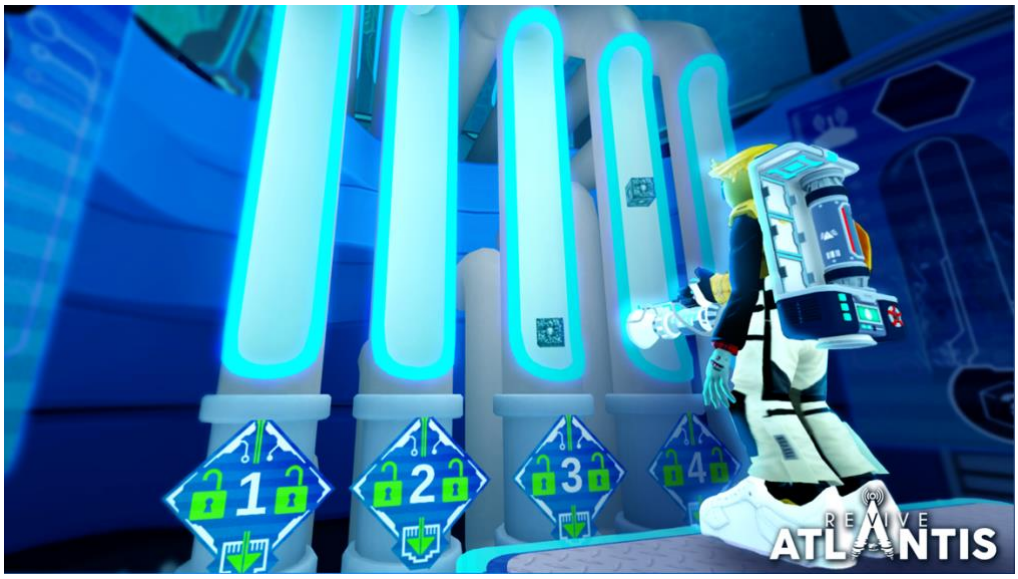
Revive Atlantis

A cybersecurity game hosted on the Roblox platform



REVIVE ATLANTIS LESSON PLAN

Summary:

"Revive Atlantis" is an educational game on the Roblox platform designed to teach high school students about cybersecurity through engaging gameplay.

The game's primary objective is to enhance students' understanding of cybersecurity concepts such as network security, asset protection, and vulnerability mitigation strategies. By immersing students in the captivating story of Atlantis, the game aims to inspire interest in cybersecurity and make the subject accessible and appealing to a broad audience.

Agenda:

30-45 minutes (1 class period or out of class discovery activity)

Suggested Uses:

This experience is designed for middle/high students with novice or intermediate knowledge in cybersecurity. The game can be used an introduction or reinforcement during the networking security module.

- **At-Home Learning:** The game serves as a self-directed learning experience where students can explore the concepts of cybersecurity at their own pace, reinforcing and extending classroom learning or satisfying personal interest in the subject.
- **After-School Programs:** "Revive Atlantis" can be used in after-school clubs, summer camps, or technology programs to increase interest in STEM fields.
- **In-School Learning (if policy allows):** "Revive Atlantis" can be used in a

High School Curriculum Guidelines Alignment:

7.1.1a Vulnerabilities are weaknesses that are exploited by a threat source

- Students will recognize that threats (malware, Meddler-in-the-Middle, Phishing, Denial of Service) exploit weaknesses (misconfiguration, weak credentials, lack of data encryption, open ports, open permissions, human factors, etc.).
- Students will understand that malware can exploit multiple vulnerabilities. (entry through Wi-Fi access points, users of a system, phishing)
- Students will understand that denial of service attacks can exploit vulnerabilities by flooding a system (through ports) with requests causing system disruption and drawing attention while other attacks occur.
- Students will understand that a Meddler-in-the-Middle attack can eavesdrop or intercept data due to the lack of encryption (plaintext data).
- Students will recognize that phishing uses deception to gain sensitive information and often install malware or ransomware.

2.3 It is easier to secure systems when you appropriately restrict unnecessary access, processes, resources, and users based on policy.

- Students will select security controls (access control, multi-factor authentication, antivirus/antimalware software, firewalls, intrusion detection systems) to appropriately restrict access to resources and users.
- Students will understand that closing ports is a mitigation to control traffic on ports and has

classroom setting, where a teacher can facilitate gameplay and integrate it into the cybersecurity curriculum (network security unit/vulnerability discussions)

Learning Pillar:

Players will respond to threats, strategically address vulnerabilities exploited in attacks, and select security measures to defend Atlantis.

