CYSE 445 Project 2
Due on Friday, Dec 12, 2025, 11:59 PM

Statement

Develop a resilient cybersecurity solution for the engineering systems of 445Cyber Co., a rapidly growing cybersecurity consulting company.

Report Submission

You can work as a group of two members on this project. Please include the members' names on the paper. Only one copy should be submitted for the group. The filename of the report should be of the format: *CYSE445_Project2_<name1>_<name2>*, where *<name1>* and *<name2>* are the team members' names.

The cybersecurity solution paper must include the following sections:

1. (15) Section 1 - Risk assessment tool. Utilizing an open-source toolkit, from GitHub, list the highest five risks of the **current** systems of 445Cyber Co.? Use the heatmap, generated from the toolkit, to visualize the risk scores.
    - Resources:
        - Model Architecture (Capella or Papyrus SysML)
        - MulVAL – logic-based attack-graph generator for multi-host scenarios.
        - MITRE CyGraph – graphs cyber terrain, dependencies, and mission impact to support cyber-resilience analyses.
2. (15) Section 2 - Requirements. Provide a table listing the requirements based on your analysis of the Problem Scenario; you need to use the template below. You should come up with at least 15 requirements. The requirement statements must be clear and concise.

Requirement No	Requirement Statement	Proposed Solution

3. (15) Section 3 - System and network detailed design.
    - Provide diagrams and descriptions of your **proposed** engineering systems. Be sure to depict:
        - The 445Cyber Co.'s major systems;
        - Any external systems used by 445Cyber Co.;
        - Major data flows;
        - Network architecture;
        - Users and clients.
    - The solution should be based on *cloud services*.
    - Utilize OWASP Threat Dragon tool – draw DFDs, capture threats/mitigations.
    - Utilize Threagile tool – "threat-model-as-code" (YAML) for auto-risk reports & diagrams.
    - Be sure to describe your **proposed** future systems for 445 Cyber Co.

4. Section 4 – Threat Modeling.
   a) (10) Identify Threats. Perform Threat modeling of your **proposed** engineering systems by using a combination of the models STRIDE/OWASP and CAPEC/AT&CK. Be sure to describe what threats you plan to protect against.
   b) STRIDE across the different components utilizing GitHub tools or your own Python code; ATT&CK mapping for phishing, credential access, discovery, exfiltration utilizing Wazuh, GitHub tools or your own Python code. Each category should be mapped to key threats and show corresponding CAPEC/ATT&CK and related primary controls.
   c) (8) Security Controls:
      - For at least one security control, utilize Detection & Response toolkit: EDR + SIEM correlation; UEBA; alert triage and SOAR runbooks.
        Provide the strategy to address the threats that you have identified in the model. Recommend security controls as well as tools and procedures to implement security controls and to improve system resilience. Be sure to discuss security controls to protect the engineering systems (including access control and account management).
      - You should also recommend security controls to detect intrusions and suspicious behavior.
      - Your recommended security strategy should include monitoring corporate assets and attack surfaces.
   d) (7) Evaluate whether your security strategy aligns with *zero trust architecture (ZTA)* and *data-centric security model* and augment your solution design with ZTA security components and measures.
5. (15) Section 5. Recommend a strategy and plan for testing system security and resiliency of your proposed systems and components leveraging AI tools utilizing GitHub tools or your own Python code.
6. (15) Section 6. Incident Response. Recommend incident handling and recovery procedures that are needed for your newly proposed systems.

Submission & Evidence Checklist

☐ Risk register and heatmap (CSV + screenshot)

☐ Requirements table with traceability to risks

☐ Architecture and diagrams (Capella/Papyrus & Threat Dragon exports)

☐ Threagile report & YAML

☐ ATT&CK Navigator layer(s)

☐ Sigma rules + SIEM conversions

☐ CALDERA/Atomic/Stratus evidence of detections

☐ Chaos Toolkit report proving RPO/RTO

☐ tool results & all code programs. Screenshot and demo videos of tools used

Important Notes

- You want to establish the set of requirements before proceeding to propose a solution design.
- Your analysis and designed solution *must not be generic*, but instead aim at s*olving the business functionalities* and *application needs* of the company 445Cyber Co.
- The solution you propose should be *commensurate* with a small consulting company that can't afford a gold-plated solution suitable for critical infrastructure, a major federal government agency, or a Fortune 100 corporation.
- On the other hand, the consulting company provides cybersecurity services so must implement best practices. The solution narrative should articulate the trade-off decisions you make in designing your solution.
- You may include outsourced services and off-premises solutions as part of your engineering systems solution. But you must defend your decisions as being suitable for the goals outlined in the scenario and commensurate with a small consulting company.

