Bachelor of Professional Studies in Applied Cybersecurity (BACS) Curriculum Map

This curriculum map is a guide to help you plan your studies in the 120-credit BACS program at Montgomery College (70 credits) and the SANS Technology Institute (50 credits).

Montgomery College Suggested Course Sequence		**Credits**
First Semester (15 credits)		
ENGL 101	Introduction to College Writing	3
MATF xxx	Mathematics foundation	3
NWIT 127	Microcomputer Essentials	3
NWIT 151	Introduction to Networking	3
BSSD xxx	Behavioral and social sciences distribution	3
Second Semester (16 credits)		
ENGF 103	English foundation (Business Writing for SANS.edu requirement)	3
CMSC 135	Introduction to Scripting	3
CMSC 253	UNIX/LINUX System Administration	4
NWIT 173	Network Security	3
NWIT 252	Cisco Networking 2	3
Third Semester (16 credits)		
PHIL 140	Introduction to the Study of Ethics	3
NWIT 245	Defending the Network	3
NWIT 263	Introduction to Digital Forensics	3
ARTD/HUMD xxx	Arts or humanities	3
NSLD xxx	Natural sciences with lab	4
Fourth Semester (13 credits)		
NWIT 230	Intro to Cyber Ops	3
NWIT 246	Attacker Tools and Techniques	3
NWIT 247	Introduction to Incident Response	3
NWIT 275	Wireless Security	3
NWIT 291	Cybersecurity Capstone	1
Total		**60**
*In addition to the 60 credits (listed above) required for an associate degree, students in the BACS program complete 10 additional general education credits at Montgomery College, for a **total of 70 credits earned at Montgomery College**.*		

SANS.edu Suggested Course Sequence			
Junior Year			
8-week term	BACS 3201	Security Foundations	6
8-week term	BACS 3301	Introduction to Cybersecurity (GSIF)	4
	BACS 3402	Effective Cyber Writing and Speaking	3
8-week term	BACS 3401	Security Essentials (GSEC)	6
8-week term	BACS 3504	Incident Handling and Hacker Exploits (GCIH)	6
Senior Year			
8-week term	BACS 3573	Automating Information Security with Python (GPYC)	4
	ACS 4xxx	Upper Division Specialization Elective (GIAC certification)	3
8-week term	BACS 4503	Intrusion Detection In-Depth (GCIA)	6
8-week term	ACS 4xxx	Upper Division Specialization Elective (GIAC certification)	3
8-week term	ACS 4xxx	Upper Division Specialization Elective (GIAC certification)	3
20-week term alongside last two elective course terms	BACS 4499	Internship	6

Upper Division Specialization Elective Options (choose 3)

Cyber Defense

- ACS 4487: Open-Source Intelligence (OSINT) Gathering and Analysis (GOSI)
- ACS 4501: Advanced Security Essentials (GCED)
- ACS 4505: Securing Windows and PowerShell Automation (GCWN)
- ACS 4511: Continuous Monitoring and Security Operations (GMON)

Penetration Testing

- ACS 4460: Enterprise and Cloud | Threat Vulnerability Assessment (GEVA)
- ACS 4542: Web App Penetration Testing and Ethical Hacking (GWAPT)
- ACS 4560: Network Penetration Testing and Ethical Hacking (GPEN)
- ACS 4575: Mobile Device Security and Ethical Hacking (GMOB)

Security Management

- ACS 4566: Implementing and Auditing the Critical Security Controls In-Depth (GCCC)

Digital Forensics and Incident Response

- ACS 4498: Battlefield Forensics & Data Acquisition (GBFA)
- ACS 4500: Windows Forensic Analysis (GCFE)
- ACS 4508: Advanced Incident Response, Threat Hunting, and Digital Forensics (GCFA)

Cloud Security

- ACS 4522: Defending Web Applications Security Essentials (GWEB)
- ACS 4540: Cloud Security and DevOps Automation (GCSA)

Industrial Control Systems Security

- ACS 4410: ICS/SCADA Security Essentials (GICSP)