Bachelor’s Degrees in Applied Cybersecurity
Curriculum Guide
Current as of May 2021

This curriculum guide was designed to help you plan your studies in the 120-credit bachelor’s degree programs. To earn a SANS.edu bachelor’s degree, you’ll need to complete 70 credit hours at a community college and/or 4-year institution, plus 50 credit hours at SANS.edu.

Bachelor of Science (BS) in Applied Cybersecurity

Start at a Community College or 4-Year College
Earn 70 credits from any accredited institution(s), which include 31 credits that meet the Maryland General Education Requirements (below).
You can begin at SANS.edu once you’ve earned 60 of the 70 required credits.

Complete 50 credits at SANS.edu
• 10 courses
• 9 GIAC certifications
• Internship
See reverse for details.

Earn a Bachelor of Science in Applied Cybersecurity from SANS.edu

Bachelor of Professional Studies (BPS) in Applied Cybersecurity

Start at a Community College
Earn 70 credits, which must include an AAS degree and 31 credits from any accredited institution(s) that meet the Maryland General Education Requirements (below).
You can begin at SANS.edu after you’ve earned your AAS degree and completed 60 of the 70 required credits.

Complete 50 credits at SANS.edu
• 10 courses
• 9 GIAC certifications
• Internship
See reverse for details.

Earn a Bachelor of Professional Studies in Applied Cybersecurity from SANS.edu

GENERAL EDUCATION REQUIREMENTS
A total of 70 credits from outside of SANS.edu are required to be brought into your bachelor’s degree.
While specific “major” courses are not required, 31 of the 70 transferable credits must meet the Maryland General Education Requirements.

- Arts and Humanities 3
- English Composition 3
- Social and Behavioral Sciences 3
- Mathematics 3
- Biological and Physical Sciences 3
- Additional General Education Electives 16

TOTAL GENERAL EDUCATION CREDITS 31
Bachelor's Degrees in Applied Cybersecurity  
Curriculum Guide

SANS.edu Suggested Course Sequence

<table>
<thead>
<tr>
<th>Junior Year</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>8-week term BACS 3275 Security Foundations</td>
<td>6</td>
</tr>
<tr>
<td>8-week term BACS 3301 Introduction to Cybersecurity</td>
<td>4</td>
</tr>
<tr>
<td>BACS 3402 Effective Cyber Writing and Speaking</td>
<td>3</td>
</tr>
<tr>
<td>8-week term BACS 3401 Security Essentials</td>
<td>6</td>
</tr>
<tr>
<td>8-week term BACS 3504 Incident Handling and Hacker Exploits</td>
<td>6</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Senior Year</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>8-week term BACS 3573 Automating Information Security with Python</td>
<td>4</td>
</tr>
<tr>
<td>ACS 4xxx Upper Division Specialization Elective</td>
<td>3</td>
</tr>
<tr>
<td>8-week term BACS 4503 Intrusion Detection In-Depth</td>
<td>6</td>
</tr>
<tr>
<td>8-week term ACS 4xxx Upper Division Specialization Elective</td>
<td>3</td>
</tr>
<tr>
<td>8-week term ACS 4xxx Upper Division Specialization Elective</td>
<td>3</td>
</tr>
<tr>
<td>20-week term BACS 4499 Internet Storm Center Internship</td>
<td>6</td>
</tr>
</tbody>
</table>

TOTAL SANS.EDU CREDITS 50

Upper Division Specialization Elective Options (choose 3)

**Cyber Defense**
- ACS 4487: Open-Source Intelligence (OSINT) Gathering and Analysis | SEC 487 + GOSI
- ACS 4501: Advanced Security Essentials | SEC 501 + GCED
- ACS 4505: Securing Windows and PowerShell Automation | SEC 505 + GCWN
- ACS 4511: Continuous Monitoring and Security Operations | SEC 511 + GMON

**Penetration Testing**
- ACS 4460: Enterprise and Cloud Threat Vulnerability Assessment | SEC 460 + GEVA
- ACS 4542: Web App Penetration Testing and Ethical Hacking | SEC 542 + GWAPT
- ACS 4560: Network Penetration Testing and Ethical Hacking | SEC 560 + GPEN
- ACS 4575: Mobile Device Security and Ethical Hacking | SEC 575 + GMOB

**Security Management**
- ACS 4566: Implementing and Auditing the Critical Security Controls In-Depth | SEC 566 + GCCC

**Digital Forensics and Incident Response**
- ACS 4498: Battlefield Forensics & Data Acquisition | FOR 498 + GBFA
- ACS 4500: Windows Forensic Analysis | FOR 500 + GCFE
- ACS 4508: Advanced Incident Response, Threat Hunting, and Digital Forensics | FOR 508 + GCFA

**Cloud Security**
- ACS 4488: Cloud Security Essentials | SEC 488 + GCLD
- ACS 4588: Cloud Penetration Testing | SEC 588 + GCPN
- ACS 4510: Public Cloud Security: AWS, Azure, and GCP | SEC 510 + GPCS
- ACS 4522: Defending Web Applications Security Essentials | SEC 522 + GWEB
- ACS 4540: Cloud Security and DevOps Automation | SEC 540 + GCSA

**Industrial Control Systems Security**
- ACS 4410: ICS/SCADA Security Essentials | ISC 410 + GICSP

SANS.edu/bacs   p2