Для сегмента интернет:

На рабочую станцию установить Kaspersky Endpoint Security ли хотя бы Total Security. Использовать ssh только по ключу RSA или 12 символьному паролю. Из вне просканировать рабочую станцию сканером OpenVas и узнать все уязвимости. Защититься от эксплойтов на рабочей станции. Настроить минимальные права для из-вне для таких файлов как /ets/passwd и /ets/shadow. В случае Windows отключить сохранение теневых копий System32\config. Поставить IDS и IPS на рабочую станцию или хотя-бы waf или другой межсетевой экран. Настроить firewall. Настроить антиспам, защиту от продвинутых атак, SOC к примеру (Sysmon, microsoft windows security auditing), SIEAM, SOAR. То что трафик использует SSH это большой плюс, но надо еще настроить поддержку HTTPS, FTPS, WSS и других. Настроить обязательно СКЗИ и anti-fraud. Использование безопасного VPN (phison).

Для Сервер Zabbix сделать все аналогично, как для рабочей станции, но в добавок добавить аутентификацию, а так же обязательно купить сертификат у доверенного центра сертификации. Все запросы сервера подписывать цифровой подписью (закрытый ключ RSA). Создание белого списка ip адресов для сервера или хотя бы черного. Пентест сервера группой Red Team в иделе с помощью Black Box, но можно и White Boxю Поставить совместно с waf NGFW.

Для Сервер Artifactory сделать тоже самое, что и для Сервер Zabbix, но проверять пакеты на целостность и использовать безопасные протоколы. Так же аутентификация сервера при общении с сетью DMZ.

Для Сервер BitBucket надо в отличии от Artifactory настроить проверку конфигурация Blue Team.

Для клинета из интернета использовать 7 простых мер безопасноти.

1 МЭ

2 IPS

3 AVZ

4 Антиспам и антифишинг

5 APT Sandbox

6 WAF

7 SOC

Плюс использовать все меры криптографической защиты СКЗИ.

RichCall делать все, что с серверами выше в сети интернет, но при обновлнении сверять цифровые подписи и давать добро только при валидных. Защищать трафик от внутренних зловредов и внешних.

Сеть DMZ заказчика:

Для сервера FQDN установить Kaspersky Endpoint Security ли хотя бы Total Security. Использовать ssh только по ключу RSA или 12 символьному паролю. Из вне просканировать сервер сканером OpenVas и узнать все уязвимости. Защититься от эксплойтов на сервере. Настроить минимальные права для из-вне для таких файлов как /ets/passwd и /ets/shadow. В случае Windows отключить сохранение теневых копий System32\config. Поставить IDS и IPS на сервер или хотя-бы waf или другой межсетевой экран. Настроить firewall. Настроить антиспам, защиту от продвинутых атак, SOC к примеру (Sysmon, microsoft windows security auditing), SIEAM, SOAR. То что трафик использует SSH это большой плюс, но надо еще настроить поддержку HTTPS, FTPS, WSS и других. Настроить обязательно СКЗИ и anti-fraud. Фильтровать данные на наличие SQLi, даже при использовании библиотек прослоек. Так же выдавать минимальные права на кротчайшее время серверам из вне. Создание белого списка ip адресов для сервера или хотя бы черного. Для запросов SQL сбрасывать все слжубные запросы, если нету привилегий root. Защитить соединение TCP 5432.

Для сервера FQDN, который общается с кластером SQL обязательно делать защищенный трафик внутри сети для защиты от троянов или внутренних злоумышленников. Внутри сети DMZ настроить NAT и wireless. Постоянно обновлять роутер драйвера и менять пароль от админки роутера. В сети использовать минимум концентраторов. Использовать коммутатеры или хотя бы сетевые мосты.

Для FQDN, ip Сервер Web RHEL + Nginx поставить самый обновленный NGINX. Просканировать веб сервер на уязвимости. Исключить такие уязвимости как переполение буфера в стке и в куче, use after free, уязвимость формата строки, целочисленного переполнения, атаки возврата в библиотеку и других. Включить на сервере DEP NX BIT, Stack Canary, ASLR, Stack Protector. Аналогичные механизмы для кучи. Так же исключить все server side уязвимости RCE, SSRF ,LFI\RFI, SQli, LDAPi, CRLF, IDOR и другие. Для безопасности от client side уязвимостей особенно защититься от CSRF, так как может поступить невалидный запрос на сброс пароля администартора. Обязательно запрашивать аутентификацию и сделать градацию по правам. Root выдавать только в самом крайнем случае самый важным аккаунтам. Для трафика из-вне исключить DHCP – spoofing, DNS- spoofing, IP – spoofing , DOS\DDOS, ssl – strip, ssl –split. Для защиты от последней атаки купить серитфикат у центра сертификации (COMODO McAfee). Защита внутреннего трафика от arp-spoofing.

