NECCDL

PRESENTS THE

NORTHEAST COLLEGIATE CYBER DEFENSE COMPETITION

HOSTED BY

UMASS
LOWELL

NECCDC 2023 SEASON REGIONAL

BLUE TEAM PACKET

v.1 | Revised 2023-02-12

CONTENTS

NORTHEAST COLLEGIATE CYBER DEFENSE LEAGUE

The Northeast Collegiate Cyber Defense League (NECCDL) is an administrative body whose sole purpose is to facilitate the smooth running of NECCDC regardless of hosting institution. The League is operated by academic volunteers and is funded by league sponsors and annual membership fees collected from participating Academic Institutions.

Find out more at: neccdl.org
Follow us on Twitter: @neccdl
GitHub: github.com/NE-Collegiate-Cyber-Defense-League

We would like to thank UMass Lowell for hosting the regional infrastructure for this season!

NECCDC 2023 SEASON

The Northeast Collegiate Cyber Defense Competition (NECCDC) is designed to provide a controlled competitive environment that will permit each participating institution to assess their students' depth of understanding and operational competency in managing the challenges inherent in protecting enterprise network infrastructure and business information systems. NECCDC provides an opportunity for qualified educational institutions in the Northeast to compete in this environment and is part of a national organization (see www.nationalccdc.org), which provides a unified approach for nine regions across the country. Qualified educational institutions include those with information assurance or computer security curricula.

COMPETITION GOALS

1. To promote fair and equitable standards for cyber defense and technology-based competitions that can be recognized by industry
2. To evaluate the defensive and responsive skills of each team under hardware, software application, and operating system configurations using a joint academic and industry rating scale
3. To demonstrate the effectiveness of each participating institution's academic security (and related) programs
4. To be executed by a preponderance of industry professionals
5. To have industry recognition, participation and acceptance of each competition
6. To rate the effectiveness of each competition against a predefined standard of competition rules
7. To provide a cooperative and competitive atmosphere among industry partners and academia in the area of cyber defense education
8. To provide recognition for participating teams

9. To increase public awareness of academic and industry efforts in the area of cyber defense education
10. To facilitate the pipeline for the next generation cybersecurity workforce
11. Develop competitor skills to respond to modern cybersecurity threats

REGIONAL OVERVIEW

The NECCDC 2023 Regional is managed by this year's Regional competition host (UMass Lowell), with strong contributions from the wider team at NECCDL. The competition is designed to test each competing team's ability to secure a networked computer system while maintaining standard business functionality. The scenario is a medium-sized Software-as-a-Service (SaaS) company that is migrating to the cloud infrastructure. The organization has a small number of clients with a specific set of services. Since the recent cloud launch in Jan went well, it is expanding its services.

The competition involves more than the application of technical skills. It is also one built upon the foundation of business operations, policy, and procedures. A technical success that adversely impacts business operations will result in a lower score, as will a business success that results in security weaknesses.

The winning team from the NECCDC 2023 Regional in March will advance to the CCDC National Championship scheduled for April 28-30, 2023.

The second place team will have the opportunity to compete in a four (4) hour event for a Wildcard spot on Wednesday, April 05, 2023. Information about that event will be sent directly to the second place team by a representative of National CCDC.

NECCDC 2023 SEASON SPONSORS

NECCDC would not be possible without the generous support of our sponsors!

Additional information regarding sponsorships for the NECCDC 2023 Season can be found at https://neccdl.org/neccdc/2023/howtosponsor/ and https://neccdl.org/neccdc/2023/sponsors/ .

GOLD
MassMutual
Raytheon Technologies

SILVER
cisco™ Networking Academy
paloalto® NETWORKS
Arete℠
RSM

NECCDC 2023 SEASON SPONSORS - CONTINUED

BRONZE	
BATTELLE It can be done	FORTRA
NuHarbor SECURITY	
NECCDL	

SUPPORTERS		
no starch press	elastic	*With extra support from Jason E*

OTHERS? HELP CONNECT US WITH POTENTIAL SPONSORS!
Let us know if you or someone you know is interested in sponsoring for the 2023 season! Have them contact sponsor@neccdl.org for more information.

