Career Kickstart Cybersecurity 2:
Cybersecurity Fundamentals Course Syllabus 2024 - 25

Instructor: Coral Riley

Email: coral.riley@pinelakeprep.org

Course Description

Career Kickstart Cybersecurity 2: Cybersecurity Fundamentals is a full-year course that covers foundational cybersecurity concepts and skills, equivalent to a collegiate Introduction to Cybersecurity course. Students will explore the current cyber threat landscape to understand the types of adversaries' organizations face and the techniques adversaries use to compromise systems and data. They will learn how vulnerabilities create risk and how organizations implement security controls to manage that risk. Topics include physical, operational, application, and network security, security controls, cryptography, access control, attacks and detection, and response and recovery. Students will research emerging trends in cybersecurity and gain hands-on experience implementing security protocols.

Course Organization

Career Kickstart (CK) is a new career-focused program that will lead to credentials and college credit for all students who want to prepare for a career, whether they are heading to 2- or 4-year colleges, technical schools, or the workforce. With a focus on high-demand fields like cybersecurity, CK will bring the best of AP to courses designed for career and technical education (CTE). CK courses are powered by the AP features that educators value: robust professional learning for teachers, dedicated educator communities, free student resources, high-quality assessments, and the broadest national network of college credit policies. CK offers two-course pathways that equip students for in-demand careers. Both industry experts and college faculty participate in defining the scope and sequence of the courses. Courses emphasize hands-on experience, teach professional and technical skills, and align to CTE standards and credentials valued by industry. Over time CK plans to launch multiple pathways across several career clusters.

I look forward to working with all students. Please sign below to indicate that you AND a parent/guardian have completely read and understand the following information.

____________________________________ ____________________________________

Student Date Parent/Guardian Date

Grading Policy

- **Major Grades (Tests and Projects): 60%**
- **Minor Grades (Quizzes, Classwork, Homework): 40%**

Class Expectations and Guidelines

Classroom Expectations:

- Active participation in all units.
- Completion of all assignments on time.
- Adherence to classroom rules regarding technology use.
- Openly engage in cooperative learning daily
- Be Prepared
- Be on time
- Follow All Policies and Procedures
- No personal electronic devices permitted during class

Classroom Guidelines:

- Be in your assigned seat and working on the assigned bell work when the music stops.
- Bring ALL the required materials to class and take them with you when you leave.
- Follow directions the first time they are given.
- Treat each person in this room with respect and dignity.
- Follow all procedures and policies as outlined by the PLP student code of conduct.

Important Dates

End of Course Exam: Thursday, April 24, 2024 (70-question multiple choice exam, timed). Students will be “required” to sit for the CK Cybersecurity exam in the spring of 2025 per our agreement with College Board, and while their exam scores will not qualify them for college credit during this pilot year, there are some serious benefits to students who demonstrate mastery of the course content at the time of the exam. Students who demonstrate mastery of the content will be gifted with a refresher course and exam voucher for COMPTIA Security + (please see more below)

BECOME A TRUSTED DEFENDER OF DIGITAL ENVIRONMENTS

Open the Door to Your Cybersecurity Career with CompTIA Security+

Launch a successful cybersecurity career
Develop a core foundation of essential skills, paving the way for a fulfilling career. More job roles use Security+ for baseline cybersecurity skills than any other certification in the industry.

Assess on-the-job skills
Security+ is the most widely adopted ISO/ANSI-accredited early career cybersecurity certification on the market with hands-on, performance-based questions on the certification exam. These practical questions assess your ability to effectively problem solve in real-life situations and demonstrate your expertise to potential employers immediately.

Embrace the latest trends
Understand and use the most recent advancements in cybersecurity technology, terms, techniques, and tools. By acquiring early career skills in the latest trends such as automation, zero trust, risk analysis, operational technology, and IoT, you will be well-equipped to excel in the ever-evolving cybersecurity landscape.

Rubric for Assessments

Assessment Type	Criteria	Points
Major Grades	Depth of understanding	40
	Quality of work submitted	30
	Timeliness	20
	Presentation and clarity	10
Minor Grades	Completion of assignment	50
	Participation in class	25
	Homework completion	25

Course Objectives

Unit 1: Assessing Risk (14 Days)

1.1 Cybersecurity Fundamentals

- Describe the impacts of cybersecurity on individuals, organizations, governments, and critical infrastructure.
- Describe the foundational concepts of confidentiality, integrity, and availability in cybersecurity.
- Explain why data must be protected.
- Describe the principles and processes that guide cybersecurity professionals.

