель - получить техническую возможность контролировать, кем используется логин/пароль, а также контролировать, что они не передаются для использования другому лицу без размещения уведомления об этом в Team notice в системе обработки данных в реальном времени. Помимо этого, получить возможность идентифицировать одновременное использование индивидуального входа / пароля.

Требования к решению:

Презентация PowerPoint, описывающая возможное решение, требуемые ресурсы, его плюсы и минусы, требуемые сроки и возможные юридические ограничения (если они известны).

Технические требования к решению:

Для презентации нет строгих формальных технических требований. Основным требованием является четкость решения и инструментов, используемых/необходимых для развертывания.

Критерии оценки:

- Надежность и точность идентификации использования индивидуального логина / пароля (как по закрытым сетям через шлюз, так и при параллельном использовании ПК и мобильного / планшета)
  Шкала оценки: максимальный балл - 5, минимальный балл - 1
- Простота и стоимость реализации
  Шкала оценки: максимальный балл - 5, минимальный балл - 1
- Оригинальность подхода
  Шкала оценки: максимальный балл - 5, минимальный балл - 1
- Возможные юридические ограничения
  Шкала оценки: максимальный балл - 5, минимальный балл - 1.