الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

The Saudi Cybersecurity Higher Education Framework

(SCHEF – 1: 2019)

October 2019

Sharing Indication: WHITE

Document Classification: Unclassified

Traffic Light Protocol (TLP):

This marking protocol is widely used around the world. It has four colors (traffic lights):

Red – Personal, Confidential and for Intended Recipient Only

The recipient has no rights to share information classified in red with any person outside the defined range of receipts either inside or outside the organization.

Orange – Restricted Sharing

The recipient may share information classified in orange only with intended recipients inside the organization and with recipients who are required to take action related to the shared information.

Green – Sharing within The Same Community

The recipient may share information classified in green with other recipients inside the organization or outside it within the same sector or related to the organization. However, it is not allowed to exchange or publish this information on public channels.

White – No restrictions

Updates to Document

Version	Date	Changes
1.0	October 2019	Initial version

Table of Contents

1 Introduction

As per the mandate of the National Cybersecurity Authority (NCA) that was issued by the Royal Order number 6801, dated October 31, 2017, the NCA is mandated to build the national cybersecurity workforce, to participate in developing education and training programs, to prepare professional standards and frameworks, and to develop and run professional assessment tests related to cybersecurity. Therefore, and due to the importance of developing national high-quality academic programs in cybersecurity, the NCA has led an initiative to build a framework to be the national reference for developing, evaluating and accrediting cybersecurity higher education programs. The framework is named the Saudi Cybersecurity Higher Education Framework (SCHEF). This initiative is in cooperation and coordination with the Ministry of Education and the Education and Training Evaluation Commission.

This framework sets the minimum curriculum requirements of cybersecurity higher education programs to assure their academic quality. The goal of this framework is to ensure that higher education programs in Saudi Arabia develop highly qualified cybersecurity professionals who can join and enrich the national cybersecurity workforce and contribute to the national efforts towards "A resilient, secure and trusted Saudi cyberspace that enables growth and prosperity".

SCHEF is designed in alignment with the guidelines of the National Center for Academic Accreditation and Assessment (NCAAA) and the Saudi Arabia Qualifications Framework (SAQF).

1.1 Scope

This framework covers the following degree programs in cybersecurity:

1. Diploma
2. Bachelors
3. Higher Diploma
4. Masters
5. Doctoral

The framework applies to all cybersecurity degree programs in Saudi Arabia's public and private post-secondary education institutions.

As of this early version of the document, the framework covers the general cybersecurity programs only. With the upcoming versions, the framework will evolve to cover more specialized cybersecurity programs. Since cybersecurity is a highly dynamic discipline, the curriculum requirements in this framework will be reviewed and updated periodically.

1.2 Methodology

Even though the field of cybersecurity is still evolving as compared to other well-established disciplines such as computer science, several international frameworks for cybersecurity education have been recently developed to ensure the quality of cybersecurity education programs. That include the framework of the National Centers of Academic Excellence in Cyber Defense (CAE-CD) Program[1], ABET Criteria for Accrediting Computing Programs, IEEE/ACM Cybersecurity Curricula 2017 and the framework of the NCSC-certified Higher Education Program[2]. These frameworks have major commonalities. The Knowledge Units in the SCHEF are derived mainly from the ones in the CAE-CD and IEEE/ACM Curricula frameworks. In most cases, the original Knowledge Units from the CAE-CD and the IEEE/ACM frameworks are slightly customized to address the Saudi national needs and to align with related national frameworks in the country. As mentioned earlier, the SCHEF is compatible with the national NCAAA and SAQF guidelines.

SCHEF specifies the minimum curriculum requirements for each degree program in terms of Program Learning Outcomes (PLOs) and Knowledge Units (KUs).

The PLOs help in designing program curriculum and comprise a set of knowledge, skills and competencies that graduates are expected to obtain upon completion of the program. The SCHEF sets the minimum PLOs for each degree program. However, an education institute can add more PLOs to its cybersecurity programs.

The KUs are thematic groupings that encompass multiple related topics; the topics cover the required curricular content for each KU. Each KU contains a set of learning outcomes. The KU-specific learning outcomes specifies what students should know or be able to do after successfully completing the KU.

[1] The CAE-CD program is an initiative sponsored by the National Security Agency and the Department of Homeland Security in the United States of America.
[2] The NCSC-certified higher education program is developed by the National Cyber Security Center in the United Kingdom.

The SCHEF sets the minimum KUs that must be covered by the program and provides a list of elective KUs. Education institutes can offer the desired elective KUs that are relevant to their programs and students can choose from them to complete their graduation requirements. A KU may be covered by one or more credit courses and a credit course may cover one or more KUs partially or completely.

For the bachelor's degree, we differentiate between a cybersecurity major degree program and an IT related major degree program with a cybersecurity track within the program.

The KUs are derived from the following sources:

1. The National Centers of Academic Excellence in Cyber Defense (CAE-CD) Designation Program Guidance and Knowledge Units 2019.
2. The IEEE/ACM Cybersecurity Curricula 2017.
3. The IEEE/ACM Computer Science Curricula 2013.

For each degree program, there are three types of requirements:

1. Admission Requirements: A list of requirements that need to be met prior to admitting a student into the program.
2. Core KUs: Mandatory KUs that a student must complete as part of the graduation requirements.
3. Elective KUs: A list of optional KUs that an education institute and/or a student can choose from. A minimum number of these elective KUs must be completed as part of the graduation requirements.

1.3 Structure of the Document

The rest of this document is organized as follows. Section 2 presents the PLOs and KUs requirements of the cybersecurity programs. Section 3 describes the details of all KUs.

2 Programs

2.1 Diploma

Sources:

- The Saudi Arabian Qualifications Framework (SAQF) Level Descriptors.
- The CAE-CD Designation Program Guidance and Knowledge Units 2019.

2.1.1 Program Learning Outcomes

- **Knowledge:**
  - General understanding of theoretical concepts within the cybersecurity discipline.
  - Analytical approach to understanding problems and interpreting information of cybersecurity to assess and diagnose security related issues.
  - Integrate knowledge from other fields to develop practical cybersecurity solutions that work successfully in real organizations.
- **Skills:**
  - Using a range of skills applicable to the field of cybersecurity that confirms theoretical understanding.
  - Skills of adapting and using a range of practices and technical tools in the field of cybersecurity.
  - Skills of using methods of investigation to inform actions in the field of cybersecurity.
- **Competence:**
  - Taking the lead in implementing agreed plans and activities in familiar or defined contexts.
  - Displaying an awareness of own actions on others.
  - Responsible for own personal development and learning.
  - Being receptive to learning, innovation and feedback for improvement.
  - Taking ownership for own learning and supportive of others.
  - Adopting good time management practices.

2.1.2 Admission requirements

- Highschool diploma or equivalent.

2.1.3 Core Knowledge Units

- Cybersecurity Foundations (CSF)
- Cybersecurity Design Principles (CDP)
- IT Systems Components (ISC)
- Basic Cryptography (BCY)
- Basic Networking (BNW)
- Basic Scripting and Programming (BSP)
- Network Defense (NDF)
- Operating Systems Concepts (OSC)
- Policy, Legal, Ethics and Compliance (PLE)

2.1.4 Elective Knowledge Units

Elective KUs are all remaining KUs. Students must complete at least 3 elective KUs before graduation.

2.2 Bachelor (Cybersecurity Track)

Sources:

- The Saudi Arabian Qualifications Framework (SAQF) Level Descriptors.
- The CAE-CD Designation Program Guidance and Knowledge Units 2019.

2.2.1 Program Learning Outcomes

- **Knowledge:**
  - Broad understanding and critical view of the principal theories, concepts and terminologies in the cybersecurity discipline.
  - Specialized knowledge informed by current and emerging developments in the cybersecurity field.
  - Knowledge in a range of different perspectives that underpin the cybersecurity profession.
- **Skills:**
  - Skills in using cybersecurity practices, techniques and tools.
  - Skills in using investigation and research methods for cybersecurity projects and activities.
  - Skills to critically evaluate and select cybersecurity methods and approaches to solve problems and perform cybersecurity work.
  - Using and utilizing advanced cognitive and technical skills for the analysis and evaluation of complex information in the field of cybersecurity.
- **Competence:**
  - Displaying confidence and the potential for leadership and entrepreneurship.
  - Developing a personal attitude towards values and ethics.
  - Taking structured decisions in contexts that require self-directed work, learning and innovation.
  - Awareness relating to the importance of building professional relationships.
  - Being respectful, team-oriented and approachable in social and professional contexts.

2.2.2 Admission requirements

- Highschool diploma or equivalent.

2.2.3 Core Knowledge Units

- Cybersecurity Foundations (CSF)
- Cybersecurity Design Principles (CDP)
- IT Systems Components (ISC)
- Basic Cryptography (BCY)
- Basic Networking (BNW)
- Basic Scripting and Programming (BSP)
- Network Defense (NDF)
- Operating Systems Concepts (OSC)
- Policy, Legal, Ethics and Compliance (PLE)
- Algorithms (ALG)
- Data Structures (DST)
- Databases (DAT)

2.2.4 Elective Knowledge Units

Elective KUs are all remaining KUs. Students must complete at least 7 elective KUs before graduation.

2.3 Bachelor (Cybersecurity Major)

Sources:

- The Saudi Arabian Qualifications Framework (SAQF) Level Descriptors.
- The CAE-CD Designation Program Guidance and Knowledge Units 2019.

2.3.1 Program Learning Outcomes

- **Knowledge:**
  - Broad understanding and critical view of the principal theories, concepts and terminologies in the cybersecurity discipline.
  - Specialized knowledge informed by current and emerging developments in the cybersecurity field.
  - Knowledge in a range of different perspectives that underpin the cybersecurity profession.
- **Skills:**
  - Advanced skills in using cybersecurity practices, techniques and tools.
  - Skills in using investigation and research methods for cybersecurity projects and activities.
  - Skills to critically evaluate and select cybersecurity methods and approaches to solve problems and perform cybersecurity work.
  - Using and utilizing advanced cognitive and technical skills for the analysis and evaluation of complex information in the field of cybersecurity.
  - Innovative and creative practical skills for performing cybersecurity work.
- **Competence:**
  - Displaying confidence and the potential for leadership and entrepreneurship.
  - Developing a personal attitude towards values and ethics.
  - Taking structured decisions in contexts that require self-directed work, learning and innovation.
  - Being respectful, team-oriented and approachable in social and professional contexts.
  - Decision-making in unpredictable work or learning contexts.

2.3.2 Admission requirements

- Highschool diploma or equivalent.

2.3.3 Core Knowledge Units

- Cybersecurity Foundations (CSF)
- Cybersecurity Design Principles (CDP)
- IT Systems Components (ISC)
- Basic Cryptography (BCY)
- Basic Networking (BNW)
- Basic Scripting and Programming (BSP)
- Network Defense (NDF)
- Operating Systems Concepts (OSC)
- Policy, Legal, Ethics and Compliance (PLE)
- Algorithms (ALG)
- Data Structures (DST)
- Databases (DAT)

- Network Technology and Protocols (NTP)
- Network Security Administration (NSA)
- Operating Systems Hardening (OSH)

2.3.4 Elective Knowledge Units

Elective KUs are all remaining KUs. Students must complete at least 14 elective KUs before graduation.

2.4 Higher Diploma for IT Background

Sources:

- The Saudi Arabian Qualifications Framework (SAQF) Level Descriptors.
- The CAE-CD Designation Program Guidance and Knowledge Units 2019.

