



Combining Your Curriculum with Cyberbit Learning Content

Create workforce ready graduates who can contribute from day one.

Introduction

Employers are in dire need of cyber talent. With over 500,000 open cyber positions in the US alone. However, only 27% of cybersecurity leaders agree that university graduates are well-prepared¹. While academic degree graduates are generally armed with the required knowledge, they often lack the hands-on skills and practical experience to be productive from day one, requiring months of additional training. As a result, most employers see hands-on training as more important than a university degree when evaluating new candidates².

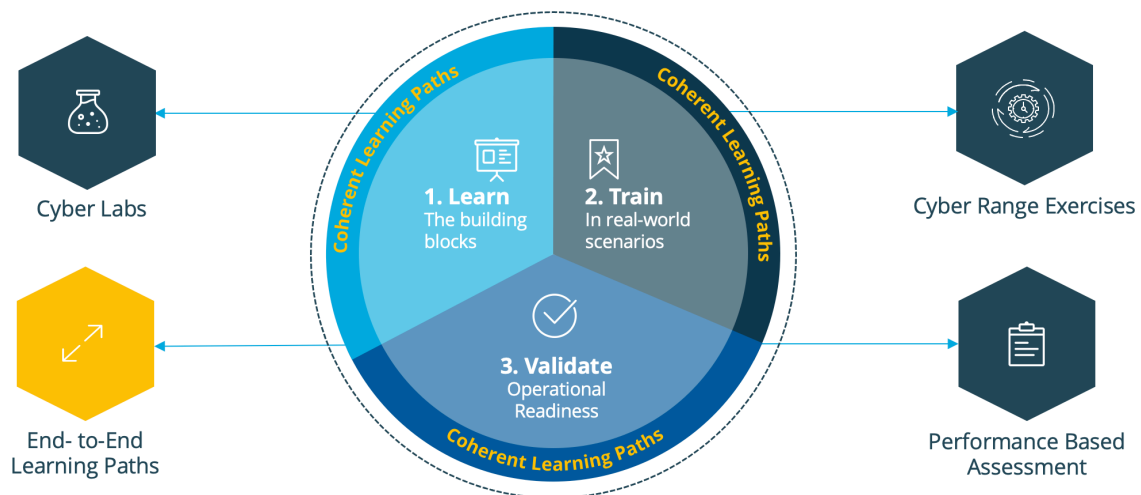
It is imperative that higher education institutions produce workforce-ready graduates who can contribute to the cyber workforce of an organization, successfully defending their digital assets and information.. Cyberbit's hands-on learning content is designed to integrate with your academic curriculum, allowing your graduates to develop their technical skills and experience while enrolled in your program. As a result, they become infinitely more valuable to their future employers.

Cover the Entire Skills Development Lifecycle

Cyberbit is the only cyber skills development platform that provides all four elements of an effective skills building program:

- Build Foundational Knowledge & Skills with Cyber Labs
- Apply Cybersecurity Skills Against Live-Fire Attack Scenarios
- Automated Assessment and Feedback

Cybersecurity training should have all elements to build skills that last for a lifetime, transforming students into cybersecurity pros who can contribute to the workforce from day one.

