HOSTED BY

PACE UNIVERSITY

IN COORDINATION WITH

IN PARTNERSHIP WITH

Raytheon
An RTX Business

PRESENTS THE

NORTHEAST COLLEGIATE CYBER DEFENSE COMPETITION

NECCDC 2024 SEASON REGIONAL

BLUE TEAM PACKET

v.1.2 | Revised 2024-03-20

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

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 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

REGIONAL OVERVIEW

The NECCDC 2024 Regional competition this year is hosted by 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 involves a private energy company, Rust Energy, that recently acquired another energy company for its significant critical infrastructure investment in the renewable energy sector, including ownership of a hydroelectric dam. Providing this new source of energy to its electrified bus charging depots, as well as to its market traders, was immediately the top priority for its engineering and IT divisions. Rust Energy's short-term business goals resulted in weak cybersecurity, with the only IT focus being the expedited integration of newly acquired OT production components with their existing energy distribution systems. Anything in conflict with this progress, including enforcement of cybersecurity best practices, was met with ruthless contempt from upper management.

Within a few months of this recklessness, several incidents of equipment malfunction caused disruption to the region's power grid. Each incident was related to systems operated by Rust Energy, resulting in state and federal audits of the company's safety controls and cybersecurity. Discovering the gross level of cybersecurity oversight, especially around IT/OT integration, as well as general understaffing and lack of risk management, the company engaged a preliminary assessment team to determine priorities. It is now assigning an elite team of cybersecurity engineers to its 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.

The winning team from the NECCDC 2024 Regional in March will advance to the CCDC National Championship The second place team will have the opportunity to compete in a wildcard competition for a spot in nationals.

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	
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY CISA	NATIONAL SECURITY AGENCY UNITED STATES OF AMERICA

BRONZE
FORTRA

SUPPORTER
BATTELLE It can be done

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.**

REGIONAL EVENT SCHEDULE

Saturday, March 23	**Event**	**Location**
8:00 am - 9:00 am	Check In, Name Tag Distribution	Reception Area/Tabling Hub Student Center, Welcome Center
8:00 am - 9:00 am	Breakfast (informal breakout)	
9:00 am - 9:30 am	Competition Opening	Student Center
10:00 am - 5:00 pm	NECCDC Student Competition	6th Floor
1:30 pm - 2:15 pm	Team Lunch	Student Center
Sunday, March 24	**Event**	**Location**
8:00 am - 9:00 am	Breakfast	Student Center, Welcome Center
9:00 am - 9:30 am	Day 02 Debrief	Student Center
9:30 am - 4:00 pm	NECCDC Student Competition	6th Floor
12:00 pm - 1:00 pm	Coaches' Meeting	5th Floor
12:30 pm - 1:15 pm	Team Lunch	Student Center
6:00 pm - 9:00 pm	Recruitment Event, Dinner	Student Center, Welcome Center
Monday, March 25	**Event**	**Location**
8:30 am - 9:30 am	Breakfast (informal breakfast)	Student Center, Welcome Center
9:30 am - 10:00 am	Keynotes	Student Center, Welcome Center
10:00 am - 10:40 am	Panel Discussions	Student Center, Welcome Center
10:45 am - 12:30 pm	Debrief & Awards	Student Center, Welcome Center
12:30 pm - 2:30 pm	Lunch, Networking	Student Center, Welcome Center

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.
- 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.

- Moderators are responsible for performing 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 the competition (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. Besides these approved repositories, teams are not allowed to use any other 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.

Peripheral Devices

Competitors are permitted to use their own peripheral devices, including, mice, keyboards, headphones, etc. However, to use such devices, please submit a formal request to **blackteam@neccdl.org** for pre-approval well in advance of packing your belongings. Please include any relevant device information, e.g., brand, model number, as well as photograph. If any participant requires specific devices due to special accommodations or medical reasons, please communicate this in the formal request. Approved devices will be recorded. All devices will be subject to a daily vetting process by the Black Team at the start of each competition day.

