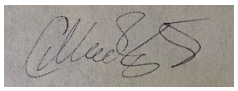
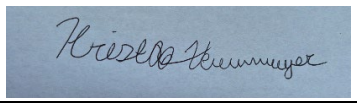
Access Management & Off-boarding Suite

by

Group 43

Nathan Balok
Felix Kouame
Murat Sagdullaev
Kristof Vennemeyer

Submitted to
the Faculty of the School of Information Technology
in Partial Fulfillment of the Requirements for
the Degree of Bachelor of Science
in Information Technology/Cybersecurity

Nathan Balok		4/27/2022
Team Member		Date
Felix Kouame		4/27/2022
Team Member		Date
Murat Sagdullaev		4/27/2022
Team Member		Date
Kristof Vennemeyer		4/27/2022
Team Member		Date
Ryan Moore		4/21/2022
Faculty Advisor		Date

University of Cincinnati
College of
Education, Criminal Justice, and Human Services

April 2022

Table of Content

Abstract

The growing turnover rate in many industries and organizations makes them highly vulnerable to cyber-attacks that leverage Identity and Access Management vulnerabilities. Despite the obvious importance of IAM, this domain of IT is often overlooked and not fully covered in training courses. To cover this gap, we developed a free, comprehensive, and widely available training course that covers the topics of access revocation, data extraction, data breach prevention, and account management. After the completion of the course, students will have a full understanding of Identity and Access Management (IAM) and will be prepared to take the initiative in building and managing a secure IT infrastructure.

The successful creation of the Access Management & Off-boarding Suite confirmed the lack of information we found when researching the Suite. This reaffirms the necessity of the course, provided through the Ohio Cyber Range Institute.

Introduction

Project Summary:

Ohio Cyber Range course to assist organizations with training IT/IS individuals on how to correctly manage account access, revoke credentials, and prevent data extraction after termination of an employee.

Problem Statement:

When an individual leaves an organization, there are often a litany of data permissions that need to be revoked. This is true for any business size that supports IT infrastructure and employees that use it. Although the act of revoking these permissions is easy, a lack of training is attributed to most access management incidents (Froehlich, 2021). This leads to vulnerabilities that can be exploited by a disgruntled former employee or bad actor. Further, these issues are amplified in frequency and cost as corporations have begun to provide work from home opportunities at an unprecedented rate (IBM Security, 2021). That said, responsibility for these revocation efforts rests on the IT department which, depending on the team, might not be able to afford the necessary training or assistance to remedy the issue.

Solution:

A free, comprehensive, and widely available training course covering the subjects of access revocation, data extraction and prevention, and account management best practices serves to alleviate stress placed on an organization by cost of obtaining the trainings or the creation of similar trainings themselves. This includes an actual learning course consisting of modules on each subject, working from the most basic skills to more advanced techniques such as the automation of revocation tasks. The course also includes a section on how to handle the processes in a hands-on way, through a virtual environment experience.

Project Source:

Murat originally conceived the Access Management and Off-boarding Suite. The idea came from experience in revoking permissions and access in a workplace environment. The team met with Ryan Moore, the team advisor, who assisted in focusing the scope of the project. Market analysis performed by the whole team found that the issue is primarily attributed to education on the matter, rather than a lack of tools to complete the process.

Discussion

Project Objectives/Goals:

A comprehensive training course that:

- Is clear, concise, and easy to follow.
- Include ways to test the knowledge of learners.
- Is widely available, applicable, and includes a low-to-no cost of entry.
- Includes a virtual environment experience offering learners a chance to test the skill they have and have learned before taking them to the sensitive live environments that they work in.

Project Scope:

Our team developed a comprehensive training suite that educates learners on how to manage access controls, data extraction, and best practices concerning the two topics on a live network. It includes the following:

- Modules covering the following topics:
    - Access Controls
        - Access Management
        - Revocation
    - Data Extraction
        - Identification
        - Handling
        - Prevention
    - Off-boarding
        - Standard Procedures
        - Best practices
- Knowledge Checks of the various topics included throughout the course(s).
    - Tests
    - Quizzes
    - Assigned Tasks

This is accompanied by a Virtual Environment that guides a learner through the following tasks:

- Issuing, Managing, and revoking credentials on a network.
- Applying crucial access management skills such as priority of least privilege.
- The creation of cryptographic keys.
- The setup and use of multifactor authentication.

Quick Project Timeline:

Below is the timeline that was created and held to throughout the creation of the course:

Task #	Task Name	Duration	Start Date	End Date
1	Research	35 days	9/27/2021	10/31/2021
2	Module Content Development	36 days	11/01/2021	12/06/2021
3	Hands-on Content Development	28 days	12/07/2021	01/03/2022
4	Virtual Environment Deployment	20 days	01/04/2022	01/24/2022
5	Hands-on Content Testing	33 days	01/25/2022	02/27/2022
6	Trial Runs	Varies	02/28/2022	IT-Expo

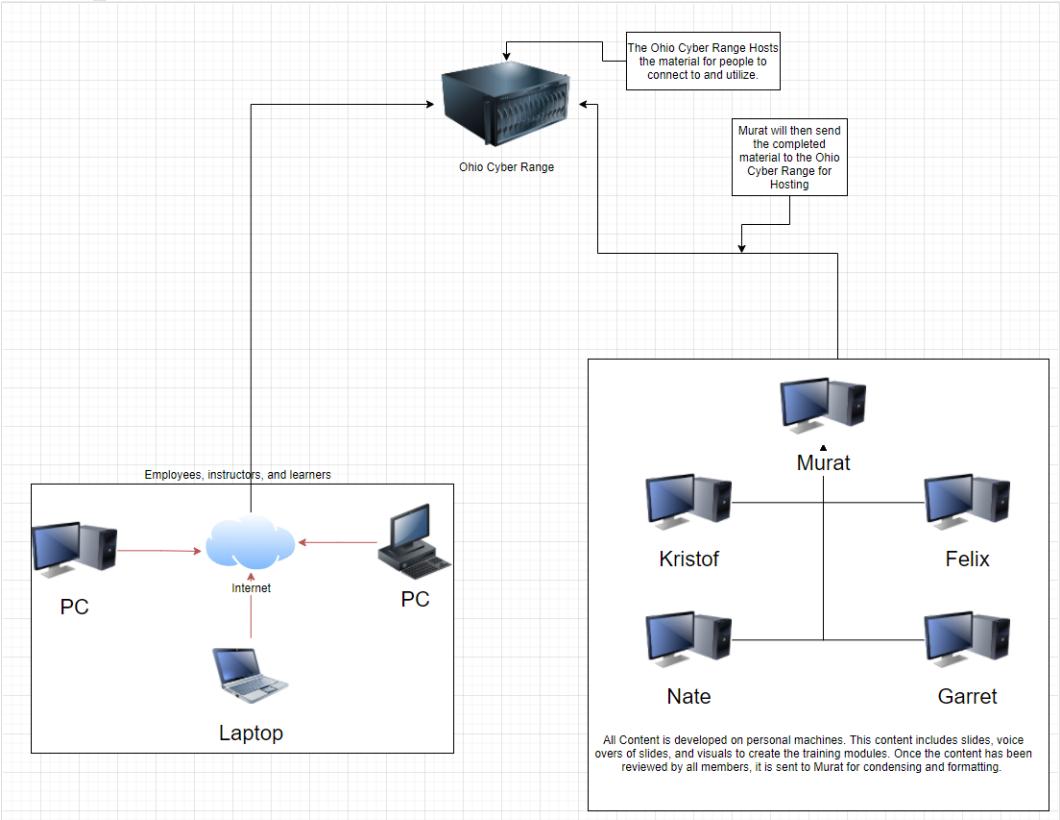
Technologies Used:

The Access Management and Off-boarding Suite was built for distribution by the Ohio Cyber Range. The course framework, knowledge checks, and virtual environments are hosted on it. Media creation tools such as the Microsoft Office suite, GIMP, and DaVinci Resolve video editing software were used to create the materials for the course. The virtual environment is run on a Windows simulated system and includes access to specific tools such as PuTTYgen, SSHKeygen, and Microsoft Azure.

Technical Architecture Diagram:

The following is a diagram created to visualize the creation of the Access Management & Off-boarding Suite by the development team, the transfer of the Suite to the Ohio Cyber Range, and the distribution of the Suite to Instructors and Learners intending to utilize the Suite.

Diagram 1 Delivery Diagram



User Personas:

The following are user profiles that are broadly representative of people that would be accessing and interacting with the Access Management and Off-boarding Suite. As a learning tool, the reasons for requesting access may vary, but the goal will be the same for each persona.

Table 1 User Persona Table

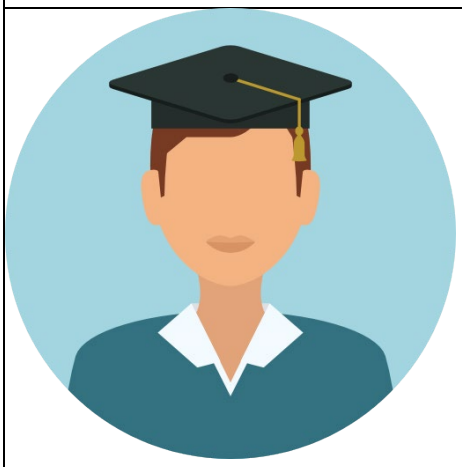
User Persona: 1	
	**Title** IT College Student
	Name Alec Pierce
	Age 22
	Gender Male
Behavior	Alec Pierce is seeking new knowledge to leverage his expertise in a specific area of IT, in this case – Access Control and Management. He has some experience in Information Technology from the classes that he has taken before, as well as from internships and co-ops that he has completed in the past.
Pain	Access Control & Management is a broad topic, which is often overlooked and not offered as a separate course/module in college, or online learning platforms. So, there is a need for a fully explained Access Control & Management course that will cover all necessary domains that Alec may work with in the workforce.
Needs & Goals	Need for the course that explains Access Control & Management domains, including Off-boarding. Hands-on experience with the tools and software that are used for Access Control & Management in the workforce.

Table 2 User Persona Table

User Persona: 2	
	**Title** IT Specialist
	Name Jodie Comer
	Age 34
	Gender Female
Behavior	Jodie is an IT Specialist working for Cincinnati Insurance Company. Her main responsibility is Systems Administration, with some coverage of Identity and Access Management, however, her expertise and understanding of Identity and Access Management is limited, based on old policies and manuals that have been with the company for quite some time.
Pain	Jodie does not have a full understanding of all the concepts and topics of Access Management. This creates a potential gap in Organization's information security posture.
Needs & Goals	Need for training that covers the topics of Access Control and Management. Hands-on experiences would greatly assist in mimicking the work that she performs daily at her job.

Table 3 User Persona Table

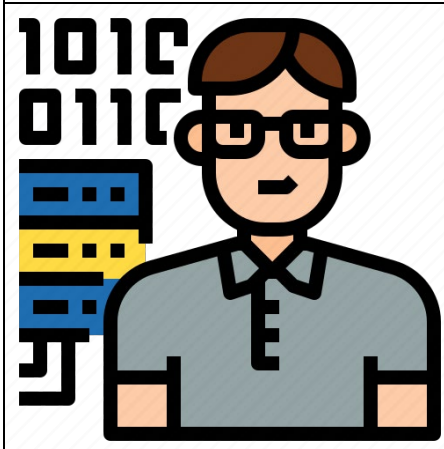
User Persona: 3	
	**Title** Job Seeker
	Name Josh Schneider
	Age 24
	Gender Male
Behavior	Josh is a recent graduate with a degree in accounting. After working in the field for 1 year, he realized that this was not what he wanted to do with his life. He decided to switch his career path to IT because of his passion for computers. After talking to IT specialists and IT recruiters, he found that he can start his career in IT without an Information Technology degree. The degree can be substituted with IT certificates that are recognized in the field, so he decided to start learning the material to prepare himself for the certification exam.
Pain	Most IT certification covers Access Management. The domain is broad, but there is a lack of free resources available to obtain the required knowledge.
Needs & Goals	The need for training courses aligning to certification exams that cover the domains within Access Management.

Table 4 User Persona Table

User Persona: 4	
	**Title** IT Instructor
	Name Franck Santoni
	Age 45
	Gender Male
Behavior	Franck Santoni is a college instructor, and he is teaching students how to implement a reliable information security system. Access Management is a key component of this process, and it is also tied to the off-boarding process.
Pain	Access Control & Management is not thoroughly implicated in the off-boarding process, and many organizations do not apply it properly potentially risking security events. There is additionally a shortage of information concerning the domain.
Needs & Goals	Get everyone familiar with a proper off-boarding process to minimize risks. Access Control & Management domains are immense and include Off-boarding as well. Hands-on experience with the tools and software may help resolve and prevent some sensitive situations as well.

Use Cases:

The following are devised use cases for being assigned, accessing, and completing the Access Management and Off-boarding Suite, as well as leading a course that utilizes the Suite. All user profiles come from diverse backgrounds and may take the course for varied reasons, but the use case for them remains the same. The Learner will request/be assigned access to the suite and then work through the suite to completion. The instructor will assign the suite, make necessary changes, and monitor Learner progress throughout the course they are instructing.

