**RMCCDC Blue Team Coaches Packet 2021**

**Scenario**

Elite Medical Hosting Corporation (EMH Corp) is a medium sized public corporation located in the western United States. Catering to small independent medical groups, EMH Corp specializes in providing hosting and administration for Medical Practice and Electronic Medical Records Management. With their stated mission: “Through excellent customer service, technical acumen, and state of the art systems, provide the independent medical practitioner escape from routine administrative burdens, allowing the development of intimate, personalized relationships with their clients.” EMH Corp has become a disrupter in the healthcare community.

EMH Corp has fully embraced Software as a Service (SAAS) as their operating model. They have partnered with one of the leading providers of Electronic Medical Records (EMR) and Medicap Practice Management to provide a turnkey solution to their customers. Building their product on OpenEMR, EMH Corp provides personalized administration and support to each medical practice. To support the myriad of regulatory requirements EMH Corp has implemented their SAAS solution in a private cloud. Two main data centers, the primary DC in the east, and secondary in the west, provide redundancy and disaster recovery. Being a nascent company, EMH Corp has concentrated on the buildout and operationalization of the technical environment. As such many of their IT controls, governance, documentation, security policies and procedures are non-existent or substantially underdeveloped. The corporation is currently scheduled for their first HIPPA certification audit in early Q4 2021.

To properly prioritize your efforts, the office of the CIO/DPO has provided the following expectations:

1. Identify, document, and communicate security concerns.
2. Provide monitoring, response, recovery, and reporting for all security incidents.
3. Ensure all client support services remain active.
4. Configure and administer the Electronics Records and Medical Practice Management system.

EMH Corp has engaged your team (here after referred to as the Blue Team) to provide security configuration and management for all hardware, software, and data. You are responsible for protecting the information systems, network infrastructure and data while maintaining all business services. Year after year the Healthcare Industry has remained a top target for cyber-attacks. As an emerging force in the independent health care practitioner market, EMH Corp considers their reputation one of their foremost crown jewels. The performance of you and your team will be decisive in the establishment of this as well as your team’s reputation.

**Core Business**

At present EMH Corp has contracted with two medical practices, The University of the Rocky Mountains Health Partners, (URHP), and The Front Range University Health Clinics (FRUHC). Each of these customers receives electronic medical record management, configuration and administration of the clinic management system(s), and an online patient portal. Clinic administrative personnel, medical staff, and patients require on demand, always on, reliable access to system and services.

Of course, there are always surprises in Cloud networks in particular security. During this year’s configuration to the Public Cloud provider’s, you will have access to the ISP Palo Alto firewalls to manage security. You should develop a strategy for securing the organization’s hosts, operating systems, application(s), databases, and any other assets. You will have access to the ISP network management tools to view inbound and outbound traffic to your space. In keeping with the popular open-source nature of the Cloud technology the company has invested in a pilot project testing the feasibility of utilizing both Private and Public Cloud services to control their data center footprint and possibly shift costs to provide a proven disaster recovery solution.

