GUIDEPOINT SECURITY UNIVERSITY

2025 INTERNSHIPS

Start your cybersecurity career with a training program built by experienced practitioners.

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.

PROGRAM OVERVIEW

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 one's background that teaches both technical and soft skills.

INTERNSHIP STRUCTURE

The internship is broken into three parts: exposure, discovery, development.

1. The first phase exposes interns to the different areas of cybersecurity, while learning some of the fundamental skills needed to be a security professional.
2. In the second phase, interns are connected with mentors in one of our specialty areas, where they get the chance to join in on team calls, shadow customer engagements, and train on specialized vendor tools.
3. In the third phase, interns begin work with senior employees on customer projects, complete a capstone project, and participate in career development activities with the GPSU team.

WHO WE'RE LOOKING FOR

The ideal candidate is a recent graduate, someone looking to transition careers, or a current Junior or Senior working toward a technical degree, all with a genuine interest in the cybersecurity field. Interns may also earn college credit, helping them advance their education while also gaining hands-on experience. We want motivated candidates that enjoy learning and thrive with autonomy in a remote environment. It is also useful for candidates to have a basic understanding of information technology and general networking concepts. Experience with Linux and/or security tools is a plus.

All are welcome to apply and will be considered!
Motivated individuals eager to learn new skills will excel in this program.

2025 SCHEDULE

- Spring: Jan 6 - Mar 28 (includes in-person onboarding)
- Summer: May 19 - Aug 8 (includes in-person onboarding)
- Fall: Sep 2 - Nov 21

ADDITIONAL DETAILS

- 100% remote following in-person onboarding (all expenses paid)
- Chance to earn industry certifications and Continuing Education Units
- Get paid for your time, up to 29 hours per week
- Work with industry-leading experts who previously managed security within the DOD, intelligence agencies and Fortune 500 companies

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

APPLY NOW

GuidePoint Security University 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.

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.

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.

INFORMATION ASSURANCE: The practice of protecting against and managing risk. Application Security reviews underlying code and tests live applications, including web apps, to identify vulnerabilities that a threat could potentially exploit. Governance, Risk and Compliance reviews and manages 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. Penetration Testing proactively tests networks, devices and applications for vulnerabilities that a hacker could exploit to steal information or cause damage.

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.

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: 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