HOSTED BY

PACE UNIVERSITY

IN COORDINATION WITH

IN PARTNERSHIP WITH

Raytheon
An RTX Business

PRESENTS THE

NORTHEAST COLLEGIATE CYBER DEFENSE COMPETITION

NECCDC 2024 SEASON QUALIFIER

BLUE TEAM PACKET

v.4 | Revised 2024-02-02

We would like to acknowledge the support from the National Science Foundation under Grant No. 2043095

CONTENTS

NORTHEAST COLLEGIATE CYBER DEFENSE LEAGUE 3
NECCDC 2024 SEASON 3
COMPETITION GOALS 3
QUALIFIER OVERVIEW 4
NECCDC 2024 SEASON SPONSORS 5
QUALIFIER EVENT SCHEDULE 7
COMPETITION (Game Points) == SATURDAY, 03 FEBRUARY, 2024 7
COMPETITION ORGANIZATION 7
COMPETITION RULES 9
Competitor Authentication 9
Questions and Answers 9
SCORING OVERVIEW 9
System Scoring 10
Inject Scoring 10
Red Team Activity 11
Incident Response Template 11
NECCDC 2024 SEASON THEME 12
NECCDC 2024 SEASON SCENARIO 13
QUALIFIER INFRASTRUCTURE 14
MANAGEMENT BRIEF 15
APPENDIX I: Qualifier Infrastructure Diagram 17
APPENDIX II: Kubernetes Diagram 18

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 on X/Twitter: @neccdl
Follow on Mastodon: @neccdl@infosec.exchange
GitHub: github.com/NE-Collegiate-Cyber-Defense-League

We would like to thank Pace University for hosting the qualification infrastructure for this season!

Thanks also to AWS for supporting the cloud environment for the competition!

NECCDC 2024 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

QUALIFIER OVERVIEW

The NECCDC 2024 Qualifier is managed by this year's competition host (Pace University), 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 private energy company that recently acquired another energy company that has significant critical infrastructure investments in the renewable energy sector including ownership of a hydroelectric dam. Discovering that the cybersecurity oversight of especially the IT/OT aspects as well as general understaffing and risk management was poorly performed, the company engaged a preliminary assessment team to determine priorities. It is now hiring an elite team of cyber security engineers to their Cascade Falls Dam location.

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.

Qualifying teams from the NECCDC 2024 Qualifier on February 3, 2024 will have the opportunity to participate in the NECCDC 2024 Regional, expected to take place March 23 - 25, 2024 at Pace University (1 Pace Plaza, New York, NY) - the host organization for 2024.

NECCDC 2024 SEASON SPONSORS

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

Additional information regarding sponsorships for the NECCDC 2024 Season can be found at https://neccdl.org/neccdc/2024/howtosponsor/ and https://neccdl.org/neccdc/2024/sponsors/

VIBRANIUM
U.S. National Science Foundation
Raytheon An RTX Business

PLATINUM	
PACE UNIVERSITY	PACE UNIVERSITY Seidenberg School of Computer Science and Information Systems

SILVER
Networking Academy
paloalto NETWORKS
RSM
CROWDSTRIKE

BRONZE
FORTRA

OTHERS? HELP CONNECT US WITH POTENTIAL SPONSORS!
Others TBD, in contracting. **Let us know if you have someone you know who is interested in sponsoring!** **Have them contact sponsor@neccdl.org for more information.**

QUALIFIER EVENT SCHEDULE

- Please be in Discord and On-Site at your educational institution-provided space ~20 minutes prior to Check-in
- Have webcam/video capacity + Student ID for authentication
- Work with your Team's Moderator(s) (and be prepared to feed them) - if your coach hasn't already, make sure they submit moderator contact information for training and coordination. The original deadline is Jan 19, 2024.

