Daniel Swihart

Howe, IN (Remote) – 317.941.8434 – dswihart@gmail.com

SUMMARY

Proactive IT Security Engineer with over 20 years of experience in IT operations and a specialized focus on information security for the past 4+ years. Expertise in performing security assessments, managing security technologies, and developing security standards. Skilled in AWS, Azure, Google Cloud, and other security tools and applications.

SKILLS

- **Cybersecurity Tools:** Proficient with CrowdStrike Falcon, Microsoft Purview, Varonis, Azure Security Center, and Google Cloud Security Command Center.
- **Security Designing Solutions for SOC teams:** Focused on incident response, threat hunting, and security monitoring, including configuring firewalls, IDS/IPS, endpoint protection, WAF, SWG, CASB and network access control.
- **Cloud Security:** Experience in performing security assessments and configuring security tools across AWS, Azure, and Google Cloud.
- **Compliance & Governance:** Knowledgeable in GDPR, CCPA, NYDFS, HIPAA, SOX, and PCI-DSS, with experience in implementing data governance and compliance monitoring frameworks.
- **Automation & Scripting:** Proficient in scripting with Python and PowerShell to drive automation and enhance security operations.
- **Data Loss Prevention:** Experience in designing and implementing DLP policies and controls to protect sensitive information.
- **Networking & Protocols:** Fundamental knowledge of network and web protocols and mitigation strategies for common attack vectors.

EXPERIENCE

DBR Cyber LLC. | Indianapolis, IN (Remote)
Owner/IT Consultant | 01/2024 – 06/2024

- Conducted comprehensive security assessments for SMB clients, identifying vulnerabilities and recommending best practices aligned with business needs.
- Developed and conducted training sessions on security procedures, enhancing workforce readiness and security awareness.
- Monitored and evaluated the effectiveness of security programs, recommending enhancements to keep pace with evolving threats and technologies.
- Helped ensure resilience against internal and external malware threats.

RealPage Inc. | Indianapolis, IN (Remote)
Information Security Engineer III – Data Loss Prevention (DLP) | 06/2022 – 12/2023

- Managed the deployment of Microsoft Purview and Varonis, improving data governance, compliance, and security analytics, reducing vulnerabilities by 30%.

- Regularly reviewed security logs and fine-tuned logging algorithms to optimize the detection of security anomalies, reducing false positives by 25%.
- Actively participated in system design and architecture reviews to ensure security best practices were integrated from the ground up, enhancing overall system security.
- Assisted with the rollout of Palo Alto firewalls, including the use of the Panorama management console to centralize and streamline firewall management across the organization.
- Configured and maintained security technologies, including Venafi policies, automated alerts, and workflows within Varonis and Office 365/Defender.

RealPage Inc. | Indianapolis, IN (Remote)
Storage Engineer III | 11/2021 – 06/2022

- Implemented EMC CyberVault for critical unstructured data protection, ensuring robust defense against ransomware and malware for 3.5+ petabytes of data.
- Performed routine security assessments and audits, identifying and mitigating potential vulnerabilities in the CyberVault environment.
- Created custom PowerShell scripts to automate the enforcement of data security protocols, ensuring compliance with PCI and SOX requirements across all storage systems.

Travel + Leisure Corporation | Indianapolis, IN (Remote)
Storage Engineer III | 09/2016 – 09/2021

- Oversaw secure migration of unstructured data to an Isilon array with 20k+ global connections, ensuring continuous availability for mission-critical applications.
- Utilized tools such as Ansible and Terraform to automate and secure cloud operations.
- Configured and maintained Azure Cloud services, integrated with Active Directory Federated Services (ADFS), and supported Windows/Linux environments.
- Reviewed and helped implement a SIEM (Splunk), enhancing security monitoring capabilities for all SAN/Storage infrastructures within the global environment.

EDUCATION

Baker College | Muskegon, MI
Associate of Applied Science in Networking Technologies | June 2005

CERTIFICATIONS

- AWS Certified Cloud Practitioner – May 2020
- VMware Certified Professional – Data Center Virtualization (VCP-DCV6)
- CrowdStrike Falcon Certified Administrator
- Varonis Certified Administrator