Table 5 Use Case Table

Use Case ID	AMOS_1
Use Case Name	Learn Access Management and Controls
End Objective	Gain knowledge in Access Management and Controls domain of IT
User/Actor	College Student, IT Workforce
Trigger	Need for understanding the concepts of Access Management and Controls
Frequency of Use	Once in a lifetime, with a possibility to refresh the knowledge every 3-4 years.
Preconditions	Student, or IT workforce representative, has some knowledge in IT
Basic Flow	1. Student obtains access to the materials of the Access Management and Off-boarding Suite 2. Student gets access to Virtual Machine where Hands-on Labs will be conducted 3. Student goes through module's learning material and quizzes 4. After completing study of the module's learning material and passing the quiz, student completes hands-on lab in a virtual environment 5. Student gains necessary knowledge and experience in Access Management & Controls
Alternate Flow	None
Postconditions	Student gains necessary knowledge and experience in Access Management & Controls

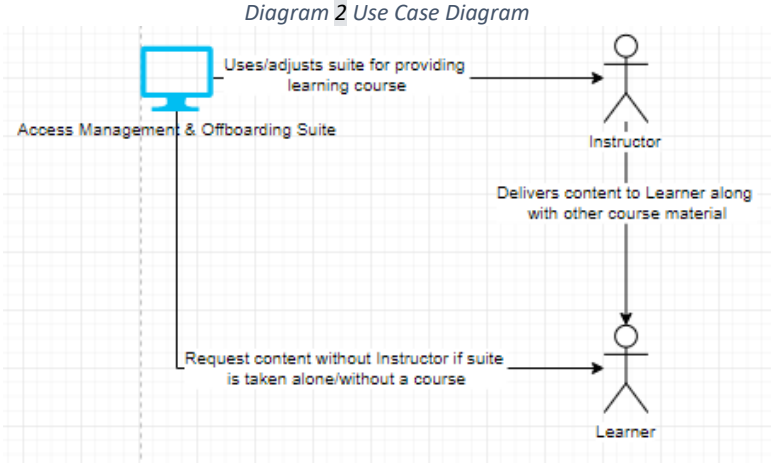
Table 6 Use Case Table

Use Case ID	AMOS_2
Use Case Name	Instructing with Access Management Suite
End Objective	Provide course to learners that is focused around, or includes the Access Management & Off-boarding Suite
User/Actor	Educational Professor/Hired Trainer
Trigger	Needed to complete their job, delivering the content to their learners
Frequency of Use	Whenever they are tasked with leading a course related to this information
Preconditions	Instructor of some kind
Basic Flow	1. User is tasked with leading an IT course that will need to cover this topic 2. Instructor requests and receives access to the Suite 3. Instructor delivers the Suite to the Learners through the course medium 4. Instructor monitors and grades Learner progress through the Suite and Course
Alternate Flow	3.1) Instructor adjusts course content to fit the topics they are teaching **(Return to Basic Flow Step 3 upon completing this alternate step.)**
Postconditions	Instructor completes tasked course along with students, having delivered the required materials and knowledge.

Use Case Diagram:

The following is a use case diagram created to display how a Learner gets access to the Suite. Whether they have a requester such as a teacher, manager, or requesting themself, it includes the steps from initial request to the issuing of the Suite's content.

Diagram 2 Use Case Diagram



Testing Plan:

Overview

Testing for the Access Management & Off-boarding Suite was focused on assessing the quality of the course content and its assessments. This included pro-active testing of the used for the course labs, ensuring that the content of the course is clear and concise and satisfies the defined Student Learning Objectives, aligning the course assessments (quizzes/labs/discussions) with created Instructional Materials, as well as verifying overall alignment of the course content with CISSP and Security+ exam objectives.

Methodology

Due to the nature of the Access Management & Off-boarding Suite as a learning content suite, common testing methods such as performance and stress-testing. Instead, Peer-review was the chosen methodology with the addition of quality assurance for virtual machine settings were used to ensure the Suite met the defined objectives.

Scope

The following is a full list of project areas that were tested, with a brief description of the areas that were chosen for assessment:

- Learning Outcomes & Student Learning Objectives
    - Ensured that LOs & SLOs were aligned with the content of the course and designed to help student succeed in developing their knowledge of the course topics.
- Instructional Material
    - Ensured that the instructional materials aligned and supported the SLOs, were clear and concise, had sufficient depth in content, and were sufficiently comprehensive for Leaners to understand the course content.
- Assessments (Quizzes/Labs/Discussions)
    - To test if the course assessments were aligned to the SLOs, tasks were clearly tied to a desired SLO, included detailed answer keys and rubrics, and included examples with instructions on how to evaluate each course assessment.
- Instructor Resources
    - Ensured that lesson plans/overviews had detailed descriptions, instructions, and expectations for the instructor, as well as presentations that were clear and included detailed instructor notes and/or transcripts.
    - Ensure assessments included instructions for the instructor and detailed evaluation tools, while also being clear in how the content is intended to be delivered.
- VM setting Testing
    - Ensured that the final delivered Virtual Environment was applicable to, and compatible with the hands-on lab exercises included in the Suite.

Objectives

a. Content was thoroughly reviewed for any misspellings, mistakes, etc.
b. Content was peer-reviewed to check if it meets SLOs and SOs.
c. Assessments were tested and peer-reviewed to check if they aligned to the course material and met SLOs and SOs.
d. VM settings were tested and reviewed to ensure that students will have a fully working Virtual Environment.

Test Logs and Procedures

The following table is the rubric that the Access Management & Off-boarding Suite content modules were compared to, to ensure that they met the team's defined objectives.

Table 7 Testing Rubric

Category	Problematic	Adequate	Excellent
Lesson Plan/Overview	Lesson plan/overview was not included (0).	Lesson plan/overview has brief descriptions of the content and materials (5).	Lesson plan/overview has detailed descriptions, instructions, and expectations for the instructor (10).
Presentations	Presentations do not include notes or transcripts (0).	Presentations include brief instructor notes (5).	Presentations include detailed instructor notes and/or transcripts (10).
Assessments	Assessments do not include instructions and evaluation tools for the instructor (0).	Assessments include evaluation tools for the instructor (5).	Assessments include instructions for the instructor and detailed evaluation tools (10).
FAQ/READ ME	No additional notes or instructions are included for the instructor with the content (0).	Some additional notes and/or instructions are included for the instructor (5).	Detailed FAQ or README file with additional information to aid and instructor in overcoming difficulties with this content are included (10).
Overall instructor resources	It is unclear how to deliver the content and assessments (0).	The delivery of the content is clear but could be left up to interpretation (5).	It is clear how the content is intended to be delivered and the expectations for the instructor are understood (10).

