Между подрядчиком и DMZ настроить Firewall. В качестве Firewall можно использовать WAF или NGFW. При настройке WAF мы защищаем трафик передающийся по протоколам семейства HTTP, SMTP, FTP. С помощью WAF мы защищаемся от атак «OWASP Top Ten Web Application Security Risk» (для веб-приложений) и «OWASP API Security Top Ten». WAF умеет делать декомпозицию HTTP, JSON, XML заросов. Если нам нужен более глубокий анализ трафика, то необходимо перейти на NGFW, который способен детально анализировать сетевые пакеты, а так же имеет поддержку IPsec и SSL VPN, мониторинг сети и сопоставления IP адресов. Есть поддержка SSL, контроль вторжений и предотвращения вторжений. В нашем случае лучше всего использовать NGFW, так как у нас VPN подключение. Плюс необходимо шифровать трафик по TLS и добавить аутентификацию.

При подключении с мобильных телефонов из внешней сети в DMZ, необходимо редирект на HTTPS, так же необходимо настроить межсетевые экраны как в первом случае для анализа трафика.

В сети DMZ при подключении по SSH использовать подключение по ключу или по 12 символьному паролю. Внутри периметра Инф-ра геймификации настроить SIEM, SOAR, IPS, IDS. С помощью SIEM собирать все данные из журналов, логов, предупреждений системы, а так же активно обновлять базы данных угроз. Пытаться предугатать сценарий развития атак в случае. Через SOAR автоматизировать действия SIEM. При возникновении атаки лучше всего распознать ее через IDS. IDS в свою очередь передает предупреждение IPS, который в реальном времени блокирует атаку, а так же передать антивируснику. В качестве антивирусника поставить Kaspersky Endpoint Security, SIEM поставить McAfee. Между сервером Геймификации и Backup, FQND, настроить только безопасные протоколы FTPS, SSH. Убрать все незащищенные порты. Доступ к Backup только узкому кругу сотрудников имеющих особые привелегии с аутентификацией. Сопоставление IP при доступе из внешней сети в DMZ. В случае атаки блокировка IP или группы IP адресов.

Inside сеть

При подключении Сервер геймификации к Личный кабинет для интранета и SMS-шлюз исключить такую атаку как SSRF, Настроить в Inside сети SIEM, SOAR, IDS, IPS, Антивирусников, сканеров уязвимостей.

Рабочее место бизнес-пользователя настроить Firewall на выходе из Inside в DMZ (WAF и NGFW). Из протоколов оставить только HTTPS и SSH. На рабочем месте настроить антивирусник Kaspersky Endpoint Security. Настроить IDS и IPS в случае угрозы блокировать атаки и обнаруживать источник атаки, сохранять информацию в логах для расследования инцидента.

При обращенни к серверам баз данных выдавать минимальные права на короткое время, так же фильтровать запросы настроить IPS, IDS на мониторинг взаимодействия с БД. Аналогично с тестовым хранилищем данных. При работе с сервером сохранных PIN кодов сделать аутентификацию при обращенни. Фильтровать данные от SQLi даже в случаем библиотек прослоек. Выдавать минимальные права. Мониторинг антивирусником активности сервера кодов и журналирование.

Аналогично с SQL сервером, так же защитить LDAP сервер и исключать LDAPi. Сделать соединение защищенное исключающее прослушку. По скольку все происходит в 1 сети, то настроить защиту от arp-spoofing, dns-spoofing, dhcp-spoofing.

Сеть аутсорс настроить NGFW и сделать защищенное соединение через TLS. Исключить IP-spoofing. Так же исключить все GSM атаки. Настроить на SMS центре IPS,IDS и антивирусник. Проверять центр смс сканером уязвимостей.