

STEPHANIE SHERWOOD

405.535.1920 • stephanie@radiantgrove.com • [linkedin.com/in/stephsherwood](https://www.linkedin.com/in/stephsherwood) • radiantgrove.com

Information Security Specialist with seventeen cumulative years in technology, fourteen of which are in security, with a heavy focus on offensive security. Seeking opportunities with an innovative, agile, and progressive company for which my generalist, consulting, offensive, and cloud security experience would enable desired and meaningful change for the organization while supporting my professional growth.

EXPERIENCE

FEBRUARY – MAY 2020

CLOUD SECURITY ARCHITECT, MIDFIRST BANK

Worked closely with traditional enterprise security, DevSecOps, development, and management teams on green field app development on the AWS platform to bring best practice and compliance aware security to both the platform and application. Educated on digital transformation, CI/CD, and DevSecOps to bridge regional in-house mid-sized enterprise thinking to modern cloud-enabled development, operations, security, and national application delivery thinking.

AUGUST 2016 – JANUARY 2020

SECURITY COMPLIANCE SPECIALIST, INTEGRIS HEALTH

Contributed as an embedded full-stack security resource within the Health Data Science /Clinical Informatics department where I focused on threat modeling, security architecture, cloud security, and secure coding. Delivered collaborative purple teaming. Developed repeatable MITRE ATT&CK based scenarios, leveraging hybrid cloud infrastructure, containerization with docker, bots, FOSS, automation, and integration with blue team SIEM/SOAR platform. Promoted DevSecOps culture. Performed attack simulations, application security assessments (DAST, SAST, IAST, manual code reviews), penetration tests, Secure SDLC improvements. Scoped and managed third party penetration tests. Managed and deployed phishing simulation and security education programs (Cofense & PSAT/Wombat). Provided O365 security architecture guidance, cloud security strategy guidance, high complexity troubleshooting, and much more.

DECEMBER 2015 – AUGUST 2016

SECURITY CONSULTANT, INDEPENDENT CONTRACTING

Delivered varied information security services, largely penetration testing, for several clients.

MAY 2015 – NOVEMBER 2015

SENIOR SECURITY CONSULTANT, TRUE DIGITAL SECURITY

Performed security program development, application code reviews, application penetration tests, network penetration tests, physical assessments, and policy writing. Responsible for managing existing client relationships and building new clientele in the Oklahoma City market.

NOVEMBER 2014 – APRIL 2015

SECURITY STAFF ENGINEER, SEAGATE TECHNOLOGY

Developed new frameworks, processes, and communication strategy for internal red team and threat intelligence programs. Championed modern risk management practices and information security

management system utilizing an ISO 27000/COBIT/NIST hybrid model and GRC platform. Performed local and cloud security reviews. Scoped and performed penetration and red teaming exercises.

JUNE 2014 – NOVEMBER 2014

SENIOR SECURITY CONSULTANT, NET SOURCE, INC.

Provided pre and post-sales support to existing clients for a wide variety of security appliances and software in a Sales Engineering role. Generated new client sales leads, while maintaining and growing existing client relationships. Created and delivered presentations on a variety of security topics. Performed penetration testing and application assessment services. Developed and delivered custom security policies for multiple clients.

APRIL 2011 – FEBRUARY 2014

SECURITY CONSULTANT, OPTIV (FORMERLY FISHNET SECURITY)

Provided security services including internal and external vulnerability assessments, internal and external penetration tests, wireless vulnerability assessments and penetration tests, phishing attacks, phone based social engineering, in-person social engineering, physical security assessments, PCI related assessments, and full red team engagements. Created, reviewed, and delivered comprehensive reports for executives, technical resources, and everyone in between. Improved test scheduling flexibility, reduced travel, reduced customer cost, and increased billable hours for security assessments by creating and maintaining a secure and standardized Linux penetration testing distribution and supporting infrastructure.