Courtesy of Dann Glover (UC CECH)

Testing Review

The testing phase for the Access Management & Off-boarding Suite revealed the realities of using the Virtual Environment after the hands-on labs were already created. Setup, troubleshooting, and differences of testing environments between all the testers led to unifying into a single submitted environment that was built from start to finish, rather than separate ones that were married together over the course of development. Given a second chance at this, the team would have started with a single environment instead, to expedite lab creation and simplify the labs themselves from the start.

Change Management Plan:

How changes were requested

- Anyone in the group could request a change at any time and for any reason they saw fit. Additionally, the sponsor of our project had the authority to request changes.

How changes were triaged

- Identified pros/cons.
    - What was the time commitment of the change?
    - How much would the change affect the outcome of the project?
- Identified approval process within the development team.
    - Discussed the change at scheduled meetings, requiring unanimous agreement between team members.
- Identified varying levels of criticality to help with prioritizing the change
    - If the changes were formatting changes or related to adjusting the look/design of the Suite, the changes would have needed to be agreed upon and carried out throughout the team.
        - Were considered a low-to-moderate level change.
    - If the changes were content or course direction related, the changes were considered critical and needed intense consideration before approval.

How communication with the stakeholder was conducted.

- Communication with the Suite sponsor was carried out through Microsoft Teams, email, and biweekly meetings.

Budget:

When calculating the budget, all pertinent information was used to determine the most accurate price. As shown in the table, one of the most expensive aspects of the project was hardware, which included parts of a virtualization server, endpoints, accessories, etc. The cost of hardware could be reduced significantly if the course is deployed on existing virtual infrastructure, such as those presently provided by the Ohio Cyber Range.

Another substantial portion of the cost was software, which included licensing for VMware, Windows, Office, and other software that was used in hands-on labs and during the development process.

Labor costs were estimated for five people working 10 hours/week for an 8-week period for development. Also included was the cost of involving people other than the team members for paid consultations and configuration settings.

For ongoing annual cost, consideration was made that the course must be updated at least once a year, which included 50 hours (about 2 days) of work effort by a project team member,

as well as 40 hours (about one and a half days) of work as regular maintenance, management, and administration of the virtual environment done by members of the OCRI Technical Team.

Table 8 Project Budget

Estimated Cost Rough Order of Magnitude:						
	Rate Per/Hr	**Work Effort (Hours)**	**1 X Costs**	**Ongoing Annual**		
				Rate Per/Hr	**Work Effort (Hours)**	**1 X Support Cost**
Labor - IT	20	400	$ 8,000.00	20	50	$ 1,000.00
Labor - External	25	20	$ 500.00	25	40	$ 1,000.00
Software - External			$ 9,500.00			$ 550.00
Hardware - External			$ 15,000.00			$ -
Misc.			$ 1,000.00			$ -
TOTAL			$ 34,000.00			$2,550.00

5-Year ROI Analysis		
Description	**5- Year Expected**	**Conservative (1.5)**
Total Costs	**$ 46,750.00**	**$ 70,125.00**
Total Benefit	**$ -**	$0
Total Costs/Benefit Differential	**$ (46,750.00)**	
Conservative Costs/Benefit Differential	**$ (70,125.00)**	

Problems Encountered and Analysis of Problems Solved:

Throughout the development of the course, multiple problems were encountered that slowed progress. Below is a list of the problems and a detailed analysis of devised solutions to remedy them.

Table 9 Problems Analysis

Problem	Phase	Solution
Content alignment to IT Certifications	Phase 1	During the researching phase, there was a discovery that the domain of IAM is a part of multiple high-level IT certification exams. This introduced a problem, being that different exams have different perspectives on the topic of IAM. The solution was to align the course's content to two of the most valuable certification exams in the Cybersecurity industry: Security+ and CISSP.
Differences in content comprehension	Phase 1	During the researching phase, the realization that the course content varied from entry-level to advanced level. The solution was to arrange the topics of the course in such a way that a learner would gradually move from the foundation of IAM to the very top of the domain.
Task assignment	Phases 1 & 2	Throughout the entire semester there were multiple problems assigning tasks to team members due to differences in understanding of the course topics. The solution was to take a learning course on IAM together as a group to refresh knowledge and gain new insights on the topic.
Content formatting	Phase 2	In the preliminary stages of Phase 2, there were issues formatting presentations and other course documents. The issue was that every team member had different views on how a document should look. To overcome the issue, the team met together as a group and created templates for each type of document that was being developed for the course.
Departure of team member	Phase 3 onward	One of the development team members departed the project unannounced. On top of missing some of the departee's previous work, the team had to redistribute the development and testing tasks that were assigned to the departee.
Temporary departure of a team member	Phases 3 and 4	An additional team member was onset with serious health issues due to the COVID-19 pandemic. The remaining three team members had to further distribute

		the workload and additionally cut some of the content intended for delivery in the final course.
Differences in development environments	Phases 5-7	Virtual environment development persisted on separated VM's owned by each individual developer. This led to differences in lab content, expectations, and environment requirements. An effort was completed that unified all the separated environments into one prepared for testing and submission to the Ohio Cyber Range Institute.

Conclusion

Throughout the development of the Access Management & Off-boarding Suite, the group encountered challenges that demanded that the development team obtain new skills and grow both professionally and personally to build a high-quality education suite. The team has acquired the skills necessary for the creation of presentational material, summative and formative assessments, and educational video creation and editing. Looking back on almost 9 months of work, the following three lessons were paramount to successful delivery of the suite:

1. Team communication is key.
   A significant amount of time was spent building communication channels between team members and determining the best ways to track progress while working completely remote from one another. Once it was all settled, there was significant improvement in the quality of the course deliverables, as well as in the speed that those deliverables were created with. When the team permanently lost one member and temporarily lost a second, the importance of this lesson was compounded even further to ensure that the Suite was still on track for completion.
2. Creation of templates and the standards for deliverables should begin as early as possible.
   At the beginning of the Content Development Phase, there were issues concerning course presentations and quizzes not following the same formats and differing in terms of content complexity. The solution to this problem was to create templates and set up standards that every team member used and followed when working on deliverables. Had this process begun from the get-go, rather than after work on the modules had begun, precious time could have been saved for the virtual environment development and testing.
3. Duties rotation assists in maintaining quality of work.
   Closer to the end of the Content Development Phase, the team decided the content quality had diminished due to lack of motivation and loss of morale. Rotation of team duties and getting everyone involved renewed interest in the Suite and restored the quality of the final product.