Paper and tool utilization Quality

The paper should be organized into sections that describe your engineering system solution and present a logical flow to tell the story of how your solution is secure and resilient (use sections numbered as above). Your paper should include all the information necessary to provide a comprehensive understanding of your proposed solution. Your tool utilization should include all the information necessary to provide a comprehensive understanding of your proposed solution and covers project requirements.

I expect professional writing suitable in technical detail and approach for a decision-maker able to understand and agree to implement your proposed engineering systems solution. You may personalize the position paper (e.g., "Personally, I would . . ."). Use headers for each numbered category of information identified in the list above. You may use bullets, charts, and tables to

help convey information concisely. You may use an appendix or appendices to provide very detailed information that otherwise would interrupt the flow of your paper.

Review of editorial suggestions in your word processor for structure, spelling, and grammar is recommended. Grade reductions will be made for unprofessional submissions (including spelling and grammar errors), poor structure, lack of cohesive structure, excessive wordiness, or extraneous matter not on point (i.e., "fluff").

You should identify any sources used in your paper by providing footnotes, endnotes, source/reference list at the end of the document, or similar. The reference format is up to you but must enable a reader to find the sources online. I recommend URLs for web-only content, otherwise APA or MLA format (Google Scholar is your friend...).

The paper should be double-spaced and formatted with one-inch margins for top, bottom, right and left. Please use 12-point Times New Roman (or similar font). There is not a page or word-count minimum or limit. The expectation is that a twelve-to-fifteen-page paper is necessary to provide a comprehensive discussion of the required information.

CYSE 445 Project 2
Due on Friday, Dec 12, 2025, 11:59 PM

Problem Scenario

You are a cyber security and resilience professional, and you have just been hired by 445Cyber Co. ("445Cyber"). The company focuses on providing cybersecurity services to clients. They have been very successful over the past couple of years. The company has won a huge contract to provide their expertise to a couple hundred organizations, and a key requirement for this contract is to show that 445Cyber has exemplary system security and resiliency for its own systems. When the contract was awarded, a Red Team came to 445Cyber and did surveys and inspections of existing systems. 445Cyber failed miserably. The Red Team wouldn't provide detailed results, but generally found that the old system had almost no cybersecurity, poor processes, and would need to be virtually rebuilt from scratch to be acceptable.

As a result, the Board of Directors for 445Cyber fired the old IT manager and decided to hire a new CISO (Chief Information Security Officer)—you. They also brought in a new CEO, and she's here to make sure the company meets or exceeds the cybersecurity expectations that they've been handed. The new CEO is Dorothy Pocklington who ran a large organization faced with evaluating cybersecurity and system resilience. She has limited time and money with which to accomplish her major goal—show that 445Cyber makes immediate improvement, has complete awareness of current situations, and has a plan to dramatically improve the system security and resilience of the 445Cyber systems and network.

You are charged with satisfying the goals of the organization from the standpoint of cybersecurity and resilience.

Dorothy Pocklington wants to know the answers to the following:

1. What needs to be connected to 445Cyber systems and networks?
2. How will we know what's running (or trying to run) on 445Cyber systems and networks?
3. How can we limit and manage the number of people who have the administrative privileges to change, bypass, or override the security settings on 445Cyber systems and networks?
4. How can we put into place continuous processes backed by security technology that would allow us to prevent most breaches, rapidly detect all that do succeed, and minimize damage to our business and our customers' files?
5. Where is your plan to protect our systems and to show resiliency in restoring systems that are compromised?
6. How do you plan to handle incidents?
7. What do we need to do to pass the Red Team Inspection in six months?

She charges you with designing and documenting exemplary secure and resilient engineering systems for 445Cyber that showcase the company's cybersecurity prowess and answers her

questions. You review the organization chart of 445Cyber, review its website and promotional literature, learn about its systems, and interview the leadership team. You learn the following.

