SHAWN BANTA

Cloud & Enterprise Security Engineer
Portland, OR • https://www.linkedin.com/in/theshawnbanta/ • banta.click

SUMMARY

Cloud and enterprise security engineer with 10+ years of experience designing, hardening, and operating controls across corporate endpoints, identity platforms, and SaaS environments. Expertise in device posture management, access governance, cloud environments, and vulnerability remediation. Focused on practical, risk-based improvements with a proven record building scalable, auditable, and resilient systems that reduce enterprise risk without slowing innovation.

EXPERIENCE

Cloud Security Engineer
Benchling – Remote | Feb 2023 – Present

- Operationalized the company's CSPM platform, successfully remediating high-risk issues while integrating findings into ticketing workflows to drive consistent remediation across teams. Resulted in the mitigation of thousands of initial findings.
- Rolled out CWPP agent coverage across ECS and EKS infrastructure, improving visibility into runtime vulnerabilities and misconfigurations. Enabled Detection and Response teams to more effectively respond to alerts.
- Designed and implemented an auditable, approval-based "Just-in-Time" access workflow that eliminated persistent administrative credentials.
- Managed the identity architecture and permission configurations for all employee and contractor access to cloud environments.
- Implemented a cross-cloud infrastructure deployment architecture (AWS <> GCP), implementing identity policies, hardening configurations, and documentation to support future audits.
- Conducted security reviews for new and existing services, providing practical recommendations that balanced risk reduction with enablement.

Enterprise Security Engineer
Benchling – San Francisco/Remote | Oct 2021 – Feb 2023

- Built corporate security from the ground up: endpoint hardening, in-office network security architecture, SSO enforcement, and SaaS configuration hardening.
- Deployed DMARC, SPF, and DKIM alignment across multiple domains, laying the foundation for implementing a DMARC reject policy, improving mail reputation and security posture.
- Established supplier risk and exception-handling workflows aligned with business enablement needs, including documented risk rubrics to standardize supplier evaluation and assessment requirements.
- Collaborated with IT to deploy a secure VDI environment to support contractor and testing use cases.

Senior Offensive Security Engineer
Salesforce | Nov 2020 – Oct 2021

- Participated in red-team operations emulating threat actor TTPs, validating detection visibility and impact.
- Built resilient C2 infrastructure and associated configurations to bypass egress controls such as domain restrictions.
- Delivered post-operation reports with actionable mitigations.

Senior Enterprise Security Engineer
Salesforce | Mar 2018 – Nov 2020

- Performed proactive security assessments against a pre-determined list of high-risk infrastructure and assets, resulting in the identification of critical risks within the environment, including full domain compromise across multiple domains and acquisitions.
- Consulted across the business providing security guidance and suggestions, from IT to Marketing and Finance. Held regular office hour sessions to get context and provide a friendly face of security.
- Participated as a member of the Cloud Center of Excellence team, made up of Security and IT to regularly discuss ongoing changes, and worked to define the cloud/network segmentation deployment aligned with data classification and access requirements.

Information Security Engineer
Rally Health | Aug 2016 – Mar 2018

- Coordinated third-party penetration tests, communicating findings to application teams and aligning on remediation SLA requirements based on risk.
- Managed the vulnerability reporting process for cloud and IT infrastructure.

- Consulted with IT on endpoint security control deployments, network configurations, and IT-led projects.
- Supported SOC 2 and HIPAA compliance readiness through evidence collection, control validation, and implementation to meet requirements.

Information Security Engineer / Senior Information Security Engineer
Vantiv (now Worldpay) | Sep 2014 – Aug 2016

- Managed endpoint security controls (McAfee, Bit9) for 10K+ corporate devices.
- Owned all enterprise web proxies for both corporate and production traffic, implementing a block policy against “unknown” domains, effectively mitigating over 85% of phishing attempts at the time.
- Worked closely with security analysts acting as a platform SME. Identified post-incident action items to mitigate gaps found during investigations.

Earlier Roles:
Fischer Homes – Information Systems Client Administrator (2012 – 2014)
Northern Kentucky Health Department – IT Intern (2012)

EDUCATION

Master of Science, Cybersecurity & Information Assurance – Western Governors University (2019–2020)
Bachelor of Science, Computer Information Technology – Northern Kentucky University (2007–2013)

CERTIFICATIONS

CISSP • OSCP • OSCE • OSWP • GCIH* • GWAPT* • GSEC* • CCSK* • CEH* • CompTIA Security+

*Previously Held