Lesson Resources:

Teaching Guide with Visuals
Sample Use Case
Term Bank
Term Bank Key
Question Bank
Question Bank Key
Supplemental Career Awareness Activity
Quiz Questions from Atlantis gaming experience
Revive Atlantis on Roblox
Roblox Educator Resources
Videos on Teach Cyber YouTube

implications for the functionality of the network.

- Students will recognize that analyzing malware can help determine how it operates.
- Students will understand that threat monitoring tools require ongoing analysis and observation.

Additional Notes:

- Educator Guide to Roblox: https://create.roblox.com/docs/education/educator-onboarding/landing
- Please note that this game is hosted on the Roblox platform free of charge. The chat feature cannot be disabled. Teachers should check school policy on the use of Roblox.

Sample Use Case

Teachers should ensure that students can access Roblox. The teacher should follow school policy regarding use of the Roblox platform.

Unit(s): Revive Atlantis can be used with the Teach Cyber Cyber 1 course in

- Module 4--Data, Software, Hardware, and Network Security
- Module 7 -- Threats, Vulnerabilities, and Attacks: A Closer Look

Overview:
The teacher uses Revive Atlantis as a discovery learning activity outside of the formal classroom setting. In this scenario, the teacher is using Revive Atlantis prior to beginning the unit on Threats, Vulnerabilities, and Attacks.

Prior to assigning the students, the teacher should review all materials available.
The teacher should create the student assignment using the available term bank and questions.

Day 1:

- Teacher gives brief overview to students on what to expect in the Atlantis environment.
- Students are asked to spend 45 minutes outside of class playing the game.
- The teacher should assign terms and questions from the banks provided as a guided assessment or homework assignment.
    - Terms and questions that pertain to Threats, Vulnerabilities, and Attacks (along with countermeasures) should be selected from the banks.

Day 2:

- Teacher collects assignment and leads a class discussion reviewing the key terms and questions from the created worksheet.
- The teacher can then begin Module 7: Threats, Vulnerabilities, and Attacks using the provided resources on Teach Cyber.

Term Bank

The terms below represent foundational cybersecurity terms that are explicitly or implicitly found in Revive Atlantis.

Hardware

- Hardware
- Software
- Router
- Server
- Port
- User Access Terminal
- Data
- Threat
- Vulnerability
- Malware
- Virus
- Worm
- DDoS attacks
- “Meddler in the middle” attack
- Phishing
- Data breach/theft
- Confidentiality
- Integrity
- Availability
- Authentication
- Firewall
- Encryption
- Access control
- Defense in Depth
- Minimization
- Least privilege

Term Bank Responses (Teacher Use)

These provided definitions match the ones used in the Teach Cyber Glossary of Terms found at https://teachcyber.org/downloads-for-registered-users/ (Account Required)

- Hardware is the physical parts of a computer and related devices.
- Software is a set of instructions that execute on hardware and are designed to achieve some objective on a physical device. Software instructions may manipulate data, manipulate physical systems or manipulate both.
- Router is a network device which sends data packets from one network to another based on the destination address. May also be called a gateway.
- Server is a computer that provides resources to other computers on a network. (digital librarian).
- Port is a software-defined number associated to a network protocol that receives or transmits communication for a specific service.
- User Access Terminal is a device, typically a display and keyboard, that allows a user to interact with a computer system. It's used to enter commands, data, and instructions, and to view output and information displayed by the computer.
- Data is information. Data exists in three different states: at rest, processing, and in transit.
- Threats are any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.
- Vulnerability is a weakness in system security procedures, software, hardware, design, implementation, internal controls, technical controls, physical controls, or other control that could be accidentally triggered or intentionally exploited and result in a violation of the system's security policy.
- Malware is short for malicious software, refers to any software intentionally designed to harm, exploit, or compromise devices, networks, or data.
- Virus is a type of malware (malicious software) that spreads by attaching itself to other programs or files, replicating, and then spreading to other computers.
- Worm is a type of malicious software (malware) that can self-replicate and spread across networks and computer systems without requiring human interaction.
- DDoS attack (Distributed Denial of Service) creates the flood by coordinating large number of distributed nodes to send traffic to a target in order to overwhelm it.
- "Meddler in the middle" attack/ ("Man in the Middle" (MITM) is an active attack where the adversary positions himself in between the user and the system so that he can intercept and alter data traveling between them.
- Phishing is an attempt by an adversary to solicit personal information from unsuspecting users by employing social engineering techniques usually through emails.
- Data breach/theft is the unauthorized transfer of information from an information system.IT can be accidental or intentional.
- Confidentiality is preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
- Integrity is guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity.
- Availability is ensuring timely and reliable access to and use of information.

