Sean A. Settgast
402-276-0813
settgastsean@gmail.com

PROFESSIONAL SUMMARY

Computer Science graduate specializing in software engineering, information technology, and cyber security. Three years of C# experience, two years of Python3 experience, approximately one year of JavaScript experience with the React framework, some Assembly and C++ experience, over three years of work experience as an information technology administrator, network administrator, and two years of experience in secure configuration management and vulnerability analysis. Four years of technical knowledge and expertise working in digital intelligence analysis with a strong attention for detail along with proven leadership and supervisory skills in leading teams made up of 12 individuals. Currently enrolled in a M.S. program at Kennesaw State University with a major in Software Engineering.

EDUCATION

Kennesaw State University   Kennesaw, GA
Master of Science in Software Engineering (MS SWE)   December 2022 (expected)
Augusta University   Augusta, GA
Bachelor of Science in Computer Science (BS CS)   May 2020
Relevant Coursework: Principles of Computer Programming I & II, Theory of Computation,
   Data Structures, Assembly Language Programming, Computer Organization, Foundations of Cryptography
Programming Language Experience: C#, C++, Python, Assembly, HTML/CSS, JavaScript
Community College of the Air Force   Maxwell Air Force Base, AL
Associate of Applied Science in Intelligence Studies (AAS)   August 2017
Defense Language Institute/Foreign Language Center   Monterey, CA
Associate of Arts in the Urdu Language (AA)   October 2014
Central Community College   Columbus, NE
Associate of Applied Science in Electronics Technology (AAS)   December 2007
Relevant Coursework: CISCO Networking I, II, III, & IV, Ethical Hacking, Microcomputer Repair

WORK EXPERIENCE

Savannah River Nuclear Solutions   Savannah River Site, SC
Software Engineer   September 2021 – Present

- Maintain various ASP.NET and JavaScript based websites and web applications, as well as develop new web applications and Windows services based on customer need.
- Maintain web applications for the on-site HRP department (Human Reliability Program for the Department of Energy) and BRS (Badge Request System).
- Responsible for developing and maintaining PL/SQL functions, procedures, and scheduled tasks on Oracle database ranging from data logging to site-wide email alerts.
- Provide cyber security guidance and carry out related cyber security directives as needed for the development team.
- Maintain relations with cyber security team serving in a technical advisor role. Also provide support as needed (sprints) and still serve as a member of the CSCMT (see below).

Cyber Security Specialist   August 2019 – September 2021

- Implemented Cyber Security risk controls based around NIST 800-53 for a large variety of networked security devices around the Savannah River Site, to include domain controllers, member servers, Windows 7 and Windows 10 workstations, laptops, and tablets, as well as various Linux-based servers serving in a variety of roles, including video surveillance systems in multiple buildings and areas to be used by on-site security, physical security databases for housing badge data for all employees throughout the site, and **N**etwork **I**ntrusion **D**etection **S**ystems (NIDS).
- Served in the **C**yber **S**ecurity **C**onfiguration **M**anagement **T**eam (CSCMT), a team composed of project security officers and secure configuration managers from different departments and cyber security teams from across the site. The purpose of this team is to review secure configuration baselines proposed by its members before submitting said baselines to the Department of Energy for review and approval to be deployed throughout development, acceptance, and production environments.
- Also established software and operating systems baselines based on appropriate DISA STIGs (**D**efense **I**nformation **S**ystems **A**gency **S**tandard **T**echnical **I**mplementation **G**uides), to include various versions of Windows 10, Windows 7, Windows Server 2012 (DC and MS), Red Hat Enterprise Linux 7, CentOS7, and various versions of Security Onion, both Ubuntu-based and CentOS7-based. Created baselines through Department of Energy approval process involving cyber

security as well as implementing said baselines on new systems through image deployment process and old systems through meticulous manual configuration.

- Served as a general systems administrator, providing Active Directory and Domain Controller administration. This includes user account maintenance and administration as well as Group Policy migration to and from various servers.
- Developed two separate secure configuration baselines for Security Onion, one for an older version based on Ubuntu and the newest version based on CentOS7, to be used as NIDS machines.

Savannah River National Laboratories   Savannah River Site, SC
Software Engineer (Internship)   June 2019 – August 2019

- Lead feature development on satellite imagery analysis software using Python3, namely dual implementation of **I**teratively-**R**eweighted **M**ultivariate **A**lteration **D**etection (IR-MAD) and **P**rincipal **C**omponent **A**nalysis with **E**xpectation **M**aximization (PCA-EM) to determine scene change detection in overhead satellite imagery.
- Developed temporal analysis methodology involving stacking change maps into a data cube that can be imported into imagery analysis software to determine when on a given timeline scene change has occurred.

United States Air Force   Fort Gordon, GA
Cryptologic Language Analyst   July 2011 – July 2017

- Gained a variety of information security experiences and education as an intelligence analyst.
- Lead various teams ranging from 3 to 12 individuals to do sprint intelligence and information gathering on given network-based targets for providing daily reports for daily briefs for high-value customers, to include the President of the United States. Information gathering sources include open-source intelligence sources as well as selector farming of compromised adversarial networked devices and online user accounts.

First National Bank & Trust, Inc.   Columbus, NE
Information Technology Administrator   May 2008 – June 2011

- Gained valuable experience in maintaining and managing over 150 computer systems, including two domain controllers, two member servers, and 146 Windows 7-based workstations across 4 physical locations as far as 45 minutes apart.
- Provided network administration to 12 network devices, including various switches, routers, and traffic shaping devices to provide **Q**uality **o**f **S**ervice (QoS) of network traffic between locations.
- Engaged monthly on organization cyber security teleconference to be made aware of and discuss up and coming information security threats, as well as to implement measures to mitigate risks.
- Engaged in monthly emergency response activities to both train and measure preparedness.

HONORS & ACTIVITIES

- Competed in the **I**nternational **C**ollegiate **P**rogramming **C**ontest (ICPC) at Kennesaw State University (2018 & 2019)
- Member of the **A**ssociation for **C**omputing **M**achinery (ACM) – Augusta University Chapter
- Dean's List for MS SWE program at Kennesaw State University 2021

PROJECTS

- Network Intrusion Detection System – Developed baseline configuration to be used on all Security Onion nodes to deploy a working network intrusion detection system to various environments throughout the site.
- Source Code Repository – Began work on implementing an Azure DevOps based repository to house configuration files for Tennable Nessus and Linux BASH scripts.
- DISA STIG implementation – Implemented DISA STIG standards for operating system baselines where appropriate DISA STIGs existed and applied DISA STIG approximations for operating systems with no appropriate DISA STIG. For example, Security Onion has no DISA STIG, but Red Hat Enterprise Linux 7 (RHEL7) does, and Security Onion v2.0 (latest) is based on CentOS7 which is based on RHEL7. I created an RHEL7 DISA STIG approximation for CentOS7, and subsequently a CentOS7 DISA STIG approximation for Security Onion in order to create the secure configuration baseline.

LANGUAGES	ENGLISH: Native, URDU: Minor	
TECHNICAL	General Applications	Excel, Word, PowerPoint, Outlook, Visio
	Project Management	IBM Jazz Rational, SharePoint, Azure DevOps
	Data Analysis	Excel
	Cyber Security	Tennable Nessus, Ivanti Patch Management, WSUS
	Software Engineering	C#, Java, Python3, JavaScript-ES6, C++, Assembly, BASH, PowerShell
ACTIVITIES	Video games, travelling, and technology	
OTHER	Active Department of Energy SECRET-Q security clearance	
	Inactive Department of Defense TS/SCI security clearance (expired 2018)	