2.4.1 Program Learning Outcomes

- **Knowledge:**
  - Theoretical knowledge and conceptual understanding that integrates the principal areas of cybersecurity to protect and defend cyber systems and respond to and recover from cyber-attacks.
  - Specialized knowledge in cybersecurity, which is based on new concepts.
  - In-depth understanding and analyzing new developments in cybersecurity.
- **Skills:**
  - Skills in selecting, evaluating and using theoretical concepts, methodologies and tools for cybersecurity research and analysis.
  - Innovative and creative practical skills for performing cybersecurity work.
  - Skills to integrate cybersecurity knowledge from a variety of sources.
- **Competence:**
  - Taking responsibility for leading others.
  - Adopting academic and professional values and ethics.
  - Taking independent and autonomous actions when acquiring new knowledge and skills in a social, cultural or occupational context.
  - Fostering professional relationships to bring about change, innovation, development or new thinking in a profession or occupation.

2.4.2 Admission requirements

- Diploma or bachelor's degree in cybersecurity, computer science or related fields.
- English proficiency.

2.4.3 Core Knowledge Units

- Cybersecurity Foundations (CSF)
- Cybersecurity Design Principles (CDP)
- IT Systems Components (ISC)
- Basic Cryptography (BCY)
- Basic Networking (BNW)
- Basic Scripting and Programming (BSP)
- Network Defense (NDF)
- Operating Systems Concepts (OSC)
- Policy, Legal, Ethics and Compliance (PLE)

2.4.4 Elective Knowledge Units

Elective KUs are all remaining KUs. Students must complete at least 7 elective KUs before graduation.

2.5 Higher Diploma for Non-IT Background

Sources:

- The Saudi Arabian Qualifications Framework (SAQF) Level Descriptors.
- The CAE-CD Designation Program Guidance and Knowledge Units 2019.

2.5.1 Program Learning Outcomes

- **Knowledge:**
  - Theoretical knowledge and conceptual understanding that integrates the principal areas of threats, risk analysis, planning, management, policy, legal, ethics and compliance in the field of cybersecurity.
  - Specialized knowledge in cybersecurity governance, risk management and compliance which is based on new concepts.
  - In-depth understanding and analyzing new developments in cybersecurity risk management.
- **Skills:**
  - Skills in selecting, evaluating and using theoretical concepts, methodologies and tools for cybersecurity risk management analysis and activities.
  - Innovative and creative practical skills for performing cybersecurity governance, risk management and compliance.
  - Skills to integrate cybersecurity policy, legal, ethics and compliance from a variety of sources.
- **Competence:**
  - Taking responsibility for leading others.
  - Adopting academic and professional values and ethics.
  - Taking independent and autonomous actions when acquiring new knowledge and skills in a social, cultural or occupational context.
  - Fostering professional relationships to bring about change, innovation, development or new thinking in a profession or occupation.

2.5.2 Admission requirements

- Diploma or bachelor's degree.
- English proficiency.

2.5.3 Core Knowledge Units

- Cybersecurity Foundations (CSF)
- Cybersecurity Design Principles (CDP)
- IT Systems Components (ISC)
- Cyber Threats (CTH)
- Cybersecurity Planning and Management (CPM)
- Policy, Legal, Ethics and Compliance (PLE)
- Security Program Management (SPM)
- Security Risk Analysis (SRA)

2.5.4 Elective Knowledge Units

Elective KUs are all remaining KUs. Students must complete at least 3 elective KUs before graduation.

2.6 Master

Sources:

- The Saudi Arabian Qualifications Framework (SAQF) Level Descriptors.
- The CAE-CD Designation Program Guidance and Knowledge Units 2019.

2.6.1 Program Learning Outcomes:

- **Knowledge:**
  - Critical interpretation and comprehension of knowledge in cybersecurity.
  - Developing or integrating methods and analytical approaches to research that contributes to extending knowledge in cybersecurity field.
  - Theoretical understanding of cybersecurity concepts and practices to protect and defend cyber systems and respond to and recover from advanced cyber-attacks.
- **Skills:**
  - Using a range of specialized skills, techniques and practices which are informed by forefront development in the cybersecurity field.
  - Skills to plan and implement cybersecurity research and innovation projects to develop cybersecurity products and services.
  - Skills in utilizing, assessing and critically reviewing a significant range of methods, techniques and practices in the cybersecurity field.
  - Integrating a range of knowledge, skills and strategic planning within the field of cybersecurity.
- **Competence:**
  - Leadership role in making an identifiable contribution to new thinking and change.
  - Exhibiting awareness of academic and professional practice impact on social and ethical issues.
  - Formulating or creating (innovative) solutions for complex tasks using project management principles.
  - Substantial autonomy in professional and academic activities.
  - Committing to integrity and ethical practice.

2.6.2 Admission requirements:

- Bachelor's degree in cybersecurity, computer science or related fields.
- English proficiency.

2.6.3 Core Knowledge Units:

- Cybersecurity Foundations (CSF)
- Cybersecurity Design Principles (CDP)
- IT Systems Components (ISC)
- Basic Cryptography (BCY)
- Basic Networking (BNW)
- Basic Scripting and Programming (BSP)
- Network Defense (NDF)
- Operating Systems Concepts (OSC)
- Policy, Legal, Ethics and Compliance (PLE)

2.6.4 Elective Knowledge Units:

Elective KUs are all remaining KUs. Students must complete at least 7 elective KUs before graduation.

2.7 Doctoral

Sources:

- The Saudi Arabian Qualifications Framework (SAQF) Level Descriptors.
- The CAE-CD Designation Program Guidance and Knowledge Units 2019.

2.7.1 Program Learning Outcomes

- **Knowledge:**
  - Systematic interpretation and expertise grounded with theoretical understanding, of cybersecurity and methods of research.
  - Critical analysis and evaluation of complex information, concepts, methods and theories necessary to create new knowledge in the field of cybersecurity.
  - Development of new knowledge gained through original research that significantly contributes to the field of cybersecurity.
- **Skills:**
  - Skills in conceiving, designing and conducting an independent process of research.
  - Cognitive and technical skills to critically analyze and synthesize complex datasets, information, concepts and theories in the field of cybersecurity.
  - Skills in developing knowledge, designing techniques and revising/modifying processes that result in strategic organizational or professional change and advancing of science and technology in the field of cybersecurity.
- **Competence:**
  - Leading in complex professional situations in relation to organizational change or change management.
  - Exhibiting and promoting integrity and ethical practice in relation to research and advancement of knowledge.
  - Performing broad independence, judgment and leadership as a practitioner or scholar.
  - Developing responses to professional or organizational issues or problems.
  - Assuming a leadership role for the actions of others in addressing and solving complex problems and issues.
  - Decision making that delivers a strategic or technological change, innovation and invention.
  - Substantial original research or work that merits publication and application.
  - Displaying professional and academic values in relation to technological, social or cultural advancement.
  - Aware of ethical and cultural implications of technology and science.

2.7.2 Admission requirements

- Master's degree in cybersecurity, computer science or related fields.
- English proficiency

2.7.3 Core Knowledge Units

- Cybersecurity Foundations (CSF)
- Cybersecurity Design Principles (CDP)
- IT Systems Components (ISC)
- Basic Cryptography (BCY)
- Basic Networking (BNW)
- Basic Scripting and Programming (BSP)
- Network Defense (NDF)

- Operating Systems Concepts (OSC)
- Policy, Legal, Ethics and Compliance (PLE)
- Independent/Directed Study/Research (IDR)

2.7.4 Elective Knowledge Units

Elective KUs are all remaining KUs. Students must complete at least 3 elective KUs before graduation in addition to the dissertation.

3 Knowledge Units (KUs)

CSF

Cybersecurity Foundations (CSF)

Sources:

- The CAE-CD Designation Program Guidance and Knowledge Units 2019.

Description:

This knowledge unit (KU) provides a high-level introduction and basic concepts of the cybersecurity discipline.

Topics:

The following topics must be included in this KU:

1. Threats and Threat Actors
2. Vulnerabilities
3. Common Attacks
4. Risk Assessment and Management
5. Security Life-Cycle
6. Cryptography Applications
7. Secure Data Transmission, Storing and Processing.
8. Security Models
9. Access Control Models
10. Confidentiality, Integrity, Availability, Access, Authentication, Authorization, Non-Repudiation, Privacy
11. Session Management
12. Exception Management
13. Security Mechanisms
14. Malicious Activity Detection
15. Appropriate Countermeasures
16. Legal issues
17. Ethics

Learning Outcomes:

Once completing this KU, students should be able to:

1. Explain the foundation concepts of cybersecurity field to secure the cyberspace.
2. Recognize common attacks and threat actors.
3. Illustrate cybersecurity methods and tools and apply them to protect cyber-systems.
4. Discuss appropriate countermeasures when a cyber incident occurs.
5. Identify and explain common terminologies in the field of cybersecurity.

CDP

Cybersecurity Design Principles (CDP)

Sources:

- The CAE-CD Designation Program Guidance and Knowledge Units 2019.

Description:

This KU provides secure-by-design foundations to design secure and trusted systems.

Topics:

The following topics must be included in this KU:

1. Separation of Duties
2. Isolation
3. Encapsulation
4. Modularity
5. Simplicity of Design
6. Minimization of implementation
7. Open Design
8. Complete Mediation
9. Layering and Defense-in-Depth
10. Least Privilege
11. Fail Safe Defaults and Fail Secure
12. Least Astonishment
13. Minimize Trust Surface
14. Usability
15. Trust relationships

Learning Outcomes:

Once completing this KU, students should be able to:

1. Express the secure-by-design principles.
2. Explain the importance of cybersecurity design principles and how each principle is useful to design trusted systems.
3. Distinguish the violated design principle for common system security weaknesses.
4. Analyze the required cybersecurity design principles needed for a given setup.
5. Discuss the importance of minimizing the implications of the secure design principles on system usability.

ISC

IT Systems Components (ISC)

Sources:

- The CAE-CD Designation Program Guidance and Knowledge Units 2019.

Description:

This KU provides general introduction to common information technology systems components and general cybersecurity implications associated with them.

Topics:

The following topics must be included in this KU:

1. Endpoint protection
2. Storage Devices
3. System Architectures
4. Virtualization and Cloud
5. SCADA, Real Time and Critical Infrastructures Environments
6. LANs, Internet and Wireless Networks
7. Network Mapping
8. Network Security Components
9. Intrusion Detection and Prevention Systems
10. Incident Response
11. Managed Services
12. Software Security
13. Configuration Management
14. Patching
15. Vulnerability Scanning
16. People and Security
17. Physical and Environmental Security
18. Internet of Things (IOT)

Learning Outcomes:

Once completing this KU, students should be able to:

1. Identify common hardware and software IT system components and illustrate their main functions.
2. Explain main cybersecurity implications of the current and future IT environments.

3. Express common cybersecurity systems, components and activities and their values to cybersecurity.

BCY

Basic Cryptography (BCY)

Sources:

- The CAE-CD Designation Program Guidance and Knowledge Units 2019.
- IEEE/ACM Cybersecurity Curricula 2017.

Description:

This KU provides introduction to basic cryptographic algorithms and applications.

Topics:

The following topics must be included in this KU:

1. Security Functions of Cryptography
2. Symmetric Cryptography
3. Block vs. Stream Data
4. Public Key Cryptography
5. Key Generation, Management, Exchange and Distribution
6. Digital Certificates
7. Hash Functions
8. Digital Signatures
9. Collision Resistance
10. Common Cryptographic Protocols and Standards
11. Types of Cryptographic Attacks
12. Cryptographic Implementation Failures

Learning Outcomes:

Once completing this KU, students should be able to:

1. Explain the main components of any cryptographic system.
2. Differentiate between symmetric and asymmetric cryptography.
3. Propose an appropriate cryptographic mechanism for a given requirement and setup.
4. Demonstrate the use and strength of each cryptographic mechanism and associated implementation issues.
5. Explain the main security functions that cryptography can provide.
6. Illustrate the use of PKI to digitally sign and encrypt data.
7. Apply brute force and frequency-based attacks to break encrypted data.

BNW

Basic Networking (BNW)

Sources:

- The CAE-CD Designation Program Guidance and Knowledge Units 2019.

Description:

This KU provides introduction to networks operations, components, layers, protocols, services, applications, tools and network security.

