

Adrian S. Buford
1-773-690-3174
buf0rd@protonmail.com

Objective

Seeking a dynamic team passionate about information security systems and technology troubleshooting, where I can leverage my skills, work ethic, and diverse experience to contribute effectively. Eager to align with an organization offering a clear career path that resonates with my vision of an ideal workplace which is one that is committed to embracing challenges, continuously expanding my knowledge, and fostering intellectual growth while empowering me to make meaningful contributions to the team and organization.

Skills

- Ability to adapt knowledge from traditional education and hands-on experience to diverse tasks.
- Goal-driven mindset with a focus on personal and professional growth.
- Exceptional proficiency in resolving customer disagreements with tact and diplomacy.
- Excellent verbal and written communication skills, facilitating effective collaboration and problem-solving.
- Positive and proactive approach to addressing challenges, fostering innovative solutions.
- Comprehensive understanding of email security and email security solutions.
- Proven track record of building high-performing and cohesive teams across various industries.
- Proficiency in leveraging Endpoint Detection and Response (EDR) tools for proactive threat hunting and anomaly detection.

Security vendor software solution experience: CrowdStrike, Proofpoint (Electronic File Defense, Proofpoint OnDemand, Secure Email Relay, Internal Mail Defense, TAP, TRAP, Browser Isolation), Tenable Nessus, Splunk, Guardicore, Workspace One Trend Micro, Windows Defender, Microsoft Exchange, Active Directory, Bloodhound, Recorded Futures, SysAid, Service Now, Netskope, CyberArk. Palo Alto.

Certifications

GIAC | Global Information Assurance Certifications

GSOC : Security Operations Certified
GCIH : Certified Incident Handler

CompTia | Computing Industry Technology Association

CSCP : Secure Cloud Professional (Security+ & Cloud+ Certifications)
CCAP : Cloud Admin Professional (Network+ & Cloud+ Certifications)
Security+
Network+
Cloud+
ITF+ Certification

ISC² | International Information System Security Certification Consortium

CC: Certified in Cybersecurity Certification

Proofpoint

Certified Phishing Specialist
Certified Identity Threat Specialist
Artificial Intelligence Machine Learning Specialist
Insider Threat Specialist
Security Awareness Specialist

Microsoft

Power Platform Fundamentals Microsoft Certified

Truman College

Advanced Automotive Technology Certification

Basic Automotive Technology Certification

Licenses

ISBE | Illinois State Board of Education
Substitute Teaching License

Education

Spring 2024

SANS Technology Institute
SEC504: Hacker Tools, Techniques & Incident Handling

Winter 2023

SANS Technology Institute
SEC450: Security Operations and Analysis

Spring 2023

Tenable
Nessus Specialist Training

Spring 2021, Fall/Spring 2022, Fall/Spring 2023

Wilbur Wright College
Cyber Security, Cont ed. career accelerator
National Cyber League, Capture the Flag National competition

2018

Wilbur Wright College
Cyber Security, Cont ed. Bootcamp

2009-2011

Southern Illinois University Carbondale
Bachelor of Science

2008-2009

Truman College
Associate of Applied Arts and Science
Advanced Automotive Certification
Basic Automotive Certification

Employment history

Chicago, IL Oct 2022– January 2025

Office of the Illinois Attorney General - Information Security Bureau, ISB | Cybersecurity Operations Analyst

- Information Security team new hire on-boarding, training, and role development.
- Security Incident Response and investigation of escalated IT incident tickets to determine course of action based on security best practices and organization policies.
- Incident Response documentation development.
- Vulnerability management and remediation assessment
- Government developed application penetration testing, vulnerability scanning, and reporting.
- SIEM environment implementation including mapping.
- Implementation and functionality testing for security operations center software.
- Research recent vulnerability trends to determine organizational exposure and risk mitigation options.
- Creation of security policies and system notification for various endpoint agents and AV systems.
- Development of new hardened system image to be utilized by all endpoints by leveraging knowledge of security best practices and report metrics including most utilized applications.
- Incident response investigation triage and prioritization.
- Firewall compliance auditing, hardening, and baseline security configuration.
- Endpoint detection response administration.
- Email security configuration, quarantine analysis, vendor communication, and day-to-day administration.
- Insider threat research, data collection, analysis, classification, and reporting.
- Utilized anomaly detection techniques to proactively identify and mitigate potential security threats within enterprise environments.
- Collaborated with cross-functional teams to analyze and investigate security incidents, provide insights based on experience and recommendations for remediation.

- Conducted comprehensive wireless internet security assessment and penetration test to identify vulnerabilities and create recommendations for countermeasures to safeguard against potential breaches, ensuring the availability, integrity and confidentiality of sensitive data.

