# Paul Benoit

Security & Development

## Work Experience

*The Crypsis Group* · McLean, VA

**Full Stack Developer** · June 2019-Present
**Junior Security Engineer** · March 2018-June 2019
**Technical Intern** · May 2016-March 2018

**Development**
*EDR Solution* — Worked on an agile team to develop Hadron, an EDR solution that combines endpoint monitoring with live response data collection. Mostly responsible for agent development.
My contributions included: forensic artifact parsers, remote agent update/uninstall, and real-time data monitoring.

*Live Response Collector and Processor* — Developed a live response collector that gathers data from victim Windows, Linux, or macOS 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 from over 100,000 systems.

Helped develop a PowerShell tool that uses the Office 365 API to collect relevant logs for breached mailboxes.

Created a Python script that looks for suspicious RDP connections in event logs.

**Host Based Forensics**
Conducted forensic examinations of Windows, Linux, and macOS systems.
Timelined Indicators Of Compromise (IOCs), and wrote reports to give to clients about forensic findings.

Analyzed PHP web shells and malicious PowerShell scripts.

**Business Email Compromise Analysis**
Used Splunk to analyze Microsoft Office 365 logs from breached mailboxes.

**Data Discovery**
Used Spirion and regex to find PII on breached systems and mailboxes.

## Contact


Vienna, VA
(703) 887-0443
benoitpaul6@gmail.com
github.com/thepaulbenoit


## Education

May 2019 **Bachelor of Science**
Cyber Security Engineering
*George Mason University*

## Activities

**Cyber Competitions**
Founded Mason Competitive Cyber, the cyber security club at GMU.

Virginia Cyber Fusion 2018 - 1st place
Capital One GMU Wargame 2017 - 1st place
Sevatec GMU Hackathon 2018 - 1st place
Multiple Top 100 placements in online CTFs

**Side Projects**
Python tool that automatically solves simple steganography CTF challenges

paulbenoit.com
Serverless personal website in Go

## Technical Skills

**Languages**
Golang, Python, PowerShell, Ruby, Visual Basic, PHP, HTML, SQL, C

**Applications/Frameworks**
Git, VMware, AWS, Docker, Splunk, Nmap, Nessus, FTK, Wireshark, Spirion, EnCase, Osquery, GRR

**OS Experience**
Windows, macOS, Linux (Ubuntu, Debian)