Introduction

April 6, 2026

Welcome to Astra 9, the frontier outpost of the Palmetto Core Drilling Corporation (PCDC). True to PCDC's founding ethos, "for the greater good of humanity," Astra 9 represents the corporation's boldest commitment to deep space resource extraction. Anchored to asteroid Druida, the colony sits atop the largest confirmed deposit of Schwartz, the ultra rare material projected to redefine next generation computing and secure PCDC's dominance across the interstellar supply chain.

The PCDC team works around the clock to ensure humanity benefits from the boldest ventures into deep space. Through its comprehensive services, PCDC works closely with interplanetary partners and industry leaders to ensure that its operations remain a vibrant hub for innovation and opportunity. With a forward-thinking approach, the PCDC team is committed to making a positive impact on both terrestrial and interstellar economies, ensuring long-term prosperity and stability for future generations.

As part of its core mission, the department focuses on the strategic development and efficient extraction of vital resources to ensure a thriving and sustainable future. Our frontier colony, Astra-9, is a testament to this commitment, positioned to deliver Schwartz, a material projected to redefine next-generation computing. The PCDC team is the reason we are able to pioneer such advanced operations, maintaining the quality and reliability of our complex extraction and supply logistics. Through its efforts, PCDC plays a key role in supporting technological growth and fostering a higher standard of living across the galaxy.

PCDC strives to continue its role as a consistent, ethical, and reliable leader in resource development. Attentive operational management, a dedicated staff, and a clear focus on the future are what set the PCDC team apart. We are excited for you to join us in this historic endeavor!

Palmetto Core Drilling Corporation

For The Greater Good of Humanity

https://pcdc-sc.com

April 6, 2026

Blue Team,

Welcome to the Palmetto Core Drilling Corporation! We are certain that your team's collective skills and innovative approach to IT will be instrumental in advancing our technological objectives. As the new IT team, your department's function is central to our operations, and we will be relying on your leadership to uphold the performance, stability and security of PCDC's systems, infrastructure and digital services.

In a recent initiative to optimize long term operational efficiency, the deployment of the Astra Tactical Intelligence Computer (ATIC), an experimental AI system intended to automate cybersecurity oversight across all PCDC assets, was authorized. It exceeded expectations, eliminating nearly the entire human cybersecurity workforce overnight. With hundreds of seasoned professionals displaced by ATIC, Astra-9's critical infrastructure, life support, automated drilling, supply logistics, and long range communications now rely on a skeleton crew of overworked system administrators struggling to maintain baseline functionality, let alone defend against coordinated threats.

Rival mining conglomerates, anti-extraction hacktivist groups, Nation-state competitors and organized space crime syndicates are threatening the productivity and safety of Astra-9. Your team must work to maintain drill uptime, secure communications, protect supply routes, and ensure the safety of the Schwartz extraction crews whose work underpins PCDC's future.

As the risk of data breaches, ransomware, phishing, and denial of service attacks continue to grow, it is paramount the security of our infrastructure be of the utmost importance to continue mining Schwartz and restore operational integrity across Astra-9. PCDC has hired your team to ensure all databases are secured, company and customer information is protected, and professional service is always provided. Unfortunately, the previous team abruptly vacated their positions, so we cannot guarantee the current state of any service or accuracy of the network diagram.

Your assignment is clear. Join PCDC and help reestablish safe, stable, and profitable off-world operations. The success of Astra-9, and the unprecedented fortune it promises, now depends on the teams prepared to defend it.

Welcome to Palmetto Core Drilling Corporation (PCDC)!

Regards,

Dark Helmet, CEO

TABLE OF CONTENTS

LIST OF APPENDICES

1.0 ACCOUNT INFORMATION

1.1 Initial Password List and Passbolt

At the start of the day, your team will be provided with your initial username and password information for all assigned assets.

Passbolt is provided to Blue Teams this year. Usage information below.

Passbolt link: http://192.168.40.111
Gold Team Email Server: http://192.168.40.13

To log into Passbolt, first ensure you have access to your Gold Team Email Account. This is an OOB (Out Of Band) email server. Log in with the provided credentials.

Username: blueXX@pcdc.local
Password: [provided in blue folder]

Your GPG Key may be required to log in. This will be emailed to you.

