

Lucas Howard

📍 NC, USA ✉ lucas.t.howard@outlook.com ☎ (336) 524-4509 🔗 lucashoward.co in lucas-howard0
🌐 lhwrđ

Education

MS	Western Governors University , Cybersecurity and Information Assurance <ul style="list-style-type: none">• Excellence Award for Secure Network Design	Sept 2023 – July 2024
BS	Western Governors University , Cybersecurity and Information Assurance	Sept 2022 – Feb 2023
AS	Guilford Technical Community College , Cybersecurity and Information Assurance	Jan 2019 – Dec 2020

Experience

Nike, Inc. , Senior Cyber Defense Incident Data Analyst (FTE)	Remote Jan 2023 – present
<ul style="list-style-type: none">• Conducted in-depth analysis of data affected by security breaches, delivering key reports to stakeholders for regulatory compliance and customer communication.• Developed automated reporting tools using Docker and Python, cutting incident report preparation time in half and enhancing stakeholder understanding.• Spearheaded the in-house transition of unstructured data analysis, saving the company \$ 1M per incident and reducing third-party dependency.• Streamlined log analysis with a risk-based approach, reducing manual data review requirements by 90% and enhancing incident response efficiency.• Championed the integration of Databricks notebooks into credential stuffing workflows, replacing AWS EMR to leverage advanced analytics features.	
Nike, Inc. , Cyber Defense Data Analyst (ETW)	Remote Oct 2022 – Jan 2023
<ul style="list-style-type: none">• Halved data collection times for Credential Stuffing incidents using optimized Pyspark jobs on AWS EMR, increasing response agility.• Engineered Grafana dashboards sourcing from PostgreSQL, enabling real-time cybersecurity metrics analysis for team members and leadership.• Collaborated interdepartmentally to refine Vulnerability Management metrics, elevating the organization's cybersecurity metric framework.	
L&E Research , Director of IT/AV and Security	Raleigh, NC July 2019 – Oct 2021
<ul style="list-style-type: none">• Led IT strategy and operations across 11 sites for a national firm, bolstering security posture and operational efficiency for a 300-person workforce.• Orchestrated deployment of Sophos endpoint protection and Qualys vulnerability management for 200+ devices, significantly enhancing security infrastructure.• Implemented automated anti-phishing and security awareness programs, cutting phishing susceptibility by 50% among employees.• Drove the advancement of information security to achieve SOC II compliance, fortifying managerial policies and incident response protocols.• Designed and deployed a robust cloud video recording platform using AWS Media Services, ensuring high security for sensitive market research data.	
North Carolina National Guard, B Battery, 5-113th Field Artillery , 25B Information Technology Specialist	Aug 2018 – July 2019
<ul style="list-style-type: none">• Supported Operation Inherent Resolve, managing secure communication networks and swiftly resolving technical issues under high-pressure conditions.	

- Automated access request workflows with a custom Python script, streamlining processes for over 120 military personnel.
- Enlisted NC National Guard Jun 2014 - Jun 2020. Highest rank achieved: E4 SPC.

XPO Logistics, Network Administrator

High Point, NC
Mar 2018 – Aug 2018

- Configured critical network infrastructure, including Cisco routers and switches, enhancing organizational communication and security.
- Innovated a web-based configuration tool, reducing network equipment deployment time and bolstering operational efficiency.

Certifications

- Certified Information Systems Security Professional (CISSP)
- Certified Cloud Security Professional (CCSP)
- Cisco Certified Network Associate (CCNA)
- Cisco Certified CyberOps Associate
- CompTIA A+, Cloud+, Network+, Security+, Project+, Linux+, Server+, Pentest+, CySA+, CASP+
- AWS Certified Solutions Architect - Associate
- Microsoft Certified: Azure Fundamentals
- ITIL Foundation

Technologies

Programming: Python, Pandas, Jupyter Notebooks, Pyspark, SQL

Other tools: Splunk, Git, Docker, Databricks, Snowflake, Grafana

Skills

- Incident Response and Management
- Application Security
- Windows and Mac OSX Knowledge
- Tactical and Strategic Solution Identification
- Strong Verbal and Written Communication Skills
- Collaboration Across Teams and Departments
- Detail-Oriented Approach
- Organizational Skills
- Proactive in Improving Security Controls