Chicago, IL – 2018 – 2022

Assurant, Inc. | *Product Testing Analyst, Client Support Specialist, Email and Chat Specialist*

- Conducted software and system troubleshooting, including the development of comprehensive playbooks for efficient issue resolution.
- Updated Salesforce platform features and conducted integration testing to ensure seamless functionality and compatibility with existing systems.
- Planned and executed various testing phases, including functional testing, integration testing, regression testing, end-to-end testing, and user acceptance testing, to validate system performance and reliability.
- Reported and investigated bugs, ensuring timely resolution and minimizing impact on system operations.
- Developed scripts, generated reports, and analyzed logs for data migration and integration of new business processes, enhancing operational efficiency and accuracy.
- Conducted manual and automated API testing using SoapUI and Postman, verifying system functionality and interoperability.
- Verified test case acceptance criteria, ensuring alignment with project objectives and requirements.
- Logged and tracked bugs and defects, facilitating effective communication and resolution between development and testing teams.
- Monitored and updated user and account access management systems, maintaining security and compliance standards.
- Conducted compliance verification through rigorous testing procedures, ensuring adherence to regulatory requirements and industry standards.
- Performed QA testing for new code deployments, ensuring stability and functionality of software updates and enhancements.
- Conducted general data validation to ensure accuracy, completeness, and consistency of data across systems and processes.

Chicago, IL – 2009 – 2018

The Warranty Group | *Client Relationship Analyst, Client Support Specialist, Claim Adjuster Specialist, Payment Specialist*

- Provided remote support for connected systems, ensuring seamless functionality and addressing user concerns promptly.
- Developed and maintained a comprehensive database for company W9 tax information, enhancing organizational efficiency and compliance.
- Optimized client relationships, fostering trust and loyalty through effective communication and personalized service.
- Administered the Salesforce platform, overseeing data migration efforts and ensuring data integrity and accuracy.
- Served as the primary point of contact for clients, addressing system, user, permission, compliance, agreement, and billing inquiries and concerns.
- Translated technical issues raised by customers into actionable insights for internal IT support and product development teams.
- Conducted diagnosis of software and hardware issues in connected systems, facilitating timely resolution and minimizing downtime.
- Analyzed claims for adjudication and legitimacy, ensuring accuracy and compliance with regulatory standards.
- Investigated vehicle connected systems, identifying potential vulnerabilities and recommending solutions to enhance security and performance.
- Conducted testing, validation, and data management tasks for AS400 systems, ensuring reliability and integrity of operations.
- Verified compliance of payment systems, conducting thorough testing to ensure adherence to industry regulations and standards.
- Developed a virtual work program, integrating VPN solutions to facilitate secure remote access and collaboration.

Chicago, IL – 2013 – 2025

Buford Research Group, Llc. | *Information Technology Security Analyst, Consultant*

- Installed and maintained hardware and software systems, ensuring optimal performance and security.
- Conducted comprehensive research in information technology and security domains to stay abreast of industry advancements and best practices.
- Constructed and replaced desktops, workstations, and servers, employing meticulous attention to detail and adherence to security protocols.

- Monitored, scaled, and managed virtual machine resources, optimizing efficiency and performance.
- Provided consultation services on information technology and security matters, offering expert guidance and recommendations.
- Designed, secured, deployed, and maintained web services, prioritizing robust security measures and reliability.
- Administered websites, ensuring seamless functionality and addressing any issues promptly.
- Managed data backup and hosting operations for Personally Identifiable Information (PII), HIPAA, and attorney-client privileged information.
- Conducted systems verification testing to ensure compliance with relevant standards and regulations.
- Oversaw server administration.
- Implemented and managed Intrusion Prevention Systems (IPS), Intrusion Detection Systems (IDS), and firewall controls, bolstering network security defenses.
- Installed and configured access control systems for physical security, safeguarding sensitive assets and infrastructure.
- Handled general help desk duties, including remote administration tasks, to support end-users effectively.
- Managed user access rights, ensuring proper permissions and security protocols were in place.
- Conducted wireless network surveys and designed architectures to optimize performance and security.
- Provided training and conducted investigations related to insider threats, enhancing organizational security awareness and readiness.

Honors

Fall 2023 National Cyber League Cyber Security CTF | 73rd of 3,593

Fall 2022 National Cyber League Cyber Security CTF | 96th of 6675

Spring 2022 National Cyber League Cyber Security CTF | Top 95th percentile.

Fall 2021 National Cyber League Cyber Security CTF | Top 97th percentile.