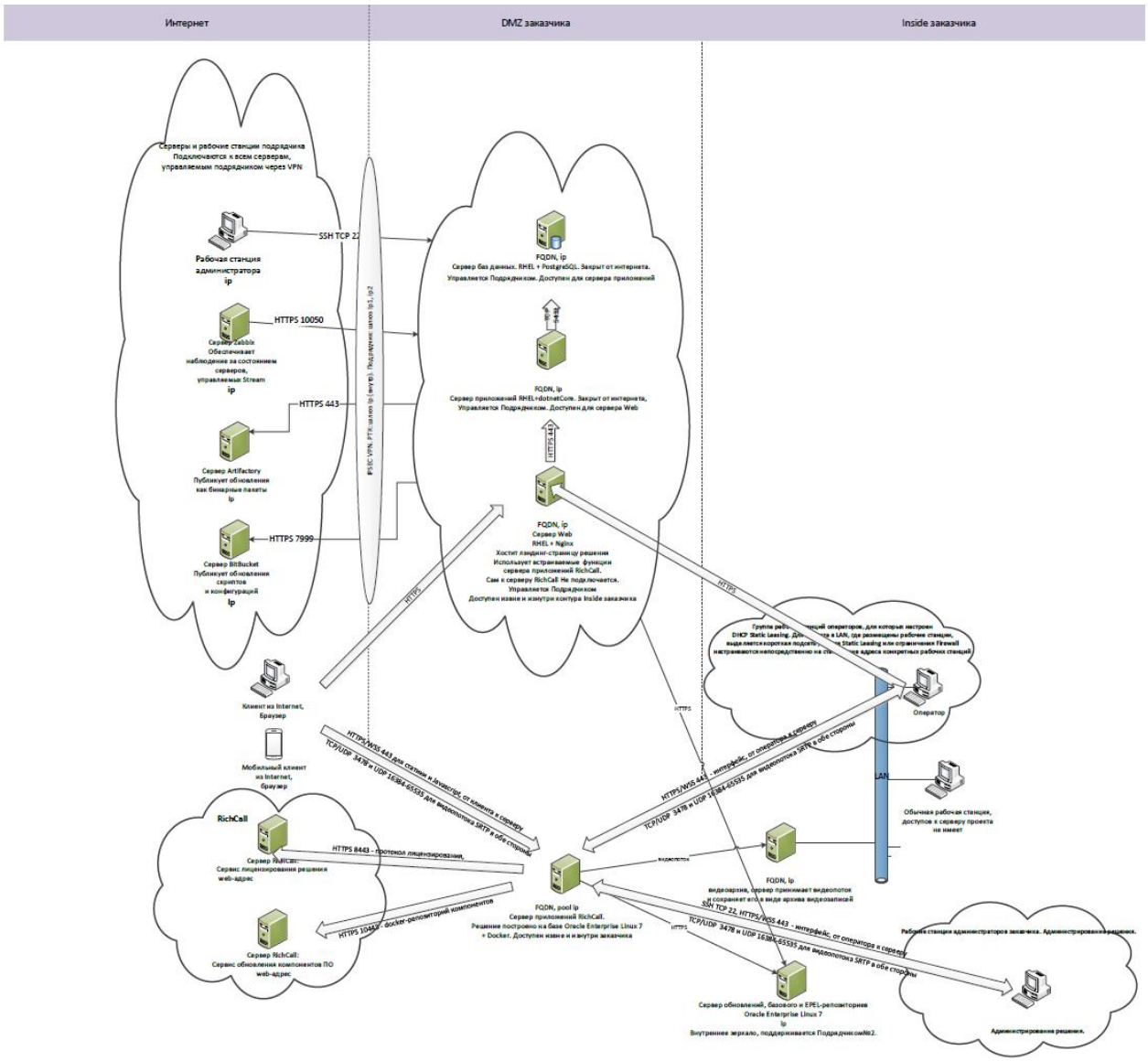
Хананиев Даниил Владимирович
Курс «Подготовка к собеседованию специалиста по информационной безопасности», поток от 20.05.2020
ДЗ № 6



Укажу только первую схему. Третья ничего нового не дала, все увидел из первой, а вторая хоть и интересная в том плане как все устроено в RichCall, но практически тоже в себе несет немного для общего результата.

