**Dave Loftus**
101 Lake Ave #2011
Orlando, FL 32801
dave@dloftus.com
+1 (734) 249-6758

## CAREER STATEMENT

With over 15 years of experience in the security industry, and 21 years of actively developing software both personally and professionally, my talents interconnect the areas of software engineering, malware analysis, and threat intelligence to provide actionable insights within the security community.

As a security researcher, my career has progressed from incident response, to identifying indicators related to criminal campaigns, to researching state-sponsored APTs. I've combined this research with extensive Python experience to develop automated infrastructure & produce software essential for security intelligence work.

These accomplishments have resulted in interviews with leading media publications, industry working groups, and presentations at private security conferences.

## PROFESSIONAL EXPERIENCE

**Pfizer**
**Senior Security Automation Developer**                                                    **2019 - 2022**

This role was a Senior Security Automation Developer with Pfizer's Global Information Security Team.

Responsibilities included:

- Engineering solutions to ensure compliance with data loss prevention policies
- Compliance driven collection of mobile application data sent within the APAC region; this project required Python bindings to C libraries, Splunk, Docker, Zookeeper, and Elastic
- Administering a Security Orchestration, Automation, and Response (SOAR) platform
- Providing automation support to incident response, threat intelligence, and insider threat teams
- Conducting code reviews
- Modernizing legacy infrastructure & engineering practices
- Assisting management and mentoring team members

**Kayod**                                                                                           **2017 - 2019**
**Owner / Lead Developer**

As the owner and lead developer, these roles included managing business affairs, marketing, and creating:

- A Yara based endpoint security product that alerted clients about files containing sensitive data & measured the length of exposure over time
- A GPS based mapping service
- A charitable, employment based recruitment platform tailored to the Republic of the Philippines

**Arbor Networks – Arbor's Security Engineering & Response Team (ASERT)**          **2013 - 2017**
**Security Research Analyst**

This role was a Security Research Analyst on Arbor's Security Engineering & Response Team

(ASERT).

Responsibilities included:

- Reverse engineering malware
- Malware classification
- Contributing to the development of Arbor's automated malware analysis infrastructure
- Malware sinkhole development
- Product feed development
- Researching DDoS related threats & developing mitigations
- Producing research & intelligence products for customers
- Briefing media & responding to law enforcement inquiries
- Point-of-contact for an ISAC
- Understanding threat-actor TTPs, and when possible, providing attribution to campaigns
- Contributing to working groups & vetted security communities
- Researching new malware families, criminal campaigns & state-sponsored APTs
- Presenting at private conferences

Highlights included:

- Research related to the extradition of a Canadian involved in a high profile data breach
- Researching targeted attacks against the aerospace & energy sectors
- Discovering compromises in a State Assembly in Eurasia
- Researching breaches at embassies & consulates in North America, Central America, and Asia-Pacific
- Researching targeted attacks against businesses along the U.S. east coast
- Co-discovering point-of-sale malware families: NewPosThings & Soraya, and novel variants of existing point-of-sale malware
- Recovering over 250,000 unique compromised payment cards and identifying numerous breached businesses

**Southern Illinois University Carbondale – Information Security**        **2008 - 2012**
**Incident Responder**

This role was working as an Incident Responder in the Information Security Department at Southern Illinois University Carbondale.

Responsibilities Included:

- Identifying, containing, and monitoring the remediation of malware infections
- Working with departments to implement best security practices
- Developing a DNS-based sensor network to identify malware traffic
- Creating infrastructure to detect malware traffic signatures from third-party feeds
- Developing a passive DNS database
- Forensic analysis of compromised devices
- Reverse engineering malware
- Identity management & compliance audits
- Responding to law enforcement inquiries
- Contributing to the TDL working group
- Developing an endpoint security product

**Southern Illinois University – Office of the President**        **2009**
**Internship in Public Affairs**

This work involved conceptualizing, executing, and implementing the largest lobbying effort in Southern Illinois University's history. This work secured millions in funding for the Illinois MAP Grant from the Illinois Student Assistance Commission. This work was recognized by SIU and the Illinois Student Assistance Commission. Recognition of this achievement has been permanently placed in the university archives.

**Southern Illinois University Carbondale**                                 **2006 - 2007**
**Research Contract**

This position involved the development of a communication paradigm for unmanned aerial vehicles under a research contract from Sierra Nevada Corporation. This work was conducted under Dr. Henry Hexmoor at Southern Illinois University.

**Southern Illinois University Carbondale**                                 **2006 - 2007**
**Palm Pilot Application Development**

This work consisted of developing a Palm Pilot application used by clinical researchers at Southern Illinois University. The application enabled researchers to monitor and record behavioral interactions between members of at-risk communities. This software was used to support a long-standing study at the university.

**Terry's Computer Shack**                                           **2004 - 2005**
**Employee**

Repaired and assembled computers, removed malware infections, sold cellular phones, assisted customers, and installed satellite dishes for customers in the Mendota, Illinois and surrounding area.

**EDUCATION**

**B.S.  Speech Communication – Southern Illinois University Carbondale**         **2013**
Specializations in Persuasive Communication & Interpersonal Communication

**B.A. Political Science – Southern Illinois University Carbondale**              **2012**
Minor in Speech Communication