REGIONAL EVENT SCHEDULE

Friday, March 10	**Event**	**Notes**
8:00 am - 9:00 am	Check In	Breakfast, Name Tags
9:00 am - 9:30 am	Competition Opening	
10:00 am - 5:30 pm	NECCDC Student Competition	
12:00 pm - 12:45 pm	Team Lunch	Boxed grab-and-go
Saturday, March 11	**Event**	**Notes**
8:00 am - 9:00 am	Check In	Breakfast
9:30 am - 5:00 pm	NECCDC Student Competition	
12:00 pm - 1:00 pm	Coaches' Meeting	
12:00 pm - 12:45 pm	Team Lunch	Boxed grab-and-go
6:00 pm - 9:00 pm	Recruitment Event	Dinner
Sunday, March 12	**Event**	**Notes**
8:30 am - 11:30 am	Events (Debrief + Panels)	Breakfast
11:30 am - 12:30 pm	Award Ceremony	Lunch
12:30 pm - 2:30 pm	Networking	Interaction and networking with peers

COMPETITION ORGANIZATION

Blue Team

Student team representing a specific academic institution or major campus competing in the NECCDC. Each team must submit a roster of up to 12 competitors to the Competition Director. Each competition team may consist of up to eight (8) members chosen from the submitted roster. The remainder of the roster is for substitution in the event a member of the active competition team cannot compete. Substitution in the competition team requires approval from the Competition Director.

- Students should maintain a full-time status (as defined by the participating institution) at the time the competition is conducted. Coaches are responsible for ensuring that participating students have the status needed to participate, and recommend 2 or more moderators. See National CCDC rules for full eligibility criteria.
- Technical access issues and the like should be **@BlackTeam** in Discord on your Team Channels for infrastructure-related questions. If competitors are unsure about other questions, then they should ask their room moderators.

Red Team

Professional network penetration testers from industry, approved by the Competition Director, and industry representatives who:

- Scan and map the network of each competition team - Attempt to penetrate the defensive capabilities of each Blue Team network
- Modify any acquired environment
- Assess the security of Blue Team networks
- Attempt to capture and/or modify specific files on targeted devices of Blue Team networks
- Attempt to leave specific files on targeted devices of each Blue Team network
- Document and provide feedback for competitors / organizers to evaluate performance
- Follow Rules of Engagement for the competition

White Team

Representatives who serve as competition officials, moderators and rule enforcement in the various competition rooms.

- Moderators are responsible for:
  - Undertaking / reviewing training for moderators offered by NECCDC
  - Understand how to use the required communication tools (i.e. Discord)
  - Submitting questions / requests from blue team to the designated #channels
  - Check rosters and authenticate competitors at check-in
  - Ensuring that competition rules are followed and any violations are reported to the White Team senior staff
  - Submit survey feedback based on competition / team observations near end of Regional (e.g., webform provided in Discord)
- White Team senior staff will:
  - Supply and score Blue Team tasks in the form of competition injects
  - Adjudicate the scoring for the competition
  - Have a chief judge responsible for final decisions with regard to scoring

Black Team

Competition technical support, the Black Team deploys and maintains the physical and virtual competition environments, as well as the service scoring engine and possible related SLA violations.

Gold Team

The competition staff includes the Director(s), logistics and sponsor relations coordinators.

Orange Team

The competition staff that builds an integrated scenario storyline, corporate branding/image, and simulates user activities in a manner that integrates with and contextualizes Black and White team activities. The team also may include individuals who act as employees, clients, and other external acting parties, e.g., CISO, law enforcement that interact with systems and Blue Team during the competition experience.