By the wrap up of the Access Management & Off-boarding Suite, the team decided that even with all the trials and tribulations of working remote, losing members, and disagreeing on communication and content, Group 43 still met and even surpassed the initial vision we had for the Suite; A free, comprehensive, and widely available training course covering the subjects of access revocation, data extraction and prevention, and account management best practices.

References

"Cost of a Data Breach Report 2021." *IBM*. Accessed April 10, 2022. https://www.ibm.com/security/data-breach.

Froehlich, Andrew. "The Top 7 Identity and Access Management Risks." *SearchSecurity*. TechTarget, July 19, 2021. Last modified July 19, 2021. Accessed April 10, 2022. https://www.techtarget.com/searchsecurity/answer/What-are-some-of-the-top-identity-and-access-management-risks.

Appendix

Appendix 1 – List of Content

Module 1 – Introduction to IAM

- Identity and Access Management (IAM)
- IAAA
- Access Management
- Identity Management
- Why is IAM important?
- Assets
    - Tangible
    - Intangible

Module 2 - Identification

- Identification Overview
- Access Controls
    - Physical
    - Logical
- Identification Mechanisms
- Access Cards
    - Magnetic Stripe Cards
    - Smart Cards
    - Card Readers
    - Proximity Cards
- Biometrics
    - Fingerprint Scanner
    - Retina vs Iris
    - Voice Recognition
    - Facial Recognition
    - Others – Vein Analysis, Hand Geometry, Gait Analysis
    - Characteristics of a good Biometric System
    - False Acceptance Rate
    - False Rejection Rate
    - Crossover Error Rate

Module 3 - Authentication

- Authentication Overview
- Authentication Factors
    - Something you know
    - Something you are
    - Something you have

        - Tokens
            - Hardware
            - Software
            - HOTP/TOTP
        - Cards
            - CAC
            - PIV
            - Smart Card
    - Other Authentication Factors
        - Somewhere you are
        - Something you do
- Multi-factor authentication

Module 4 - Authentication Methods

- Federation
- Single Sign-On
    - Shibboleth
    - Transitive Trust
- SSO vs Federation
- OAuth2 & OpenID
- SAML
- Authentication Protocols
    - AAA
        - TACACS+
        - RADIUS
    - PPP
        - PAP
        - CHAP
        - MSCHAP
    - Other
        - Kerberos
        - LDAP
- Certificate-based Authentication
- IDaaS

Module 5 - Authorization

- In development

Module 6 - Accountability

- Overview
- Auditing
    - Logs
- Account Monitoring
    - Permission auditing and review
    - Usage auditing and review
        - Deviations from normal behavior
        - Deviations in volume of data transferred
    - Attestation
    - Continuous Account Monitoring System
        - Location-Based Policies
        - Unusual network location logins
        - Time-of-day restrictions
    - Geotagging and Geofencing
- Session Management
    - Timeouts
    - Screensavers
- Privileged Access Management
    - Password Vaulting
    - Command Proxying
    - Enhanced Monitoring
    - Credential Management
    - Emergency Access Workflow

Module 7 - Accounts and Account Management

- Account Management
    - Account Management Life Cycle
- Account Types
    - User Account
    - Privileged Accounts
    - Guest Accounts
    - Shared/Generic Accounts
    - Service Accounts
- Privilege Management
    - Least Privilege
    - Separation of Duty
    - Job Rotation
    - Mandatory Vacation Policy
- Account Policies
    - Group Policy Object
- Password Policies

    - Complexity
    - Expiration
    - Password history
    - Password reuse
    - Recovery
    - Disablement
    - Lockout
    - NIST Recommendations
- Roles Management

Module 8 - On-boarding & Off-Boarding

- Registration Process
    - Request
    - Approval
    - Issuance
- Identity Proofing
    - Background Check
    - List of Acceptable Documents (Photo ID)
    - Fingerprinting
- Naming Convention Best Practices

Appendix 2 – Module Overview

Authentication

Module Description

This module is focused on introducing the concepts of authentication. Identification is the second step in IAAA process and is crucial to verify the identity of the users. After completion of this module, students will have a strong understanding of authentication processes, authentication factors, authentication technologies, as well as introduce students to multifactor authentication concept.

Section Break

Level:

☒Beginner

☒Intermediate

☐Advanced

Audience:

☒K-12

☒Higher Education

☒Adult /Workforce Development

Module Learning Outcomes:

By the completion of this module, students are expected to gain the following knowledge and skills:

- Strong understanding of Identification mechanisms
- Ability to distinguish identification and authentication
- Ability to distinguish types of access cards
- Strong understanding of Biometrics
- Ability to distinguish types of Biometrics mechanisms
- Ability to calculate FAR, FRR, CER

Module Prerequisite Knowledge

Students are encouraged to complete the previous modules of the course first, which are/is:

- Module 1: Introduction to IAM
- Module 2: Identification

Prior Knowledge Alignments:

This module covers the material necessary to successfully pass CompTIA Security+ and CISSP examination. Specifically, the following domain topics are covered in this module:

- CISSP:
  - Managing identification and authentication of people, devices, and services
    - Single/Multi-Factor Authentication
- Security+:
  - Compare and contrast identity and access management concepts
    - Identification, authentication, authorization and accounting (AAA)
    - Multifactor authentication
  - Given a scenario, implement identity and access management controls
    - Biometric factors
    - Physical Access Control
    - Certificate-based Authentication

Module Instructional and Assessment Materials:

Instructor Resources

- Authentication – Quiz Answer Key.pdf
- Authentication – Presentation Script.docx

Instructional Materials

Presentation 1: Authentication.pptx
Description: PowerPoint presentation to go through all important concepts and topics of the module. Presentation contains visual adds to help students better understand the course material

Video 2: Module Recording
Description: Video walkthrough to go through the content of the module and assist students with pre-recorded lecture of the module

Assessment Materials

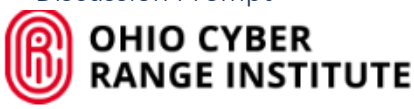
Quiz 1: Authentication – Quiz.docx
Description: Quiz on the topics covered in the module to test student's understanding of the module's content

Lab 1: Authentication – Lab.docx
Description: Lab that is built to test student's understanding of module's content using real-life scenarios, tools, and critical/analytical skills

Discussion 1: Authentication – Discussion Assignment.docx

Description: Discussion-based assignment, where students are asked to answer some questions based after completion of some research or based on their own experience/knowledge

Appendix 3 – Discussion Prompt



Identification – Discussion Assignment

Complete additional research on identification topics and build an initial identification mechanism to secure the IT environment of an imaginary company you work for. Your company has a low to medium budget to implement the controls, and does not work with governmental data, however, it is interested in protecting its business and trade secrets. In your submission, describe what access control mechanisms you choose, why you made such choice, and include any additional details that you may want to introduce to your executives to advocate for your choice. Feel free to use your imagination to add details to the type of your business, size of organization, etc.