COMPETITION (Game Points) == SATURDAY, 03 FEBRUARY, 2024

TIME (EST, 24-Hour format)	ACTIVITY	NOTES
09:00	Blue Team Check-in Begins in Discord / Should be on on-site location at your educational institution	Have student ID accessible
09:30	Welcome Inject	Injects in Google Classroom
10:00	Competition Begins	Scoring starts and Blue Team access to environment systems enabled. Credentials are shared in Discord team channels.
14:30	Competition Ends	Blue Team access to environment systems will be disabled.

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 National CCDC via: https://www.nationalccdc.org/index.php/competition/competitors/registration (due by Jan 19, 2024). 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 two (2) or more moderators. See National CCDC rules for full eligibility criteria.
- Technical access issues and the like should be **@BlackTeam** in Discord in your specific Team channel 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 the 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. You can @WhiteTeam for any inject-specific questions that are not sent through moderators.

- Each team competing remotely from their home institutions must have at least one (1), ideally two (2) or more, site moderator(s) present at the blue team location as well as within the virtual environment during active times of the competition provided by the Team Representative.
- Moderators are responsible to perform tasks such as:
    - Undertake/Review moderator training offered by NECCDC
    - Gain familiarity on using the required communication tools (e.g. Discord)
    - Submit questions/requests from the blue team members to the designated communication #channels
    - Check rosters to authenticate competitors at check-in
    - Ensure that competition rules are followed and any violations or situations of concern are reported to the White Team senior staff
    - Submit survey feedback based on competition/team observations near the end of Qualifier (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, logistics, and sponsor relations coordinators.

Orange Team

The competition staff builds an integrated scenario storyline and simulates user activities in a manner that integrates with and contextualizes Black and White team activities. The Orange Team is also responsible for the corporate branding and image of the contest. The team also

may include individuals who act as employees, clients, and other external acting parties, e.g., C-suite personnel, law enforcement agents, etc. These actors may interact with infrastructure systems and the Blue Team members 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 a list of published Blue Team GitHub links for Qualifier. Besides these approved repositories, teams are not allowed to use any other privately team-developed staging materials.

Competitor Authentication

Competitors will be expected to show a valid/current student ID, issued by their educational institution to authenticate during the qualifier check-in. Authentication will be done by room moderators on-site at your educational institution.

Blue team members should ask for rule clarifications through their room moderators at any time. Scenario-based activities can take a wide variety of paths, so if there is any doubt or need for clarification on injects or other competition-related events, make sure to check with room moderators who can relay questions to appropriate competition staff.

Questions and Answers

We maintain a set of Questions and Answers from our information sessions, publicly available here: FAQ. As teams onboard, updated communications will be in Discord.

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 different risks and criticality. 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 number of points reduced as a result of Red Team activity.

System Scoring

System availability and integrity make up half of the Blue Team's 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. 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 and can experience lag when submitting.

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 the combined service and inject scores. 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 when incidents occur in order to potentially reduce future Red Team impacts
- 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