COMPETITION RULES

NECCDC subscribes to the National CCDC Rules, which have been continuously updated in recent years. In particular, Article 7 on Professional Conduct which applies to competitors and non-competitors alike. Not only is this expected in today's workforce, we truly strive to create a fun and safe professional + technical learning environment every year.

The Director will update an aggregate list of published Blue Team GitHub links from this year's season prior to the Regional. Besides these approved repos / files, teams are not allowed to use any others with privately team-developed staging materials.

Competitor Authentication

Competitors and coaches will be expected to physically check in with the Gold Team Registration on the first day of competition.

Questions and Answers

We maintain a set of updated Questions and Answers, publicly available here: FAQ .

SCORING OVERVIEW

Blue Teams gain points throughout the competition in two (2) categories using the following point distribution:

50%	System Scoring
50%	Inject Scoring

Both service uptime and completion of injects are equally important. As with any business, systems often have differing risks and critically. Additionally, any disabling/disconnection of network services is considered unauthorized and thus, depending on severity and service criticality, might incur appropriate SLA violations. The more points Blue Teams can gain, the better.

Additionally, successful Red Team Activity will subtract up to 50% of points from a team's possible total points:

- 50%	Red Team Activity

The more points Blue Teams can prevent the Red Team from taking away, the better.

Accurate and high-quality Incident Reports will reduce the amount of points reduced as a result of Red Team activity.

System Scoring

System availability and integrity makes up half of the Blue Team final score. This scoring consists of service checks that happen on a predetermined interval. Each successful check will increase point totals (depending on service criticality). Unsuccessful checks will not add or decrease point totals.

Inject Scoring

Injects are business tasks provided to each team throughout the competition and make up half of the Blue Team's final score. Injects are typically provided to teams in the form of communication from a supervisor/stakeholder, a project work order, or a break/fix ticket. Injects may not always explicitly outline specific deliverables expected. It is the responsibility of the Blue Team to interpret the request and respond professionally. Questions can be asked for clarification via moderators or directly to White Team or Black Team. Some injects may be scored objectively, while other injects may be scored on a ranked scoring model. Injects may not all have the same point value, and are weighted based on items such as complexity and time required to complete. The specific point value for each inject is not disclosed to the Blue Team.

You are reminded to not list your personal information or University name in the inject submissions in an effort to ensure that grading can remain unbiased.

Injects have their own deadlines, and injects submitted past deadlines do not earn points. Keep in mind that the Google Classroom clock may be different from your system time.

Red Team Activity

Successful Red Team activity is subtracted from Blue Team total points. Red Team Activity has a ceiling and may not take away more than half of the total possible points from combining service and inject scoring. Accurate, evidence-based, and professional Incident Reports submitted by the Blue Team may provide the opportunity to reclaim Red Team points for specific Red Team activity. However, very low-quality Incident Reports may result in additional points awarded towards Red Team Activity and Blue Teams should only submit Incident Reports they have confidence in (detailed in National's Rule 9.d). A standardized Incident Report document is provided below and teams are encouraged to utilize the document to submit Incident Reports.

Incident Response Template

Please feel free to use this Incident Response Template, or use a similar professional IR report which captures data referenced in National Rules 9.d.

Tips for Effective IR Reports

- Submit IR reports in the order that you encounter incidents to potentially reduce future Red Team impact
- Ensure any executive summaries and business impact analyses are appropriately written for the intended audience (try not to include too much technical jargon)
- When writing, ensure that it is professional and includes enough necessary information and depth while not including any extraneous information
- When discussing business impact, ensure that you accurately identify the effects on the business
- Attempt to accurately determine the root cause
- Once an incident has occurred, you want to perform remediation. Any actions taken towards remediation / prevention should be detailed.
- Make sure that you include relevant screenshots, visuals & evidence
- Think about whether what you are experiencing is really due to Red Team activity or due to a misconfiguration / actions taken by the team

NECCDC 2023 SEASON THEME

The theme of NECCDC 2023 is “Resilient Cloud Infrastructures”. Modern cloud providers, containerization, and orchestration technologies have enabled organizations to massively scale their infrastructures. At the same time, the presence of availability zones has enabled organizations to guarantee high availability (> 99.99%) of critical services.