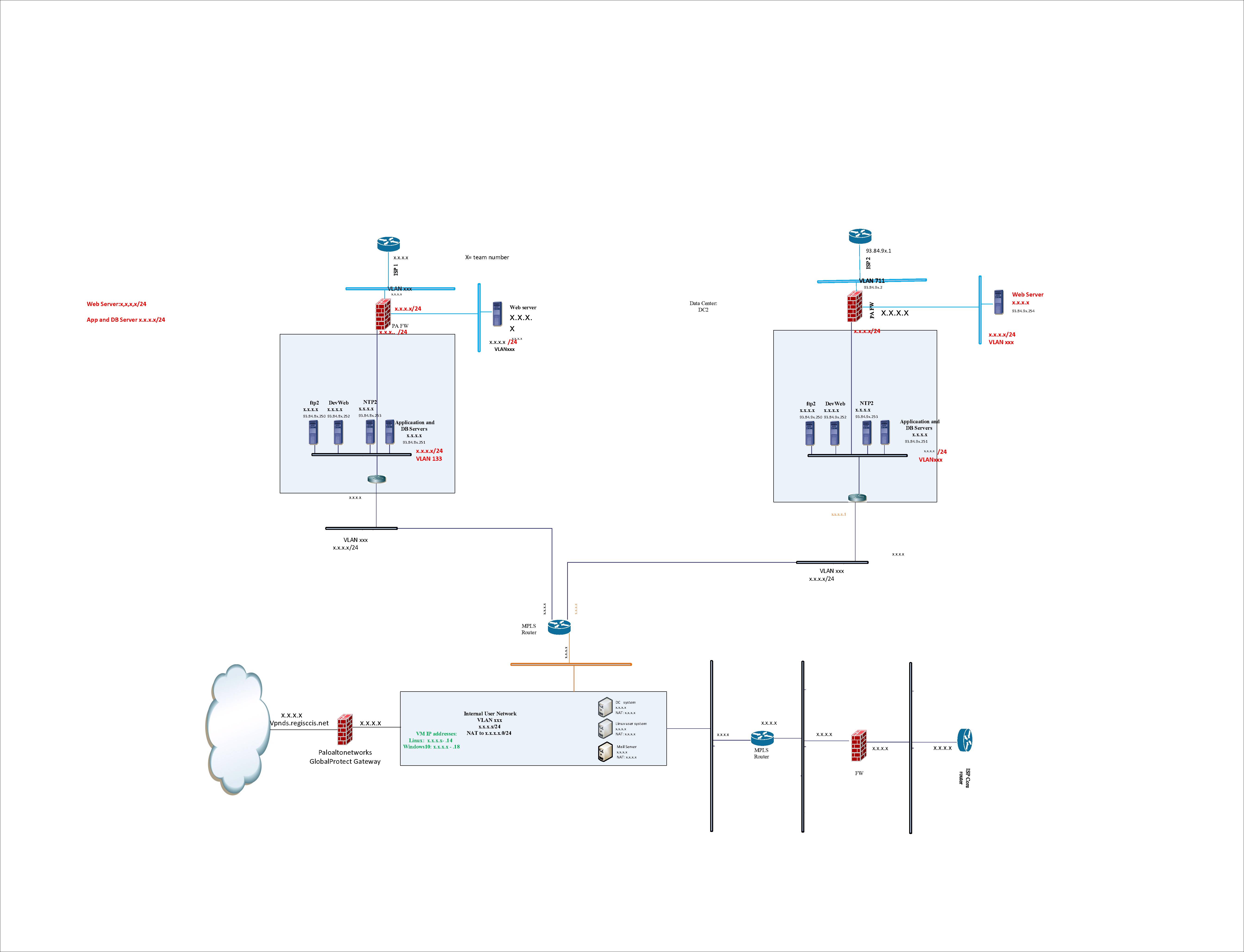
**Core Services**

The following are samples of core business services, which the Blue Team is responsible for keeping running during the event:

* + HTTP
  + HTTPS
  + FTP
  + DNS
  + SMTP & POP3
  + SSH
  + RDP
  + Video and sound
  + Internet Connectivity
  + Remote connectivity for systems administration
  + Virtual Firewalls, switches and routers
  + Printing
  + Wireless networks
  + Company employee email
  + Student/faculty Learning Managing System (LMS)
  + Student/faculty workstations

**Network Details**

At the start of the competition, each team will be assigned a network environment with identical hardware, software and system configurations. The following network diagram is an example of this year’s networks. There are details for each blue team not included in this document. Your official Blue Team Packet with details will be distributed the day of the competition. Blue Teams are required to protect core services at all times. **DO NOT REMOVE OR CHANGE THE PASSWORDS FOR BLUE TEAM COMPETITION PACKET ACCOUNTS HIGHLIGHTED IN RED OR mentioned in the blue team meeting prior to the event.** Throughout the competition Blue teams may be asked to bring up additional services by the EMH Corp. Each team should stive to have the appropriate services listed above always running. Failure to provide these public services will result in a reduced score. An example of the companies’ network diagram is provided below in *figure 1- Network Diagram*.



General Network Diagram

Blue teams will have control of their EC2s, operating systems, services, and devices. However, all the organization’s systems and services will be hosted on a Private and Public Cloud. The Public Cloud Provider will provide a data center located on the East Coast for Business Continuity, load balancing and Disaster Recovery. Your team will have to monitor and then implement security policies at the system, service, application, and user levels as needed to maintain services.

All communications (injects, announcements, updates, and team response) will be communicated through a separate system in their room identified and known as *RMCCDC portal*. This team portal is not part of the EMH systems and not the responsibility of the Blue team to control, modify or protect. Blue teams will have remote desktop access via RDP, SSH and Putty to all virtual servers and hosts.

SSL and SSH sessions to external file shares (github, .edu sharepoint, etc.) will be blocked. No access to Blue Team repositories except for the RMCCDC provided Citrix Share File accounts will be allowed because only publicly available information can be used during the competition. Access information and credentials will be provided on the first day of competition. Blue teams will have Internet access to research topics and up-date operating systems. **Blue teams may not conduct social engineering, nor will RMCCDC support teams conduct social engineering.** Competition officials will escort VIPs and camera crews. Blue teams must grant access to team rooms by competition officials. A Gold team member may contact you for information regarding submissions and you may answer any questions they have on your submission.

There will be a Chief Information Officer (CIO) for the EMH Corp, Inc. system who will reside in the CIO virtual office. The CIO will be your point of contact for questions during the competition. The only way that a Blue team will communicate to the competition officials will be through the CIO office.

You will use provided accounts to share documents across team members and store documents. The Black team will be monitoring all inbound and outbound network traffic.

**Team Roles**

Throughout the competition, there will be several teams, each responsible for different aspects of the competition. The roles of the different teams are outlined in *Table 1: Team Responsibilities*.

|  |  |
| --- | --- |
| **Color** | **Purpose** |
| White | Observers. A White team member will remain in each competition room to observe activities and ensure RMCCDC rules are being followed. |
| Gold | The Gold team will focus on scoring injects which are given to the teams throughout the event. There will be no Blue team-initiated interaction with the Gold team however the Gold team may contact the Blue team for clarification of injects as needed. |
| Black | Operations. The Black Team will monitor network traffic, service availability, and system availability. There will be no Blue team-initiated interaction with the Black team however the Black team may notify Blue teams of unavailability of system or system services. |
| Gray | Employees. Internal EMH Corp staff. The role of the Gray team is to act as users of the system during the event. Gray team users will be in the individual rooms exercising the systems during the event. The Blue team captain can communicate with the Gray team members to verify services but will not provide IT support. |
| Blue | Student competitors. The Blue teams are the competition teams. |
| Red | Adversaries. The Red team will be working to attack the systems being protected by Blue teams. There will be no Red team interaction initiated by the Blue team. |

Team Responsibilities

**Expectations**

Blue teams must be familiar with regional and national CCDC rules. Go to the following URL for details.

https://rmccdc.regis.edu/ and https://www.nationalccdc.org/index.php/competition/competitors/rules

**Emergency Contact**

Emergency Contact dial, Bob Bowles at (719-331-7582). Please only use this number in case of an emergency. Not for competition troubleshooting or requests.