Topics:

The following topics must be included in this KU:

1. ISO OSI and TCP/IP Networking models
2. Wired, Optical and Wireless Network Media
3. Network Architectures and Topologies
4. PAN, LAN, WAN, DMZ, VLAN and NAT
5. Subnetting and Supernetting
6. Common Network Devices: Routers, Switches and Firewalls
7. Network Protocols, Services and Applications: IP, TCP, UDP, ICMP, DNS, NTP, VLAN, SMTP, HTTP, VoIP, SSH, etc.
8. Basic network administration tools
9. Overview of Network Security Issues

Learning Outcomes:

Once completing this KU, students should be able to:

1. Explain foundational concepts of data networks including components, layers, protocols, services, applications and tools.
2. Propose a network design architecture for a given setup scenario.
3. Identify packets trace for simple connections.
4. Apply network tools to recognize packet flows.
5. Demonstrate how to perform network mapping.
6. Illustrate common network threats and vulnerabilities.

BSP

Basic Scripting and Programming (BSP)

Sources:

- The CAE-CD Designation Program Guidance and Knowledge Units 2019.

Description:

This KU provides necessary skills and abilities to write simple scripts and programs to implement algorithms to solve given problems using programing languages with general secure coding guidelines.

Topics:

The following topics must be included in this KU:

1. Variables and Data Types
2. Regular Expressions
3. Assignment Statements
4. Basic Boolean Logic Operations
5. Decisions and Branching
6. Loops
7. Functions, Procedures and Calls
8. Debugging Techniques
9. Basic Data Structures and Algorithms
10. Strings, Arrays and Structures
11. Sequential and Parallel Execution
12. Scripting on Windows and Linux
13. Basic Secure Coding Concepts: Permissions, Bounds Checking, Input Validation, Type Checking and Parameter Validation

Learning Outcomes:

Once completing this KU, students should be able to:

1. Implement scripts and programs with compound conditions and loops to automate system tasks and to solve given problems.
2. Implement secure and reliable programs to solve complex problems.

NDF

Network Defense (NDF)

Sources:

- The CAE-CD Designation Program Guidance and Knowledge Units 2019.
- IEEE/ACM Cybersecurity Curricula 2017.

Description:

This KU provides necessary concepts, skills, knowledge and tools to defend and protect a network against cyber threats.

Topics:

The following topics must be included in this KU:

1. Network Attacks
2. Network Hardening
3. Minimizing Exposure, Attack Surface and Vectors
4. Defense in Depth
5. Implementing Firewalls
6. DMZs and Proxy Servers
7. VPNs
8. Honeypots and Honeynets
9. Implementing IDS/IPS
10. Network Security Monitoring
11. Network Traffic Analysis
12. Threat Hunting
13. Attack Pattern Detection
14. Network Access Control
15. Network Policy Development and Enforcement

Learning Outcomes:

Once completing this KU, students should be able to:

1. Illustrate main network defense concepts.
2. Demonstrate the use of network defense tools to protect a network from vulnerabilities, threats and attacks and to respond to incidents.
3. Analyze the security policies implementations to protect a network.
4. Examine network operations relevant to network defense.

OSC

Operating Systems Concepts (OSC)

Sources:

- The CAE-CD Designation Program Guidance and Knowledge Units 2019.

Description:

This KU provides a general introduction to the basic roles, functions and services of operating systems.

Topics:

The following topics must be included in this KU:

1. Privileged and Non-Privileged States
2. Application Processes and Threads
3. Memory Management
4. File systems
5. Virtualization and Hypervisors
6. Security Design in Operating Systems: Access controls, Domain Separation, Process Isolation, Resource Encapsulation and Least Privilege

Learning Outcomes:

Once completing this KU, students should be able to:

1. Illustrate the basic roles, functions and services of operating systems.
2. Demonstrate operating systems interactions with hardware components and other software applications.
3. Explain main cybersecurity issues related to operating systems.

CTH

Cyber Threats (CTH)

Sources:

- The CAE-CD Designation Program Guidance and Knowledge Units 2019.

Description:

This KU provides general information about cyber threats and attacks.

Topics:

The following topics must be included in this KU:

1. Cyber Adversary Model: Resources, Capabilities, Intent, Motivation, Risk Aversion and Access
2. Password Guessing and Cracking
3. Backdoors, Trojans, Viruses and Wireless attacks
4. Sniffing, Spoofing and Session Hijacking
5. Denial of service, DDoS and Bots
6. MAC spoofing, Web app attacks and zero-day exploits
7. Advanced Persistent Threat (APT).
8. Attack Indication Events
9. Attack Timing
10. Attack Surfaces, Vectors and Trees
11. Covert Channels
12. Social Engineering
13. Insider Problem
14. Threat Information Sources
15. Cyber Threats Legal Issues

Learning Outcomes:

Once completing this KU, students should be able to:

1. Categorize adversary resources, capabilities, techniques and motivations.
2. List, explain and compare types of cyberattacks.

CPM

Cybersecurity Planning and Management (CPM)

Sources:

- The CAE-CD Designation Program Guidance and Knowledge Units 2019.

Description:

This KU provides necessary skills and abilities to design cybersecurity plans and processes for an organization.

Topics:

The following topics must be included in this KU:

1. Cybersecurity Common Body of Knowledge (CBK) with Relation to Planning and Management
2. Operational, Tactical and Strategic Planning and Management
3. Cybersecurity Related C-Level Functions
4. Cybersecurity in the Core Strategy
5. Business Continuity and Disaster Recovery
6. Incident Response Processes and Procedures
7. Intellectual Property Protection Plan
8. Access Controls Implementation Management
9. Patch Management and Change Control

Learning Outcomes:

Once completing this KU, students should be able to:

1. Analyze system security functions and their strengths and weaknesses.
2. Design and prepare contingency plans including business continuity, disaster recovery and incident response.
3. Design patch and change management plan, intellectual property protection plan and access controls implementation plan.
4. Identify and illustrate the roles and responsibilities in cybersecurity planning and managing security.

PLE

Policy, Legal, Ethics and Compliance (PLE)

Sources:

- The CAE-CD Designation Program Guidance and Knowledge Units 2019.

Description:

This KU provides information related to cybersecurity laws, standards, regulations, guidelines, policies and ethics.

Topics:

The following topics must be included in this KU:

1. Cybersecurity Laws and Authorities
2. Information Crime Law
3. International Jurisdictions
4. Cybersecurity International Standards (e.g. HIPAA, ISO 27001)
5. International Organizations and Cybersecurity
6. Privacy Laws and Regulations (e.g. GDPR)
7. Payment Card Industry Data Security Standard (PCI DSS)
8. Bring Your Own Device (BYOD) Issues

Learning Outcomes:

Once completing this KU, students should be able to:

1. Discuss main cybersecurity laws, regulations, guidelines and policies.
2. Recognize important legal and ethical issues in dealing with data.

SPM

Security Program Management (SPM)

Sources:

- The CAE-CD Designation Program Guidance and Knowledge Units 2019.

Description:

This KU provides necessary knowledge to design, run and manage a cybersecurity program to protect and defend the organization in the cyberspace.

Topics:

The following topics must be included in this KU:

1. Security Program Goals and Objectives
2. Measuring Effectiveness
3. Roles and Responsibilities
4. Security Policies
5. Compliance with Applicable Laws and Regulations
6. Security Best Practices and Frameworks
7. Security Baselining
8. Program Monitoring and Control
9. Security Awareness, Training and Education
10. Physical Security
11. Personnel Security
12. System and Data Identification
13. System Security Plans
14. Configuration and Patch management
15. System Documentation
16. Incident Response Program Management
17. Disaster Recovery Program Management
18. Certification and Accreditation

Learning Outcomes:

Once completing this KU, students should be able to:

1. Design, prepare and manage a security program with goals, objectives and metrics for a given organization.
2. Measure the effectiveness of a security program.

SRA

Security Risk Analysis (SRA)

Sources:

- The CAE-CD Designation Program Guidance and Knowledge Units 2019.

Description:

This KU provides necessary knowledge of the models, methodologies and processes for risk assessment, management and mitigation.

Topics:

The following topics must be included in this KU:

1. Risk Assessment and Analysis Methodologies
2. Risk Measurement and Evaluation Methodologies
3. Risk Management Models
4. Risk Management Processes
5. Risk Mitigation Economics
6. Risk Transference, Acceptance and Mitigation
7. Communication of Risk

Learning Outcomes:

Once completing this KU, students should be able to:

1. Relate risk to a security policy.
2. Demonstrate the main risk analysis methodologies.
3. Evaluate and categorize risk with respect to technology, individuals and entities.
4. Select the desired methodology for a given needs considering advantages and disadvantages.

AAL

Advanced Algorithms (AAL)

Sources:

- The CAE-CD Designation Program Guidance and Knowledge Units 2019.
- IEEE/ACM Computer Science Curricula 2013.

Description:

This KU provides the ability to apply and analyze advanced optimization and approximation algorithms to correctly and effectively solve given problems.

Topics:

The following topics must be included in this KU:

1. Bloom filters
2. Naive Bayes
3. Map-Reduce
4. Dynamic Programming algorithms
5. Markov Chain Monte Carlo
6. Coding and Compression
7. Artificial Intelligence algorithms
8. Max-Flow/Min-Cut and its applications
9. Stable Matching
10. NP-hardness
11. Linear Programming: Properties and Applications
12. Approximation Algorithms
13. Randomized Algorithms

Learning Outcomes:

Once completing this KU, students should be able to:

1. Apply and analyze advanced algorithmic techniques to optimally and efficiently solve real problems.
2. Define the classes P and NP.
3. Explain the significance of NP-hardness.
4. Demonstrate examples of classic NP-complete problems.
5. Apply Bloom filters, Naive Bayes, Map-Reduce, Coding and Compression and AI algorithms to solve relevant problems.

ACR

Advanced Cryptography (ACR)

Sources:

- The CAE-CD Designation Program Guidance and Knowledge Units 2019.
- IEEE/ACM Cybersecurity Curricula 2017.

Description:

This KU provides knowledge of advanced cryptographic algorithms and applications

Topics:

The following topics must be included in this KU:

1. Number Theory
2. Probability and Statistics
3. AES, RSA and EC
4. Naive RSA and padded RSA
5. Suite B Algorithms
6. Families of Attacks: Differential, Man-in-the-Middle, Linear
7. Hashing and Signatures
8. Key Management
9. Modes and Appropriate Uses
10. Classical Cryptanalysis
11. Side-Channel Attacks: Timing, Power-Consumption and Differential Fault Analysis Attacks
12. Identity-based Cryptography
13. Digital Signatures
14. Virtual Private Networks
15. Quantum cryptography

Learning Outcomes:

Once completing this KU, students should be able to:

1. Demonstrate the work of advanced cryptographic algorithms and protocols.
2. Analyze security levels considering cryptography.
3. Demonstrate the roles of cryptography in common applications.
4. Analyze error propagation through a cryptosystem.
5. Analyze the security strength in encryption algorithms.
6. Apply advanced encryption algorithms to solve given setup scenario.
7. Perform classical cryptanalysis and side-channel attacks.

ANT

Advanced Network Technology and Protocols (ANT)

Sources:

- The CAE-CD Designation Program Guidance and Knowledge Units 2019.

Description:

This KU provides knowledge of advanced networking concepts and complex network security issues.

Topics:

The following topics must be included in this KU:

1. Advanced Routing algorithms and protocols: BGP, OSPF and MPLS
2. Software Defined Networking
3. IPv6 Networking
4. IPv6 Security Issues
5. Quality of Service
6. Network Services
7. Social Network Implementation and Security Issues
8. Voice over IP (VoIP)
9. Multicasting
10. Secure DNS
11. Network Address Translation
12. Deep Packet Inspection
13. Transport Layer Security

Learning Outcomes:

Once completing this KU, students should be able to:

1. Demonstrate the work of common advanced network protocols.
2. Analyze the security of advanced network protocols.
3. Operate network tools to examine an advance network protocol behavior.

