CredLock

**Senior Design Team Contract**

University of Cincinnati

College of Education, Criminal Justice and Human Services

School of Information Technology

Nick Blank

Ian Listopad

Jordan Miller

Marouane Faissali

Patrick Buerk

Table of Contents

[Intent 3](#_Toc139472962)

[Senior Design Contract 4](#_Toc139472963)

[Project Summary 4](#_Toc139472964)

[Problem Statement 4](#_Toc139472965)

[Solution 4](#_Toc139472966)

[Contact Information 4](#_Toc139472967)

[Sponsor Information (if applicable) 4](#_Toc139472968)

[Project Source 4](#_Toc139472969)

[Project Objectives/Goals 4](#_Toc139472970)

[Team Members and Responsibilities 5](#_Toc139472971)

[Project Scope 5](#_Toc139472972)

[Quick Project Timeline 5](#_Toc139472973)

[Technologies Used 5](#_Toc139472974)

[Ethical Considerations 5](#_Toc139472975)

[Team Rules 5](#_Toc139472976)

[Team Signatures: 6](#_Toc139472977)

[References 7](#_Toc139472978)

# Intent

The following contract was written and agreed upon by Nick Blank, Ian Listopad, Jordan Miller, Marouane Faissali, and Patrick Buerk. The contract provides expectations, objectives, and results for developing the CredLock.

The contract is effective for all team members participating in the Senior Design Capstone class series in the 2025-2026 academic year.

# Senior Design Contract

## Project Summary

CredLock is a hands-on cybersecurity project that safely recreates how ransomware spreads after an attacker steals login credentials. In our lab, we will show how files can be locked, how the attack can move across systems, and how data can be stolen for double-extortion. The project helps organizations test how well they can spot, stop, and recover from the ransomware attacks, and gives us a clear framework to improve their defenses.

## Problem Statement

Ransomware attacks are getting more advanced and often locking critical data and stealing it for double-extortion. Recent reports, according to the Optiv’s Q1 2025 Ransomware Trends, show that the tactics are now a standard part of many attacks. Yet, many organizations still lack a safe environment to test how well their defenses, backups, and incident response plans hold up. CredLock addresses this gap by providing a controlled lab simulation that starts with stolen credentials and demonstrates how an attack could spread step by step.

## Solution

“Visibility is a fundamental cybersecurity strategy to protect network assets and information. Even if your organization has taken great care to implement critical foundational cybersecurity elements like access control, segmentation and appropriate levels of cryptography, it will not change a simple, common-sense truth. You can’t protect what you can’t see” Phil Quade. CredLock simulates ransomware attacks in a lab environment on a customer's network. Utilizing ransomware to encrypt decrypt files, simulated exfiltration of data, and later movement of compromised credentials. These techniques will be used to test the detection and mitigation usefulness of the SIEM. CredLock then creates a scorecard based on the success of the simulated attacks combined with the effectiveness of the SIEM that companies use to grade their environment.

## Contact Information

|  |  |  |  |
| --- | --- | --- | --- |
| Team Member | Degree + Track  Track N/A for BSCyber | Email | Phone Number OR Other Contact Info |
| Marouane Faissali | BSIT – Computer Networking + BSCYBER | faissame@mail.uc.edu | 513-641-7386 |
| Jordan Miller | BSCYBER +MSIT | mill3jt@Mail.uc.edu | 614-980-8434 |
| Nick Blank | BSIT - Computer Networking + BSCYBER | Blanknj@mail.uc.edu | (614) 404-3530 |
| Ian Listopad | BSCYBER + MBA | [Listopir@mail.uc.edu](mailto:Listopir@mail.uc.edu) | 224-326-8343 |
| Patrick Buerk | BSCYBER | Buerkpa@mail.uc.edu | 567-694-4956 |

## Project Source

The inspiration for our project, CredLock, came from the idea that many organizations across the country lack a practical testing environment to test how well their systems can hold up, respond to and defend against a ransomware attack. The idea was proposed by Nick Blank after noticing the problem that these organizations currently have. As Information Technology majors with a track in Cybersecurity, our team shares a common interest in helping these organizations improve their security posture through a lab-based cybersecurity project that simulates ransomware attacks. Our requirements analysis focused on key features such as simulating the behaviors of a Ransomware attack by including features such as file encryption, file renaming and ransom notes.