1.2 Password Changes

Changes of domain user accounts need to be reported to the Gold Team. Please submit password changes to the Gold Team Ticketing service in the **"Blue##-Helpdesk"** channel to lessen service check downtime. Failure to promptly report changes to domain user accounts can negatively impact service checks from the competition scoring engine. DO **NOT** CHANGE THE GOLD TEAM PASSWORD.

1.3 Email Access

Blue Teams will access their web-based email through the following web address: **https://mail.blueXX.pcdc.local** which is in scope. Any email from @pcdc.local is out of scope from the Red Team, however, that does not mean all emails from @pcdc.local are credible. All emails should be evaluated properly, and any suspicious activity should be reported immediately. Dark Helmet (dark.helmet@blueXX.pcdc.local) is the Chief Executive Officer for Palmetto Core Drilling Corporation and will be receiving various messages throughout the day. You are required to monitor this account at all times.

2.0 NETWORK OVERVIEW

Your assigned network consists of virtual machines that are accessed via standard remote access protocols (RDP and SSH) from the assigned laptops. Usernames and passwords for all assets will

be provided in the Initial Password List at the start of competition. An old network diagram was found and is located in Appendix A. Your network will consist of a mix of Windows and Linux operating systems.

2.1 Backups and Recovery

Teams do not have access to create backups of VMs or to recover a VM. Recovery requests can be submitted via a post in the **"Blue##-Helpdesk"** channel. Use the following format:

RECOVERY REQUEST
Request: _____
Justification: _____

If you do not use the correct request format, your recovery request will not be completed by the Gold Team. A detailed justification is required. Please note that recovery comes with a **substantial cost** and reverts the machine to its initial operating condition.

2.2 Active Defense

While this term is still being defined in industry (some say it includes offensive capabilities and others say it does not), we are referring to Defending Forward – countering or preventing a perceived cyber-attack by taking the fight to your adversary to take away their ability to perform offensive cyber operations against you. This is **not permitted under any circumstances**. Teams should keep their actions within their own assigned assets.

2.3 Report Station

Blue Teams will have a Report Station set up in their team areas this year (White Raspberry Pi and monitor). The Report Station is to be used by the Blue Teams to submit **ALL** Inject Responses and Incident Reports. Any Inject Responses or Incident Reports submitted from a laptop other than the Report Station will not be scored.

2.4 Injects

Injects and services are weighted evenly; it is disadvantageous to ignore injects.

Injects should be completed and submitted in the timeframe outlined in the assignment. While only on-time submissions can earn full credit, inject responses submitted late are eligible to receive partial credit.

If a business task (a.k.a. inject) requires multiple files for fulfillment, please compress the files into a single file in .zip format. This ensures that each inject has only one upload. Please name inject emails/files in the following format:

<teamNumber>_<injectNumber>_<injectTitle>

If an inject is directed to be submitted to the Gold Team Help Desk, use the **"Inject-Responses"** channel to submit the file.

AI is **NOT PERMITTED** to be used to write/submit any Inject Responses. If White Team or Gold Team suspects a Blue Team is utilizing AI to complete Injects, they reserve the right to question the Blue Team. Any Injects submitted that appear to be written utilizing AI will be rejected by the Gold Team and/or judges. Multiple warnings/indications of AI use will result in a point penalty. All Injects are **REQUIRED** to be submitted from the Report Station located in the Blue Team's competition area.

2.5 Incident Reporting

Accurate incident reports that can be verified will net your team a modest number of points in the end-of-day team assessment. Incident reports must contain a description of how and what occurred (including source and destination IP addresses, timelines of activity, passwords cracked, access obtained, damage done, etc), a discussion of what was affected, and a remediation plan. Overly inaccurate Incident Reports, especially abuse of Incident Reports, will net no points and may result in a loss of points.

Written reports must be coherent, detailed, and professional. Should you recognize that an incident has occurred, you may escalate an incident response report by submitting a post to the **"Incident-Reports"** channel in the Gold Team Help Desk. Use the following format:

INCIDENT REPORT:
Time(s) of Incident: _____
Asset(s) Affected: _____
Source (IP Address) of Attack: _____
Description of Attack/Incident: _____
Remediation/Plan to Resolve: _____

AI is **NOT PERMITTED** to be used to write/submit any Incident Reports. If White Team or Gold Team suspects a Blue Team is utilizing AI to write Incident Reports, they reserve the right to question the Blue Team. Any Incident Reports submitted that appear to be written utilizing AI will be rejected by the Gold Team and/or judges. Multiple warnings/indications of AI use will result in a point penalty. All Incident Reports are **REQUIRED** to be submitted from the Report Station located in the Blue Team's competition area.