445Cyber:

- Staff includes:
  - 48 consultants and technicians
  - Dorothy Pocklington, CEO
  - Albert Ibrahim, VP of Development, staff of 3 (2 developers and 1 sys admin)
  - Susan Butler, VP of Finance & Accounting & staff of 2 (accounting and contracts specialists)
  - John Gallagher, VP of Sales & staff of 2 (a contracts specialist and a pre-sales engineer)
  - Jewel Aitken, HR Director & staff of 1 (a receptionist)

- The organization's goals are to provide cybersecurity services to a range of clients. The staff typically goes onsite to a client and provides an analysis of their network, their dataflows, and their overall cybersecurity hygiene, and then provide a plan to improve hygiene, secure the boundaries, lock down all hosts and related computing resources, and implement tools and processes to make clients fully confident that all proper steps are being taken to ensure their cybersecurity within the client budget. The developers on staff provide configurations, DevOps utilities, and help to engineer changes that the Lead Cyber Consultant on any engagement defines. Each engagement ends up generating analysis documents, design papers, and more that are stored on the network and keep separate from other client files. The files are stored in a big file folder and the client's name is used in the document title.

- Current Systems
  - Each staff member has a laptop running Microsoft Windows, individually configured by the staff member. The CEO specifically asked you to develop a secure provisioning plan for new laptops.
  - The network is made up of Windows-based servers providing file storage, email hosting, network configuration, DHCP, etc.
  - The database contains client interaction records, billing and payment information, and deliverables that have been provided to the customer. The old IT manager built it using MS-Access, and no one knows if it is secure or not. Everyone uses the same username/password which is "dbuser/Passw0rd." The IT Manager was about to put it out on the Internet when he was fired. You should propose a secure and resilient replacement. You are also empowered to direct them to use secure coding techniques.

  - 445Cyber outsources accounting functions with a firm that provides hosting for accounting systems. The CEO considers the accounting systems used by the accounting firm to be secure themselves and therefore out of scope of this project. But 445Cyber's VP of Finance and VP of Sales need to be able to work in the office or remotely and access this outsourced accounting service securely.
  - 445Cyber's current file server is on its last legs. You should recommend a solution to meet the company's requirements. The CEO is open to cloud or hosted solutions as well as simply hosting in house if you can guarantee good system security and resilience. She is open to keeping paper transactions around for a week and thinks that losing a day's worth of data is reasonable but wants your input. The work done by the consulting staff for clients is even more valuable, so the CEO wants a more robust security and resilience plan for that information. If a laptop got lost, the clients' work must not be lost, too.
- The CEO wants a new system for the company's Cyber Library. The CEO wants to use a Wiki Repository of tools, configuration guides, and related material to help the consultants understand the tools (open-sourced, proprietary, and created in-house) that the company uses. Access to this is to be limited to staff only, accessible within the office and remotely. In the future, the CEO would like to be able to share some information with clients by publishing client-facing information separately.
- The CEO wants you to recommend improvements for the company's web presence. Currently, the company uses brochure-ware (read only) material about who we are that clients and potential clients can read on the website or download. The CEO would like to add functionality to the company website (or otherwise is available remotely) to provide a shared calendar for scheduling client events, a staff-only project management portal that can contain contracts, deliverables, schedules, etc., as well as a client-facing ability to accept credit card payments. This can be outsourced but should be professional and able to expand to 250 employees in three to five years. You don't have to design the solution, but you do have to make recommendations for securing it and being able to include it in the resiliency strategy.
- The CEO mentions that she has heard about the NIST Cybersecurity Framework and CIS Controls but doesn't know much about it.
- Results of the Red Team Inspection were sanitized, but you can assume that poor or weak system security and resiliency was found throughout the network. For the purposes of this project, you should assume there is very little from the existing system that can be used. In other words, assume a mostly unprotected network, and begin from there.

