ACRONYMS

ACL - Access Control Lists
AES - Advanced Encrytion Standard
ASI - Authorized Service Interruption
BGP - Border Gateway Protocol
CIA - Confidentiality, Integrity, Availability
COOP - Continuity of Operations Plan
DLP - Data Loss Prevention
DNS - Domain Name Server
HBSS - Host Based Security System
IAM - Identity Access Management
IDS - Intrusion Detection System
IPS - Intrusion Prevention System
JSON - JavaScript Object Notation
LDAP - Lightweight Directory Access Protocol
LUA - Lightweight Programming Language
NICE - National Initiative for Cybersecurity Education
NIST - National Institute of Standards and Technology
OSI - Open Systems Interconnection
PCAP - file format for Packet Capture
PCI - Payment Card Industry
PHI - Protected Health Information
PI - Proprietary Information
PKI - Public Key Infrastructure
PMI - Preventive Maintenance Interruption
POAM - Plan of Actions & Milestones
RADIUS - Remote Authentication Dial-In Service
RFI - Request for Information
RMA - Risk Management Assessment
RMF - Risk Management Framework
SEIM - Security Event and Incident Management
SQL - Structured Query Language
STIG - Service Technical Implementation Guide
TACAS - Terminal Access Controller Access System
TCP - Transmission Control Protocol
VLAN - Virtual Local Area Network
VPN - Virtual Private Network
WPA - WiFi Protected Access

DACUM Panel

Dr. Gregory Braxton, Newport News Shipbuilding

Kane Crisler, Packet Forensics

Joshua Cox, Towne Bank

Eric Hacecky, Thomas Jefferson National Accelerator Facility

Colleen Lammers, Booz Allen Hamilton

Jim Newman, Peregrine

Richard Severinghaus, CRTN Solutions, LLC

Stephen Watkins, G2 Ops, Inc.

Major Dennis A. Adezas, Joint Forces Staff College

Jenniffer Romero, CISSP, AERMOR, LLC

DACUM Facilitator

Jennifer Stevens, Chief Operating Officer
Virginia Advanced Study Strategies

Developed under a grant provided by the National Institute of Standards and Technology's National Initiative for Cybersecurity Education.

DACUM Research Chart

Cybersecurity Analyst

Old Dominion University
IDEA FUSION

HR CYBER

Virginia Space Grant Consortium

Produced by:

virginia advanced study strategies

324 Factory Street
South Boston VA 24592
jenniferstevens@vaadvstudies.org
434.575.0692

DACUM Job Analysis Research Chart for **Cybersecurity Analyst**

---- *Duties* ----	---------- *Tasks* ----------										
A Assess Cyber Risks	A.01 Identify info system assets	A.02 Identify security vulnerabilities	A.03 Identify attack vectors	A.04 Quantify business value of assets	A.05 Brief stakeholders *	A.06 Review policies and procedures	A.07 Test response processes	A.08 Create virtual test environments			
B Protect Information Assets	B.01 Create protection plan	B.02 Create contingency plan	B.03 Create disaster recovery plan	B.04 Provision user accounts	B.05 Implement access controls (i.e. black lists, white lists, geofence)	B.06 Install network devices (i.e. IDS, IPS, firewall, web filter)	B.07 Configure network devices (i.e. IDS, IPS, firewall, web filter)	B.08 Install host-based security systems (i.e. antivirs, malware, sensors)	B.09 Configure host-based security systems (i.e. anti-virus, malware, sensors)	B.10 Create investigative and configuration scripts	B.11 Ensure data encryption (i.e. data at rest, data in transit removeable media)
	B.12 Ensure physical security controls	B.13 Ensure environmental controls	B.14 Recommend security requirements	B.15 Manage wireless access points	B.16 Create network diagrams	B.17 Maintain network diagrams	B.18 Create penetration test plans	B.19 Request ASI	B.20 Backup critical data	B.21 Manage network device life-cycles	B.22
C Detect Cybersecurity Events	C.01 Monitor network devices	C.02 Analyze output of network devices	C.03 Analyze threat feeds	C.04 Monitor wireless access points	C.05 Review network diagrams	C.06 Set audit flags	C.07 Analyze external data (i.e. darknet, passive DNS, BGP)	C.08 Document historical findings	C.09 Maintain historical Packet Capture (PCAP)	C.10 Analyze audit logs	C.11 Analyze vulnerability scans
	C.12 Hunt potential threats in network traffic	C.13 Conduct organizational penetration tests	C.14 Generate penetration test documentation	C.15 Challenge personnel need-to-know/authorizations							
D React to Cybersecurity Events	D.01 Initiate response procudures	D.02 Assess security event	D.03 Report event to supervisor *	D.04 Determine escalation	D.05 Communicate with stakeholders *	D.06 Maintain stakeholder call list	D.07 Contain security incident	D.08 Trace source of threat	D.09 Preserve evidence of event	D.10 Document steps taken	D.11 Estimate damage of security incident
	D.12 Sever network activity	D.13 Report estimated time of restoration	D.14 Document evidentiary process								
E Restore Secure Environment	E.01 Determine scope of restoration	E.02 Create restoration plan	E.03 Coordinate restoration efforts	E.04 Rebuild info system	E.05 Reimage information system	E.06 Restore critical data	E.07 Test restored environment	E.08 Validate restored environment	E.09 Document lessons learned	E.10 Document recovery processes	
F Increase Security Awareness	F.01 Create security awareness materials	F.02 Create acceptable use policies	F.03 Participate in security exercises	F.04 Distribute security info to users	F.05 Conduct cybersecurity training	F.06 Conduct phishing campaign	F.07 Reverse engineer malware	F.08 Conduct security awareness assessment	F.09 Report assessment results	F.10 Recommend procedures to correct security issues	
G Maintain Professional Knowledge	G.01 Complete cybersecurity training	G.02 Maintain industry certifications	G.03 Read technical literature (i.e. books, blogs, articles, etc.)	G.04 Attend professional conferences	G.05 Maintain operating environment qualifications	G.06 Practice through trial and error	G.07 Maintain professional memberships				