ALG

Algorithms (ALG)

Sources:

- The CAE-CD Designation Program Guidance and Knowledge Units 2019.
- IEEE/ACM Computer Science Curricula 2013.

Description:

This KU provides the ability to apply and analyze algorithms to correctly and effectively solve given problems.

Topics:

The following topics must be included in this KU:

1. Algorithm Analysis
2. Computational Complexity
3. Best, Worst and Average Case Behavior
4. Optimization
5. Searching and Sorting
6. String Matching Algorithms
7. Iterative
8. Recursion
9. Greedy Algorithm
10. Hill Climbing
11. Stable Matching
12. Divide and Conquer
13. Dynamic Programming
14. Max Flow

Learning Outcomes:

Once completing this KU, students should be able to:

1. Implement and analyze algorithms to correctly and effectively solve given problems.
2. Differentiate between best, worst and average case behavior of an algorithm.
3. Apply greedy, divide-and-conquer and dynamic programming algorithms to optimally solve appropriate problems.

ATC

Analog Telecommunications (ATC)

Sources:

- The CAE-CD Designation Program Guidance and Knowledge Units 2019.

Description:

This KU provides general introduction to analog communications systems.

Topics:

The following topics must be included in this KU:

1. Signaling Methods
2. Architecture
3. Trunks, Switching
4. Grade of Service
5. Blocking
6. Call Arrival Models
7. Interference Issues

Learning Outcomes:

Once completing this KU, students should be able to:

1. Illustrate the main components of analog communications systems and sketch block diagrams for such systems.
2. Differentiate between types of modulation and explain their advantages and applications.

CCO

Cloud Computing (CCO)

Sources:

- The CAE-CD Designation Program Guidance and Knowledge Units 2019.
- IEEE/ACM Computer Science Curricula 2013.

Description:

This KU provides general introduction to cloud computing technologies, services, models and security.

Topics:

The following topics must be included in this KU:

1. Virtualization Platforms
2. Cloud Services: SaaS, PaaS, DaaS and IaaS
3. Hypervisors and Cloud Computing Implementations.
4. Service Oriented Architectures
5. Deployment Models: Private, Public, Community and Hybrid
6. Cloud Security
7. Storage
8. Legal and Privacy Issues

Learning Outcomes:

Once completing this KU, students should be able to:

1. Explain cloud computing services.
2. Discuss the advantages and disadvantages of virtualization.
3. Deploy a cloud-based application.
4. Efficiently allocate resources to users and applications.
5. Discuss the importance of resource management in cloud computing.
6. Deploy a secure cloud environment.

CCR

Cyber Crime (CCR)

Sources:

- The CAE-CD Designation Program Guidance and Knowledge Units 2019.

Description:

This KU provides general information about cybercrimes and abuses in the cyberspace.

Topics:

The following topics must be included in this KU:

1. Cyber Crime Types: Intrusions, Ransomware, Espionage, Intellectual Property and Fraud
2. Cyber Stalking and Predators
3. Cyber Bullying
4. Identity Theft
5. Cyber Assisted Crimes
6. Cyber Terrorism
7. Cyber Crime Laws: National Laws, International Laws, Treaties

Learning Outcomes:

Once completing this KU, students should be able to:

1. Explain potential cybercrimes, cyber-stalking, cyber-bullying and other abusive behaviors in the internet.
2. Demonstrate the use of cybersecurity applications for defense against crime and abuse.

CSE

Cybersecurity Ethics (CSE)

Sources:

- The CAE-CD Designation Program Guidance and Knowledge Units 2019.

Description:

This KU provides general information about ethical issues in the cyberspace.

Topics:

The following topics must be included in this KU:

1. Ethical Codes and Frameworks
2. Ethics and Cyberspace
3. Ethical Issues: Property, Availability, Rights of Others, Respect of Community, Resource Use, Allocation, Abuse and Censorship
4. Ethics-Based Decision Tools
5. Cybersecurity and Social Responsibility

Learning Outcomes:

Once completing this KU, students should be able to:

1. Apply ethical foundations to given scenarios in the cyberspace.
2. Discuss ethical issues from different perspectives.
3. Explain the cybersecurity roles regarding ethics and discuss scenarios where cybersecurity can cause ethical conflicts.

DBA

Data Administration (DBA)

Sources:

- The CAE-CD Designation Program Guidance and Knowledge Units 2019.

Description:

This KU provides information about data life cycle, data quality and data security.

Topics:

The following topics must be included in this KU:

1. Data Lifecycle: Capture, Maintenance, Transformation, Usage, Distribution, Archival and Purging
2. Data Quality: Accuracy, Completeness, Relevance, Consistency, Integrity, Cleansing, Verification and Validation
3. Data Accessibility
4. Data Utility
5. Data Storage and Archiving: Data Warehousing, Long Term Archival and Big Data
6. Hadoop, MongoDB and HBASE
7. Data Control: Ownership, Stewardship, Management, Possession, Governance
8. Data Policies: Internal and External
9. Data Security: Access Control and Encryption

Learning Outcomes:

Once completing this KU, students should be able to:

1. Explain data lifecycle stages and discuss related security issues.
2. Analyze data quality, accessibility and utility.
3. Manage the creation, change, distribution, storage and termination of data in a secure way.
4. Discuss and explain data ownership, stewardship, management, possession and governance.
5. Illustrate the importance of data classification in cybersecurity.

DST

Data Structures (DST)

Sources:

- The CAE-CD Designation Program Guidance and Knowledge Units 2019.

Description:

This KU provides knowledge of abstract data types and how to use them to solve relevant problems.

Topics:

The following topics must be included in this KU:

1. Numerical
2. Strings
3. Lists: Linked List, Double Linked List and Hash Tables
4. Arrays
5. Vectors
6. Heaps
7. Queues
8. Stacks
9. Buffers
10. Trees
11. Objects
12. Data Formats in languages
13. Categories

Learning Outcomes:

Once completing this KU, students should be able to:

1. Implement common abstract data types.
2. Use given abstract data types and their operation to implement solutions to given problems.
3. Differentiate between different data structures and their use, benefits and drawbacks.
4. Design specifications of a required data structure based on given needs.
5. Illustrate the abstraction concept and recognize abstract violations for given data structure specifications.

DMS

Database Management Systems (DMS)

Sources:

- The CAE-CD Designation Program Guidance and Knowledge Units 2019.

Description:

This KU provides skills and abilities to operate and secure database management systems.

Topics:

The following topics must be included in this KU:

1. Database Types: Flat, Relational, Network, Hierarchical, Object-Oriented, Object-based, Key-Value and Distributed
2. SQL Data Manipulation Language: SELECT, INSERT, DELETE and UPDATE
3. SQL Data Definition Language
4. SQL Database Administration: User Creation and Deletion, Permissions and Access Controls
5. Database concepts: Indexing, Inference, Aggregation and Polyinstantiation
6. Database Security and Protection

Learning Outcomes:

Once completing this KU, students should be able to:

1. Differentiate between database models.
2. Differentiate between the roles of a database, a DBMS and a database server.
3. Create, administer and operate databases.
4. Manage DBMS access controls, privilege levels.
5. Sketch structures for storing data in DBMS.
6. Design and implement a database for a given application.

Databases (DAT)

Sources:

- The CAE-CD Designation Program Guidance and Knowledge Units 2019.

Description:

This KU provides skills and abilities to manage, use and protect database systems.

Topics:

The following topics must be included in this KU:

1. Database Management Systems Types: Relational, Hierarchical, NoSQL Databases, Object-Based, Object-Oriented and Distributed
2. Database Security Models: Inference, Aggregation, Injection, Hashing, Encryption and Data Corruption, Unauthorized Access, Database Access Controls (DAC, MAC, RBAC, Clark-Wilson)

Learning Outcomes:

Once completing this KU, students should be able to:

1. Compare database models and implement given database requirements using a given model.
2. Illustrate security aspects related to databases and DBMS.

DVF

Device Forensics (DVF)

Sources:

- The CAE-CD Designation Program Guidance and Knowledge Units 2019.
- IEEE/ACM Cybersecurity Curricula 2017.

Description:

This KU provides skills and abilities to forensically investigate a device.

Topics:

The following topics must be included in this KU:

1. Mobile Device Analysis: Smartphones and Tablets
2. Embedded Systems: GPS, Games Consoles, Smart TVs
3. Internet of Things Devices

Learning Outcomes:

Once completing this KU, students should be able to:

1. Perform hands-on forensics techniques and activities on mobile, embedded systems and IOT devices.
2. Discuss legal aspects linked to forensic operations on mobile, embedded systems and IOT devices.

Digital Communications (DCO)

Sources:

- The CAE-CD Designation Program Guidance and Knowledge Units 2019.

Description:

This KU provides knowledge of digital communications systems and related protocols.

Topics:

The following topics must be included in this KU:

1. Digital Communications System Components
2. Coding Schemes
3. Digital Signaling
4. Spread Spectrum Signals
5. Multi-User Communication Access: CDMA, TDMA, FDMA, SDMA, PDMA

Learning Outcomes:

Once completing this KU, students should be able to:

1. Illustrate digital communications systems, subsystems and modulations.
2. Demonstrate state of the art digital communications methods.
3. Differentiate between digital communications models and discuss pros and cons for each.

DFS

Digital Forensics (DFS)

Sources:

- The CAE-CD Designation Program Guidance and Knowledge Units 2019.
- IEEE/ACM Cybersecurity Curricula 2017.

Description:

This KU provides knowledge of forensics techniques for investigation with related legal issues.

Topics:

The following topics must be included in this KU:

1. Digital Forensics Terminologies
2. Legal Compliance: Applicable Laws, Affidavits, Testimony, Testifying, Case Law and Chain of Custody
3. Investigatory Process
4. Acquisition and Preservation of Evidence: Write-blocking, Imaging Procedures, Live Forensics, Analysis and Authentication of Evidence (Hashing)
5. Analysis of Evidence: Root Cause Analysis, Metadata and File Carving
6. Reporting and Presentation of Results: Timeline and Attribution

Learning Outcomes:

Once completing this KU, students should be able to:

1. Solve a given cyber investigation problem using digital forensics techniques and tools.
2. Illustrate legal and regulation issues related to digital forensics and investigation.

EBS

Embedded Systems (EBS)

Sources:

- The CAE-CD Designation Program Guidance and Knowledge Units 2019.

Description:

This KU provides skills and abilities to implement software applications on embedded systems environments.

Topics:

The following topics must be included in this KU:

1. Microcontroller and Embedded Processor Architectures
2. PLC's, Gate Arrays
3. I/O, A/D and Registers
4. Embedded Devices Communications
5. Interrupt Handling and Timing Issues
6. Resource Management in Real Time Systems
7. Devices without Operating Systems
8. Real-Time Operating Systems
9. Security Issues on Devices with Limited Resources
10. Embedded Systems Programming languages and Environments: Tool Chains, Target Operating Systems and Devices and Cross Compilers

Learning Outcomes:

Once completing this KU, students should be able to:

1. Illustrate common architectures for embedded systems.
2. Demonstrate embedded systems requirements and capabilities.
3. Experiment concurrency, synchronization and other real time related issues.
4. Analyze, optimize and manage resources in real time environments.
5. Discuss resource and timing challenges in real-time operating systems.

FAC

Forensic Accounting (FAC)

Sources:

- The CAE-CD Designation Program Guidance and Knowledge Units 2019.

Description:

This KU provides knowledge and abilities of forensics techniques for financial investigations.

Topics:

The following topics must be included in this KU:

1. Investigative Accounting
2. Fraudulent Financial Reporting
3. Misappropriation of Assets
4. Indirect Methods of Reconstructing Income
5. Money Laundering
6. Transnational Financial Flows
7. Litigation Services
8. Evidence Management
9. Economic Damages and Business Valuations

Learning Outcomes:

Once completing this KU, students should be able to:

1. Detect common financial statement fraud.
2. Estimate concealed revenue and income.
3. Illustrate money laundering methods with associated detection and prevention techniques.
4. Evaluate fraud and theft loss and damages.