## Project Objectives/Goals

* Simulate a virtual environment that has real world applications.
  + Goal: using host VM’s build machines that can be susceptible to real world attacks
  + Impact: By simulating environments that real world users could encounter we show the importance of being prepared for similar attacks
* Show data exfiltration opportunities
  + Goal: by using double extortion scenarios show the importance of having ways to sense extortion attacks
  + Impact: By showing extortion attack scenarios companies will be better equipped to detect and defeat exfiltration
* Use Ransomware to simulate an attack
  + Goal: Using scripting and lateral movement create an encrypted ransomware script that will be able to exfiltrate data from the virtual environment
  + Impact: Companies and viewers will be able to see the impact of encrypted ransomware and prepare for ways to combat it
* Create a scorecard for each attack and defense
  + Goal: After the attacks have been run on virtual environments creating a scorecard to better conceptualize the data is necessary.
  + Impact: by making the data readable and understandable takeaways will be easier to conclude
* Create a reproduction aspect
  + Goal: Create a way for companies and individuals to simulate similar attacks / labs on their own environment
  + Impact: By having a form of reproduction, the other users will be able to better learn hands on how to keep their environment safe

## Team Members and Responsibilities

Project Manager: Marouane Faissali

Developer: Ian Listopad

Quality Assurance Tester: Patrick Buerk

Researcher: Jordan Miller  
 Designer: Nick Blank

## Project Scope

The Scope of CredLock is designed to help organizations test how well their systems can hold up, respond to, and defend against a ransomware attack. CredLock is a lab-based cybersecurity project that simulates ransomware attacks, and it uses credential compromise as a starting entry point. The goal is to provide those organizations with a safe, reproducible framework that simulates ransomware campaigns so organizations can measure their security posture and improve their detection, containment, and recovery capabilities.

The system will feature safe ransomware simulations that include three core behaviors seen in real-world ransomware attacks: file encryption, file renaming, and a ransom note. Test files that are used in the lab environment will be encrypted or renamed to mimic the behaviors of ransomware while ensuring no real data is harmed. Ransom notes will be generated to simulate the communication that black hat hackers typically leave for victims, this will ensure that a realistic scenario for testing detection and response. These core features will ensure that our users have a clear understanding of how ransomware operates all while keeping a safe, controlled, and ethical environment for experimentation.

## Quick Project Timeline

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Task # | Task Name | Duration | Start Date | End Date |
| 1 | Research | 2-3 weeks | 09-22 | 10-13 |
| 2 | Setup virtual environments | .5 week | 10-13 | 10-16 |
|  | VM’s |  |  |  |
|  | Network |  |  |  |
|  | Users/accounts |  |  |  |
| 3 | Develop Attacks | 2-3 weeks | 10-16 | 11-06 |
| 4 | Develop Detection, or place for users to input their current detection | 2 weeks | 11-06 | 11-20 |
| 5 | Rough working product (even without all attacks working) | 3.5 weeks | 11-06 | 12-01 |
| 6 | Ensure all attacks are working and can be simulated | Winter Break | 12-01 | 01-26 |
| 7 | Create Dashboards and scorecards for how the attack did | 3 weeks | 01-26 | 02-16 |
| 8 | Presentation and documentation | 2 weeks | 02-16 | 03-02 |

## Technologies Used

There are many parts that are involved in our project, each requiring different technologies to be utilized in order to be successful. Currently our plan is as follows:  
Virtualization:

* VMware: Host our Linux / Microsoft lab environments to safely test software and for easy deployment. Also allows for logical networking.
* Virtualbox: VMware: Host our Linux / Microsoft lab environments to safely test software and for easy deployment. Also allows for logical networking.

