Contact

williamzujkowski@gmail.com

www.linkedin.com/in/
williamzujkowski (LinkedIn)

Top Skills

OWASP ZAP

DevSecOps

Ansible

Languages

English (Native or Bilingual)

Certifications

The Fundamentals of Digital
Marketing

CompTIA Security Analytics
Professional – CSAP Stackable
Certification

Crash Course on Python

Honors-Awards

NHLBI Exceptional Performance
Recognition

Certificate of Excellence

NIH OCIO Contractor Exceptional
Performance Recognition

William Zujkowski

Senior InfoSec Engineer @ Cloud.gov -- Championing FedRAMP
Moderate Compliance Through Zero-Trust, DevSecOps &
Automated Monitoring
Rockville, Maryland, United States

Summary

With over 15 years of experience in IT and cybersecurity, current
work as a Senior Information Security Engineer at cloud.gov
focuses on safeguarding critical government technology. This role
involves driving FedRAMP Moderate compliance and security
through innovative Zero-Trust principles, DevSecOps practices, and
automated monitoring systems to ensure secure and compliant cloud
infrastructure for federal agencies.

Deeply motivated by the mission to enhance government efficiency
and innovation, contributions include enabling scalable cloud
solutions that meet rigorous security standards. Expertise spans
vulnerability management, secure configuration, web application
security, and incident remediation. Known for a proactive approach
to addressing emerging threats, consistently empowering teams to
deliver impactful results in high-stakes environments.

Experience

Technology Transformation Services (TTS)
Information Technology Specialist (INFOSEC)
November 2023 - Present (1 year 8 months)
Remote

• Spearheaded security initiatives for cloud.gov, enhancing the security posture
of government technology.
• Collaborated with cross-functional teams to ensure compliance with federal
security standards.
• Developed and implemented security protocols that improved incident
response times by 30%.
• Advocated for the mission of cloud.gov, empowering agencies to deliver
innovative services efficiently.

Guidehouse

Lead HPC Site Reliability Engineer (Contract)
May 2023 - November 2023 (7 months)
United States

• Led the orchestration of advanced systems engineering initiatives for the LoBoS high-performance computing cluster, enhancing computational capabilities for molecular dynamics research.
• Collaborated with top-tier researchers to optimize the cluster's performance, ensuring seamless serviceability for scientific projects.
• Spearheaded the integration of automation tools like Ansible and workload management systems such as SLURM, improving operational efficiency.
• Pioneered GPU compute capabilities with NVLINK, significantly boosting data throughput for computational chemistry applications.

Edgewater Federal Solutions, Inc.
1 year 5 months

Vulnerability Management Lead
May 2022 - March 2023 (11 months)
Bethesda, Maryland, United States

• Led a large team of cybersecurity engineers and analysts in managing the vulnerability management portfolio for NIH.
• Oversaw activities including host-based security, web application security, and penetration testing.
• Implemented secure configuration baseline management and data loss prevention strategies, enhancing overall security posture.
• Achieved a significant reduction in vulnerabilities across the NIH enterprise, contributing to a safer digital environment.

Deputy Vulnerability Management Lead
November 2021 - May 2022 (7 months)
Bethesda, Maryland, United States

• Provided strategic leadership in vulnerability management for the NIH enterprise, enhancing overall security posture.
• Implemented secure configuration baselines, reducing potential vulnerabilities by 30%.
• Led initiatives in web application security, resulting in a 25% decrease in security incidents.

Carson & SAINT Corporations
3 years

Lead Information Security Engineer & Alternate ISSO
December 2020 - November 2021 (1 year)

• Led a dedicated team in enterprise-wide information systems security management for the National Human Genome Research Institute.
• Enhanced cyber defense infrastructure, ensuring a robust security architecture and effective vulnerability management.
• Spearheaded incident response initiatives, significantly reducing response times and improving overall security posture.

Information Technology Security Engineer
December 2018 - December 2020 (2 years 1 month)
Bethesda, Maryland

• Delivered comprehensive cyber defense infrastructure support for the National Human Genome Research Institute.
• Implemented secure architecture and vulnerability management strategies, enhancing system resilience.
• Led incident response initiatives, significantly reducing response times and mitigating potential threats.
• Collaborated with cross-functional teams to develop security planning protocols, ensuring compliance with NIH standards.

GRSi
Lead Service Desk Engineer (Tier III SME)
February 2018 - December 2018 (11 months)
Washington D.C. Metro Area

• Supervised a team of IT technical staff in a high-stakes NIH Federal Medical Research environment.
• Acted as the escalation point for advanced technical issues across Windows, Mac, and Linux systems.
• Managed security controls and remediated vulnerabilities on over 900 sensitive endpoints, enhancing research integrity.
• Utilized advanced tools like FireEye and ServiceNow to document and resolve vulnerabilities effectively.

Medical Science & Computing (MSC)
Lead Service Desk Engineer (Tier III SME)
January 2017 - February 2018 (1 year 2 months)
Bethesda, MD

• Supervised a team of IT technical staff in a high-stakes NIH Federal Medical Research environment.
• Acted as the escalation point for complex issues across Windows, Mac, and Linux systems.

• Managed security controls and remediated vulnerabilities on over 350 sensitive endpoints.

• Utilized advanced tools like FireEye and Tenable Security Center to enhance system security.

Partners International
Technical Support Engineer
August 2016 - January 2017 (6 months)
Washington D.C. Metro Area

• Provided Tier II-III technical support for diverse operating systems, ensuring seamless user experiences.

• Managed Active Directory user accounts, enhancing security and access control for clients.

• Engaged in cybersecurity incident response, effectively mitigating risks for client organizations.

• Consistently surpassed SLA performance metrics, contributing to high client satisfaction rates.

Sensible Software, Inc.
1 year 4 months

IT Infrastructure & Support Manager
February 2016 - August 2016 (7 months)
Frederick, Maryland

• Managed a technical support team across five time zones, enhancing service delivery efficiency.

• Led the migration of SMB clients from legacy systems to a SaaS cloud product, improving operational performance.

• Developed security processes that reduced vulnerabilities, ensuring client data integrity and compliance.

Technical Support Engineer
May 2015 - February 2016 (10 months)
Frederick, Maryland

• Provided technical support for various operating systems, enhancing user experience and satisfaction.

• Led cyber-security incident response efforts, ensuring swift remediation and escalation of issues.

• Collaborated with client IT departments to troubleshoot complex technical problems, improving resolution times.

• Advocated for security process improvements, resulting in a more robust IT infrastructure at Sensible Software, Inc.

e-End
IT Specialist (IT Asset Management)
August 2014 - May 2015 (10 months)
Frederick, MD

• Executed NIST and NAID compliant data destruction processes, ensuring compliance with ITAR, GLB, SOX, FACTA, FISMA, and HIPAA regulations.
• Streamlined inventory and refurbishment processes for over 400 IT assets weekly, boosting operational efficiency.
• Developed and implemented the "Bulk Purchasing/Sales" program, establishing it as the company's leading profit center through strategic initiatives.

Self Employed
Information Technology Consultant
April 2005 - February 2014 (8 years 11 months)
Harrisburg, Pennsylvania Area

• Provided expert troubleshooting and repair for hardware and software across workstations, servers, and networking equipment.
• Implemented a centrally managed antivirus solution, enhancing security and reducing malware incidents by 30%.
• Designed a comprehensive disaster recovery plan, ensuring minimal downtime for critical systems.
• Delivered training and ongoing technical support to end-users, improving user satisfaction and efficiency.

———