Note: Keyboards and mice will already be provided to each team.

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. Use of AWS that incurs excessive cost will negatively impact scores.

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.

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.

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

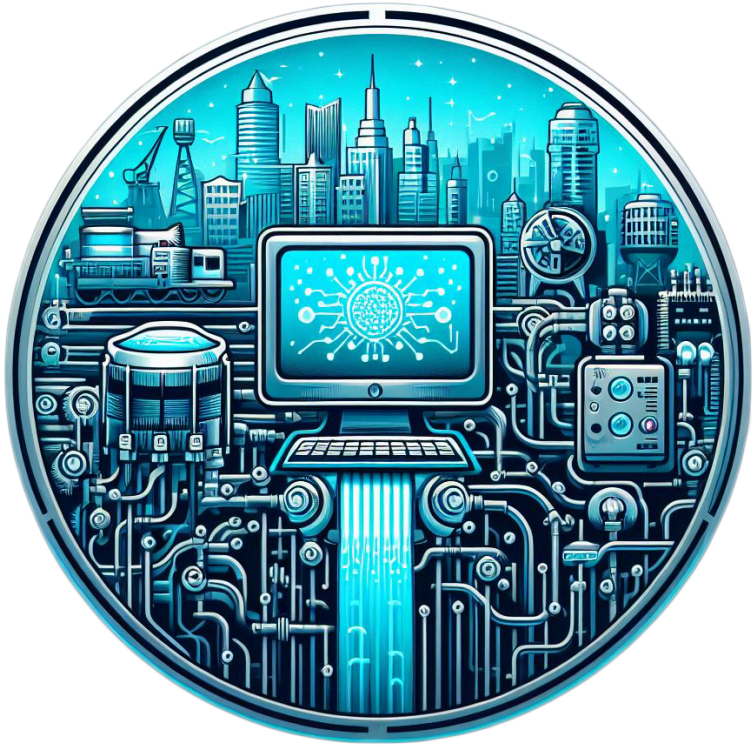
Critical infrastructure, which includes power grids, water systems, transport networks, and healthcare facilities, is pivotal to our nation's operation. Cyberattacks on these systems can not only disrupt daily life and endanger national security but also have profound economic and social implications. 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
    - AWS IAM
- Containerization
    - Kubernetes
    - Docker / Containerd
    - OCI
- Additional Technologies
    - Secrets/Credential Management
    - Wazuh
    - GitOps

NECCDC 2024 SEASON SCENARIO



CRITICAL CONTROLS: PROTECTING OUR INFRASTRUCTURE

Despite its success in electric car batteries, Rust Energy transitioned into a major power supplier through acquisitions and innovation, including AI-powered energy trading. Capitalizing on a competitor's losses, it acquired both a hydroelectric dam and technology to support an electrified bus network. However, its reliance on a rival's distribution points led to power supply issues, prompting them to utilize the dam as a renewable energy source for the bus depots. This plan was challenged by the dam's only recent focus on cybersecurity, requiring significant efforts to ensure its secure integration of IT and OT systems. While facing daunting challenges, Rust Energy remains committed to innovation, security, and sustainability for the future. Its dedicated elite team of cybersecurity engineers (the Cascade Falls Dam Integration Team) has its work cut out for it.

REGIONAL INFRASTRUCTURE

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	Kubernetes	HAProxy
Microsoft Active Directory	Containerd	Nginx
WMI, SSH, Telnet, and RDP	Docker	GitLab
Certificate Authorities	Cloud networking	PostgreSQL
Kerberos	Ubuntu	Nextcloud
Windows-based DNS	RHEL	ArgoCD
Red Hat Identity Management (IdM)	Wazuh	AWS IAM
CloudTrail	Ansible / YAML	DOOM

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 regional.