Appendix 4 – Module Quiz

OHIO CYBER RANGE INSTITUTE

Authentication

Time Allotted: 15 minutes

Instructions

Students must carefully read the question and choose the right option to answer it.

Multiple Choice Questions

1. What is the purpose of Authentication?
    a. Identify an individual
    b. Validate user's credentials
    c. Determine the level of access for a user
    d. Trace user's actions

2. A required credential necessary for authentication is (find the best answer)
    a. Username
    b. Password
    c. Factor
    d. Username + Password

3. What is an example of the most basic factor available?
    a. Geographic Location
    b. Password
    c. Fingerprint
    d. Username

4. What factor would be used if uniqueness of the credential is the top priority (almost impossible or unfeasible to change)?
    a. Somewhere you are
    b. Something you own
    c. Something you do
    d. Something you are

5. Your organization would like to implement a multi-factor authentication to add to existing password-based one. Which of the following, if added, would not add an additional factor to the authentication mechanism?
    a. Retinal Scan
    b. Geo-Location
    c. Software token

d. Security Question

6. Which of the following technologies is a component of multifactor authentication?
   a. OTP
   b. Single Sign-On
   c. Transitive Trust
   d. RADIUS

True/False Questions

7. Authentication defines users' level of access that is granted as a result of authorization
   a. True
   b. False

8. "Something you do" factor is not commonly used due to its complexity
   a. True
   b. False

9. Having fingerprint scan, password, and facial recognition is an example of 3-factor authentication
   a. True
   b. False

Appendix 5 – Virtual Exercise

Lab Title: Creating Users and Granting Permissions

WARNING:

Use of some of the tools, techniques, or concepts learned here on a live network could result in expulsion and/or criminal prosecution. Techniques are to be used in lab environments, for educational use only or on networks for which you have written explicit permission to use.

Time Required: 1 hour 30 minutes

Section Break

Level:

☐Beginner

☒Intermediate

☐Advanced

Audience:

☐Instructor-led

☒Self-taught

Section Break

Lab Description:

This lab for the Access Management & Off-Boarding Suite will guide users through revoking permissions, disabling accounts, and deleting accounts in a Windows environment.

- Windows 10(x64) or newer

Instructions:

Part 1: User Creation

On Windows 10 GUI:

1. Log-in to the **Administrator** Account on your VM, Password is **Pa$$w0rD**.
2. Navigate to the following:

   Start > Settings > Accounts > Family and Other Users
3. Under ***Other Users*** > Add someone else to this PC
4. In the next window: Select ***I don't have this person's sign-in info*** and ***Next***
5. Choose ***Add a user without a Microsoft account*** and ***Next***.
6. Create the following users (Username, Password):

   John, Password1

   Jane, Password2

   (For the sake of expediting this lab, we use unsafe and easy to remember passwords. Always use secure passwords that meet best practices and any organization policies when in a live environment.)

---

7. Select user ***John*** and ensure that account type is set to ***Standard***.
8. Select user ***Jane*** and set account type to ***Administrator***.

What is the difference between the two types of accounts you have created? What can one do that the other cannot?

With CMD Commands :

9. In the search ***Windows search*** bar, type **cmd**, right-click ***Command Prompt*** and select ***Run as administrator***

10. The command to create users in Windows is as follows:

    net user Username Password /add

11. Type the following:

    net Tim Password3 /add

12. Create an additional user using the command prompt with the following:

    Username: Tina

    Password: Password4

Take a screenshot of the command prompt window with both commands used to create the users.

Take a screenshot of the Family & other users settings page showing all 4 users.

Part 2: Group Creation

1. Right-click ***Start***, select ***Computer Management***, then click on ***Local Users and Groups***.
2. Click on ***Users*** and you will see the users you created, as well as the Windows default accounts.
3. Right-click ***Groups*** and select ***New Group*** to create your first group.
4. Create the following 3 groups:
   a) ***Group Name***: Standard
   Group Description: Standard access group.
   b) ***Group Name***: Privileged
   Group Description: Privileged access group.
   c) ***Group Name***: Disabled
   Group Description: Disabled users.
5. Double-click the **Standard** group.
6. Click ***Add*** to add a user to the group.
7. Type ***Tim*** into the ***Objects*** names box, then check names.
8. Click ***OK*** to add ***Tim*** to the ***Standard*** group.
9. Click ***Apply*** and ***OK*** when you are finished.
10. Add ***Tina*** to the ***Standard*** Group as well.
11. Add ***Jane*** to both the ***Standard*** and ***Privileged*** groups.
12. Add your ***administrator*** account to the ***Privileged*** group.

In Computer Management, take a screenshot of both the Users and Groups folders, showing all the users and groups you have created.

Part 3: User Permissions

1. Open ***File Explorer***, navigate to ***C:\Users\Public\Documents***, and create a folder named **Secured**.
2. Open the ***Sensitive Data*** folder you just created. Right click inside the folder and create a new text file.
3. Name the file ***Sensitive Data***
4. Right-click the folder (***Secured***), select ***Properties*** and then the ***Security*** tab.
5. Under the ***Group or usernames*** section click Edit.
6. Click ***Add*** and add the ***Privileged Group*** to the ***Permissions***.
7. Ensure that you have the ***Privileged Group*** selected on the permissions tab and click ***Full Control***.

8. Now add the ***Standard*** group. Ensure that this group only has ***Read & Execute***, ***list folder contents, and read.***
9. Click ***Apply***.
10. Click the ***Advanced*** button at the bottom of the window.
11. Click ***Disable Inheritance***, convert to ***Explicit*** permissions.

What is the difference between an inherited and explicit permission?

12. Go back to editing permissions, remove all groups that you did not explicitly add above.
13. Click ***Apply***.

Which user that you have created would have the ability to move or rename items within the Sensitive Data folder?