OS:

* Windows: Utilized to write scripts, host VMs, encryption, and as a victim test machine
* Linux: Utilized to write scripts, host SIEM, collect logs, host attacker tools.

Scripting:

* Python: Utilized to write scripts for our ransomware attacks.
* PowerShell: Script automation, simulation of malicious content, forge windows event logs, lateral movement.

SIEM / EDR:

* Wazuh: Acts as our SIEM and log analyzer.
* Splunk: SIEM platform that utilizes Windows logs. Detection and alerting system.

Networking:

* VLANs: Necessary for networking our various VMs together
* Firewalls: Utilized to test the effectiveness of our written malicious code and to test the resiliency of the firewall.

## Ethical Considerations

Transparency: Showing the exact process of creating a malicious program and making sure that all users who use this software understand the implications. Showing possible risks that could be encountered in this environment, and explaining things that this program does not cover is important before allowing users to run this simulation. As stated by the Cleveland state university college of law “Users should be informed how an organization collects, uses, and protects [data]… communicating clearly and openly about cybersecurity practices is essential.”

Accessibility: When designing simulations, it is important to make sure that the product can be redone. By having proper documentation of the simulation and possible outcomes, as well as a cutoff switch, we keep this product accessible to users who want to simulate their environment.

Privacy: The simulation being conducted in a virtual environment guarantees that no personal data can be accessed or exploited. In the event of personal data being uploaded the simulation will be locked and destroyed so that private data will not be at risk

Legal Considerations: Given the fact that this simulation can be used maliciously if put in the wrong hands it is up to the team to make sure that this cannot be copied for malicious intent. It is up to the ones running the simulation to make sure that all

## Team Rules

1. Plagiarism will not be tolerated. Any team member that plagiarizes will be subject to university policies and a team meeting will be called.
2. Each team member will stay current on their tasks to ensure the project milestones are being met. If an event conflicts that will affect the completion of a deliverable, the team member will notify the other team members at least 24 hours in advance of the scheduled due date.
3. Every team member is expected to be at every meeting unless a 24-hour notice is given before the meeting date.
4. Team members are expected to be respectful of all opinions considering everyone and giving a voice to all members.
5. All team members are expected to use the communication chats established and respond to the best of their ability within 24-36 hours.
6. Each team member is expected to provide updates on progress of their specific roles
7. Team members are expected to complete their assigned tasks within the given time limits and is expected to tell members if they are in need of advice or assistance of their tasks.

# **Team Signatures:**

Signature: \_\_\_\_\_\_Marouane Faissali\_\_\_\_\_\_ Signature: \_\_\_\_\_\_Jordan Miller\_\_\_\_\_\_

Date: \_\_\_\_\_\_\_\_\_9/18/2025\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_9/18/2025\_\_\_\_\_\_

Signature: \_\_\_\_\_\_\_\_\_Ian Listopad\_\_\_\_\_\_ Signature: \_\_\_Patrick Buerk\_\_\_\_\_\_\_

Date: \_\_\_\_\_\_\_\_\_9/18/2025\_\_\_\_\_\_\_\_\_\_ Date: \_\_9/18/2025\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature: \_\_\_\_\_\_\_\_\_\_Nick Blank\_\_\_\_\_\_\_\_\_\_\_\_\_

Date: \_\_\_\_\_\_\_\_\_\_\_9/18/2025\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# References

Lee, E. (2025, July 3). First quarter 2025 ransomware trends. Optiv Security. <https://www.optiv.com/insights/discover/blog/first-quarter-2025-ransomware-trends>

Cleveland State University College of Law. (n.d.). Understanding cybersecurity ethics and navigating moral complexities. <https://onlinelaw.csuohio.edu/understanding-cybersecurity-ethics-and-navigating-moral-complexities/>

Quade, P. (2018, March 26). You can’t protect what you can’t see. Fortinet Blog. <https://www.fortinet.com/blog/industry-trends/you-can-t-protect-what-you-can-t-see>