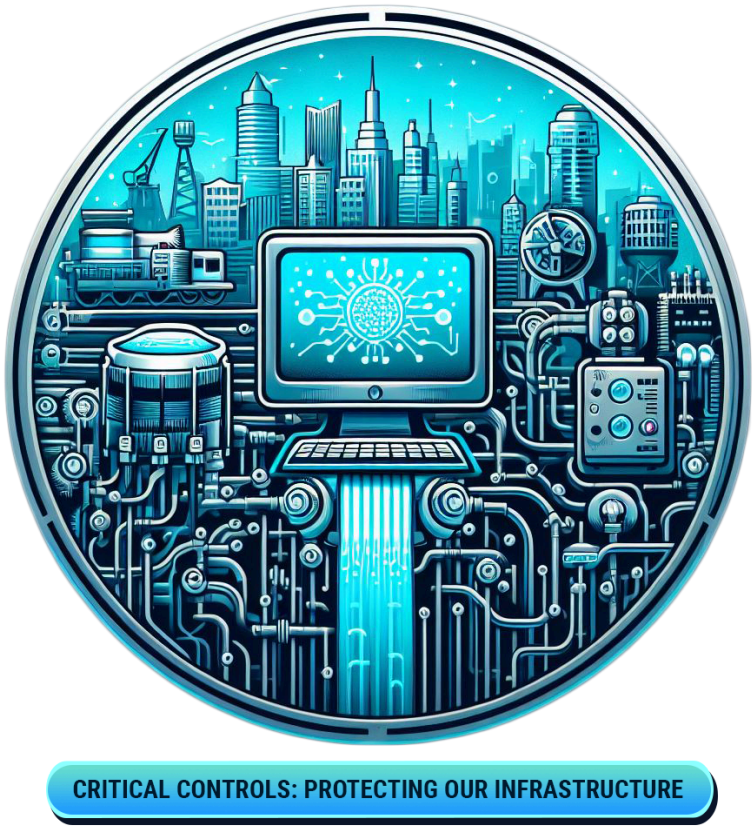
NECCDC 2024 SEASON THEME

Critical infrastructure, which includes power grids, water systems, transport networks, and healthcare facilities, is pivotal to our nation's operation. Cyberattacks on these systems can not only disrupt daily life and endanger national security but also have profound economic and social implications. These infrastructures often blend IT with OT to boost production and meet demands, presenting a unique cybersecurity challenge. While defending the established IT domain is already demanding, protecting the less-prepared OT environment intensifies the task, with both tangible and intangible damages at stake.

Core Foci -

- General
    - Resiliency
    - High Availability
    - Vulnerability Management
    - Endpoint Security
- Identity Management
    - Active Directory
    - RHEL IDM/FreeIPA
- Containerization
    - Kubernetes
    - Docker / Containerd
- Additional Technologies
    - Ansible
    - Secrets/Credential Management
    - SIEM (Wazuh)

NECCDC 2024 SEASON SCENARIO



The scenario is a private energy company that recently acquired another energy company that has significant critical infrastructure investments in the renewable energy sector including ownership of a hydroelectric dam. Discovering that the cybersecurity oversight of especially the IT/OT aspects as well as general understaffing and risk management was poorly performed, the company engaged a preliminary assessment team to determine priorities and is now hiring an elite team of cyber security engineers to their Cascade Falls Dam location.