FMD

Formal Methods (FMD)

Sources:

- The CAE-CD Designation Program Guidance and Knowledge Units 2019.
- IEEE/ACM Computer Science Curricula 2013.

Description:

This KU provides mathematical logic skills needed to design cybersecure systems.

Topics:

The following topics must be included in this KU:

1. Concept of Formal Methods
2. Mathematical Logic
3. Role in System Design and Software Engineering
4. Limitations
5. Bell-LaPadula
6. Automated Reasoning Tools
7. System Modeling and Specification
8. Proofs
9. Model Checkers and Model Finders
10. Program Assertion Languages

Learning Outcomes:

Once completing this KU, students should be able to:

1. Apply formal methods to real situations.
2. Illustrate the value of formal methods and analysis techniques over testing as software validation and verification techniques.
3. Apply formal methods to software designs.
4. Explain formal specification languages advantages and disadvantages.
5. Analyze software and systems security.

FPM

Fraud Prevention and Management

Sources:

- The CAE-CD Designation Program Guidance and Knowledge Units 2019.
- IEEE/ACM Cybersecurity Curricula 2017.

Description:

This KU provides knowledge and abilities to design plans and processes to prevent fraud.

Topics:

The following topics must be included in this KU:

1. Fraud Introduction and Terminologies
2. Fraud Prevention and Auditing: Scientific Method and Benford's Law
3. Dealing with Data: Collecting, Cleaning, Verifying and Normalizing
4. Understanding Data: Analysis, Visualization, Sorting, Indexing, Summarizing and Stratifying
5. Numeric Tests for Fraud: Frequently Used Values, Even Amounts, Rounding, Ratio/Variance Analysis, Testing for Outliers, Statistical Tests and Randomization Testing
6. Modeling Fraud: Machine Learning Techniques for Fraud Detection
7. Advanced Fraud Detection and Prevention

Learning Outcomes:

Once completing this KU, students should be able to:

1. Evaluate cost and effectiveness of fraud detection and prevention methods.
2. Explain legal and ethical issues related to fraud detection and prevention.
3. Apply fraud tools and techniques for detection and prevention.

HRE

Hardware Reverse Engineering (HRE)

Sources:

- The CAE-CD Designation Program Guidance and Knowledge Units 2019.
- IEEE/ACM Cybersecurity Curricula 2017.

Description:

This KU provides knowledge, abilities and skills to determine the functionality of given hardware components using reverse engineering procedures and techniques.

Topics:

The following topics must be included in this KU:

1. Reverse Engineering Principles
2. Stimulus, Data Collection and Data Analysis
3. Specification Development
4. Capability Enhancement and Modification Techniques
5. Detecting Modification
6. Stimulation Methods and Instrumentation
7. JTAG IEEE 1149.1
8. Defining and Enumerating Interfaces
9. Functional Decomposition

Learning Outcomes:

Once completing this KU, students should be able to:

1. Demonstrate hardware reverse engineering techniques.
2. Apply probing, measuring and data collection to identify the functionality of a given hardware component.

HFS

Hardware/Firmware Security (HFS)

Sources:

- The CAE-CD Designation Program Guidance and Knowledge Units 2019.

Description:

This KU provides knowledge of hardware/firmware components and the related security issues.

Topics:

The following topics must be included in this KU:

1. Physical Vulnerabilities: Unused/Unsecured Communications Channels, Test Pads, Test Paths, Back Doors, Trojans, Hidden Circuits, Doping, Induced Faults, Reverse Engineering, Unauthorized Memory Access
2. Hardware Side Channel Attacks: Timing, Power Analysis, Electromagnetic, RF analysis, Hardware Insertion and Out-of-Band Channels
3. Sourcing Attacks: Pirated, Fake, Counterfeit Parts and Supply Chain Disruption
4. Equipment Destruction Attacks
5. Hardware Security Components: Verifiable Device IDs, Random Number Generators, Boot ROM Digital Signatures, Hardware-Base Encryption Modules, Security Controllers/Co-Processors and Encryption Accelerators
6. Physical Security Attributes: Device Validation, Open/Accepted Security Algorithms, Strong Random Number Generation, Secure Time Source, Standardized Developer Interface, Clear Documentation, Key Backup/Protection, Tamper-Resistance and Scalability
7. Bootloader Vulnerabilities: Boot Sector Attacks, Single User Mode, Boot to Non-Secure OS's and Boot Loader Reconfiguration
8. Microcode Vulnerabilities
9. Firmware Vulnerabilities: Reflashing BIOS/PROMs
10. Security Role of Intermediate Layers: Hardware Abstraction Layer and Virtualization Layers

Learning Outcomes:

Once completing this KU, students should be able to:

1. Illustrate main hardware vulnerabilities.
2. Utilize hardware security capabilities.
3. Explain systems initialization and software loading and validation.
4. Discuss the security role of hardware abstraction layers.

HOF

Host Forensics (HOF)

Sources:

- The CAE-CD Designation Program Guidance and Knowledge Units 2019.
- IEEE/ACM Cybersecurity Curricula 2017.

Description:

This KU provides skills and ability to investigate a network host using forensics techniques.

Topics:

The following topics must be included in this KU:

1. File Systems and File System Forensics
2. Hypervisor Analysis
3. Cryptanalysis
4. Rainbow Tables
5. Known File Filters (KFF)
6. Steganography
7. File Carving
8. Live System Investigations
9. Timeline Analysis

Learning Outcomes:

Once completing this KU, students should be able to:

1. Identify retrievable data from multiple operating system environments.
2. Demonstrate host forensics methodologies.

IAA

Information Assurance Architectures (IAA)

Sources:

- The CAE-CD Designation Program Guidance and Knowledge Units 2019.

Description:

This KU provides knowledge of security architectures used for protecting information systems.

Topics:

The following topics must be included in this KU:

1. Defense in Depth
2. DMZs
3. Proxy Servers
4. Composition and Security
5. Cascading
6. Emergent Properties
7. Dependencies
8. TCB Subsets
9. Enterprise Architectures and Security Architectures
10. Secure Network Design

Learning Outcomes:

Once completing this KU, students should be able to:

1. Differentiate and relate between information assurance architecture stages and components.
2. Demonstrate knowledge of the capabilities and limitations of current methods for evaluating, planning, implementing and maintaining IA Architectures solutions.
3. Examine potential vulnerabilities for a given architecture.
4. Design information assurance architectures for given applications.

IAC

Information Assurance Compliance (IAC)

Sources:

- The CAE-CD Designation Program Guidance and Knowledge Units 2019.

Description:

This KU provides knowledge of audit and compliance with laws and regulations related to cybersecurity.

Topics:

The following topics must be included in this KU:

1. Relationship Between Compliance and Audit
2. Audit Types: Internal and External
3. Audit Purposes: Requirements, Specifications, Policy, Standards, Laws, Regulatory and Internal Controls
4. Audit Process: Charter, Baseline, Activities, Reporting, Results, Recommendations, Response and Mitigation Strategy
5. Compliance Monitoring
6. Compliance Training

Learning Outcomes:

Once completing this KU, students should be able to:

1. Differentiate between mandatory and optional compliance requirements.
2. Design, plan and perform audits to examine compliance.

IAS

Information Assurance Standards (IAS)

Sources:

- The CAE-CD Designation Program Guidance and Knowledge Units 2019.

Description:

This KU provides knowledge of information assurance related standards.

Topics:

The following topics must be included in this KU:

1. Saudi Laws & Regulations
2. International standards (e.g. NIST)
3. Rainbow Series
4. Commercial Standards (e.g. PCI/DSS)
5. Open Standards (e.g. OWASP)

Learning Outcomes:

Once completing this KU, students should be able to:

1. Differentiate between laws, regulations, policies, frameworks and standards.
2. Explain the impact of standards on given systems.
3. Illustrate standards implications on sub-contractors and customers.
4. List and explain main standards provisions.

IDR

Independent/Directed Study/Research (IDR)

Sources:

- The CAE-CD Designation Program Guidance and Knowledge Units 2019.

Description:

This KU provides knowledge of emerging issues related to cybersecurity.

Topics:

The following topics must be included in this KU:

1. Emerging Technologies with Relevant Security Issues
2. Emerging Tools, Techniques and Methods Related to Cybersecurity

Learning Outcomes:

Once completing this KU, students should be able to:

1. Discuss advanced and emerging technology with associated security issues.
2. Apply, demonstrate and discuss the use of emerging and advanced cybersecurity tools, methods and techniques.

ICS

Industrial Control Systems (ICS)

Sources:

- The CAE-CD Designation Program Guidance and Knowledge Units 2019.

Description:

This KU provides knowledge of industrial control systems with associated potential vulnerabilities.

Topics:

The following topics must be included in this KU:

1. Hardware Components of ICS
2. Ladder Logic
3. Programmable Logic Controllers (PLCs)
4. Protocols (MODBUS, PROFINET, DNP3, OPC, ICCP, SERIAL)
5. Networking (RS232/485, ZIGBEE, 900MHz, BlueTooth, X.25)
6. Types of ICSs (e.g., Power Distribution Systems, Manufacturing)
7. Models of ICS systems: Time Driven vs. Event Driven
8. Common Vulnerabilities in Critical Infrastructure Systems
9. SCADA Security Components

Learning Outcomes:

Once completing this KU, students should be able to:

1. Apply PLCs for automation.
2. List, explain and discuss industrial control systems components and applications.
3. Describe control schemes and differentiate between them.
4. Implement and evaluate security functionality within an industrial network.
5. Demonstrate and compare popular ICS protocols.

ITC

Introduction to the Theory of Computation (ITC)

Sources:

- The CAE-CD Designation Program Guidance and Knowledge Units 2019.
- IEEE/ACM Computer Science Curricula 2013.

Description:

This KU provides knowledge and skills to apply finite automata to identify how efficiently a solution to a problem can be computed.

Topics:

The following topics must be included in this KU:

1. Automata
2. Turing Machines
3. Deterministic and Non-Deterministic Finite Automata
4. Formal Language Theory
5. Computability and Non-Computability
6. Turing Computability
7. Analysis of Algorithms
8. Complexity Measures: Time, Storage, Communications and Numbers of Processors
9. Big O Notation
10. Best, Worst and Average Complexity
11. Upper and Lower Bounds on Complexity
12. Classes of Complexity: P, NP and Intractability

Learning Outcomes:

Once completing this KU, students should be able to:

1. Explain abstract machines theory and automata.
2. Differentiate between computable and incomputable functions.
3. Explain complexity and quantify resources requirements for problems computation.
4. Analyze given problems using deterministic and non-deterministic finite automata.

IDS

Intrusion Detection/Prevention Systems (IDS)

Sources:

- The CAE-CD Designation Program Guidance and Knowledge Units 2019.

Description:

This KU provides knowledge and skills for vulnerabilities and threats detection and related risks mitigation.

Topics:

The following topics must be included in this KU:

1. Deep Packet Inspection
2. Log File Analysis
3. Log Aggregation
4. Cross Log Comparison and Analysis
5. Anomaly Detection: Establishing Profiles, Anomaly Algorithms, Statistical Techniques, Correlation Techniques, Fuzzy Logic Approaches, Artificial Intelligence, Filtering Algorithms and Neural Networks
6. Misuse Detection: Signature Detection
7. Specification-Based Detection
8. Host-Based Intrusion Detection and Prevention
9. Network-Based Intrusion Detection and Prevention: Stealth mode
10. Distributed Intrusion Detection
11. Hierarchical IDS's
12. Honeynets/Honeypots
13. Intrusion Response: Device Reconfiguration, Notifications, Logging, SNMP Trap, Email, Visual/Audio Alert, Trace Recording, Opening Application, Session Interruption and Reach Back

Learning Outcomes:

Once completing this KU, students should be able to:

1. Detect and respond to host and network intrusions.
2. Apply tools to detect malware and unauthorized devices on a network.
3. Tune IDS/IPS systems configurations to reduce false alarms and unidentified threats.
4. Design corrective procedures to respond to discovered intrusions.
5. Setup, install and configure intrusions detection/prevention system.

