GUIDEPOINT SECURITY UNIVERSITY

MILITARY FELLOWSHIPS PROGRAM

Jumpstart your transition from the military to a career in cybersecurity.

Cybersecurity is more important than ever, but the skills gap continues to abound.

Despite increased investment in cybersecurity, commercial and government organizations continue to face a massive skills shortage due to heavier workloads, unfilled positions and worker burnout. We can help jumpstart and enhance your cybersecurity career.

GuidePoint Security University (GPSU) is a training and development pipeline to help those interested in a cybersecurity career develop critical industry skills and apply cyber knowledge to develop real-world solutions. GPSU has an internship component, which is tailored to create an individualized experience based on your background and aptitude that teaches both technical and soft skills.

Transitioning from Military? Using skills honed in the military, we collaborate with the DoD Skillbridge, Army Career Skills Program, and Hiring Our Heroes to provide service members with meaningful opportunities to transition into cybersecurity careers.

Coming from the Intelligence Community? Leverage your skills to become a member of the Data Analytics team, which uses analytics to prevent and detect threats.

New to Cybersecurity? Many cyber professionals begin as a SOC Analyst, monitoring networks to identify incidents and responding to alerts from across the organization.

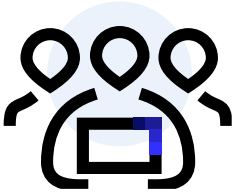
Background in IT Administration? Consider Cloud Security or Identity Management to utilize your understanding of network architectures and authentication processes.

Recent Software Engineering or Computer Science Graduate? Use your understanding of underlying code to shift into Application Security and help identify vulnerabilities. If you enjoy creating solutions and know how to write in python, a career in Security Orchestration, Automation, and Response (SOAR) may be for you.

Prior Technical Leadership Roles? Explore becoming a project manager, where you can work with various departments throughout the organization, while using a variety of collaboration tools and techniques to drive operations.

Benefits:

- Work remotely or on-site at our HQ in Herndon, VA or a regional office
- Flexible internship length that works with your timeline (3-6 months)
- Training labs and courses all provided at no cost to you
- Recently separated veterans help guide your transition process
- Work with industry-leading experts who previously managed security within the DOD, intelligence agencies and Fortune 500 companies
- Chance to earn industry certifications and Continuing Education Units
- Work individually or in a cohort of other learners



Learn from an ELITE Team of Cybersecurity Practitioners

More than 70% of our workforce consists of tenured cybersecurity engineers, architects and consultants

Gain experience in any of our major focus areas through:

- Hands-On Technical Development
- Commercial or Federal Work Experience
- Team and Position Shadowing
- Real-World Security Response
- Collaborative Project Work
- Partner-led Vendor Training and Certifications

Authorized Industry Partner

of DoD SkillBridge, Army Career Skills Program, and Hiring Our Heroes

* The Life and Times of Cybersecurity Professionals 2021, ISSA and ESG

GuidePoint Security University Technical Focus Areas

Application Delivery: A combination of services that work together to provide a functional and secure application - spanning from end user interactions through data processing to where the data is stored.

Application Security: The process of reviewing underlying code and testing live applications to identify vulnerabilities that a threat could exploit. Members of the application security team often work in tandem with other technical specialties, such as penetration testers, to provide a more holistic approach to proactive security.

Cloud Security: Enable organizations to secure their Amazon Web Services, Microsoft Azure and Google Cloud Platform environments. Cloud security covers many aspects of cybersecurity security: operations, administration, compliance and architecture.

Governance, Risk and Compliance (GRC): Review and manage the processes, roles, controls, and metrics of handling information - while also ensuring that organizations understand relevant laws, regulations, and their current risk and compliance posture.

Identity & Access Management: A framework for managing digital identities and controlling user access to critical information and systems without impeding business operations. *Privileged Access Management (PAM)* oversees the technologies that exert control over account privileges and elevated access levels across the network. *Identity Governance and Administration (IGA)* enables administrators and security teams to manage and reduce risk related to unnecessary user access levels.

Network Security: The network security team helps ensure the integrity and security of physical and virtual networks, by evaluating and administering devices, such as firewalls and other network access controls.

Penetration Testing: This offensive aspect of security proactively tests networks, devices, and applications for vulnerabilities that a threat could exploit to steal information or cause damage to an organization. Pentests often conclude with a detailed description of an organization's overall security posture, along with suggestions to mitigate cyber risk.

Project Management: Help drive all operations and ensure cybersecurity projects are seen through to completion. PMs are involved in all disciplines covered by GuidePoint Security.

Security Analytics & Automation: An approach where data is analyzed to produce proactive security measures. Organizations often use Security Information and Event Management (SIEM) and Security Orchestration, Automation and Response (SOAR) technologies to help conduct security analytics efforts. *SIEM platforms* are used to collect and analyze data from multiple sources in order to conduct threat detection, compliance and incident management. *SOAR technologies* are used to ingest data and automate security tasks through playbooks that integrate various products and application mechanisms.

Security Operations: The ability to effectively identify and respond to incidents early within the threat life cycle. Threat intelligence directly supports security operations by collecting and correlating data from external and internal sources to provide information on a malicious actor or incident. Network Monitoring, the process of watching data as it passes across all networking components, is typically conducted by SOC analysts in real-time to identify abnormal activity requiring further review by a technical expert.

About Us

GuidePoint Security provides trusted cybersecurity expertise, solutions and services to help organizations make better decisions that minimize risk. GuidePoint's unmatched expertise has enabled a third of Fortune 500 companies and more than half of the U.S. government cabinet level agencies to improve their security posture and reduce risk.

GUIDEPOINT SECURITY UNIVERSITY

2201 Cooperative Way, Suite 225, Herndon, VA 20171
guidepointsecurity.com/gpsu/ • gpsu@guidepointsecurity.com • (877) 889-0132