- Authentication is to verify the identity of a user. It is also a security measures designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.
- Firewall is hardware or software which uses a defined rule set to constrain network traffic to prevent unauthorized access to or from a network. (hardware or software)
- Encryption is the process of changing plaintext into ciphertext that conceals the data's original meaning to prevent it from being known or used.
- Access control is the process of granting or denying specific requests to 1) obtain and use information and related information processing services; and 2) enter specific physical facilities (e.g., federal buildings, military establishments, border crossing entrances).
- Defense in Depth is a layered security approach that employs multiple security mechanisms and controls to protect an organization's information technology (IT) systems and data. No single defense is foolproof.
- Minimization is the act of reducing the size or footprint of a window, application, code, or data without losing functionality.
- Least privilege is the principle that security architectures should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function.

Question Bank

These questions are designed to be used by the teacher for review of concepts embedded through the game. Not all concepts contained in the question bank are explicit in the game. The teacher should use the questions that best match the skill level and instruction provided to the students.

- One of the first tasks in the game is to collect data cubes. Each data cube is worth a different point value. Why the difference in point values?
    - Give an example of a data cube in a real-world scenario that might be worth 10 points (green).
    - Give an example of a data cube in a real-world scenario that might be worth 300 points (gold).
- In network security, how does one go about balancing the importance of protecting both green and gold data cubes? What tactics can be used in network security can be used to protect both?
- In an interconnected world, why should you care about secure networks and the human factor (educated users)?
- What countermeasure methods help to defend against the human factor in network security?
- Define malware. How do you protect your personal devices against malware?
- Give three examples of malware types and provide a definition or description of each.
- Identify the ways that malware enters a system.
- This game follows the loop of threat-vulnerability-countermeasure. Give one example of this loop found within the game.
    - Give one real world example of a threat and vulnerability and provide an appropriate countermeasure.
    - In the real-world example provided, could the threat have been alleviated through better initial network security? If so, how?
- There are instances in Atlantis in which artificial intelligence (AI)tools could help to make network security stronger and more efficient. Give two examples of positive uses of AI to help in network security processes.
- What methods help to defend against the human factor in network security?
- The secure design principles of defense in depth, minimization, and least privilege can help mitigate risks in networks.
    - Define each term.
    - In Atlantis, cite an example of each term or how it could have been applied to increase network security.
- Port security—at one point, you had to run a port scan to figure out how Malusks were getting into the city. You selected which ports to close.
    - Why didn't you close all ports?
    - Is there ever a scenario in which closing all ports would be the best response tactic?
- What does a meddler in the middle attack attempt to accomplish?
    - What can users do to help prevent being a victim of this type of attack?
- Define social engineering.
- What is a phishing attack?
    - How can phishing be prevented without technical solutions?
    - How has AI both helped and hindered the threat of phishing attacks?
- Security v utility is a difficult issue for network administrators. Explain this problem.
    - How can network administrators navigate this problem and provide more balance between the two concepts?
- What are the most common forms of authentication?

    - If responsible for network security for a wide number of users-what authentication measures would you put into place and why? Please consider the following user groups:
        - Network guests:
        - General Network users (employees/managers):
        - Network Technicians/Administrators:
        - Chief Information Officer/ Chief Information Security Officer/Chief Data Privacy Officer and small team:
- Access control is another important network security feature. How are access control and authentication different?
- Tina, a network administrator on your team, recently left the company for a new job. What should be done immediately in regard to access control and authentication?
- What is a DDoS attack?
    - Why would a threat attacker initiate a DDoS attack?
    - What prevention measures protect against DDoS attacks?
    - Give a real-world example if a DDoS attack. Could it have been prevented? How?
- Firewalls are used as preventative measures in network security. Draw a depiction of a network firewall.