1.2 Develop a Threat Model

- Analyze cyber threat intelligence (CTI) related to a scenario.
- Describe types of adversaries and their motivations.
- Determine the type of cybersecurity threat based on the methodology used by the adversary.

- Document a threat model for a specific scenario.

1.3 Conduct a Risk Assessment

- Apply the risk-assessment process to an asset.
- Determine the value of assets in an organization that can be compromised by a cyber-attack.
- Determine vulnerabilities that would impact assets.
- Determine threats that could leverage vulnerabilities to cause harm, loss, disruption, or destruction.
- Analyze the risk posed by each vulnerability/threat.
- Document vulnerabilities/threats in scope for the assessment, the risk posed, and suggested risk management strategies.

Unit 2: Configuring Security Controls (21 Days)

2.1 Defense in Depth

- Explain why a defense-in-depth security strategy is necessary to optimally protect an organization.
- Explain how an organization selects which security controls to implement.
- Determine appropriate security controls to harden a computer or network.

2.2 Physical, Administrative, and Operational Controls

- Explain how physical controls are used to protect computers and networks.
- Explain how common administrative controls are used to protect computers and networks.
- Explain how implementing operational security controls hardens an organization's overall security.
- Determine vulnerabilities in an existing security policy.

2.3 Technical Controls: Network Security

- Describe the different types of firewalls.
- Explain how a firewall allows or denies the flow of network traffic.
- Explain how allow and deny lists impact access.
- Describe the benefits of network segmentation.
- Explain how different techniques for network segmentation increase a network's security.
- Determine the appropriate placement of firewalls in a network.
- Configure a firewall to manage the flow of traffic into a network.

2.4 Technical Controls: Computer Security

- Apply appropriate technical controls to protect a computer.
- Determine the type of authentication used to verify the identity of a user.
- Explain how anti-malware software can make a computer more secure.
- Explain how keeping a computer's operating system and software updated makes it more secure.
- Configure login settings to make a computer more secure.

2.5 Technical Controls: Access Control

- Determine an appropriate access control model to protect software and data on a computer.
- Configure access control settings on a Linux based system to protect software and data.

Unit 3: Encrypting Data (19 Days)

3.1 Technical Controls: File Security

- Apply technical controls to protect data.
- Explain how data loss prevention (DLP) software protects data from being exfiltrated.
- Apply a cryptographic hash function to verify the integrity of a file.
- Determine whether a file has been altered by checking its hash.

3.2 Symmetric Cryptography

- Determine the appropriate cryptographic algorithm to protect data.
- Apply symmetric encryption algorithms to encrypt and decrypt data.
- Explain why key exchange algorithms are necessary when communicating with symmetric encryption.

3.3 Asymmetric Cryptography

- Determine the appropriate asymmetric key to use when sending or receiving encrypted data.
- Explain why longer keys are more secure.
- Explain how symmetric and asymmetric encryption work together to protect data in-transit.
- Apply asymmetric encryption algorithms to encrypt and decrypt data.

3.4 Digital Signatures & PKI

- Determine the integrity of a message and its source using a digital signature.
- Describe the role of public key infrastructure (PKI) in secure communications.
- Explain how the authenticity of online identities is verified.

Unit 4: Detecting Cyber Attacks (14 Days)

4.1 Attack Detection

- Describe the types of automated security tools used to detect cyber-attacks.
- Determine a detection method based on goals and constraints.

4.2 Attack Methodology

- Analyze a cybersecurity attack.
- Explain the types of information that can be gathered by attacks in the reconnaissance phase.
- Determine the type of malware used in a cyber-attack.
- Determine the social engineering tactic used by an adversary.

4.3 Password Attacks

- Explain why hashes are used to store passwords.
- Explain how password attacks exploit vulnerabilities.
- Analyze log files for indicators of password attacks.

4.4 Application Attacks

- Explain how application attacks exploit vulnerabilities.
- Analyze log files for indicators of application attacks.

4.5 Network Attacks

- Explain how network attacks exploit vulnerabilities.
- Analyze log files for indicators of network attacks.

Unit 5: Responding to Cyber Attacks (9 Days)

5.1 Investigation and Analysis

- Describe common types of digital evidence.
- Analyze digital evidence to determine the type of cyber compromise.

5.2 Containment and Eradication

- Apply containment measures to prevent the spread of a cyber-attack.
- Explain how to eradicate malware from a computer.

5.3 Recovery

- Evaluate organizational cyber resiliency.
- Evaluate a disaster recovery plan (DRP).