See the Appendix for a larger version of the Infrastructure Diagram

MANAGEMENT BRIEF

Company: Rust Energy | **Location**: New York | **Industry:** Energy

Origin and Growth:
Rust Energy, a pioneer in electric car battery manufacturing, began its journey in New York City. Quickly establishing itself as a national key player, Rust Energy secured significant contracts with automotive industry giants. This partnership propelled the company into a period of exponential financial growth, solidifying its position in the market. Through its recent acquisition and market leadership, Rust Energy became profitable enough to become a major supplier and trader of electrical power in the North American market, controlling nuclear, fossil fuel and renewable sources. As it continues to grow, Rust Energy is at the cutting-edge of technology strategy and is one of the first companies in the industry to use artificial intelligence for energy market trading.

Strategy and Acquisition:
Due to the impact of cybersecurity exposures, Rust Energy's competitor, ElectraPower Dynamics (a notable force in the electric battery industry), experienced near bankruptcy and plummeting stock value as well as unintended release of confidential documents.This allowed Rust Energy acquire ElectraPower Dynamics and, with it, the Cascade Falls Hydroelectric Dam. In addition, the merger with ElectraPower Dynamics allowed Rust Energy to have the resources to move their technology towards the development of a recently launched electrified bus service, which serves several large municipalities in the northeastern United States including a network of electrified bus charging depots supported by Rust Energy and backed-up by ElectraPower Dynamics super-efficient charging technology - allowing for recharge of bus batteries within minutes instead of hours. During times when battery charging

was not needed, Rust Energy could send excess energy to the market, balancing production and supply with this varied demand through sophisticated IT/OT integration.

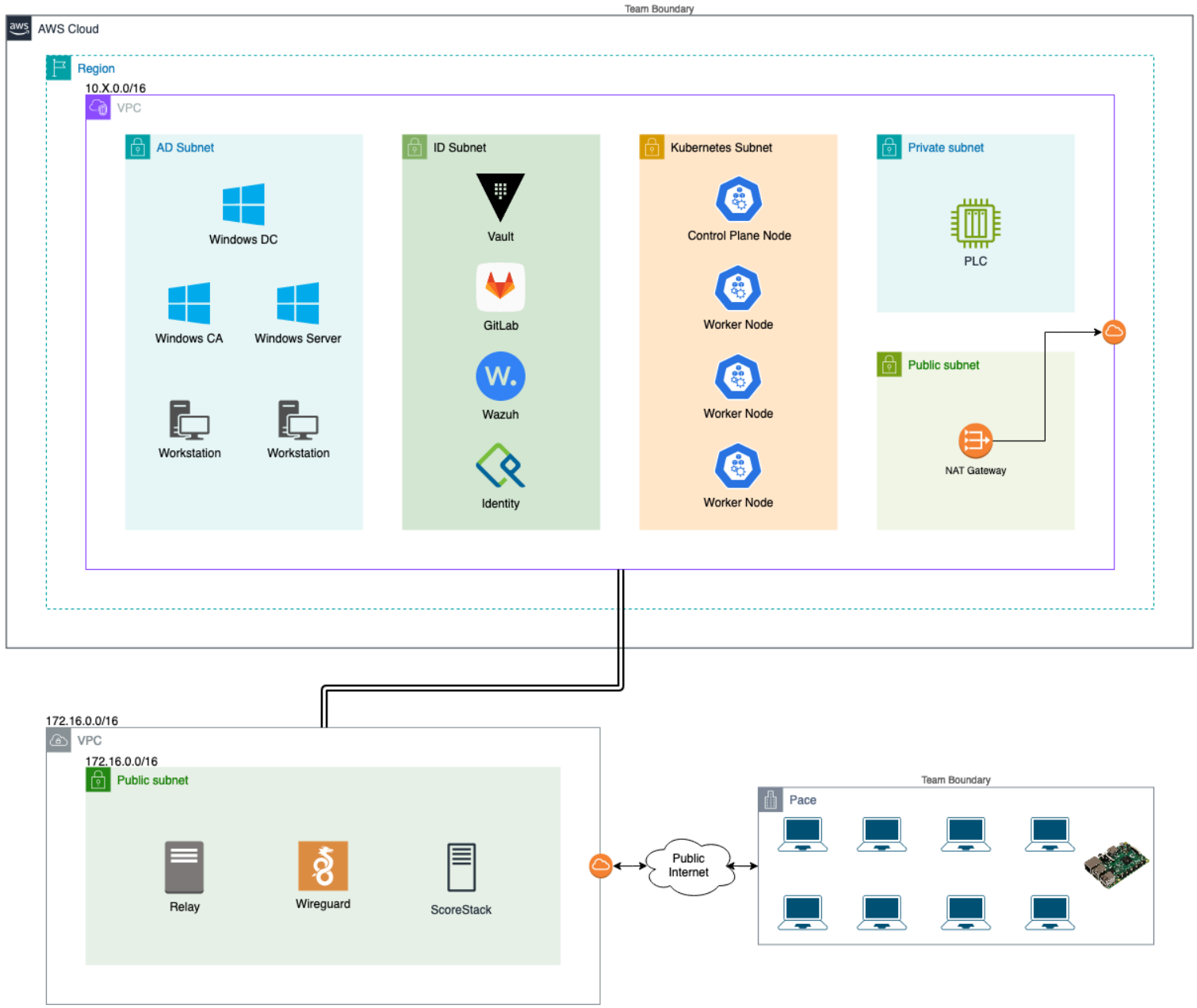
Power Supply Issues & Solution
Despite being a dominant force in the distribution of electricity in the northeast, a rival company, GridXL, controlled several distribution points that affected power flow to Rust Energy's electrified bus charging depots. When the energy supply to several of these depots became unstable and unreliable, Rust Energy accused GridXL of purposefully manipulating the energy supply to disrupt Rust's operations for competitive advantage. In order to alleviate instability of the power supply due to the reliance on the GridXL controlled distribution points, Rust Energy's CEO Jayson Rust decided to take advantage of the recently acquired Cascade Falls Hydroelectric Dam. Rust's plan was to move some local bus charging depots to locations that could better utilize the Cascade Falls Dam as a potential renewable energy source. This would then be able to be expanded to use other dams throughout the region.