Question Bank Responses (Teacher Use)

- One of the first tasks in the game is to collect data cubes. Each data cube is worth a different point value. Why the difference in point values?
    - Possible responses: the point value of the data cubes reflects the real-world difference in value of actual data. Some data is worth more than others. Some data requires collective effort to increase in value. However, all data is important and should be protected.
  - Give an example of a data cube in a real-world scenario that might be worth 10 points (green).
    - Possible responses should reflect low value data/public data or one individual data point that alone is not worth much; examples include information available on public websites (i.e. "About Us"), job postings, public announcements, etc.
  - Give an example of a data cube in a real-world scenario that might be worth 300 points (gold).
    - Possible responses should reflect high value data or highly confidential information: examples include passwords for online banking, collective list of PII (names, social security numbers, birthdates, etc.), locations of high value people, places, things, etc.)
- In network security, how does one go about balancing the importance of protecting both green and gold data cubes? What tactics can be used in network security can be used to protect both?

  Possible responses: Publicly available information does not require large-scale protective measures. However good practices in data security include multi-level authentication, access control measures, access logs, encryption, etc.
- In an interconnected world, why should you as an individual care about secure networks and educated users?
    - Possible responses: Due to the interconnectedness of devices, some types of malware and other threats only require one person to fall for a phishing email, run an antiquated operating system with vulnerabilities, or to transfer data on an open public Wi-Fi network for the adversary to have an entry point into a network. Once inside, the adversary potentially has access to anyone connected to that network.
- Define malware. How do you protect your personal devices against malware?
    - Possible responses: Malware refers to any software intentionally designed to harm, exploit, or compromise devices, networks, or data. Devices can be protected using good cybersecurity hygiene practices (not using http websites, not clicking unknown links or attachments), running provided updates on devices, using firewalls/VPNs, and other countermeasures.

- Give three examples of malware types and provide a definition or description of each.
    - Virus is a type of malware (malicious software) that spreads by attaching itself to other programs or files, replicating, and then spreading to other computers.
    - Worm is a type of malicious software (malware) that can self-replicate and spread across networks and computer systems without requiring human interaction.
    - Spyware collects information about users' activities without their knowledge or consent
    - Trojan disguises itself as desirable code or software (games, apps, etc.) Once downloaded by unsuspecting users, the Trojan can take control of victims' systems for malicious purpose
    - Ransomware is software that uses encryption to disable a target's access to its data until a ransom is paid

- Rootkits is software that gives malicious actors remote control of a victim's computer with full administrative privileges. Rootkits can be injected into applications, kernels, hypervisors, or firmware
- Keyloggers is a type of spyware that monitors user activity. Keyloggers have legitimate uses; businesses can use them to monitor employee activity and families may use them to keep track of children's online behaviors
- And others…

- Identify the ways that malware enters a system.
  - Possible responses: Malware can enter through unsecured Wi-Fi, compromised shared drives, careless user actions, infected downloads, and/or through social engineering techniques (such as phishing).
- This game follows the loop of threat-vulnerability-countermeasure. Give one example of this loop found within the game.
  - Possible responses: Malusks, enter through unsecured and wide-open data ports; close the ports that are allowing for malicious traffic; install control measures (such as firewall).
  - Give one real world example of a threat and vulnerability and provide an appropriate countermeasure.
    - Possible responses: **Threat**: a malicious actor wants to steal employee data/information to sell for profit; **Vulnerability**: a company's employee files are stored on a company website with no authentication measures in place; **Countermeasure**: Company could implement a strong password policy, use multi-factor authentication, and/or use a web application firewall (WAF) to block unauthorized access
  - In the real-world example provided, could the threat have been alleviated through better initial network security? If so, how?
    - Possible response: Installing the countermeasures at the beginning; prior to a security incident is best practice.
- There are instances in Atlantis in which AI tools could help to make network security stronger and more efficient. Give two examples of positive uses of AI to help in network security processes.
  - Possible responses: AI can be used to monitor as a threat analyzation tool (with human oversight and final decision authority), AI can be used for port control by automatically responding to anomalies in port traffic; AI can produce threat reports so that network administrators have current statistics on malicious actor behavior patterns, AI can monitor firewalls, etc.
- What methods help to defend against the human factor in network security?
  - Possible responses: Education, required training, Access Control, Authentication measures, Automatic Updates
- The secure design principles of defense in depth, minimization, and least privilege can help mitigate risks in networks.
  - Define each term.
    - Defense in Depth is a layered security approach that employs multiple security mechanisms and controls to protect an organization's information technology (IT) systems and data. No single defense is foolproof.
    - Minimization is the act of reducing the size or footprint of a window, application, code, or data without losing functionality.

