Paul Benoit

Tysons, VA / 703-887-0443 / benoitpaul6@gmail.com

Full Stack Developer - The Crypsis Group McLean, VA 6/19-Present
Worked on an agile team to develop Hadron, a scalable Endpoint Detection and Response solution that combines endpoint monitoring with forensic analysis. My contributions included: forensic artifact parsers, remote agent update/uninstall, and offline mode. Presented release updates to the company. (Golang, AWS, Osquery, ELK)

Junior Security Engineer - The Crypsis Group McLean, VA 3/18-6/19
Developed a forensic collector that gathers live response data from compromised systems. The collector uploads the data to AWS where it is processed and ingested into Splunk or ELK. Crypsis used this tool to collect forensic data on over 100,000 systems. (Ruby, AWS, Docker, Splunk, ELK)

Conducted forensic examinations of Windows, Linux and macOS systems. Timelined Indicators of Compromise and wrote reports to give to clients about forensic findings.

Analyzed breached Microsoft Office 365 mailboxes to identify when accounts were compromised and how much personally identifiable information was exposed. (PowerShell, Splunk)

Internship - The Crypsis Group McLean, VA 5/16-3/18
Created a tool that identifies suspicious remote desktop connections in event logs. (Python)

Analyzed webshells and malicious scripts. (PHP, PowerShell)

EDUCATION
George Mason University, 2019
B.S. in Cyber Security Engineering

ACTIVITIES & SIDE PROJECTS
Founded Mason Competitive Cyber, the cyber security club at GMU. Grew the organization to over 600 members in Slack when I graduated.

- Virginia Cyber Fusion 2018 - 1st Place
- Capital One GMU Wargame 2017 - 1st Place
- Sevatec GMU Hackathon 2017 - 1st Place

paulbenoit.com - Serverless personal website. (AWS)

HOBBIES
Avid Capture the Flag (cyber security competition) player. Multiple top 100 placements in online CTFs.

Amateur mountaineer. Summited Mt. Washington in a blizzard in -20°F weather