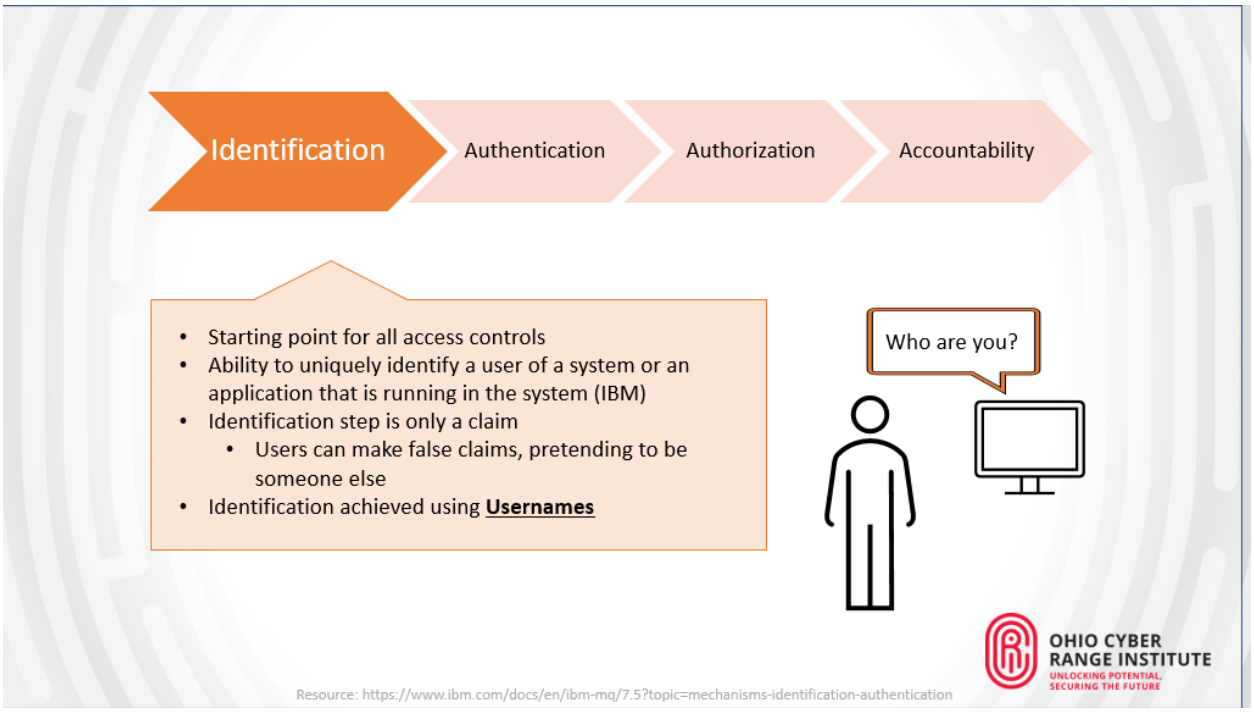
14. Navigate to the ***Sensitive Data*** text file again.
15. Right click the text file, click ***Properties***, navigate to the security tab in the properties window.
16. Select ***Edit*** and add ***John*** to the list.
17. Give ***John*** only ***Read*** access.
18. Once ***John*** has Read access, log out of your current account and login as ***John***.
19. Navigate to ***C:\Users\Public\Documents***
20. Enter the ***Secured*** folder and attempt to open the ***Sensitive Data*** file.

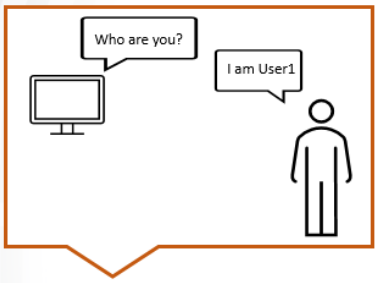
John has access to the *Sensitive Data* text file. Can he reach it to read it? Why or why not?

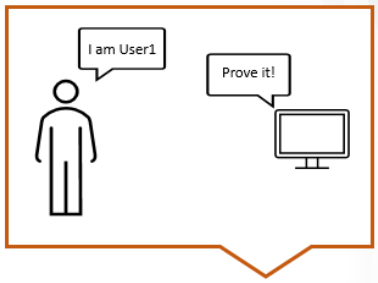
21. Return to you ***Administrator*** account.
22. Give ***John Read*** access to the ***Secured*** folder.
23. Log back in with the ***John*** account and attempt to access the ***Sensitive Data*** file.

Take and post a screenshot of the Properties>Security>Advanced tab for the Secured folder that you have created.

Appendix 6 – Module Presentation



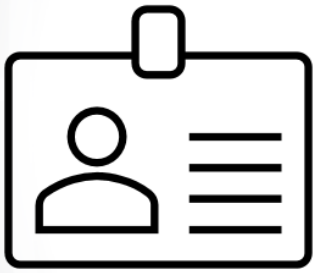




Identification ≠ Authentication

OHIO CYBER RANGE INSTITUTE
UNLOCKING POTENTIAL, SECURING THE FUTURE

Identification Mechanisms



Usernames

- Easy to use
- Often, made of combination of first and last name
- Not a secret

Access Cards

- Can serve as a proof of employment
- Can serve for both Identification and Authentication

Biometrics

- "Something you are" approach

OHIO CYBER RANGE INSTITUTE
UNLOCKING POTENTIAL, SECURING THE FUTURE

Access Cards

A card with a chip, or magnetic stripe, that contains **encoded** data that an electronic device can read when passing the card through or over it.

OHIO CYBER RANGE INSTITUTE
UNLOCKING POTENTIAL, SECURING THE FUTURE

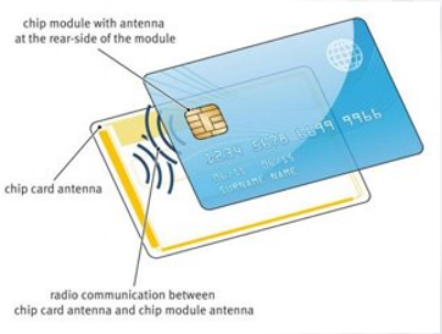
Access Cards: Magnetic Stripes

- Also called, Magstripe cards. These cards **use magnetics** to store personal identification like credit card numbers, hotel numbers, or company credentials.
- Needs to be read by a card reader where the user swipes the card, and the reader pulls the information from it.
- Examples are credit cards, debit cards, and door access cards.

OHIO CYBER RANGE INSTITUTE
UNLOCKING POTENTIAL, SECURING THE FUTURE

Access Cards: Smart Cards

- A smart card is a physical card that has an **embedded integrated chip** that acts as a security token. This security token holds **authentication** for access to a specific area.
- They are read by a special reader mounted beside what is trying to be accessed.
- They can connect to the reader by physical contact (also known as chip and dip) or through a short-range wireless connectivity standard such as radio-frequency identification (RFID) or near-field communication (NFC).