Для FQDN, pool ip делать все, что и с другими серверами из DMZ, но еще проверить докер на вирусы и другие вредоносные программы. Так же строгое распределение прав в Linux 7. Использование криптостойких паролей. При запросе о сборе статистики выдавать только права на чтение, так же поддерживать только защищенные протоколы HTTPS/WSS.

Для inside заказчика.

Для оператора все настроить как в DMZ сети политики безопасности. Так же добавить аутентификацию при общении с сервером. Настроть политику в роутере NAT и wireless для WI-fI

Сделать защищенную точку доступа проверять внешнюю сеть на атаки, так и внутреннею. Защититься от сетевых уязвимостей описанных ранее. Регулярно проводить сканирование ПК оператора и обновлять антивирусное ПО.

Для обычной рабочей станции исключить доступ недоверенных внутренних сотрудников. Поставить пароль на BIOS.

Для администраторов заказчика оставить только защищенные протоколы. Добавить аутентификацию настроить NGINX, Waf, SIEM, SOAR, IDS, IPS, SOC, антивирус и другие решения для безопасности. В случае острой необходимости добавить собственный протокол с надежной критографической защитой и шифрование (AES). Купить сертификат у COMODO или McAfee.

Для Сервер обновлений, базового и EPEL-репозиториев Oracle Enterprise Linux 7 защититься от НСД и применить все, что применено к админам, так как заражение репозиториев грозит ущербом репутации и компрометации данных.

**Для слайда 2**

Для сигнализации верно сделано, что используется HTTPS, но можно добавить FTPS для файлов, а так же WSS. Сделать подключение к сигнализации из вне сложно доступным. Изолировать все сигналы извне, а так же защититься от излучения, если такое имеется. Для видео камер установить защищенное соединение. Никто извне не должен видеть с них изображения. Сделать WebRTC защищенным (TLS + сертификат COMODO или McAfee). Аналогично для Kurento. Для free switch исключить внутренние сетевые атаки, а так же шифровать трафик между сотрудниками и приложениями. Для всех управляющий сигнализация сделать изолированную извне сеть возможно отдельный роутер с NAT и wireless + криптостойкий пароль и отключить код сброса перейти с STOMP протокола на протокол с поддержкой TLS. Сделать передачу звука по TLS протоколам или по GSM сети с надежным оператором.

Сигнализации между модулями бизнес логики строго сделать по 443 порту или wss.

Заменить протокол WS на WSS! Внедрить все политики безопасности которые были описаны для inside сети. Для всего звукового оборудования и видеооборудования перейти с протоколов SRTP на HTTPS/WSS. Установить программы для работы с видео и аудио проверенные на наличие уязвимостей. Просканировать все модули бизнес логики на client side/ server side/ binary/ network уязвимости так же нанять специалистов для поиска 0-day и 1-day уязвимостей. Провести атаку Red Team Black/White box. Проанализировать конфигурации Blue Team. В сети оператора настроить роутер на Nat и wireless. Заменить STUN на аналог с TLS + аутентификация. То же самое сделать с SRTP. Для сервера RichCall настроить коммутаторы и сетевый мосты, а так же МЭ между модулями бизнес логики и заменить все HTTP на HTTPS. Провести политику безопасности описанную выше. При выходе в интерне настроить извне прокси сервер или vpn (phison).

**Схема проекта "Виртуальный магазин" , страница 3**

Для web (nginx, web) – все верно, но можно добавить аутенитфикацию.

Для сигнального порта TURN/STUN замена на защищенные протоколы.

Для sip тоже защищенные протоколы поставить и настроить инкапсуляцию внутри сети роутера (коммутаторы и сетевые мосты).

Для rtp – весь трафик перевести на TLS + сделать только внутри периметра, то есть настроить МЭ, WAF, NGFW

Для сервиса лицензирования обращение только к доверенным центрам COMODO, McAfee.

Для внешних клиентов HTTPS все верно

Но TURN/STUN, rtc инкапсулировать в TLS

Аналогично для агентов RichCall.