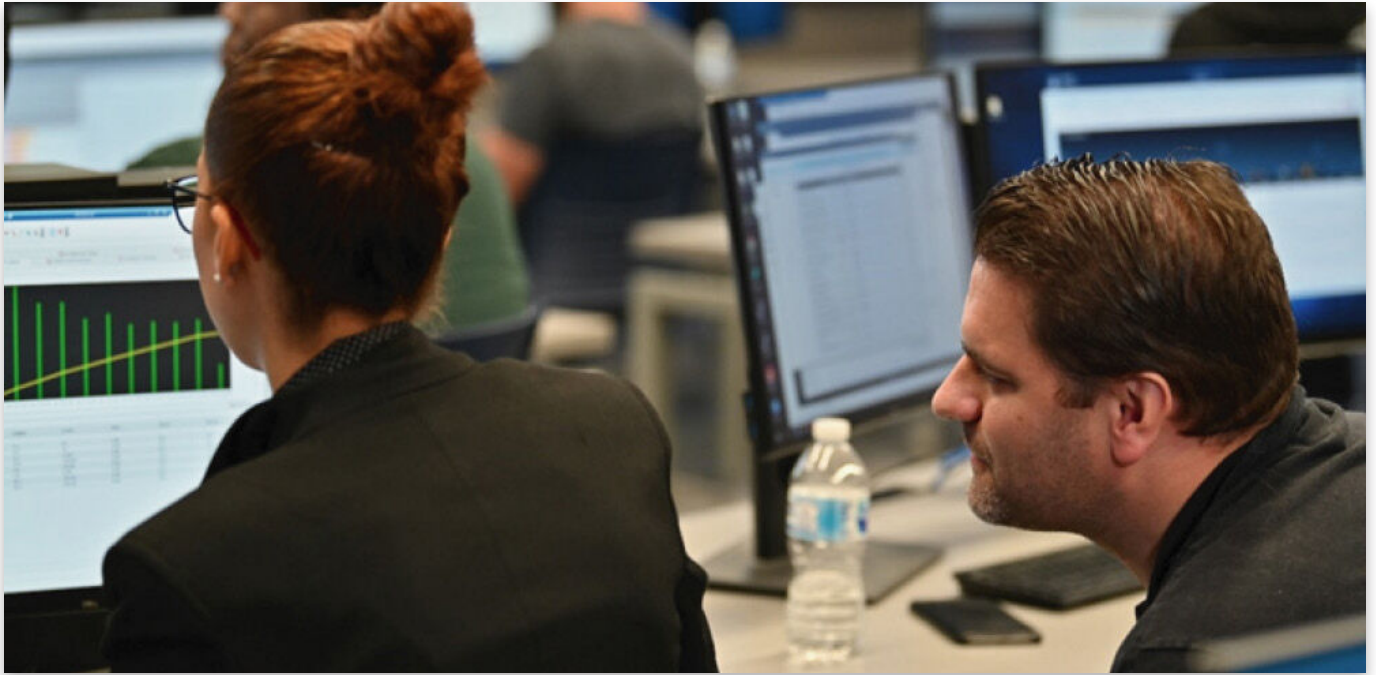


¹ISACA State of Cybersecurity 2020 Survey

²ISACA State of Cybersecurity 2020 Survey

Competency Based Training Breeds Best-In-Class Professionals

What does it take to build a skill? Focus. Cyberbit empowers students to focus on the skills required for them to succeed as a member of the workforce, in conjunction with your curriculum and the integrated NICE Cybersecurity Framework. For example, when your student endeavors to be a Forensic Analyst following graduation, they must have the skills to succeed in forensic analysis. Using the both the cyber labs and cyber range included within Cyberbit, your student will be assigned a custom learning path to ensure they build forensic analysis skills as well as relevant experience in a live incident to ensure they know how to perform as a forensic analyst in the workplace. As a result, students who have had Cyberbit integrated into their curriculums are higher quality job candidates who require a shorter onboarding and are promoted more quickly upon entry to the workforce.



Students participate in a live-fire cyber range exercise at Miami Dade College

We Map Your Curriculum to Our Content

Upon your decision to integrate Cyberbit into your students' learning experience, an educational expert immediately begins to work with you to integrate the right content from the platform into your curriculum. Assignments are created for students including a diverse selection of cyber labs and cyber range exercises to ensure the development of both practical skills and applicable experience aligned to the specific goals of individual courses.



Based on the cybersecurity curriculum at University of Maine at Augusta

Cyberbit Meet's the Needs of Your Students

Learning on Cyberbit is adaptive, creating a more effective and time efficient learning experience for your students. Learning paths can be customized to meet the needs of a specific student anytime, included as part of the teacher's toolset. Creating an adaptive learning experience is proven to improve your students ability to learn and recall information by as much as 0.67SD according to a 2020 study published by the University of Virginia. Additionally, working with Cyberbit allows you to create a more flexible and effective experience including:

- Distributed Learning:** Space your learning sessions out over time versus single learning events or multi-hour or even multi-day study sessions.
- Optimized Learning Timing:** Humans forget information at a predictable rate. Using Cyberbit, you can time the intervals between learning sessions, allowing for maximum knowledge and skills retention based on the performance of your students.
- Retrieval Practice:** Using Cyberbit you can measure a student based on performance and their ability to retrieve information in a practical setting rather than asking them to regurgitate information in a standard testing format which does not account for the real-world environment.