LCS

Life-Cycle Security (LCS)

Sources:

- The CAE-CD Designation Program Guidance and Knowledge Units 2019.

Description:

This KU provides knowledge and ability to apply security principles throughout the system life-cycle.

Topics:

The following topics must be included in this KU:

1. System Life-Cycle Phases and Issues: Initiation, Requirements, Design, Development, Testing, Deployment, Operations, Maintenance and Disposal
2. Vulnerability Mapping, Management and Tractability
3. Threat Modeling
4. Software Assurance Maturity Model
5. Role of Project/Program Management
6. Role of Process Management
7. Importance of Culture and Training
8. Development Processes and Paradigms
9. Configuration Management
10. Developmental Threats

Learning Outcomes:

Once completing this KU, students should be able to:

1. Demonstrate and apply practices, processes and methodologies to secure software.
2. List system life-cycle phases and explain each phase along with security related issues.
3. List and explain maturity model elements.

LSA

Linux System Administration (LSA)

Sources:

- The CAE-CD Designation Program Guidance and Knowledge Units 2019.

Description:

This KU provides skills to perform LINUX administration operations.

Topics:

The following topics must be included in this KU:

1. OS Installation
2. User Accounts Management: Access Controls, Password Policies, Authentications Methods and GroupPolicies
3. Command Line Interfaces
4. Configuration Management
5. Updates and Patches
6. Event Logging and Auditing
7. Managing System Services
8. Virtualization
9. Backup and Restoring Data
10. File System Security
11. Network Configuration
12. Host Intrusion Detection
13. Security Policy Development

Learning Outcomes:

Once completing this KU, students should be able to:

1. Install, configure, operate and maintain LINUX OS in a secure way.
2. Setup user accounts and configure polices for authentication.
3. Design and implement audit configurations
4. Perform backups and successfully restoring them.
5. Demonstrate the importance of reviewing security logs and installing updates and patches periodically.

LLP

Low Level Programming (LLP)

Sources:

- The CAE-CD Designation Program Guidance and Knowledge Units 2019.

Description:

This KU provides skills to securely perform low level operations using low level programing languages.

Topics:

The following topics must be included in this KU:

1. Low Level Access Support in C.
2. Programing in Assembly
3. Library Functions Security
4. Pointers and Pointer Manipulation
5. Modularization in Low Level Programs
6. Defensive Programming Techniques
7. Compile, Assemble and Link
8. Calls in Assembly.

Learning Outcomes:

Once completing this KU, students should be able to:

1. Apply low level programming to implement OS components and hardware drivers.
2. Discuss the benefits and the risks of using low level programming.

MEF

Media Forensics (MEF)

Sources:

- The CAE-CD Designation Program Guidance and Knowledge Units 2019.
- IEEE/ACM Cybersecurity Curricula 2017.

Description:

This KU provides skills and ability to investigate media using forensics techniques.

Topics:

The following topics must be included in this KU:

1. Drive Acquisition
2. Evidence Authentication: Verification, Validation and Hashing
3. Metadata: MAC timestamps
4. Live vs. Static Acquisition
5. Sparse vs. Full Imaging
6. Slack Space
7. Hidden Files, Clusters and Partitions

Learning Outcomes:

Once completing this KU, students should be able to:

1. Demonstrate forensic analysis techniques on given media.
2. Perform forensic methods on specified media.

MOT

Mobile Technologies (MOT)

Sources:

- The CAE-CD Designation Program Guidance and Knowledge Units 2019.

Description:

This KU provides knowledge of mobile technologies including hardware, communications, management and programing.

Topics:

The following topics must be included in this KU:

1. 2G, 3G, 4G/LTE and 5G: Standards Heritage and Core Architecture Evolution
2. Design Choices
3. Encryption
4. Mobile Use of SS7
5. RRC Signaling
6. Billing/Charging
7. Mobile Security

Learning Outcomes:

Once completing this KU, students should be able to:

1. Demonstrate mobile systems function to secure voice and data access.
2. Explain how network connectivity is maintained during motion.

NWF

Network Forensics (NWF)

Sources:

- The CAE-CD Designation Program Guidance and Knowledge Units 2019.

Description:

This KU provides ability to investigate and analyze network traffic using forensics techniques.

Topics:

The following topics must be included in this KU:

1. Packet Capture and Analysis
2. Intrusion Detection and Prevention
3. Interlacing of Device and Network Forensics
4. Log-File Analysis

Learning Outcomes:

Once completing this KU, students should be able to:

1. Demonstrate network forensic methodologies.
2. Analyze network traffic.
3. Detect malicious and anomalous activities and their effects.

NSA

Network Security Administration (NSA)

Sources:

- The CAE-CD Designation Program Guidance and Knowledge Units 2019.

Description:

This KU provides knowledge of administration and maintaining enterprise security infrastructures.

Topics:

The following topics must be included in this KU:

1. Mapping Business Objectives to Technology Objectives
2. Main Security Solutions and Product Categories and Features
3. Information Security Conflicts with Potential Solutions
4. Cybersecurity Best Practices
5. Applying Network Security Policies
6. Risk Posture and Risk Appetite
7. Network and Systems Monitoring Tools
8. Issue Evaluation, Response and Management
9. Incident Identification
10. Incident Response Processes and Management
11. Deployment and Upgrade Processes
12. User Acceptance Testing
13. Blackout Plans
14. Maintenance Windows and Management

Learning Outcomes:

Once completing this KU, students should be able to:

1. Analyze needs and recommend solutions, products and technologies.
2. Select best security practices to satisfy business objectives according to risk assumptions.
3. Protect IT assets and infrastructure from potential threats.
4. Perform systems monitoring for anomalies and periodically perform system updating and patching.
5. Demonstrate incident response activities to breaches, intrusions and theft.
6. Plan, test, implement and evaluate software and hardware deployment.

NTP

Network Technology and Protocols (NTP)

Sources:

- The CAE-CD Designation Program Guidance and Knowledge Units 2019.

Description:

This KU provides knowledge of networking, network protocols, network tools and network vulnerabilities.

Topics:

The following topics must be included in this KU:

1. Network Switching: ARP, RARP and Layer 2 Security Issues
2. IPv4 Suite: IPv4 Addressing
3. IPv6 Suite: IPv6 Addressing
4. Routing in IPv4 and IPv6: Routing Tables and Metrics, Layer 3 Security Issues and IPsec
5. Network Naming: DNS and NetBIOS
6. Network Analysis and Troubleshooting: Netflow

Learning Outcomes:

Once completing this KU, students should be able to:

1. Demonstrate and explain layer 2 networking.
2. Illustrate IPv4 and IPv6 structure.
3. Discuss common network vulnerabilities.
4. Detect and mitigate layer 2 and layer 3 security issues.
5. Apply networks analysis tools for troubleshooting.
6. Explain WEP weaknesses and how to address them if possible.

OSA

Operating Systems Administration (OSA)

Sources:

- The CAE-CD Designation Program Guidance and Knowledge Units 2019.

Description:

This KU provides skills perform OS administration operations.

Topics:

The following topics must be included in this KU:

1. OS Installation
2. User Accounts Management: Access Controls, Password Policies, Authentications Methods and Group Policies
3. Command Line Interfaces
4. Configuration Management
5. Updates and Patches
6. Event Logging and Auditing
7. Managing System Services
8. Virtualization
9. Backup and Restoring Data
10. File System Security
11. Network Configuration
12. Host Intrusion Detection
13. Security Policy Development

Learning Outcomes:

Once completing this KU, students should be able to:

1. Setup user accounts and configure polices for authentication.
2. Design and implement audit configurations
3. Perform backups and successfully restoring them.
4. Demonstrate the importance of reviewing security logs and installing updates and patches periodically.

OSH

Operating Systems Hardening (OSH)

Sources:

- The CAE-CD Designation Program Guidance and Knowledge Units 2019.

Description:

This KU provides skills and ability to improve the security and robustness of operating systems.

Topics:

The following topics must be included in this KU:

1. Secure Installation
2. Removing Unnecessary Components
3. File system Maintenance: Isolation of Sensitive Data
4. User Restrictions: Access and Authorizations
5. User, Group and File Management
6. Password Standards and Requirements
7. Shutting Down Unnecessary and Unneeded Services
8. Closing Unnecessary and Unneeded Ports
9. Patch Management and Software Updates
10. Virtualization
11. Vulnerability Scanning

Learning Outcomes:

Once completing this KU, students should be able to:

1. Demonstrate hardening steps for a given OS according to given applications.
2. Perform secure OS installation and disable unneeded components, services and ports.
3. Perform periodically OS patching and updating.

OST

Operating Systems Theory (OST)

Sources:

- The CAE-CD Designation Program Guidance and Knowledge Units 2019.

Description:

This KU provides knowledge, skills and ability to design and implement operating system concepts, components and interfaces.

Topics:

The following topics must be included in this KU:

1. Privilege States
2. Processes, Threads and Process/Thread Management
3. Memory Management and Virtual Memory
4. Inter-Process Communications
5. Concurrency, Synchronization and Deadlocks
6. File Systems
7. Input and Output
8. Real-time Operating Systems and Security Issues
9. Distributed OS Architectures and Security Issues
10. Race Conditions
11. Buffer Overflows
12. Virtualization
13. Clear Interface Semantics

Learning Outcomes:

Once completing this KU, students should be able to:

1. Illustrate and demonstrate operating systems theory and implementation.
2. Design and implement OS architectural changes.

PTT

Penetration Testing (PTT)

Sources:

- The CAE-CD Designation Program Guidance and Knowledge Units 2019.

Description:

This KU provides knowledge, skills and ability to discover and exploit vulnerabilities to gain control or access to systems.

Topics:

The following topics must be included in this KU:

1. Flaw Hypothesis Methodology
2. Other Methodologies (e.g., OSSTMM)
3. Identifying Flaws from Documentation
4. Identifying Flaws from Source Code Analysis
5. Vulnerability Scanning
6. Families of Attacks
7. Flaws that Lead to Vulnerabilities
8. Enumeration and Foot Printing
9. Attack Surface Discovery
10. Attack Vectors

Learning Outcomes:

Once completing this KU, students should be able to:

1. Demonstrate, design and perform penetration testing on a network.

Privacy (PRI)

Sources:

- The CAE-CD Designation Program Guidance and Knowledge Units 2019.

Description:

This KU provides knowledge of privacy concepts, issues, tools and practices.

Topics:

The following topics must be included in this KU:

1. Personally Identifiable Information (PII)
2. Fair Information Practice Principles (FIPPs): Transparency, Individual Participation, Purpose Specification, Data Minimization, Use Limitation, Data Quality, Integrity, Security, Accountability and Auditing
3. Privacy
4. Anonymity and Pseudonymity
5. Privacy Policies, Laws and Regulations
6. Risks to Privacy
7. Tracking and Surveillance
8. Privacy tools: Encryption, VPNs and Scramblers
9. Privacy Laws and Legal Basis

Learning Outcomes:

Once completing this KU, students should be able to:

1. Explain privacy concepts.
2. Discuss the Internet effects on privacy.
3. Demonstrate appropriate approaches to protect privacy by individuals, organizations and governments.
4. Discuss privacy policies and laws nationally and internationally.

QAT

QA/Functional Testing (QAT)

Sources:

- The CAE-CD Designation Program Guidance and Knowledge Units 2019.

Description:

This KU provides knowledge of assessment methods of meeting requirements by functional units.