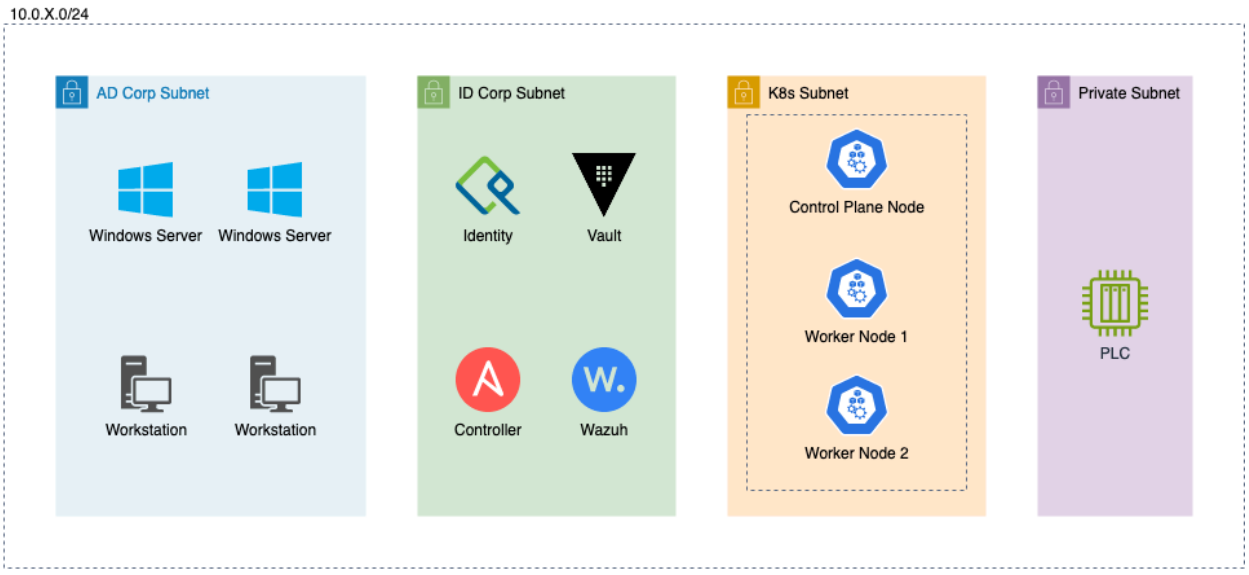
QUALIFIER INFRASTRUCTURE

Note: Ensure you have Wireguard installed on machines used for competition prior to start of Qualifier. Employees should be prepared to assess the various aspects of the organization's infrastructure. Technologies that may be found in the company's infrastructure include*:

Windows Server 2019 Microsoft Active Directory WMI, SSH, Telnet, and RDP Certificate Authorities Kerberos Windows-based DNS RHEL Identity Management	Kubernetes Containerd Docker Ubuntu RHEL Wazuh Ansible	HAProxy Nginx GitLab PostgreSQL Red Hat Identity Management (IdM) Semaphore Nextcloud

Remote Access will be provided by Black Team to allow teams to connect to the Qualifier environment from their personal/campus computers and should be on an on-site location provided by their own educational institution. **It is critical that teams use the beta period to test and validate this remote access solution.**

Additional details on testing/setup instructions will be provided by competition staff as we get closer to the date of the Qualifier. **See Appendix I for a larger version of the Qualifier Infrastructure Diagram (below), and see Appendix II for the Kubernetes Diagram.**



MANAGEMENT BRIEF

Company: Rust Energy

Location: New York

Origin and Growth:
Rust Energy, a pioneer in electric car battery manufacturing, began its journey in New York City. Quickly establishing itself as a key player, Rust Energy secured significant contracts with industry giants like Tesla and Ford. This partnership propelled the company into a period of exponential financial growth, solidifying its position in the market.

Rivalry and Acquisition:
Simultaneously, a competitor, ElectraPower Dynamics, emerged as a notable force in the electric battery industry, yet with a market share of only 19.9% compared to Rust Energy's commanding 62.92%. ElectraPower Dynamics also had significant investments in renewable energy, notably owning the Cascade Falls Hydroelectric Dam, a critical infrastructure for New York City's water supply.

However, ElectraPower Dynamics faced a severe setback following a cyber attack by an Advanced Persistent Threat (APT) group. The refusal to negotiate with the APT led to a scandalous exposure of malpractices, plummeting stock values, and near bankruptcy. Seizing this opportunity, Rust Energy acquired ElectraPower Dynamics.