Cyberbit understands that knowledge, complemented with real world experience, is vital to the retention of critical information. To become a master of the cyber domain, your students must have the ability to rapidly recall information in critical moments. Information recall is easy if you learned about a topic recently, but unless you build long lasting knowledge retention, this knowledge will quickly fade, becoming unavailable when needed. Learning on Cyberbit is proven to reduce the chances knowledge will be forgotten by creating muscle-memory level response alongside long-lasting knowledge and practical skill application.

Sample Mapping to Curriculum and Certification

All examples listed below are based on work Cyberbit has completed based on the curriculum of University of Maine at Augusta, just one of the many educational institutions integrating Cyberbit into their curriculum.

Bachelor's Degree in Cybersecurity

Required Courses:

- CIS 101 Introduction to Computer Science
- CIS 110 Programming Fundamentals
- CIS 120 Introduction to Data Structures
- CIS 221 Linux
- CIS 240 Networking Concepts
- CIS 440 Network Security
- CIS 460 Computers & Culture
- ISS 210 Introduction to Information Security
- ISS 232 Introduction to Cyber Forensics
- ISS 240 Security Policy and Governance
- ISS 340 Computer Security
- ISS 350 Databases and Database Security
- ISS 380 Cybersecurity Internship
- ISS 410 Cybersecurity I
- ISS 470 Information Security Management

Integrated Cyberbit Learning Path:

NICE Work Roles: Cyber Defense Analyst, Cyber Defense Incident Responder, Cyber Defense Forensics Analyst

Name	Learning Content Type	Duration (Hours)	Level of Difficulty
Basic CMD Network Commands	Lab	0:45	Easy
Basic Filters in Wireshark	Lab	1:00	Easy
Secure Socket Shell Pro-tocol	Lab	0:40	Easy
HTTP and HTTPS Proto-cols	Lab	0:45	Easy
Firewalls – Vulnerability Scanning	Lab	0:60	Easy
Network Protocol Analysis	Lab	2:00	Easy
Working with Linux Commands	Lab	0:50	Easy
Linux File Ownership & Permissions	Lab	0:40	Easy
Shadow Copies	Lab	0:40	Easy
Evasion Using Hidden Files and Directories	Lab	0:40	Easy
Sysinternals Process Explorer	Lab	0:40	Easy
Identify Files Using File Explorer	Lab	0:40	Easy
Malware Persistence with Scheduled Task	Lab	1:00	Easy
RDP Cache Investigation	Lab	1:10	Easy
Win Screenshot	Lab	2:00	Easy
SIEM Exercise - SQLi	Lab	2:00	Easy
MySQL Forensics	Lab	1:00	Medium
Exploiting SQLi	Lab	0:50	Easy
Cross the Site - XSS	Lab	0:50	Easy
Coin-Miner	Live Fire Exercise	3:00	Medium
Apache Shutdown	Live Fire Exercise	2:30	Medium

Focus Area: Cybersecurity Analyst

Required Courses:

- ISS 282 Cyber Operations
- ISS 320 Security Monitoring
- ISS 360 Incident Response
- ISS 370 Cyberwarfare and Cyberterrorism
- ISS 385 Malware Analysis
- ISS 412 Cybersecurity II
- ISS 438 Cyber Investigations

Integrated Cyberbit Learning Path:

NICE Work Roles: Cyber Defense Analyst, Cyber Defense Incident Responder

Name	Learning Content Type	Duration (Hours)	Level of Difficulty
Threat Hunting - Investigating Sysmon Events	Lab	2:00	Easy
Threat Hunting - Investigating Security Events	Lab	0:50	Easy
Threat Hunting - Data Leakage	Lab	0:50	Easy
Threat Intelligence - Keylogger	Lab	0:50	Easy
Threat Intelligence - Find the Worm	Lab	1:30	Easy
Analysis with EDR - TrickBot	Lab	1:00	Medium
Analysis with EDR - Fileless attack	Lab	0:50	Medium
Analysis with EDR - Lateral movement	Lab	0:50	Medium
Analysis with EDR - Turla	Lab	1:10	Medium
SIEM Exercise - SMB Thief	Lab	2:00	Easy
Security Scans via OWASP ZAP	Lab	0:35	Medium
OWASP - Sensitive Data Exposure	Lab	0:50	Medium
OWASP - Broken Access Control	Lab	0:60	Medium
OWASP - Broken authentication	Lab	0:60	Medium
OWASP - Security Misconfiguration	Lab	0:60	Medium
Domain Keylogger	Live Fire Exercise	3:30	Medium
Killer Trojan	Live Fire Exercise	3:30	Medium

Focus Area: Cyber Forensics

Required Courses:

- ISS 332 System Forensics I
- ISS 334 Cyberlaw
- ISS 360 Incident Response
- ISS 432 Systems Forensics II
- ISS 434 Mobile Forensics
- ISS 436 Digital Evidence Analysis
- ISS 438 Cyber Investigations

Integrated Cyberbit Learning Path:

NICE Work Roles: Cyber Defense Analyst, Cyber Defense Forensics Analyst

Name	Learning Content Type	Duration (Hours)	Level of Difficulty
DNS Enumeration	Lab	0:40	Easy
ARP Analysis	Lab	0:50	Easy
Firewalls – Analyzing Internet Relay Chat (IRC)	Lab	0:60	Easy
SMB Protocol	Lab	0:75	Medium
Linux Malware Persistence With Cronjobs	Lab	0:40	Easy
Linux Process Exploration	Lab	0:50	Easy
Gold in Trash - Forensics of Recycle Bin	Lab	0:30	Medium
Macro File Investigation	Lab	0:45	Medium
Compressed Data	Lab	0:50	Medium
Windows Registry Forensics	Lab	0:50	Medium
Practicing with Cyber-Chef	Lab	0:50	Medium
Filtering with REGEX	Lab	1:00	Medium
Reverse Engineering of MBR Malware	Lab	1:00	Medium
Autoruns Persistence Investigation	Lab	1:00	Medium
ZeroLogon	Lab	1:00	Medium
Memory Dump Investigation	Lab	1:15	Hard
Share-Lock Ransomware	Live Fire Exercise	4:00	Hard
WMI Worm	Live Fire Exercise	4:30	Hard

Masters Degree in Cybersecurity

Required Courses:

- CYB 501 Cybersecurity Fundamentals
- CYB 515 Research Methods
- CYB 530 Project Management in Cybersecurity
- CYB 551 Cyber Laws, Policies, and Ethics
- CYB 576 Network Security Management
- CYB 582 Cybersecurity Investigations
- CYB 583 Database and Application Security
- CYB 584 Cybersecurity Operations
- CYB 591 Capstone Project Proposal
- CYB 592 Capstone Project Presentation
- CYB 698 Thesis Research

Integrated Cyberbit Learning Path:

NICE Work Roles: Cyber Operator, Vulnerability Assessment Analyst, Exploitation Analyst