1. Сразу укажу, что подрядчики должны предоставить сертификаты соответствия по ISO 27ххх и результаты последнего аудита, если они есть.
2. Исхожу из того, что все маршрутизаторы и файрволы работают по принципу белого списка, т.е. запрещено все, что явно не разрешено, стандарт.
3. Сервер приложений RichCall, прописать доступ с него на внешние сервера RichCall за лицензирование и обновлениями на конкретные ip-адреса по протоколам 8443 (лицензирование) и 10443 (обновления).
4. Операторы web-сервера лендинга лучше чтобы находились в отдельном VALN-е, если, как я вижу, есть задача разделить их и пользователей обычных раб.станций. Сервера web-сервера,

RichCall, и сервера обновлений внутренний интерфейс в тот же VLAN. Если этим операторам нужны будут ресурсы основного LAN-сегмента, сделать маршрутизацию.

5. Не знаю, как архивируются видеопотоки(протоколы, шифрование), но на всякий случай отмечу, что шифрование там нужно. Сервер видеоахива смотрит в центральный LAN, думаю, его лучше переместить в VLAN.
6. Рабочие станции администрирования решения тоже во VLAN.
7. На входе DMZ, так и Inside сегментов, NIDS сенсоры, на серверах – HIDS и APIDS. Центральный сервер IPS в сегменте Inside, с защитой себя.
8. На серверах приложений WAF, в зависимости от финансовых возможностей заказчика, opensource или проприетарный. Но должен быть, соотвествующий прописанным рискам организации.
9. Сервер SIEM в сегменте Inside, коннекторы ко всем серверам, работающим у них приложениям, БД, маршрутизаторам, хостам. Информация с IPS тоже должна сливаться в SIEM. Тут тоже отмечу, что и SIEM системы могут быть opensource, т.е. бесплатными или условно бесплатными, с оплатой за поддержку, что много дешевле проприетарных решений. Смотрим на условия и требования.
10. Сервера БД, web, рабочие станции операторов web - защита от несанкционированного доступа. Физически - физическая охрана серверной, протоколы физического доступа строго определенных лиц, СКУД, журналируемая, логи опять же в SIEM, комплекс средств НСД для защиты физических сред передачи данных. И программно – запрет usb носителей и вообще полный контроль подключаемых носителей, строгий доступ пользователей согласно прав, следование принципу минимально необходимых привилегий. Все логи опять в SIEM. Принцип AAA, как всегда. (пп. 7, 9, 10 скопированны из предыдущего ДЗ с добавлениями).
11. Антивирусы на всех хостах, включая сервера, и на маршрутизаторах, как я уже писал, лучше разных вендоров, для перекрытия сигнатур. Контроль почты, почтового сервера отдельного я не вижу, но контроль как минимум на хостах, плюс антивирус на маршрутизаторе должен фильтровать smtp трафик, многое на этом этапе отваливается.
12. В зависимости от критичности данных внедряем DLP систему.
13. Контроль кода приложениий, необходимые сканера кода, тестирование, пентестинг как тестовых сборок, так и продакшна.
14. Шифрование трафика между серверами между с собой и с операторами.
15. И вот эту всю красоту надо интегрировать в одну SOC, установив туда еще и систему реагирования на инциденты. SOC надо строить постепенно, подключая туда модули по мере готовности интеграции, параллельно обучая и подбирая персонал. Начиная с SIEM, подрастая до SOAR, подключая модули, можно построить вполне современную работоспособную SOC.

P.S. Внутренний сегмент компании не рассматривался, но очевидно, что и он нуждается в безопасности, сервера внутрениих БД, 1С, почтовые, сервера администрирования и т.д., и рабочие станции пользователей.