* Denotes a recurring task

Worker Behaviors

Able to problem solve
Able to work autonomously
Able to work independently
Self-starter
Attention to detail
Methodical
Strong work ethic
Integrity
Oral/written communication skills
Tenacious
Team player
Teachable
Passionate about field
Self-motivated
Inquisitive
Ethical
Desire to learn
Professionalism
Common sense
Conflict resolution
Desire to work beyond minimum expectations
Willing to be on call after hours
Discretion
Multi-tasker
Creative

----------Knowledge & Skills----------

Server management
OSI model
TACACS +
LDAP
Kerveros
AES
RADIUS
X TACACS
Rainbow Tables
Visualization tools
Cryptography
Common application protocols
Node JS
GIT
Java Script
Metasploit
Kaii (Linux)
VLAN
Virtual environments
Forensics
Web services
Proxies
PHP
Apache
WPA2
WEP
IP Sec
Debugging

Load balancing
SQL
Oracle
NoSQL
Common application ports
TCP/IP
Volatility
SPLUNK
Maltego
SEIM tools
Cloud environments
Regulation policies
LUA
NIST
JSON
Parsing
HP Fortify
VPN
2 Factor Authentication
MDM
Lint
Packet sniffers
802.1x
Open source intelligence
Firewalls
Encryption
PKE/PKI
Multiple inheritance

UNIX
LINUX
Cisco
Switches
Routers
Snort
Wire shark/T shark
Nessus
STIG viewer
Endpoint protection software
Scapy
Raspberry pi
“Google-fu”
APIs
Programming languages
TCP dump
Super scan
SSH/Serial Communications
MS Operating systems
Software update services
Powershell
Python
Scripting
Restful APIs
YARA
C Programming
Assembly Programming
RESTful Interfaces

Tools, Equipment, Supplies, and Materials

Visio (MS)
Packet analysis software
Google
Putty
Printer
Laptop
Monitors
Serial console cable
Ethernet cable
USB cable

Notepad ++
Web browsers
Router
Switch
Cell phone
Site survey tools
Wireless LAN tools
Cable tester/TDR
Multimeter
File transfer client

FTP Voyager
Packet tracer
GNS3
Virtual machines
Lab environment
Through put tester
Latency simulator
T-Bird
Vision network icon
Crimper

Recommendations for Recruiting Students

Cybersecurity club
Capture the flag events
Creation /use of a cyber-range to build, test, destroy, and restore
College/university partner with companies - real data and scenarios needed for training
Companies offer internships and opportunities for project-based learning
Cyber Honors Program – computer science majors apply and do extra cyber work for rewards
Scholarships (Cyber Corps)
Offer course on security culture

Future Trends

Cybersecurity jobs in high demand
Trained individuals have ability to choose where they work
Cybersecurity yields higher salary (vs. networking)
Stigma of cybersecurity as a “boring” or “stuffy” field
Public lacks understanding of the wide variety of cyber roles
Concerns about industrial SCADA
Internet of Things
Cybercrime escalation - direct impact on lives
Cyber espionage
Cybercrime over software-defined radio