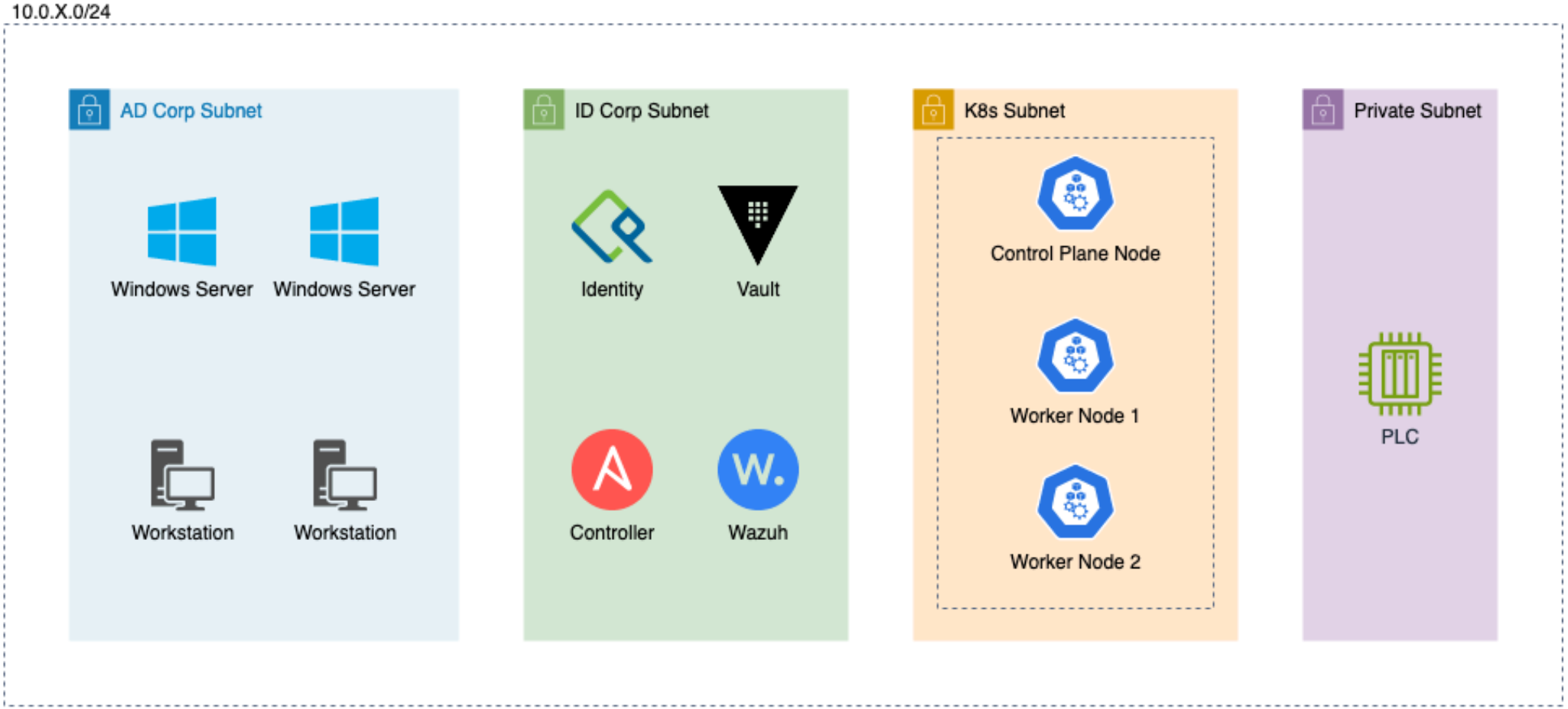
Integration and Challenges:
This acquisition marked Rust Energy's entry into the renewable energy sector. The company quickly integrated the high-quality battery products from ElectraPower Dynamics. However, managing the Cascade Falls Hydroelectric Dam presented unforeseen challenges. Due diligence focused on financials had overlooked the sector's operational and infrastructural aspects.

A critical issue was soon uncovered: the hydro-electric sector, specifically the Cascade Falls Dam, was understaffed, technologically outdated, and in disarray. The limited IT staff, originally hired for hydro-pump mechanics, lacked the expertise to secure the infrastructure against cyber threats.

Cyber Security Overhaul:
In response, Rust Energy deployed a preliminary assessment team to initiate the integration of essential services. Recognizing the gravity of the situation, Rust Energy is now escalating its efforts. An elite team of eight top cyber security engineers is set to be deployed to Cascade Falls Dam. Their mission is to address security vulnerabilities and overhaul the IT infrastructure, ensuring the safety and security of this critical facility.

The Future:
As Rust Energy ventures into this new domain, it remains committed to innovation, security, and reliability. The challenges ahead are daunting, but with a focused team and a clear vision, Rust Energy is poised to not only address the legacy issues of ElectraPower Dynamics but also to secure a sustainable and safe future for its customers and the community it serves.

APPENDIX I: Qualifier Infrastructure Diagram



APPENDIX II: Kubernetes Diagram