These massively scalable, highly available, and public infrastructures present unique security challenges that require innovative security solutions. This year’s qualifier and regional competition will focus on the multitude of techniques that ensure enterprise network uptime, security, and flexibility—-even when operating at a massive scale.

Blue Teams will need to maintain, secure, and scale highly available services while also juggling compliance with service-level agreements.

Core Focus -

- Resiliency
- High Availability
- Distributed File Systems
- AWS Console
- Containers
- Orchestration
- CI/CD pipelines
- Vulnerability management
- Endpoint security

NECCDC 2023 SEASON SCENARIO

This year's qualifier and regional competition will focus on the multitude of techniques that ensure enterprise network uptime, security, and flexibility – when operating at a massive scale. These ideas will be critical to the success of the organization Blue Teams will be supporting, Prometheus Group. The company is scaling its business to have greater reach and flexibility for existing and future customers. These goals will only materialize if all of these ideas can come together and be operationalized well.

Blue Teams will need to maintain, secure, and scale highly available services while also juggling compliance with service level agreements. Teams will be expected to follow modern best practices such as CI/CD; modern technologies such as Docker containers; and orchestration frameworks such as Docker Swarm to create robust, secure, and dedicated services for Prometheus' clients.

REGIONAL INFRASTRUCTURE

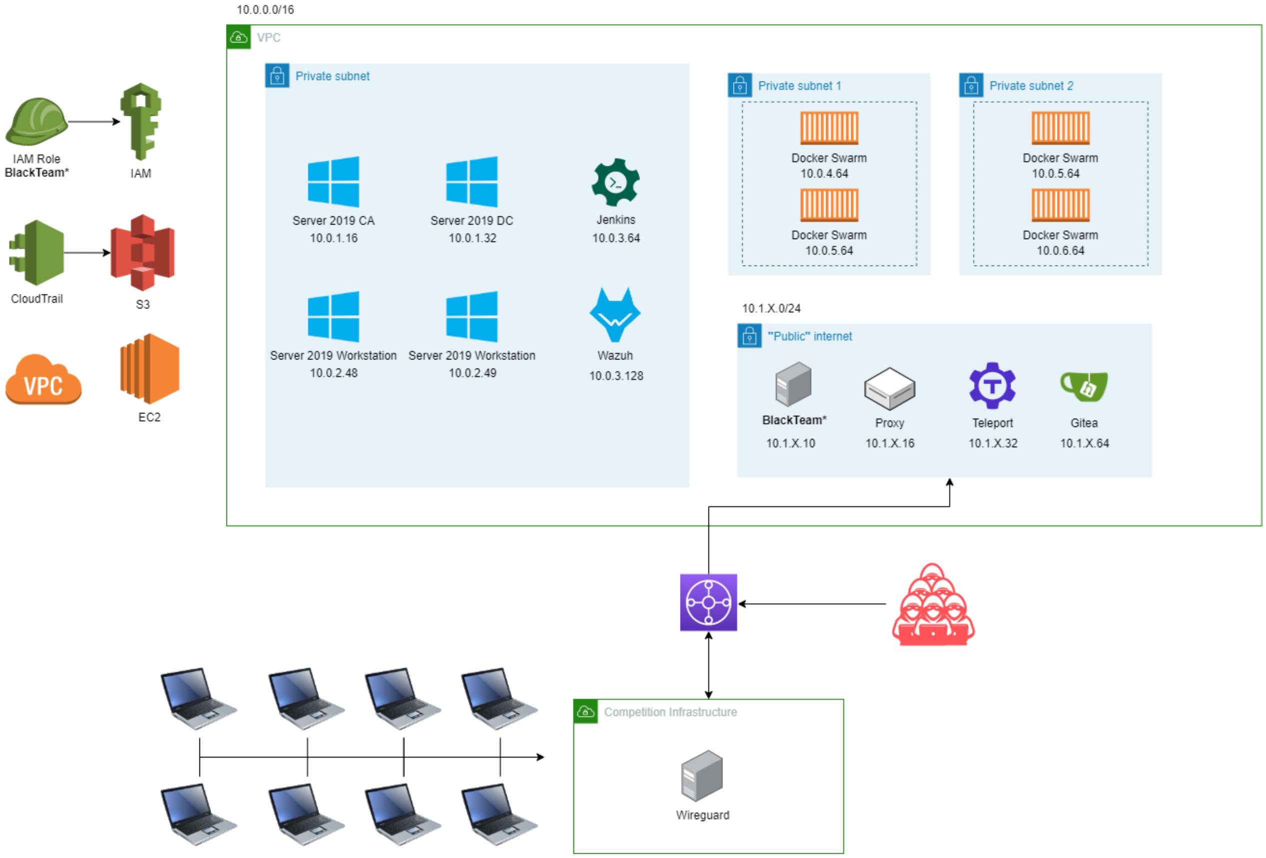
Employees of Prometheus Group should be prepared to assess the various aspects of the organization’s infrastructure. Technologies that may be found in the company’s infrastructure include* but are not limited to:

