SAMANTHA CARNEY, MSc

♦ samanthacarney1011@gmail.com ♦ www.linkedin.com/in/scarney-infosec-analyst

SECURITY ANALYST

Security Analyst with hands-on experience supporting SOC-aligned security operations in a regulated financial environment. Perform daily alert monitoring, triage, and investigation using Microsoft 365 Defender, with a strong focus on phishing, endpoint, and identity-based security events. Experienced in incident investigation, root cause analysis, and incident documentation, with a growing emphasis on endpoint telemetry analysis and automation. Strong background in identity and access management and security operations collaboration, actively pursuing a full-time SOC / MDR analyst role. Consistently ensured continuous compliance with industry standards through successful internal and external audits, while strengthening the security functionalities of the organization.

AREAS OF EXPERTISE

♦ Monitor & Triage Alerts	♦ Identity & Access Management	♦ Leadership & Mentoring
♦ Microsoft 365 Defender Investigations	♦ Security Awareness Training	♦ Process Automation
♦ Threat Intelligence & Analysis	♦ Risk Mitigation & Frameworks	♦ Investigate Incidents
♦ Security Assessments	♦ Compliance & Best Practices	♦ Cross-Team Collaboration

PROFESSIONAL EXPERIENCE

PEOPLES BANK | Marietta, OH **MAR. 2023 – PRESENT**

Security Analyst II (Apr. 2025 – Present)

Information Security Analyst I (Aug 2023 – April 2025)

Worked closely with peers and leadership to refine threat intelligence reporting, improving alert context and supporting more proactive detection and investigation of emerging threats. The improved reporting enabled the team to shift from a reactive stance to one of proactive risk mitigation, better safeguarding critical assets from emerging threats.

- ***Threat Intelligence & Risk Mitigation:*** Perform daily SOC monitoring and investigations using Microsoft 365 Defender, analyzing alerts and security incidents across email, identity, and endpoint-related telemetry.
- ***Operational Resilience:*** Investigate phishing activity, suspicious user behavior, and access anomalies.
- ***Access Management:*** Reorganized user access reviews by pulling detailed access reports, coordinating communications with application owners, and making necessary system changes to address access discrepancies.
- ***Process Automation:*** Streamlined the onboarding of systems into SailPoint by developing PowerShell-based automation, reducing manual effort, improving consistency, and generating measurable cost savings for the organization.
- ***Compliance & Audit Support:*** Assisted in preparing for internal and external audits, compiling evidence and documentation to demonstrate adherence to security policies and regulatory requirements.

Information Security Analyst – Heitmeyer Consulting (Peoples Bank) (Mar. 2023 – Aug. 2023)

Instrumental in streamlining workflows and building strong relationships. By optimizing ticketing processes, they have significantly reduced resolution times, and their commitment to industry standards and regulatory frameworks ensures full compliance. This proactive approach, combined with the ability to nurture strong working relationships with peers and upper management, consistently drives team success and enables the achievement of organizational goals.

- ***Enhanced Customer Satisfaction:*** Through the implementation of proactive communication strategies and personalized support, customer satisfaction is enhanced.
- ***Proactive Security:*** Advanced security measures have been implemented to decrease the frequency of security incidents, fortifying the organization's defenses.
- ***Optimized Identity & Access:*** Identity and access management protocols were optimized to reduce unauthorized access incidents, ensuring a more secure environment.
- ***Audit & Compliance:*** Successfully coordinated and supported internal and external audits, compiling all necessary evidence and documentation to ensure adherence to regulatory requirements and industry best practices.
- ***Incident Response:*** Developed and executed incident response plans, effectively containing security breaches, minimizing their impact, and leading post-incident analysis to prevent future occurrences.

Professional Experience – Continued on Page 2

- ***Security Training:*** Created and delivered engaging security awareness training for employees, fostering a culture of security and reducing human error as a primary attack vector.

Earlier Experience: Custodian – Jackson County Board of Education, Ripley, WV, (Oct 2015 – Aug 2023)

ADDITIONAL EXPERTISE & ACCOMPLISHMENTS

- Leveraged an outstanding knowledge of information security to develop and implement robust security frameworks, successfully safeguarding organizational assets from cyber-attacks. This included conducting thorough risk assessments, developing and enforcing security policies, and ***ensuring continuous compliance with industry standards.***
- Excelled in threat and vulnerability management by actively monitoring emerging threats and conducting in-depth research and analysis. ***This proactive approach enabled the development of targeted mitigation strategies, significantly reducing the organization's risk exposure.***
- Provided best-in-class technical support, addressing complex security inquiries and troubleshooting issues to deliver comprehensive solutions. This hands-on expertise was critical in fortifying the organization's security posture.
- Utilized excellent communication skills to build and maintain strong relationships with co-workers and key stakeholders. ***Collaborated with multiple cross-functional teams to streamline security initiatives, which significantly increased overall work efficiency and drove successful project outcomes.***
- Identity Management: Demonstrated excellence in identity and access management by implementing and maintaining secure protocols, which fortified user authentication and protected critical data from unauthorized access. This expertise was crucial in maintaining the organization's security integrity.
- Developed and delivered engaging security awareness training for all employees, which ***fostered a culture of security and significantly reduced human error as a primary attack vector.***
- Proficiently utilized a wide range of security tools and technologies to automate threat detection, streamline vulnerability management, and enhance overall security posture. This strategic implementation of technology improved efficiency and provided more actionable intelligence.
- Successfully managed the end-to-end process for internal and external security audits, ensuring the organization met all regulatory requirements and industry best practices with zero findings.

PROFESSIONAL DEVELOPMENT

Hands-on labs conducted using industry-aligned SOC training platforms and simulated environments ♦ Practical SOC Analyst Associate (PSAA) ♦ CompTIA Security + ♦ (ISC)² Certified in Cybersecurity ♦ CompTIA CySA+ Microsoft Certified: Security, Compliance, and Identity Fundamentals ♦ CompTIA Cloud Essentials +

EDUCATION

Master of Science in Cybersecurity, 2023, 4.0 GPA
University of Charleston, Charleston, WV

Bachelor of Science, Cybersecurity & Business Administration, 2022, 3.9 GPA
University of Charleston, Charleston, WV