- Least privilege is the principle that security architectures should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function.

  - In Atlantis, cite an example of each term or how it could have been applied to increase network security (Please note that not all of the following were included in the gaming environment, so student need intermediate knowledge).
    - Possible responses: Examples of Defense in Depth include the use of firewalls, intrusion detection systems, antivirus software, and network segmentation. Examples of minimization include collecting only the data cubes necessary, restricting access or authentication levels, installing updates to patch known vulnerabilities to minimize the attack surface, etc. Examples of Least privilege were included when setting authentication levels ensuring that only those that needed access were authenticated.
- Port security—at one point, you had to run a port scan to figure out how Malusks were getting into the city. You selected which ports to close. Why didn't you close all ports? Is there ever a scenario in which closing all ports would be the best response tactic?
    - Possible responses: Closing all the ports would have made the network inoperable and had an impact on Atlanteans daily lives. By closing only the ports impacted, it allowed for some usability of the network while defending against the threat. Closing all ports would be necessary if all ports were compromised or if the threat was extremely dangerous in that security was more important than network functionality/availability.
- What does a meddler in the middle attack attempt to accomplish? How can this attack be prevented by device users?
    - Possible responses: the attacker insert themselves between the legitimate communication channel, allowing them to eavesdrop, steal data, or even alter the information being exchanged. Countermeasures include authentication, encryption, use of secure Wi-Fi, and education/training.

- Define social engineering.
    - Social engineering is the tactic of manipulating, influencing, or deceiving a victim in order to gain control over a computer system, or to steal personal and financial information. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information
- What is a phishing attack?
    - Phishing is an attempt by an adversary to solicit personal information from unsuspecting users by employing social engineering techniques usually through emails.

  - How can phishing be prevented without technical solutions?
    - Possible responses: Education and training for device users. Also ensuring that employees are given access to regular breaks during the day will help from making mistakes such as clicking on unknown emails.
  - How has AI both helped and hindered the threat of phishing attacks?
    - Possible responses: AI can be used by malicious actors to develop more sophisticated phishing attacks. AI can help malicious actors overcome language/grammar barriers. AI can

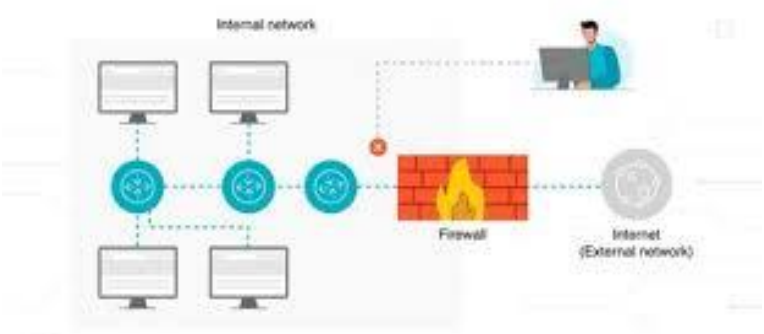
also be used as the first line of defense and highlight/filter incoming messages or alert users to anomalies in emails.

