Brad Woodward
brad@bradwoodward.io

Certifications

AWS SAP+SCS, OSWE, OSCE, OSCP, CRT, CISSP-ISSAP, CRISC, MCITP: EA, MCSA, OCM100

Presentation History

RSA: February 28th, 2020 - High Powered Hash Cracking with NPK
DefCon Skytalks; August, 2019 - [[Redacted]]
Hexacon; November 6th, 2018 - Building Your Way Out: Rooting the Google Container Build Service
ASIS International; May 12th, 2017 - Managing Risk and Optimizing Security in the Cloud
Seattle Technology Leadership Summit; March 20th, 2017 - Embracing (dis)Trust
Finance Executives International; May 19th, 2016 - Cyber-Fraud through Social Engineering
Kansas City ISSA; April 29th, 2016 - DevOps Security: Protecting the Pipeline
SnowFROC; February 18th, 2016 - Exploitation 101

Open Source Projects Managed

River Styx; Pure-native AWS AssumeRole broker for rapid cross-account console and CLI access.
Warcannon; Hyperscale parallel common-crawl WARC processing supported by a serverless fabric.
Hirogen; Federated identity exploitation tailored for use against AWS Cognito.
NPK; Mostly-serverless distributed hash cracking in AWS.

Relevant Experience

Security Practice Lead - Observian — May 2020 - Current

Championed the creation of novel tech enablement strategies to simplify customer onboarding, environment review, and cross-account privilege use in AWS in support of professional services customers. Some of these techniques were later developed into the open-source 'Styx' pure-native AssumeRole broker.

Assembled and deployed product solutions to encompass customer AWS accounts in full-stack behavioral analytics, endpoint protection, API-level anomaly detection, and compliance posture management. Created in-house SOC and associated procedures for triage, handling, and mitigation of breach indicators and identified vulnerabilities.

Presented in AWS- and other third-party-hosted webinars and training sessions to illustrate the capabilities of sophisticated adversaries against enterprise cloud environments.

Director; Labs - Coalfire — Sept. 2017 - April 2020

Led the spin-off and successful development of Coalfire's first fully-remote pentesting team. Successes here stem from an insight-based leadership style which empowers contributors to drive to their own goals, while developing a sense of community and camaraderie among geographically-distributed team members.

Demonstrated expertise in cloud services and security architecture through direct efforts and cross-training of colleagues; the most significant being the preparatory training for AWS, which culminated in a contract win worth approximately $3m. These cloud security and architecture skills, in combination with historic successes with project and people management, resulted in me being called upon to act as the engagement lead for Google and AWS simultaneously.

Developed NPK, a 'mostly-serverless' cloud-based password cracking system which significantly extends the capabilities of internal resources. Among its strengths is an easy-to-use UI, which provides easy insight into current and past campaigns.

Taught at BlackHat, presented at DefCon and Hexacon, and created Coalfire's in-house AWS Exploitation CTF to help develop cloud exploitation skills across the pentesting division.

Senior Engineer - AppliedTrust Engineering — May 2015 - Sept. 2017

Led multiple, successful HIPAA and NIST 800-66 security assessments for 10,000+ employee hospitals and large healthcare organizations, with exceptional conversion to ongoing remediation efforts. I also received unsolicited commendations for professionalism and expertise from executive leadership at many of these organizations.

Led and participated in multiple red team, social engineering, penetration test, and both generic and compliance-based security assessment engagements for clients ranging from small municipalities to multinational organizations. Researched and introduced many previously-unused attack vectors to significantly improve success rates and resulting security posture for the customer.

Developed multiple tools to drive business process improvements around AppliedTrust's assessment offerings, including substantial automation of reporting and better effectiveness in the QA process, resulting in higher-value deliverables.

Established a reputation for excellence in service delivery, people and project management, mentorship, and empowering my colleagues; successfully guiding several to new certifications and expertise in multiple fields.

Systems Management Specialist; Process/Tools Automation - IBM — July 2014 - May 2015

Responsible for configuring, monitoring, and maintaining Windows, Suse Linux, AIX, HP-UX, and Solaris servers on the Services Enablement Automation team, which maintains 160,000 servers worldwide.

Designed and deployed two 2008 R2 functional-level domains, championed the deployment of an ELK stack for log analysis, deployed GitLab for version control and continuous integration, and Zabbix for metrics and alerting.

Built a test automation procedure to standardize testing, maximize efficiency, and tighten developer feedback loops.

Senior Systems Administrator - Connect First — May 2013 - July 2014

Designed and built the STAGGR service augmentation and management platform, which facilitated rapid gains in capability maturity through fully-customized change management and end-to-end deployment automation.

Championed the implementation of an Active Directory Domain Services infrastructure, rebuilt the corporate network from the ground-up to provide greater functional segmentation, and implemented a procedure for CentOS 6 servers to authenticate and authorize users against Active Directory.

Implemented multiple technologies to centralize and simplify common maintenance tasks, improve visibility, and reduce administrative overhead. This included Zabbix for service monitoring and alerting, KVM for virtualization of supporting tools and applications, and Cacti for network monitoring and metrics aggregation.