Windows Server 2019	Docker	Container Networking
Microsoft Active Directory	Docker Swarm	HAProxy
Microsoft IIS	Ubuntu	Harbor
WMI, SSH, and RDP	RHEL	MySQL
Certificate Authorities	Wazuh	MariaDB
Kerberos	Podman	MongoDB
Windows based DNS	Jenkins	Nginx
Alpine Linux	Gitea	NextCloud
Amazon Linux 2	Ansible	RocketChat
AWS IAM	CloudTrail	Availability Zones
AWS EC2	AWS S3	Teleport

* The focus will be on containerized versions of applications

Remote Access to the Regional environment will be provided by the Black Team through Wireguard (similar to Qualifiers). Details about access will be given closer to the regionals.

For a larger version of the Regional Infrastructure Diagram (below), see Page 16.



LETTER FROM MANAGEMENT

From: Dade Murphy
To: DevSecOps Team, Infrastructure Team
Subject: Team Reorganization

Team:

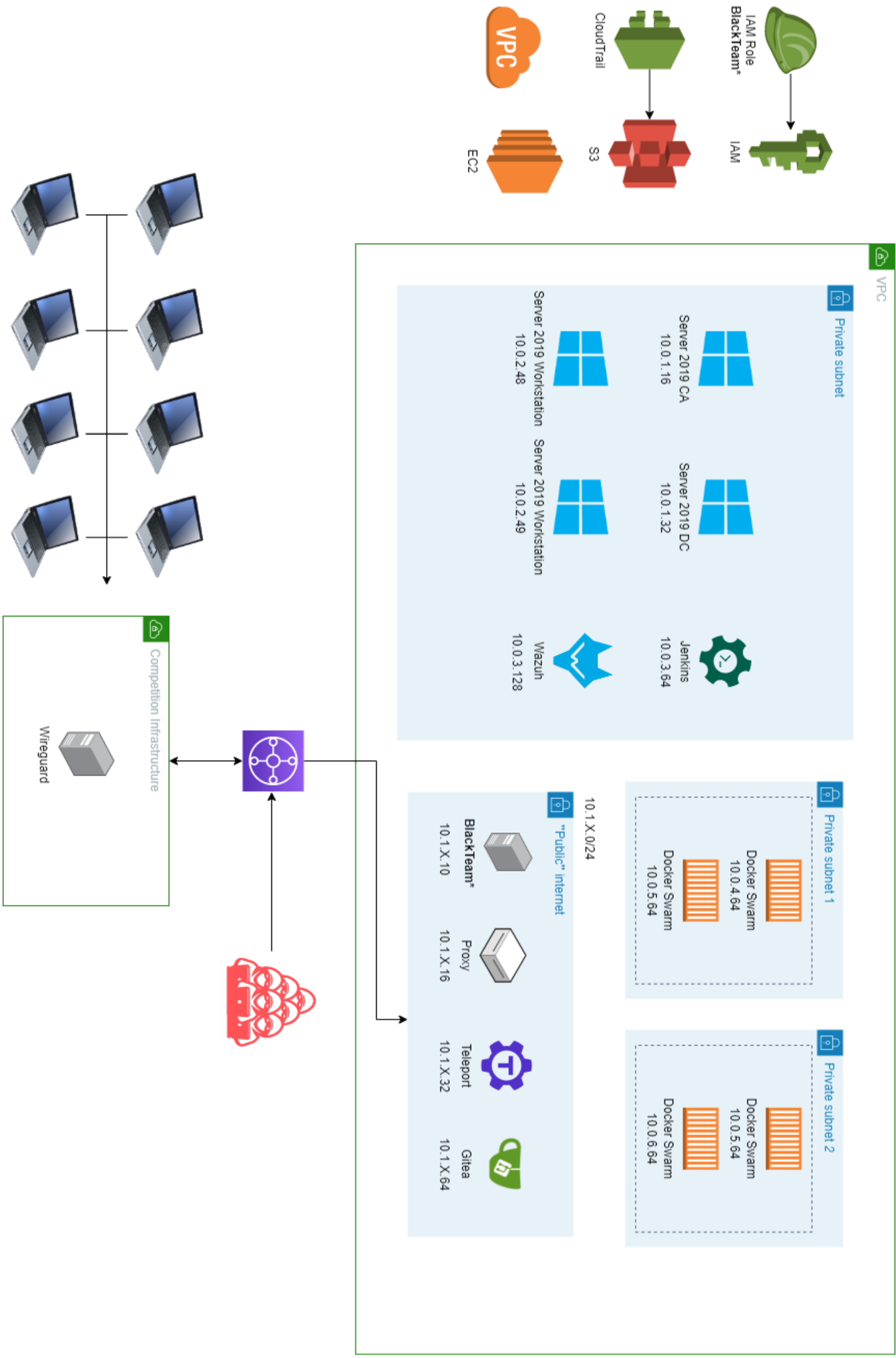
The launch was fantastic! Sure, a couple hiccups here and there–but we've learned a lot and most importantly, the customer is happy. Sales has done a great job keeping our customers on the waitlist excited. Now we're excited to onboard them!

The Dev and Infra teams have been working hard to push new features. We're leaning more heavily on AWS technologies as well as Jenkins features now that we're shipping software developed in-house. We're also excited to implement Teleport to lock down company asset access further. There were some close calls last time. We definitely want to protect our customer data and maintain our reputation.

Thanks so much for being a part of our team and we look forward to you growing together with us as we take this new step toward our future as an organization.

Kind Regards,

Dade Murphy, CIO
Prometheus Group


IAM Role
BlackTeam*
IAM
CloudTrail
S3
VPC
EC2
10.0.0.0/16
VPC
Private subnet
Server 2019 CA
10.0.1.16
Server 2019 DC
10.0.1.32
Server 2019 Workstation
10.0.2.48
Server 2019 Workstation
10.0.2.49
Jenkins
10.0.3.64
Wazuh
10.0.3.128
Private subnet 1
Docker Swarm
10.0.4.64
Docker Swarm
10.0.5.64
Private subnet 2
Docker Swarm
10.0.5.64
Docker Swarm
10.0.6.64
10.1.X.0/24
"Public" internet
BlackTeam*
10.1.X.10
Proxy
10.1.X.16
Teleport
10.1.X.32
Gitea
10.1.X.64
Competition Infrastructure
Wireguard