Name	Learning Content Type	Duration (Hours)	Level of Difficulty
Firewalls - Vulnerability Scanning	Lab	1:00	Easy
Network Protocol Analysis	Lab	2:00	Easy
Threat Hunting - Investigating Sysmon Events	Lab	2:00	Easy
Threat Hunting - Investigating Security Events	Lab	0:50	Easy
Threat Hunting - Data Leakage	Lab	0:50	Easy
Threat Intelligence - Keylogger	Lab	0:50	Easy
Threat Intelligence - Find the Worm	Lab	1:30	Easy
Threat Intelligence - PCAP investigation	Lab	1:30	Easy
Analysis with EDR - Fileless attack	Lab	0:50	Medium
Analysis with EDR - Lateral movement	Lab	0:50	Medium
Analysis with EDR - Kovter	Lab	1:00	Medium
Analysis with EDR - TrickBot	Lab	1:00	Medium
Analysis with EDR - Turla	Lab	1:10	Medium
Win Screenshot	Lab	2:00	Easy
SIEM Exercise - SQLi	Lab	2:00	Easy
SIEM Exercise - SMB Thief	Lab	2:00	Easy
MySQL Forensics	Lab	1:00	Medium
Security Scans via OWASP ZAP	Lab	0:35	Medium
OWASP - Sensitive Data Exposure	Lab	0:50	Medium
OWASP - Broken Access Control	Lab	1:00	Medium
OWASP - Broken Authentication	Lab	1:00	Medium
OWASP - Security Misconfiguration	Lab	1:00	Medium
Apache Shutdown	Live Fire Exercise	3:30	Medium
Share-Lock Ransomware	Live Fire Exercise	4:00	Hard
Trojan Share Privilege Escalation	Live Fire Exercise	4:00	Hard
WMI Worm	Live Fire Exercise	4:30	Hard

Graduate Certificate in Cybersecurity

Required Courses:

- CYB 501 Cybersecurity Fundamentals
- CYB 530 Project Management in Cybersecurity
- CYB 551 Cyber Laws, Policies, and Ethics
- CYB 576 Network Security Management
- CYB 582 Cybersecurity Investigations
- CYB 583 Database and Application Security
- CYB 584 Cybersecurity Operations

Integrated Cyberbit Learning Path:

NICE Work Roles: Cyber Defense Infrastructure Support Specialist, Cyber Defense Analyst, Cyber Operator

Name	Learning Content Type	Duration (Hours)	Level of Difficulty
Firewalls – Analyzing Internet Relay Chat (IRC)	Lab	1:00	Easy
Firewalls - Vulnerability Scanning	Lab	1:00	Easy
Network Protocol Analysis	Lab	2:00	Easy
MySQL Forensics	Lab	1:00	Medium
OWASP - Broken Access Control	Lab	1:00	Medium
OWASP - Broken Authentication	Lab	1:00	Medium
OWASP - Security Misconfiguration	Lab	1:00	Medium
OWASP - Sensitive Data Exposure	Lab	0:50	Medium
Security Scans via OWASP ZAP	Lab	0:35	Medium
Apache Shutdown	Live Fire Exercise	3:30	Medium
SQLi Domain Hijacking	Live Fire Exercise	3:00	Medium

Certificate in Cyber Forensics

Required Courses:

- ISS 232 Introduction to Cyber Forensics
- ISS 332 System Forensics I
- ISS 334 Cyberlaw
- ISS 432 System Forensics II
- ISS 434 Mobile Forensics
- ISS 436 Digital Evidence Analysis

Integrated Cyberbit Learning Path:

NICE Work Roles: Cyber Defense Analyst, Cyber Defense Incident Responder, Cyber Defense Forensics Analyst

Name	Learning Content Type	Duration (Hours)	Level of Difficulty
Malware Persistence with Scheduled Task	Lab	1:00	Easy
Practice PEiD tool	Lab	0:40	Easy
Shadow Copies	Lab	0:40	Easy
Evasion Using Hidden Files and Directories	Lab	0:40	Easy
Sysinternals Process Explorer	Lab	0:40	Easy
Identify Files Using File Explorer	Lab	0:40	Easy
RDP Cache Investigation	Lab	1:10	Easy
Compressed Data	Lab	0:50	Medium
Autoruns Persistence Investigation	Lab	1:00	Medium
Macro File Investigation	Lab	0:45	Medium
Windows Registry Forensics	Lab	0:50	Medium
Gold in Trash - Forensics of Recycle Bin	Lab	0:30	Medium
Practicing with Cyber-Chef	Lab	0:50	Medium
Memory Dump Investigation	Lab	1:15	Hard
WMI Worm	Live Fire Exercise	4:30	Hard
Fileless Techniques	Live Fire Exercise	4:00	Hard

Certificate in Cyber Security

Required Courses:

- CIS 101 Introduction to Computer Science
- CIS 110 Programming Fundamentals
- CIS 240 Networking Concepts
- ISS 210 Introduction to Information Systems Security
- ISS 220 Security Risk Management
- ISS 340 Computer Security
- ISS 410 Cybersecurity I
- ISS 470 Information Systems Security Management

Integrated Cyberbit Learning Path:

NICE Work Roles: Cyber Defense Analyst, Cyber Defense Incident Responder, Cyber Defense Forensics Analyst

Name	Learning Content Type	Duration (Hours)	Level of Difficulty
Network Protocol Analysis	Lab	2:00	Easy
Secure Socket Shell Protocol	Lab	0:40	Easy
Threat Hunting - Investigating Sysmon Events	Lab	2:00	Easy
Threat Hunting - Investigating Security Events	Lab	0:50	Easy
Threat Intelligence - Find the Worm	Lab	1:30	Easy
Threat Intelligence - Keylogger	Lab	0:50	Easy
Reverse Engineering of MBR Malware	Lab	1:00	Medium
SMB Protocol	Lab	1:15	Medium
Ransomware DIY	Lab	1:00	Medium
Ms.GPO	Live Fire Exercise	2:00	Easy
Share-Lock Ransomware	Live Fire Exercise	4:00	Hard

Post Baccalaureate Courses

Required Courses:

- CIS 101 Introduction to Computer Science
- CIS 110 Programming Fundamentals
- CIS 120 Introduction to Data Structures
- CIS 240 Networking Concepts
- CIS 221 Linux
- CIS 440 Network Security
- CIS 460 Computers & Culture
- ISS 210 Introduction to Information Security
- ISS 232 Introduction to Cyber Forensics
- ISS 240 Security Policy and Governance
- ISS 340 Computer Security
- ISS 350 Databases and Database Security
- ISS 380 Cybersecurity Internship
- ISS 410 Cybersecurity I
- ISS 412 Cybersecurity II
- ISS 470 Information Security Management

Integrated Cyberbit Learning Path:

NICE Work Roles: Cyber Defense Analyst, Cyber Defense Incident Responder, Cyber Defense Forensics Analyst

Name	Learning Content Type	Duration (Hours)	Level of Difficulty
Basic CMD Network Commands	Lab	0:45	Easy
Basic filters in Wireshark	Lab	1:00	Easy
Secure Socket Shell Protocol	Lab	0:40	Easy
HTTP and HTTPS Protocols	Lab	0:45	Easy
Firewalls - Vulnerability Scanning	Lab	1:00	Easy
Network Protocol Analysis	Lab	2:00	Easy
Working with Linux Commands	Lab	0:50	Easy
Linux File Ownership & Permissions	Lab	0:40	Easy
Shadow Copies	Lab	0:40	Easy
Evasion Using Hidden Files and Directories	Lab	0:40	Easy
Sysinternals Process Explorer	Lab	0:40	Easy
Identify Files Using File Explorer	Lab	0:40	Easy
Malware Persistence with Scheduled Task	Lab	1:00	Easy
RDP Cache Investigation	Lab	1:10	Easy
Win Screenshot	Lab	2:00	Easy
SIEM Exercise - SQLi	Lab	2:00	Easy
MySQL Forensics	Lab	1:00	Medium
Exploiting SQLi	Lab	0:50	Easy
Cross the Site - XSS	Lab	0:50	Easy
Coin-Miner	Live Fire Exercise	3:00	Medium
Apache Shutdown	Live Fire Exercise	3:30	Medium

ABOUT CYBERBIT™

Cyberbit is the market-leading provider of cyber skill development platforms. Cyberbit addresses one of the most acute cybersecurity challenges: preparing cybersecurity teams for attacks. The Cyberbit platform delivers a "Zero to Hero" skilling, training, and assessment solution on-demand dramatically increasing

security team performance, improving teamwork, and improving evaluation, hiring, and certification processes. Customers include leading Fortune 500 companies, MSSPs, system integrators, academies and governments in 5 continents. Cyberbit is headquartered in Israel with offices in the US, Europe, and Asia.