# Pseudonymous User

**resume@pseudonymous.net · (101)-010-0110 · Ninja Village, GA · pseudonymous.com**

**SUMMARY**

I have over 5 years of IT security experience. I thrive in multitask environments and I’ve held multiple positions that require confidentiality and handling of sensitive information. I’m a continuous learner with a passion for innovation in security risk management and ethical hacking.

**CERTIFICATIONS & EDUCATION**

**· Cisco Certified Network Associate: CyberOps (CCNA) · CompTIA A+, Network+, Security+ ce**

**· Microsoft Certified Professional (MCP) · ITIL Foundation ·** eLearnSecurity Junior Penetration Tester (eJPT)

**· LPI Linux Essentials** **· Apple Certified Associate – Mac Integration (ACA)** **· AWS Certified Cloud Practitioner**

**· Ashworth College Diploma with Honors in Small Business Management**

**PROFESSIONAL EXPERIENCE**

Company 2 | February 2018 – June 2019

**IT & SECURITY ADMINISTRATOR**

* Manage corporate IT and relationships with 3rd party providers delivering support services.
* Conduct system configuration and policy compliance audits.
* Perform daily reviews of security notifications and alerts regarding brute force attempts, account changes, malware, and access requests.
* Vulnerability scanning and assessment.
* Maintain approved software list, assist with vetting new software.
* Image, manage, and deploy Windows / Mac workstations for over 100 employees.

Company 1 | July 2014 – February 2018

**TECHNICAL SUPPORT TEAM LEAD**

* Managed a team of around 20 new and experienced analysts to ensure quality customer service
* Provided Tier I and Tier II support to over 100 law firms and over 1000 clients.
* Was responsible for access management for some of the firms we supported (mainly access to emails and documents, creating and revoking RSA tokens, and various settings in active directory).
* Responded to security incidents such as viruses, suspicious emails, attachments, and stolen equipment.

**KEY SKILLS**

* Solid knowledge about ethical hacking, penetration testing, vulnerability management, network security.
* Identifying, researching, validating, and exploiting various known and unknown security vulnerabilities.
* Social Engineering campaigns, e.g. email phishing, phone calls, pretexting, and Quid Pro Quo attacks.
* Ability to work independently on initiatives with little oversight and adapt quickly to change.
* Articulate security issues to technical and non-technical audience.

**SECURITY TOOLS**

WireShark, TCPDump, NMAP, John the Ripper, Nessus, Sparta, Tor, Hydra, Burpsuite, Dirbuster, enum4linux, arpspoof, Metasploit, Meterpreter, Kali Linux, Parrot OS