Topics:

The following topics must be included in this KU:

1. Testing Methodologies: White, Grey, Black Box Testing
2. Test Coverage Analysis
3. Automatic and Manual Generation of Test Inputs
4. Test Execution
5. Validation of Results

Learning Outcomes:

Once completing this KU, students should be able to:

1. Design and develop effective, structured and organized tests.
2. Perform security functional testing to demonstrate that security policies and mechanisms are completely and correctly implemented.
3. Demonstrate functional testing to validate security policies implementations.

RFP

Radio Frequency Principles (RFP)

Sources:

- The CAE-CD Designation Program Guidance and Knowledge Units 2019.

Description:

This KU provides knowledge of radio frequency communications.

Topics:

The following topics must be included in this KU:

1. Basics of Electromagnetic Radiation
2. Antennas
3. Information Modulation
4. Digital Modulation
5. Spectral Representation
6. Bandwidth
7. BER
8. Eb/No vs. S/N
9. Limiting Access in RF
10. Propagation Principles

Learning Outcomes:

Once completing this KU, students should be able to:

1. Explain isolating RF emissions methods.
2. Explain obfuscating RF transmissions techniques.
3. Demonstrate the tradeoffs related to bandwidth data rate, modulation, complexity, acceptable BER and signal spreading.

SPP

Secure Programming Practices (SPP)

Sources:

- The CAE-CD Designation Program Guidance and Knowledge Units 2019.

Description:

This KU provides knowledge, skills and ability to implement secure software programs with no vulnerabilities.

Topics:

The following topics must be included in this KU:

1. Security Requirements Interpretation and Realization
2. Principles of Secure Programming
3. Robust Programming
4. Defensive Programming: Input Validation, Type Checking, Cover all Cases, Exceptions Handling, Avoidance of Risky Coding, Avoid Information Leakage, Apply Classes Security Practices, Avoidance of External Data Changes by Reference, Data Updates Verification Support and Authentication.
5. Programming Flaws: Buffer Overflows and Integer Errors
6. Static Analysis
7. Data Obfuscation
8. Data Protection
9. Secure Programming Paradigms: Pair Programming, Code Reviews and Test-Driven Development

Learning Outcomes:

Once completing this KU, students should be able to:

1. Implement required software components without making new vulnerabilities.
2. Discuss secure programming characteristics.
3. Explain common vulnerabilities in each programming language.
4. Discover vulnerabilities in libraries and mitigate them.

SAS

Software Assurance (SAS)

Sources:

- The CAE-CD Designation Program Guidance and Knowledge Units 2019.

Description:

This KU provides knowledge of methods and techniques for securing software.

Topics:

The following topics must be included in this KU:

1. Security Principles: Separation, Isolation, Encapsulation, Least Privilege, Simplicity, Minimization, Fail Safe Defaults, Fail Secure, Modularity, Layering, Least Astonishment, Open Design, Usability and Reduce Attack Surfaces
2. Security of Alternative Designs
3. Review Secure Design Patterns
4. Security Level for System data
5. Audit Trail
6. Security Modeling Techniques and Vulnerability Mapping
7. Resiliency Increase
8. Design Reviews

Learning Outcomes:

Once completing this KU, students should be able to:

1. Apply security design principles.
2. Illustrate the effects of system design and architecture on security.
3. Design a given system to optimally satisfy security requirements.
4. Construct a secure design using modeling and vulnerability assessment.
5. Discuss how Design Reviews can significantly help improving security.

SRE

Software Reverse Engineering (SRE)

Sources:

- The CAE-CD Designation Program Guidance and Knowledge Units 2019.
- IEEE/ACM Cybersecurity Curricula 2017.

Description:

This KU provides skills and ability to perform reverse engineering to determine the function, effect and implementation details of a given executable code.

Topics:

The following topics must be included in this KU:

1. Malware Analysis
2. Reverse Engineering Tools & Techniques
3. Static vs Dynamic Analysis
4. Sandboxing
5. Anti-Reverse Engineering Techniques

Learning Outcomes:

Once completing this KU, students should be able to:

1. Demonstrate software reverse engineering techniques.
2. Apply software reverse engineering tools to discover functionality and implementation of software or malware.

SSA

Software Security Analysis (SSA)

Sources:

- The CAE-CD Designation Program Guidance and Knowledge Units 2019.

Description:

This KU provides skills and ability to analyze software in binary or source code form.

Topics:

The following topics must be included in this KU:

1. Testing Methodologies
2. Source and Binary Code Analysis
3. Static and Dynamic Analysis Techniques
4. Sandboxing
5. Common Analysis Tools and Methods

Learning Outcomes:

Once completing this KU, students should be able to:

1. Explain the use of tools and techniques for software security analysis.
2. Apply software security analysis tools to analyze unknown software components.

SCS

Supply Chain Security (SCS)

Sources:

- The CAE-CD Designation Program Guidance and Knowledge Units 2019.
- IEEE/ACM Cybersecurity Curricula 2017.

Description:

This KU provides knowledge of security issues related to third-party components used in building complex systems.

Topics:

The following topics must be included in this KU:

1. Global Development
2. Offshore Production
3. Transport and Logistics of IT Components
4. Evaluation of 3rd Party Development Practices
5. Software and Hardware Reverse Engineering Capabilities and Limitations
6. Supply Chain Risks: Hardware and Software
7. Procurement Process: Physical Security, Split Manufacturing, Traceability, Cargo Screening and Validation

Learning Outcomes:

Once completing this KU, students should be able to:

1. Discuss security issues related to outsourcing hardware, software development and integration.
2. List and explain common vulnerabilities in supply chain components.
3. Demonstrate mitigation methods to supply chain security issues and explain the challenges of these mitigation methods.

SCA

Systems Certification and Accreditation (SCA)

Sources:

- The CAE-CD Designation Program Guidance and Knowledge Units 2019.

Description:

This KU provides knowledge of analysis and evaluation for operational systems and the authorities and associated processes, regulations.

Topics:

The following topics must be included in this KU:

1. Components of the Certification and Accreditation Process
2. Roles and Players
3. Certification Boards and Panels
4. Case Study: US DoD Policies and Directives
5. Case Study: US NIST Risk Management Framework (SP800-37)

Learning Outcomes:

Once completing this KU, students should be able to:

1. Define certification and accreditation.
2. Illustrate the processes of system certification and accreditation.

SPG

Systems Programming (SPG)

Sources:

- The CAE-CD Designation Program Guidance and Knowledge Units 2019.

Description:

This KU provides knowledge, skills and ability to develop complex and low-level software systems.

Topics:

The following topics must be included in this KU:

1. Hardware and Software Interfaces and Interactions
2. Types of Systems Programs: Development Environments, Operating Systems, Utilities, Networking Functions, Device Drivers, Storage Frameworks and Gaming Engines
3. Layered Services Design
4. Application Programming Interfaces (API's)
5. Programming to Operating Systems Internal Interfaces
6. Low Level Programming: Assembly, C
7. Resource Optimization
8. Resource Management
9. Run Time Overhead Minimization
10. Direct Control of Memory Access and Flow Control
11. Managing Memory in Systems Software
12. Security Concerns in Systems Software
13. Monitoring and Logging Systems Software

Learning Outcomes:

Once completing this KU, students should be able to:

1. Develop programs that can correctly operate under limited resources.
2. Apply a layered approach for API's access.
3. Implement new functions in an OS kernel or device driver.
4. Implement systems functions without the use of external libraries.

SSE

Systems Security Engineering (SSE)

Sources:

- The CAE-CD Designation Program Guidance and Knowledge Units 2019.

Description:

This KU provides skills to participate in the development of large-scale secure systems using techniques, methods and issues throughout system life-cycle.

Topics:

The following topics must be included in this KU:

1. Testing Design
2. Testing methodologies
3. Emergent Properties
4. Systems Engineering
5. System Integration
6. Make or Buy Analysis
7. Systems Security Analysis
8. Enterprise System Components

Learning Outcomes:

Once completing this KU, students should be able to:

1. Analyze system components in a composed system.
2. Analyze given system design according to system security requirements.

VTT

Virtualization Technologies (VTT)

Sources:

- The CAE-CD Designation Program Guidance and Knowledge Units 2019.

Description:

This KU provides knowledge of modern host virtualization and its implementation, deployment, use, system components and security.

Topics:

The following topics must be included in this KU:

1. Virtualization Architectures
2. Virtualization Techniques for Code Execution
3. Memory Management in Virtual Environments
4. Networking in Virtual Environments
5. Storage in Virtual Environments
6. Scheduling of Virtual Machines
7. Migration and Snapshots
8. Virtual Management Layers
9. Digital Forensics in Virtual Environments

Learning Outcomes:

Once completing this KU, students should be able to:

1. Explain virtualization concepts.
2. Explain virtualization architectures and differentiate between them.
3. Design, Construct, implement and configure virtualization environments.

VLA

Vulnerability Analysis (VLA)

Sources:

- The CAE-CD Designation Program Guidance and Knowledge Units 2019.
- IEEE/ACM Cybersecurity Curricula 2017.

Description:

This KU provides knowledge and skills for system vulnerabilities detection and mitigation.

Topics:

The following topics must be included in this KU:

1. Vulnerability Definition
2. System Modeling Techniques
3. Vulnerability Mapping
4. Vulnerability Characteristics and Classification.
5. Taxonomy: Buffer Overflows, Privilege Escalation, Rootkits, Trojans, Backdoors, Viruses, Return Oriented Programming, Social Engineering Vulnerabilities and Administrative Privileges Effect on Vulnerabilities
6. Vulnerabilities Root Causes
7. Mitigation Strategies
8. Analyze Countermeasures
9. Disclosing Vulnerabilities
10. Vulnerabilities Detection Tools and Techniques

Learning Outcomes:

Once completing this KU, students should be able to:

1. Apply vulnerabilities detection tools and techniques.
2. Construct vulnerability map of a given system.
3. Trace vulnerabilities to identify their root causes.
4. Demonstrate countermeasures for vulnerabilities mitigation and analyze these countermeasures.
5. Discuss scenarios when vulnerabilities must be disclosed.

WAS

Web Application Security (WAS)

Sources:

- The CAE-CD Designation Program Guidance and Knowledge Units 2019.

Description:

This KU provides knowledge of technology, tools and practices related to web applications.

Topics:

The following topics must be included in this KU:

1. Web Application Technologies: HTTP Protocol, Encoding Schemes, Web Application Architectures, AJAX, XML and JSON
2. Server-Side Controls
3. Authentication
4. Session Management
5. Access Controls
6. Client-Side Controls
7. Input-Based Vulnerabilities: SQL Injection, Blind SQL Injection, Cross-Site Scripting and Cross-Site Request Forgery
8. Function-Specific Input Vulnerabilities
9. Attacking Application Logic
10. Recent Attack Trends
11. Shared Hosting Vulnerabilities
12. Application Server Vulnerabilities

Learning Outcomes:

Once completing this KU, students should be able to:

1. Demonstrate common web application technologies and explain security concerned related to them.
2. Develop and deploy secure web applications.
3. Illustrate web applications security principles.

WSA

Windows System Administration (WSA)

Sources:

- The CAE-CD Designation Program Guidance and Knowledge Units 2019.

Description:

This KU provides knowledge and skills to perform Microsoft Windows administration operations.

Topics:

The following topics must be included in this KU:

1. OS Installation
2. User accounts management: Access controls, Password Policies, Authentications Methods and Group Policies
3. Command Line Interfaces
4. Configuration Management
5. Updates and Patches
6. Event Logging and Auditing
7. Managing System Services
8. Virtualization
9. Backup and Restoring Data
10. File System Security
11. Network Configuration: Port Security
12. Host Intrusion Detection
13. Security Policy Development

Learning Outcomes:

Once completing this KU, students should be able to:

1. Install, configure, operate and maintain MS Windows OS in a secure way.
2. Setup user accounts and configure polices for authentication.
3. Design and implement audit configurations
4. Perform backups and successfully restoring them.
5. Demonstrate the importance of reviewing security logs and installing updates and patches periodically.