OHIO CYBER RANGE INSTITUTE
UNLOCKING POTENTIAL, SECURING THE FUTURE

Access Cards: Proximity Cards

- Transmits secure information from a distance and works via an integrated circuit that holds secure info.
- This card is held up to a reader that pulls the information via RFID or NFC and allows access.
- 2 types of proximity cards:
  - **Passive** – powered by radio frequency and must be held **very close** to the reader. Used to grant access to secure areas for individual people (office building, server rooms, etc.)
  - **Active** – powered by small lithium-Ion batteries and can have a range of **up to 100 meters**. Active card examples are transit buildings where the truck will have the card in the truck to allow access from inside. This is less secure as it let multiple people in at once.

OHIO CYBER RANGE INSTITUTE
UNLOCKING POTENTIAL, SECURING THE FUTURE

Access Cards: Card Readers

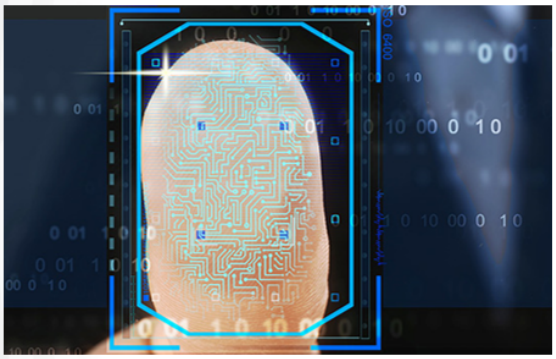
- Card readers are special devices that read information from a plastic or metal card with personal Identification on it.
- This personal ID can be stored on Magnetic Stripes, integrated chips, or Circuits within the card.
- The type of card used determines what type of reader is needed. Smart and proximity cards require the use of NCF or RFID technology to be read.

OHIO CYBER RANGE INSTITUTE
UNLOCKING POTENTIAL, SECURING THE FUTURE

Biometrics

- Users identify themselves with their own body
- Can serve for both Identification and Authentication
- Less vulnerable than traditional access systems
  - Every user has a unique biometric profile
  - Difficult to duplicate
- More convenient
  - Easy access
  - Can't be lost or forgotten
- Common biometric modalities:
  - Fingerprint, retina and iris, hand geometry, face, gait, etc.

OHIO CYBER RANGE INSTITUTE
UNLOCKING POTENTIAL, SECURING THE FUTURE



Fingerprints

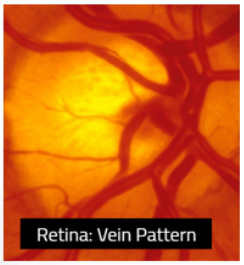
Grants access to users based on the line pattern on the surfaces of the fingers, which are unique to everyone. One drawback is that the finger does not necessarily have to be attached to the body in order to scan, however because it's commonly used, the technology is easy to use and cheap.

OHIO CYBER RANGE INSTITUTE
UNLOCKING POTENTIAL, SECURING THE FUTURE

Retina Scan vs Iris Recognition

- Grants access to users based on unique map of person's retina.

- Grants access to users based on unique pattern of the iris.



Both share the same pros and cons:

+ Enrolling and identifying is very simple
+ Extremely difficult to spoof
+ Very high accuracy

- Difficult image acquisition
- Limited user application

OHIO CYBER RANGE INSTITUTE
UNLOCKING POTENTIAL, SECURING THE FUTURE

Voice Recognition

Grants access to users based on the results of analysis of a person's voice. If the voice matches the record in the biometric database, it verifies a person's identity. Airways, soft-tissue cavities, shape and movement of the mouth and jaw are the key factors that make each person's voice unique.

OHIO CYBER RANGE INSTITUTE
UNLOCKING POTENTIAL, SECURING THE FUTURE

Facial Recognition

Grants access to users based on the shape and position of different features of a user's face. This system can also be used to deny access based on certain faces. A common facial recognition system is deployed by Apple, in their iOS FaceID.

OHIO CYBER RANGE INSTITUTE
UNLOCKING POTENTIAL, SECURING THE FUTURE

Other Biometric Technologies

Vein Analysis

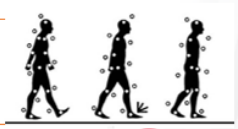
- Grants access based on the vein pattern on the finger or palm

Hand Geometry

- Grants access based on measurements of an individual's hand, which may include length, width, thickness, and surface area.

Gait Analysis

- Grants access based on analysis of an individual's movements of each body part, including the knee, the foot, the shoulder, etc.



OHIO CYBER RANGE INSTITUTE
UNLOCKING POTENTIAL, SECURING THE FUTURE

Characteristics of a Good Biometric System

- Easy Enrollment
- Low Intrusiveness
- Low False Acceptance Rates (FAR)
- Low False Rejection Rates (FRR)

OHIO CYBER RANGE INSTITUTE
UNLOCKING POTENTIAL, SECURING THE FUTURE

False Acceptance Rate (FAR)

- It is a percentage that a biometric security **recognizes** an **unauthorized** person to an account as a legitimate user.
- Measures and evaluates the efficiency and accuracy of the biometric system.
- How often does someone who should **not** have access receive it

$$FAR(\%) = \frac{FA\ (number\ of\ false\ attempts)}{TA\ (total\ number\ of\ attempts)}$$

OHIO CYBER RANGE INSTITUTE
UNLOCKING POTENTIAL, SECURING THE FUTURE

False Rejection Rate (FRR)

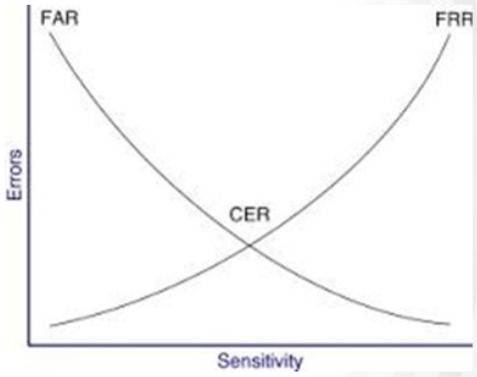
- It is a percentage that a biometric security **incorrectly** identifies an **authorized** person as an imposter.
- Measures and evaluates the efficiency and accuracy of the biometric system, as well as its convenience level.
- I **have** access, but Biometric System **does not recognize** me.

$$FRR(\%) = \frac{FR\ (number\ of\ false\ rejections)}{TA\ (total\ number\ of\ attempts)}$$

OHIO CYBER RANGE INSTITUTE
UNLOCKING POTENTIAL, SECURING THE FUTURE

Crossover Error Rate (CER)

- Also known as Equal Error Rate (ERR)
- CER is the point where the false rejection rate (FRR) and false acceptance rate (FAR) are equal
- Lower CER – more accurate system



OHIO CYBER RANGE INSTITUTE
UNLOCKING POTENTIAL, SECURING THE FUTURE