JUNE 2007 – MARCH 2011

INFORMATION SECURITY ENGINEER, INTEGRIS HEALTH

Developed and delivered presentations on security awareness topics for general, IT, and executive audiences. Developed a security professional training program that included classes, reading lists, book clubs, and videos. Developed policy, standards, procedures, metrics, and reporting for risk management (general program documents), risk assessments, risk analysis, vulnerability assessments, vulnerability disclosure, application assessments, and host configuration assessments. Performed application security assessments, configuration assessments, and vulnerability assessments in service of delivering risk assessment reports for new and existing systems. Operational responsibilities included IR lead, vulnerability management lead, and the daily management of nCircle IP360, nCircle SIH, SourceFire, Palo Alto NGFW, and Microsoft PKI. Worked on DMZ and other network segmentation and security projects. Deployed and/or administered Cisco ASAs, Checkpoint FW, McAfee Enterprise, Microsoft PKI, Palo Alto, nCircle IP360, SourceFire, ArcSight, Imperva, LogLogic, Proofpoint, ActiveScout Edge, Packeteer, and other solutions.

AUGUST 2005 – JUNE 2007

NETWORK TECHNICIAN, FIRST AMERICAN PROFESSIONAL LAND SERVICES

Created and updated policies. Created vulnerability management program. Performed password auditing, system hardening, awareness training, and executive education. Centralized logging. Maintained switches, routers, firewalls, servers, workstations, storage devices, remote users, load balances, and everything else.

SKILLS

- Programming – Numerous languages and experience levels with highest competency in Python
- Application Security
- Security Program Development
- Security Architecture
- Exploit Development
- Threat Modeling
- Red and Purple Teaming

- Penetration Testing
- Social Engineering
- Threat Intelligence
- Training & Education
- Compliance
- Sales
- Containerization – Docker
- Operating Systems
- Security Appliances and Solutions – Numerous
- Applications and Middleware – Numerous
- Wireless Security
- Physical Security
- Public Speaking
- Security Policy
- Client Relationship Management
- Cloud – AWS and Azure
- Automation and Orchestration
- Networking
- Databases – Numerous
- Enterprise Hardware – Numerous

EDUCATION

Briefly attended at the University of Oklahoma in pursuit of a B.S. in Computer Engineering in 2006.

PROFESSIONAL CERTIFICATIONS

- CISSP (expired, acquired twice)
- HITRUST CSFP
- Security +
- A +
- Various product certifications

TRAINING

- Conferences: Attended the vast majority of DEFCON events since DC9 (2001), many years of BlackHat Vegas, and numerous other local and regional security and tech conferences.
- Reverse Engineering with IDA Pro – Chris Eagle
- Reverse Engineering Win32 Malware with IDA Pro – Pedram Amini and Ero Carrera
- Effective Fuzzing: Using the Peach Fuzzing Platform – Michael Eddington
- Penetration Testing with Backtrack
- HITRUST (HIPAA) Training for Practitioners
- Innumerable product specific training classes.

COMMUNITY AND PUBLIC SPEAKING

- OKC2600 and DC405 Hacking Groups – I am the founder/co-founder and served as an organizer and hub for the Oklahoma City hacking scene from its inception and many following years.
- FBI InfraGard/ISSA OKC 1st Annual Information Warfare Summit – Wi-Fi Threatscape 2008: From Theoretical to YouTubeable (I also developed a large scale MITM attack tool for the talk.)
- ISSA OKC – Network Architecture: You're Doing it Wrong
- FBI InfraGard/ISSA OKC 2nd IWS– Live Hacking Panel/Demo
- DEFCON 19: I'm Not A Doctor but I Play One on Your Network
- RVAsec: I'm Not A Doctor but I Play One on Your Network 2.0
- FBI InfraGard/ISSA OKC 5th IWS Seeing and Believing: Setting the Frame and Gathering Information
- Security Binge – a pre-YouTube vodcast that covered a variety of hacker topics
- Contest organizer and judge for Defcon Wi-Fi Shootout – a Wi-Fi link distance competition in 03–05