WSN

Wireless Sensor Networks (WSN)

Sources:

- The CAE-CD Designation Program Guidance and Knowledge Units 2019.

Description:

This KU provides knowledge of wireless sensor networks and related security concerns.

Topics:

The following topics must be included in this KU:

1. Managed vs. Ad-hoc Network Participation
2. Cross Layer Optimization
3. Network Architecture: Mesh, Structured and Hierarchical
4. MAC Approaches: Coordination and Self-organization
5. Routing Protocols
6. Membership Management: Authentication Hash Tables
7. Security Issues: Data Integrity, Data Poisoning and Resource Starvation
8. Encryption
9. Energy Efficiency: Power budget, Energy Optimization and Energy Harvesting
10. Radio Frequencies: RF Selection, RF Management and Interference

Learning Outcomes:

Once completing this KU, students should be able to:

1. Skitch, design and deploy a wireless sensor network according to given requirements.
2. Discuss wireless sensor networks challenges of coordination, synchronization, energy efficiency and self-organization.
3. Apply appropriate security measures for wireless sensor networks and analyze these measures
4. Perform wireless sensor network simulations for given scenarios.
5. Conduct real experiments for secure wireless sensor networks based on given setup.

DIA

Data Integrity and Authentication (DIA)

Sources:

- IEEE/ACM Cybersecurity Curricula 2017.

Description:

This KU provides knowledge of data integrity and authentication techniques.

Topics:

The following topics must be included in this KU:

1. Authentication Strength: Multi-Factor Authentication, Cryptographic Tokens, Cryptographic Devices, Biometric Authentication, One-Time Passwords and Knowledge-Based Authentication
2. Password Attack Techniques: Dictionary Attack, Brute Force Attack, Rainbow Table Attack, Phishing, Social Engineering, Malware-Based Attack, Spidering, Off-line Analysis and Password Cracking Tools.
3. Password Storage Techniques: Cryptographic Hash Functions, Collision Resistance, Salting, Iteration Count and Password-Based Key Derivation
4. Data integrity: Message Authentication Codes (HMAC, CBC-MAC), Digital Signatures, Authenticated Encryption and Hash Trees

Learning Outcomes:

Once completing this KU, students should be able to:

1. Differentiate between authentication, authorization, access control and data integrity.
2. Illustrate strengths and weaknesses of authentication techniques.
3. Demonstrate common attacks on passwords.

ISS

Information Storage Security (ISS)

Sources:

- IEEE/ACM Cybersecurity Curricula 2017.

Description:

This KU provides knowledge of information storage security techniques.

Topics:

The following topics must be included in this KU:

1. Disk and File Encryption: Hardware vs. Software Encryption
2. Data Erasure: Overwriting, Degaussing, Physical Destruction Methods and Memory Remanence
3. Data Masking: for Testing, for Obfuscation and for Privacy
4. Database Security: Access, Authentication, Auditing and Application Integration Paradigms

Learning Outcomes:

Once completing this KU, students should be able to:

1. Illustrate disk and file hardware and software encryption.
2. Describe data erasure techniques.
3. Explain data masking applications.
4. Discuss database access, authentication, auditing and application integration.

ACC

Access Control (ACC)

Sources:

- IEEE/ACM Cybersecurity Curricula 2017.

Description:

This KU provides knowledge of access control techniques.

Topics:

The following topics must be included in this KU:

1. Physical Data Security: Data Center Security, Keyed Access, Key Cards, Video Surveillance, Rack-Level Security and Data Destruction
2. Logical Data Access Control: Access Control Lists, Group Policies, Passwords, Discretionary Access Control (DAC), Mandatory Access Control (MAC), Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), Rule-Based Access Control (RAC), History-Based Access Control (HBAC), Identity-Based Access Control (IBAC), Organization-Based Access Control (OrBAC), Federated Identities and Access Control
3. Secure Architecture Design: Principles of a Security Architecture and Protection of Information in Computer Systems
4. Data Leak Prevention Techniques: Controlling Authorized Boundaries, Channels, Destinations and Methods of Data Sharing

Learning Outcomes:

Once completing this KU, students should be able to:

1. Explain access control list.
2. Differentiate between physical and logical access control.
3. Illustrate and compare authorization and authentication.

SCP

Secure Communication Protocols (SCP)

Sources:

- IEEE/ACM Cybersecurity Curricula 2017.

Description:

This KU provides knowledge of secure communication protocols.

Topics:

The following topics must be included in this KU:

1. Application and transport layer protocols: HTTP, HTTPS, SSH and SSL/TLS
2. Attacks on TLS: Downgrade Attacks, Certificate Forgery, Implications of Stolen Root Certificates and Certificate Transparency
3. Internet/Network Layer: IPsec and VPN
4. Privacy Preserving Protocols: Mixnet, Tor, Off-the-Record Message and Signal
5. Data Link Layer: L2TP, PPP and RADIUS

Learning Outcomes:

Once completing this KU, students should be able to:

1. Demonstrate and deploy HTTPS, SSH, SSL/TLS, IPsec, VPN, L2TP, PPP and RADIUS protocols.
2. Illustrate common attacks on TLS.

CPP

Component Procurement (CPP)

Sources:

- IEEE/ACM Cybersecurity Curricula 2017.

Description:

This KU provides knowledge ensuring components security is preserved during procurement processes.

Topics:

The following topics must be included in this KU:

1. Supply Chain Risks
2. Supply Chain Security
3. Supplier Vetting

Learning Outcomes:

Once completing this KU, students should be able to:

1. Describe hardware and software security threats and risks in component procurement.
2. Detect and prevent component security compromises.
3. Establish trusted components suppliers and transporters.

HAA

Hardware Architecture (HAA)

Sources:

- IEEE/ACM Cybersecurity Curricula 2017.

Description:

This KU provides introduction to the advantages of hardware architectures standards and potential vulnerabilities.

Topics:

The following topics must be included in this KU:

1. Standard Architectures
2. Hardware Interface Standards
3. Common Architectures

Learning Outcomes:

Once completing this KU, students should be able to:

1. Understand the idea of standard architectures and the advantages of standardization.
2. Describe various hardware interface standards starting with IC package design, through busses such as ISA and PCI for integration platforms and on to networking standards like IEEE 802.3.

DSA

Distributed Systems Architecture (DSA)

Sources:

- IEEE/ACM Cybersecurity Curricula 2017.

Description:

This KU provides knowledge of distributed systems and how they are connected.

Topics:

The following topics must be included in this KU:

1. Distributed Systems General Concepts
2. Example of Distributed Systems
3. Protocols and Layering
4. High Performance Computing
5. Hypervisors and Cloud Computing Implementation
6. Vulnerabilities and Example Exploits

Learning Outcomes:

Once completing this KU, students should be able to:

1. Describe the components and interfaces of a networking standard provided.
2. Explain a process in an operating system and introduce various architectures for running processes and enabling their communication.
3. Understand the 7-layer OSI model along with the 5-layer Internet model and the difference between them
4. Describe HPC and use cases that distinguish HPC from the standard Internet
5. Introduces the concepts of providing infrastructure as a service (IaaS), Software as a Service (SaaS), Platform as a Service (PaaS)
6. Examine the attack surfaces of the various distributed computing models emphasizing the fact that every interface introduces potential vulnerabilities.

SCC

System Control (SCC)

Sources:

- IEEE/ACM Cybersecurity Curricula 2017.

Description:

This KU provides knowledge of system control techniques including detecting, compensating for, defending against and preventing attacks.

Topics:

The following topics must be included in this KU:

1. Access control: Controlling Access to Resources and the Integrity of the Controls
2. Authorization Models: Management of Authorization across many Systems and the Distinction from Authentication
3. Intrusion Detection: Anomaly, Misuse [Rule-Based, Signature-Based] and Specification-Based Techniques.
4. Attacks: Trees and Graphs and Specific attacks
5. Defenses: ASLR, IP Hopping and Intrusion Tolerance
6. Audit: Logging, Log Analysis and Relationship to Intrusion Detection
7. Malware: Viruses, Worms and Ransomware
8. Vulnerabilities Models: RISOS and PA, CVE and CWE
9. Penetration Testing: Flaw Hypothesis Methodology, ISSAF, OSSTMM, GISTA, PTES
10. Forensics: System Requirements for Forensics
11. Recovery and Resilience: Availability Mechanisms

Learning Outcomes:

Once completing this KU, students should be able to:

1. Examines the security considerations involved in controlling the system itself.
2. Detect, compensate for, defend against and prevent attacks related to system control.

IMM

Identity Management (IMM)

Sources:

- IEEE/ACM Cybersecurity Curricula 2017.

Description:

This KU provides knowledge of identity management techniques.

Topics:

The following topics must be included in this KU:

1. Identification and Authentication: People and Devices, Network Access Control (NAC), Identity Access Management (IAM), Roles, Multi-Method Identification and Authentication Systems, Biometric Authentication Systems, Accuracy/FAR/FRR, Resistance, Privacy, Usability and tolerability of the methods
2. Physical and Logical Assets Control: System Hardware, Network Assets, Backup/Storage Devices, Rules-Based Access Control (RAC), Role based Access Control (RBAC), Inventory Tracking Methods, Identity Creation Methods
3. Identity as a Service (IaaS)
4. Third-Party Identity Services
5. Access Control Attacks and Mitigation Measures: Password, Dictionary, Brute Force and Spoofing Attacks, Multi-Factor Authentication, Strong Password Policy, Secure Password Files and Restrict Access to Systems

Learning Outcomes:

Once completing this KU, students should be able to:

1. Differentiate between identification, authentication and access authorization.
2. Discuss the audit trails and logging importance in identification and authentication.
3. Apply least privilege and segregation of duties concepts.
4. Explain access control attacks and discuss mitigation measures.

AUU

Awareness and Understanding (AUU)

Sources:

- IEEE/ACM Cybersecurity Curricula 2017.

Description:

This KU provides knowledge of risk, cyber hygiene, user education and vulnerabilities and threat awareness.

Topics:

The following topics must be included in this KU:

1. Risk Perception and Communication
2. Cyber Hygiene
3. Cybersecurity User Education
4. Cyber Vulnerabilities and Threat Awareness

Learning Outcomes:

Once completing this KU, students should be able to:

1. Illustrate cyber hygiene, cybersecurity user education and cyber vulnerabilities and threat awareness.
2. Demonstrate Security Education, Training and Awareness (SETA) programs.
3. Discuss SETA countermeasures importance.
4. Explain risk perception and communication in cybersecurity and privacy.

ATT

Analytical Tools (ATT)

Sources:

- IEEE/ACM Cybersecurity Curricula 2017.

Description:

This KU provides knowledge, skills and ability to recognize, monitor, block, divert and respond to cyberattacks.

Topics:

The following topics must be included in this KU:

1. Performance Measurements
2. Data Analytics
3. Security Intelligence

Learning Outcomes:

Once completing this KU, students should be able to:

1. Design, implement and manage the use of specific measurements to determine the effectiveness of the overall security program
2. Use approaches and techniques to define and evaluate the utility of performance measurements
3. Use techniques to manipulate large volumes of data to recognize, block, divert and respond to cyberattacks
4. Collection, analysis and dissemination of security information including but not limited to threats and adversary capabilities

BDR

Business Continuity, Disaster Recovery and Incident Management (BDR)

Sources:

- IEEE/ACM Cybersecurity Curricula 2017.

Description:

This KU provides knowledge of business continuity, disaster recovery and incident management techniques.

Topics:

The following topics must be included in this KU:

1. Incident Response: Anticipate, Detect and Mitigate
2. Disaster Recovery: DR Plans
3. Business Continuity: Contingency Planning, Incident Response, Emergency Response, Backup and Recovery

Learning Outcomes:

Once completing this KU, students should be able to:

1. Explain what resilience is and identify an environment in which it is important.
2. Discuss the basics of a disaster recovery plan and business continuity plan.
3. Write case-based or actual plans for disaster recovery and business continuity.
4. Explain why backups pose a potential security risk.