2.6 Firewall Requests

The perimeter firewall will be managed by the PCDC Gold Team. All requests to modify the perimeter firewall must be submitted to the Gold Team via the Help Desk Ticketing system by submitting a post in the **"Blue##-Helpdesk"** channel. The request must be detailed, including IP addresses and a defined justification, otherwise it will be denied by Gold Team. Host based firewalls may be managed by the Blue Teams.

2.7 Laptop Information

Certain programs and applications have been setup on the laptop for use during the competition. They include but are not limited to:

- puTTY (SSH)
- Remmina (RDP)
- Chrome
- KeePass

2.8 Out of Band Information

The below items are out of band. Please pay careful attention to this section.

- The laptops and Report Station (Raspberry Pi) are out of band and are fully out of scope from the Red Team.
- The account "goldteam" on all physical machines, virtual machines and network devices is out of band and off limits for all Blue Teams and the Red Team.
- All existing machines and devices on the 192.168.40.0/24 network are out of band for the Red Team. Blue Teams are **not authorized** to block traffic from this network, unless a request is submitted to Gold Team and approved.
- Edge routers are off limits and out of band for all Blue Teams and the Red Team.
- Blue Teams are **not authorized** to block traffic from 192.168.20.10.

2.9 Gold Team Help Desk

There will be an online help desk system provided for teams to request assistance from the Gold Team, receive injects from the Orange Team, and submit competition items and documents to White Team. This can be reached by navigating to: http://helpdesk.pcdc.local:8065/login

Login credentials will be provided on the day of the competition.

Each team will have several chat channels available during the competition, as outlined below:

Blue##-Helpdesk | Where blue teams will ask questions about infrastructure, rules, general competition things, etc.

Competition-Announcements | Where the gold or white team will send competition-related announcements to the blue teams.

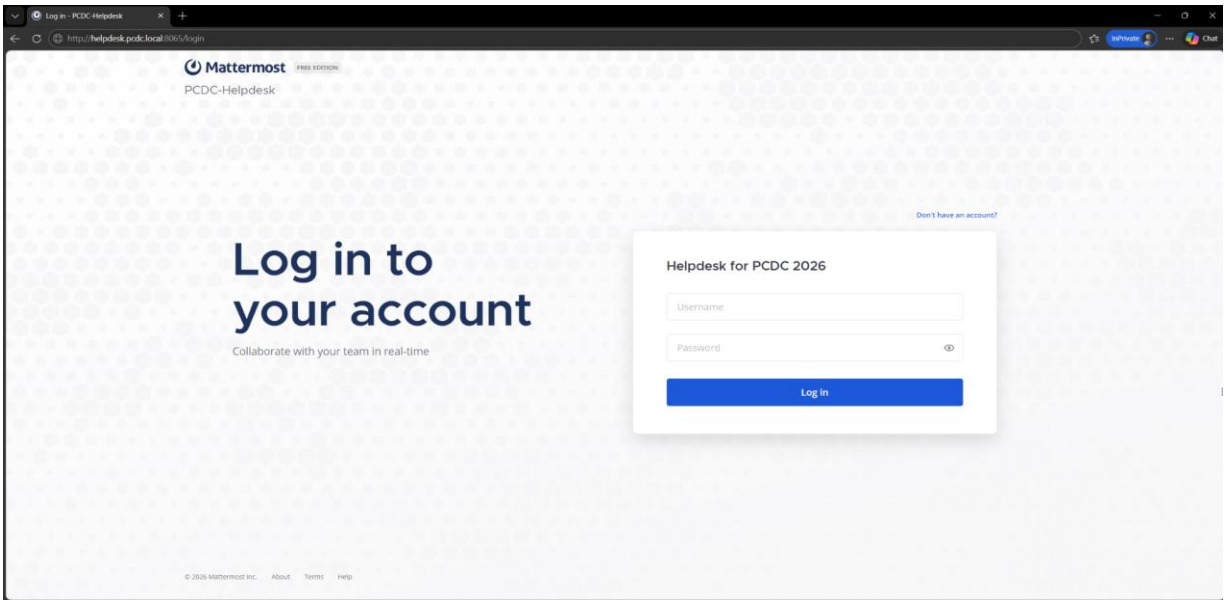
Incident-Reports | Where the blue team will submit incident reports for assessment

Incident-Alerts | Where the orange team may post injects for the blue teams

Inject-Responses | Where the blue team will submit inject responses for assessment

The Gold Team will only respond to questions asked in the Blue##-Helpdesk channel, and will respond as soon as possible to your request.