Notes from VP of Development Albert Ibrahim:

- I have two developers that work for me. They can provide customers with detailed implementations of the cyber products we recommend. They can help migrate databases or entire servers or systems. We make money off their hours, but they're available for internal projects as well.
- All the consultants and technicians report to me. I don't know all the technologies that they know. But our clients like having me in the loop since many of them are concerned about converting their systems and they don't just want a cyber perspective, but a holistic perspective of how it will affect their organizations.
- The only system administrator we have reports to me, too. He is taking some IT courses at college and works for us about ten hours a week.
- The files are a mess. Most of the files have titles that indicate the customer and a date, but some do not. We have about 10 TB of files, of which there are hundreds of executables, installed packages, scripts, config files, and everything else. I'm afraid to think how many of our files have been sent to the wrong customers. I like the fact that our staff can search through this giant collection, but we need to keep our client files separate from one another, and we need to keep our utilities and executables separate.
- My folks maintain the website and some Intranet pages, but we could really use more of all that, and I would like the solution to be able to keep those secure. As far as resiliency, I'd rank the internal files for the Sales and Finance department most important since we don't get paychecks if we're not billing. But just as important is the client files. I suppose if the website and intranet items could come back up within hours, I'd be fine. We don't change the website very often, but if we're going to start collecting data from it, I guess that'll go into a database, and that data we can't afford to lose.
- I'm glad we are going to get a better form for our cyber library that all the folks use. When the file server has gone down in the past, we have lost access for a week or more. That's unacceptable.
- The developers are good, but we haven't had the luxury of spending time thinking about how to make our code secure. We could use some guidelines to help with that.
- Our staff is on customer sites for weeks at a time, so we need some way to have them upload their files, or back up their work without them being back here. What can we do to make sure that if a laptop in the field was stolen, the data would be secure? What can we do if that laptop was stolen to make sure the work done by that staff member is preserved? And how can we make sure that stolen laptop can be replaced overnight? This is important to solve.
- I've never heard of the NIST Cybersecurity Framework that the CEO has mentioned a few times. I like the CIS-18 controls and want to take advantage of the CIS Benchmarks.

Notes from VP of Finance & Accounting Susan Butler:

- You might think that cybersecurity is important, but nothing is more important than invoicing our clients and billing them. Since our outside accounting firm is good, all I care about is the website's ability to capture credit card information.
- We've never been hacked before, so I'm not so sure we should be worried -- we just need to make it look good to get through the Red Team thing and then we can get back to work.
- We use an outside accounting firm, but one of the things we must do weekly is to exchange confidential information with our customers' contracting officers, as well as send invoices and time reports. This contains information we would never want to get lost or intercepted. For now, I email them, but I suppose we need a better way, especially now that we'll have so many of these customers.
- I'm probably the best person to contact first if we have any cybersecurity problems since I've been with the company the longest.
- My two staff members generate all the invoices and contract finance reports. I need to be able to see what they do, and I should be able to snoop on their machines to make sure they're working all the time.

Notes from VP of Sales John Gallagher:

- The most important thing we need to protect and make sure is ready to go is the cyber library. If the cyber team doesn't have that, the customers complain. I want to share that out on the web (but not all of it) so that our potential customers know we have a huge capability. I'd also like to allow all our cyber staff to be able to get to that while they're on customer sites.
- I have a pre-sales engineer that really needs to be able to demonstrate our solutions to customers and potential customers. Can we let customers into our network to see some sample solutions?
- We generally do our sales process by meeting with leads (we keep them in the MS-Access database—it's awesome and has color coding). I need to know that we can hit that database from the office, the customer sites, or from my car on my phone if I want to. If you want, we can just download the lead's information to my phone and then copy it back later after I've updated it.
- Also, we often have our potential customers come into the office. I need them to be able to get on our network so they can check their work email, and whatever. How can we support that?

CYSE 445 Project 2
Due on Friday, Dec 12, 2025, 11:59 PM

Notes from HR Director Jewel Aitken:

- I'm really a team of one, but hiring staff is probably the most important thing we do, since our greatest assets are the ones sitting in the chairs.
- The only hiring system we have is email and a bunch of spreadsheets. One time I accidentally attached my salaries spreadsheet to an email to some applicants, but I don't think they looked at it. Managing offer letters, resumes, salary records, and everything else on my laptop is time-consuming. I hide it using a different name or zip files with a password. I have no place on the network to store all this data.
- I want applicants to upload a resume, name, social security number, and salary requirements to our website so I don't have to update my spreadsheets.

Critical analysis of the known information and critical thinking about that which you don't know should provide you with sufficient information to proceed with the assignment. You will, however, be able to demonstrate well-rounded knowledge of best practices and the ability to think critically about priorities, vulnerabilities, and solutions that you have at your disposal to solve the greatest problems first and work your way through this challenge.