Integration and Challenges:
A known challenge was that Rust's hydroelectric facilities, including the Cascade Falls Dam, were understaffed, technologically outdated, and were vulnerable to many threats, including cyberattack. The limited IT staff, originally hired for hydro-pump mechanics, lacked the expertise to secure the infrastructure against emerging cyberthreats. In response, Rust Energy deployed a preliminary assessment team to initiate the integration of essential services.

Cyber Security Overhaul:
An elite team of eight top cyber security engineers were deployed to Cascade Falls Dam. Their mission was to address security vulnerabilities and overhaul the IT infrastructure, ensuring the safety and security of the critical facility. Although the Cascade Falls Integration Team was recently brought in to help focus on these risks, the increased dependence on the Cascade Falls Dam facility to support the electrified bus charging depots brought to light some significant issues related to the integration of IT/OT elements, that if not dealt with, would lead to severely unintended consequences. Recognizing the gravity of the situation, Rust Energy is now escalating its efforts.

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 their hydroelectric infrastructure, but also to secure a sustainable and safe future for its customers and the community it serves.

APPENDIX: REGIONAL INFRASTRUCTURE DIAGRAM




Cluster
Control Plane Node
kubelet
coredns
storageClass
scheduler
controller-manager
postgresql
networkPolicy
haproxy-ingress
kube-proxy
Worker Node
kubelet
ingress
nextcloud
csi driver
postgresql 0
falco
apiserver
haproxy-ingress
kube-proxy
Worker Node
kubelet
argocd server
repo server
redis
etcd
dex server
nextcloud
haproxy-ingress
kube-proxy
Worker Node
kubelet
Doom

CHANGELOG

Change	Date	Description
v1.0	Feb 26, 2024	Initial release
v1.1	Mar 4, 2024	Update infrastructure diagram
v1.2	Mar 21, 2024	Updated Event Schedule & Raytheon RTX logos
v 1.3	Mar 22, 2024	Updated CISA & NSA logos for Silver, some minor grammar issues / typos