The "Town Square" channel should be ignored by the blue team. If it becomes utilized, the gold team will moderate with prejudice.



As a reminder, communication with other teams or any person(s) not a part of your respective Blue Team is **strictly prohibited.**

2.10 Physical Table Components

The 2026 competition will include physical boxes on the competitor tables as part of the scenario. These boxes contain proprietary microcontrollers and various electrical components to simulate critical and non-critical utility services on the board. The microcontrollers and other items within the box are logically **in scope** for Red Team and should be secured as part of the network. However, the boxes themselves and everything in them, are **not to be touched** by any member of a Blue Team or Red Team, unless given explicit permission from a Gold Team Lead.

3.0 TEAM ASSESSMENT

Employee performance is assessed at the end of each day. A single score is given to each team of employees.

3.1 Scoring

Scoring is based on keeping required services up, controlling/preventing unauthorized access, completing business tasks (a.k.a. injects) from colleagues, supervisors, and other departments throughout the day, and continuing to provide critical business products/services. Teams accumulate points by successfully completing these injects and maintaining services. Teams lose points by violating service level agreements, usage of recovery services, and successful penetrations by hackers, a.k.a. the Red Team.

Any team action that interrupts the scoring system is exclusively the responsibility of that team and will result in a lower score. Any team member that modifies a competition system or system component, with or without intent, in order to mislead the scoring engine into assessing a system or service as operational, when in fact it is not, may be suspended or fired. **Validation of this act will come with a significant points penalty** as it gives the Blue Team an unfair points advantage for a service that is not actually up.

4.0 ADDITIONAL INFORMATION

4.1 Blue Team Tools and Supplies

At the start of competition there will be supplies provided that could include notepads, pens, mouse pads, dry erase board markers and erases, folders, and network cable tools. Please be sure to leave these on the team tables at the end of the day.

4.2 Scripting

Scripting during the competition is allowed, and teams are encouraged to write their own scripts. All team written scripts should be submitted to the Gold Team Help Desk for review and approval prior to use. Any resources or tools pulled down from the internet to assist with scripting shall be **publicly available and free of cost.** The use of scripts or tools not created by the team should be submitted to Gold Team by opening a Help Desk ticket, **including the citation** for the tool or resource used if applicable. Failure to notify Gold Team of script or tool usage that was not provided by the Gold Team, or the use of non-public resources **may incur a penalty.**

If the blue team has written a script in advance of the competition, it may only be brought into the competition typed and printed on a sheet of paper or hand-written in a notebook. It must be submitted to the Gold Team Help Desk including any sources used for approval.

To submit a script or resource to Gold Team for approval, create a ticket with ***Request*** as the ticket category and use the below template:

SUBJECT: Resource Approval Request
BODY:
Team #: _____
Resource Name: _____
Citation: _____
How Resource Will Be Used: _____