- Security v utility is a difficult issue for network administrators. Explain this problem.
    - Possible responses: Just like the example of port control, network administrators must balance keeping data and networks secure but allowing for availability of the network for people's work and lives to remain uninterrupted. For example, an online business who is consistently having to "go offline" to fix security issues, will lose customers who are not able to places orders when they desire.
  - How can network administrators navigate this problem and provide more balance between the two concepts?
    - Possible responses: Generally speaking, security should be a built-in feature from inception. "Secure by Design" is an important component of cybersecurity. Many do not adhere to this because of increased expense on the front-end but in the long run "Secure by Design" concepts help to alleviate longstanding security issues.
- What are the most common forms of authentication?
    - Possible responses: passwords, biometrics, multi-factor authentication (something you know, something you have, something you are), certificate-based authentication, behavior-based authentication, single sign-on
  - If responsible for network security for a wide number of users-what authentication measures would you put into place and why? Please consider the following user groups:
        - Possible responses should show the common theme to secure the network for all users but also increase security for those that have more responsibility to protect the most crucial assets on network.
    - Network guests: passwords, single sign on, and MFA
    - General Network users (employees/managers): passwords, single sign on, and MFA
    - Network Technicians/Administrators: passwords, MFA, behavioral based, certificate based
    - Chief Information Officer/ Chief Information Security Officer/Chief Data Privacy Officer and small team: passwords, MFA, behavioral based, certificate based
- Access control is another important network security feature. How are access control and authentication different?
    - Possible responses: Authentication and access control are two distinct, but interconnected processes used to secure systems and data. Authentication verifies a user's identity, while access control determines what resources that user can access after successful authentication.
- Tina, a network administrator on your team, recently left the company for a new job. What should be done immediately in regard to access control and authentication?
    - Possible responses: Tina's credentials and any MFA devices (such as an RSA token) should be returned and deactivated. Her log in credentials should be inactive, blocking access to the internal network. Depending upon company policy and Tina's level of clearance, all access should be removed and accounts retired to close any potential dormant entry points.
- Why would a threat attacker initiate a DDoS attack?
    - DDoS attack (Distributed Denial of Service) creates the flood by coordinating large number of distributed nodes to send traffic to a target in order to overwhelm it. An attacker may use this as a

distraction to prepare another attack, to disrupt for financial gain, to make a socio-political statement, or to crash a critical website.

- What prevention measures protect against DDoS attacks?
  - Possible responses: monitoring network traffic, web-based firewalls
- Give a real-world example if a DDoS attack. Could it have been prevented? How?
  - Possible responses: The Google attack (2020), Novel DDoS Attack: HTTP/s Rapid Reset (2023), AWS (2020), Krebs DDoS (2016), Mirai Dyn Attack (2016)

- Firewalls are used as preventative measures in network security. Draw a depiction of a network firewall.
  - Possible responses: Students should draw a firewall such as the one pictured below…



Graphic credit: Palo Alto Networks

Supplemental Career Awareness Activity:

Background Information:
The teacher should become familiar with the DoD Cyber Workforce Framework and the NICE Workforce Framework for Cybersecurity. The teacher can decide which resource to use (links provided below).

Activity:

- Utilizing the NICE Cybersecurity Workforce Roles or the DoD Cybersecurity Workforce Framework, research one of the suggested work roles pertaining to network security.
- Using open-source materials such as cyberseek.com, answer the following:

  - Job title:
  - NICE or DoD job role:
  - Job description/responsibilities:
  - Education/Certs needed:
  - Certs recommended:
  - Entry level pay:
  - Experience level pay:
  - Strengths/Appeal of the job:
  - Weaknesses of the job:

Department of Defense Cyber Workforce Framework:
The DoD Cyber Workforce Framework establishes the DoD's authoritative lexicon based on the work an individual is performing, not their position titles, occupational series, or designator. The DCWF describes the work performed by the full spectrum of the cyber workforce as defined in DoD Directive (DoDD) 8140.01. The DCWF leverages the original National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NCWF) and the DoD Joint Cyberspace Training and Certification Standards (JCT&CS).
https://public.cyber.mil/wid/dcwf/
Suggested Workforce Elements for Activity (click on Workforce Element and then choose an appropriate Workforce Element):

- IT Cyberspace
- Cybersecurity

NICE Cyber Workforce Framework:
The Workforce Framework for Cybersecurity, commonly referred to as the NICE Framework, is a nationally focused resource to help employers develop their cybersecurity workforce. It establishes a common lexicon that describes cybersecurity work and workers regardless of where or for whom the work is performed. The NICE Framework applies across public, private, and academic sectors.
https://niccs.cisa.gov/workforce-development/nice-framework
Suggested Work Categories and Work Roles for Activity:

- Oversight and Governance
  - Systems Security Management

    - Security Control Assessment
- Protection and Defense
    - Defensive Cyber
    - Incident Response
    - Threat Analysis
    - Vulnerability Analysis

Quiz Questions Embedded for Players (In-Game Experience)

Correct responses included

Atlantis Bonus Challenge Questions

First Wave of Malusks

1. **Question:** Malusks exploit open Wi-Fi ports. What's the main risk of using unsecured Wi-Fi?
   A. Hackers stealing sensitive data
   B. Slower internet connections
   C. Limited device compatibility
   Answer: Hackers stealing sensitive data