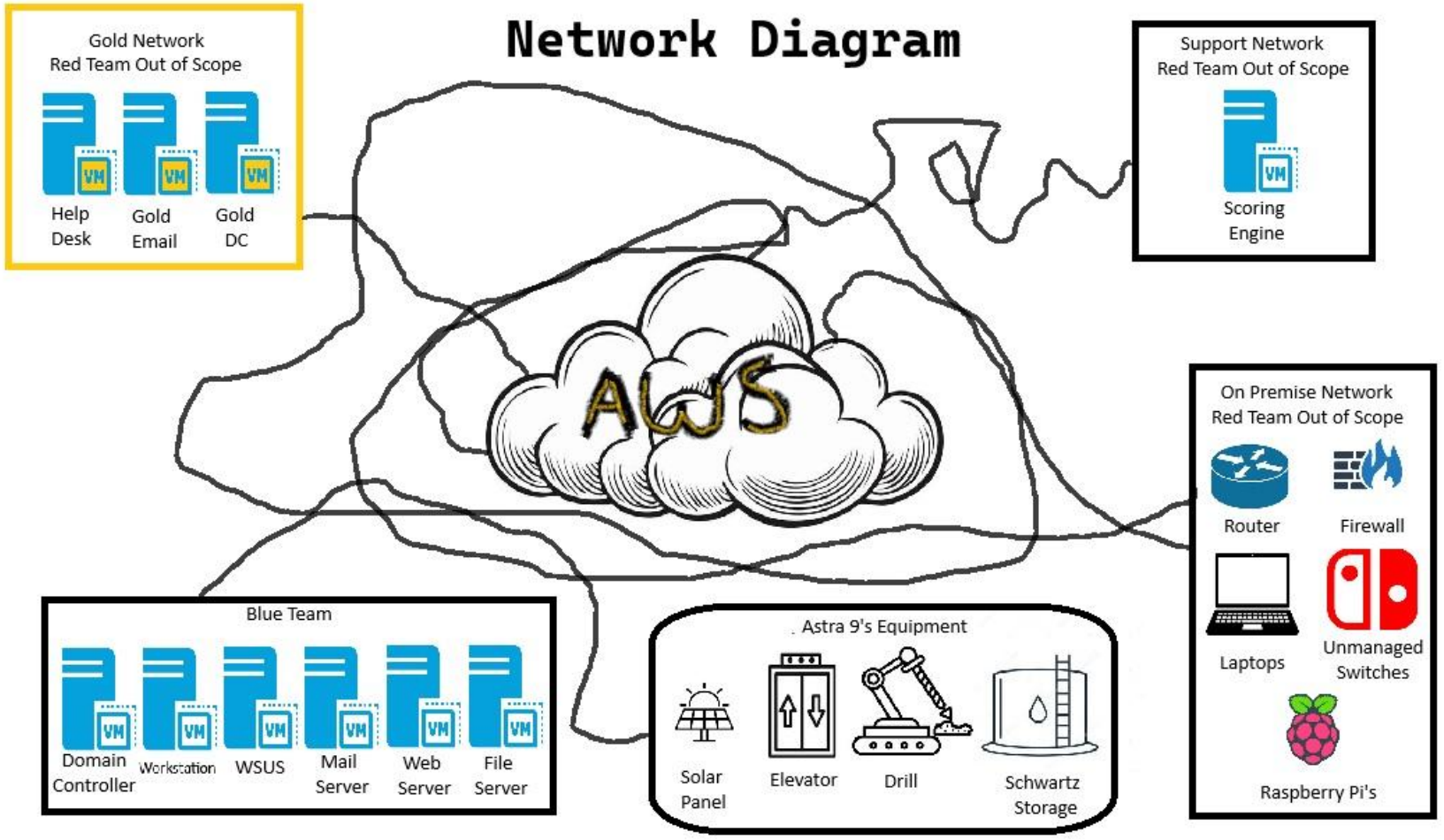
The request must be approved by Gold Team **prior** to use.

4.3 Artificial Intelligence (AI) Information

A note about AI: While the use of AI is expected and encouraged for background research, the use of personal accounts to log into AI tools (e.g. ChatGPT) is strictly prohibited. Blue Teams may only use free and publicly available versions of tools. The use of "free trials" of paid software is also prohibited. The use of personal accounts to access pre-stored material may result in significant penalties or ejection from the competition. White Team Leads, Judges, and Gold Team Leads reserve the right to question the Blue Team if it is believed an unapproved resource is being used.

While the use of AI is permitted for research and/or troubleshooting, it cannot be used to complete Injects or Incident Responses. This jeopardizes the integrity of the team's knowledge, skills and abilities which are an essential criterion for this competition. The use of AI will be monitored closely by judges. If it is determined that AI is being used to complete Injects or Incident Reports, it could result in significant penalties or ejection from the competition.

Appendix A Network Diagram



Appendix B PASSWORD TRACKER

Username	Password	Account Description

Appendix C ORGANIZATION CHART

This list only contains the Palmetto Core Drilling Corporation (PCDC) department leads and does not include all PCDC employees.

First Name	Last Name	Position	Domain Admin
Dark	Helmet	CEO	No
Emily	Evans	CISO	Yes
Princess	Vespa	CFO	No
Jeffrey	Sanders	Engineering - Mining Lead	No
Alice	Ziegler	Engineering - Site Sustainment Lead	No
Steven	Lewis	Information Systems Leadc	Yes
Jordan	Hall	Sales Lead	No
Wayne	Sweeney	Security Lead	No
Jerry	Ziegler	Shipping Lead	No

This Page Intentionally Left Blank