2. **Question:** Malusks consume data cubes in Atlantis. What happens when malware infects a computer?
   A. Data becomes encrypted for security
   B. System slows or crashes
   C. Files automatically back up
   Answer: B. System slows or crashes

3. **Question:** Malusks infect Atlantis through datacubes. Which real-world malware type spreads by attaching itself to other programs?
   A. Spyware
   B. Viruses
   C. Phishing
   Answer: B. Viruses

Meddler Leech Incursion

1. **Question:** Meddler Leeches intercept data in transit. What real-world threat works similarly?
   A. Meddler-in-the-Middle attacks
   B. Password reuse attacks
   C. Device overheating issues
   Answer: A. Meddler-in-the-Middle attacks

2. **Question:** Meddler Leeches create vulnerabilities. What's a real-world way attackers exploit insecure communication channels?

   A. Installing fake antivirus software
   B. Sending phishing emails
   C. Intercepting unencrypted traffic
   Answer: C. Intercepting unencrypted traffic

3. **Question:** Players remove Meddler Leeches to secure data. What's the best real-world practice for protecting data in transit?
   A. Share passwords securely
   B. Use a VPN
   C. Disable firewalls temporarily
   Answer: B. Use a VPN

Phish

1. **Question:** You will have seen Phish in Atlantis. What weakness do phishing attacks exploit?
   A. Two-factor authentication
   B. Encrypted firewalls
   C. Weak authentication
   Answer: C. Weak authentication

2. **Question:** Sophisticated Phish disguise themselves. What's a common sign of phishing emails?
   A. Suspicious links or attachments
   B. Length of the message
   C. Encrypted message delivery
   Answer: A. Suspicious links or attachments

3. **Question:** Players study Phish behavior. What's the real-world equivalent of identifying potential attacks?
   A. Cyber threat analysis
   B. Ignoring flagged emails
   C. Disabling VPN connections
   Answer: A. Cyber threat analysis

Second Wave of Malusks

1. **Question:** Type 2 Malusks rapidly replicate. What malware spreads similarly in real life?
   A. Adware
   B. Keyloggers
   C. Worms
   Answer: C. Worms

2. **Question:** Malusks enter through open ports. How can you secure your network in real life?
   A. Turn off encryption features
   B. Use a firewall and antivirus software
   C. Hide your router physically
   Answer: B Use a firewall and antivirus software

3. **Question:** Atlantis players close ports to block Malusks. What vulnerability does a port present?
   A. Lack of encryption
   B. Lack of access control
   C. Lack of traffic
   Answer: B. Lack of access control

DDoS Swarm

1. **Question:** Dee Dos Swarms overwhelm Atlantis servers. What real-world attack floods systems with traffic?
   A. Distributed Denial of Service (DDoS)
   B. Ransomware attacks
   C. Spyware infections
   Answer: A. Distributed Denial of Service (DDoS)

2. **Question:** Players stop DDoS swarms by closing ports. How can companies mitigate DDoS attacks?
   A. Use network traffic monitoring
   B. Disable encryption temporarily
   C. Increase router speed
   Answer: A. Use network traffic monitoring

3. **Question:** DDoS swarms can flood a website. What's a common real-world result of a DDoS attack?
   A. Encrypted file storage

B. Boosted download speeds
C. Service outages for users
Answer: C. Service outages for users

Combined Meddler Leech and Phish Threat

1. Sometimes Phish distract while Meddler Leeches steal. What's the risk of clicking a suspicious link on an unsecured network?
   A. The link is automatically deleted
   B. Your device overheats
   C. Your data could be intercepted during transmission
   Answer: C. Your data could be intercepted during transmission

2. Phish and Meddler Leeches can work together to fool users. What's a smart way to protect yourself when checking email on public Wi-Fi?
   A. Turn off spam filters
   B. Use a VPN and avoid clicking unknown links
   C. Restart your device often
   Answer: B. Use a VPN and avoid clicking unknown links

3. You spot a Phish and a Meddler Leech at the same time in Atlantis. What's the real-world lesson?
   A. Cyber attacks often happen one at a time
   B. Attackers may combine techniques to steal information
   C. These threats always cancel each other out
   Answer: B. Attackers may combine techniques to steal information