Carter Jones
resume.carterjones.info

Infrastructure Security Team Lead • DevSecOps Team Lead • Principal Infrastructure Security Engineer
Infrastructure and Security Automation • Stakeholder Influencer and Avocate • Complex Project Execution
Secured PHI Data • Minimized Complexity • Increased Developer Velocity • Achieved Compliance
Strategically Focused • Results Oriented • Bias Toward Action • Scalability and Maintainability Prioritization

---

Employment experience

Nuna (remote) • Sep 2016 - Present

Staff Security Engineer • Mar 2018 - Present

- Improved the fundamental security of entire AWS accounts, complex systems, and cross-functional team processes as well as improved the maintainability and scalability of the infrastructure of multiple government projects by leveraging the client's strong focus on achieving adherence to a compliance standard (ARS 3.1).
- Provided efficiency, alignment, transparency, and clarity in multiple high impact commercial and government projects by crystallizing and amplifying the most high impact target goals of key stakeholders within multiple cross-functional teams.
- Influenced key stakeholders to prioritize making risk-based decisions based on practical risk (to both the business as well as the security of the infrastructure) rather than focusing on strict adherence to compliance checklists, while balancing the business's needs to deliver critical functionality on time that met mandatory compliance standards.
- Decreased maintenance burdens shared by multiple teams by prioritizing highly impactful tech debt removal efforts, inspiring teammates as well as other teams to target similar tech debt reduction opportunities. Achieved success with this effort through technical means as an individual contributor as well as a voice of influence.
- Lead multiple complex software upgrades by way of fast iterative improvements, favoring small change sets to remove tech debt, decouple tightly coupled code bases, and decrease the maintenance burden and general maintenance risk for future engineers.
- Enabled a 50% reduction in build and deployment time by prototyping loosely coupled, functionally-architected Jenkins pipelines that could replace highly fragile tightly coupled Jenkins freestyle jobs. This prototype served as the foundation for the eventual replacement that reached the 50% reduction in build and deployment time.
- Championed the DevOps concepts of continuous improvement through daily efforts in both an individual contributor capacity as well as a cross-functional team leadership capacity, successfully influencing change in priorities with key stakeholders (Product Owner, ISO) at the client as well as within our contracting organizations.
- Increased the visibility into security deficiencies in multiple projects by implementing open source utilities into CI pipelines (bandit, prowler, s3tk, OWASP ZAP), utilizing internal tooling that controlled Nessus, as well as created custom tooling where open source and COTS solutions were unavailable.

Senior Security Engineer • Sep 2016 - Mar 2018

- Empowered other employees through constant pairing, mentoring, and knowledge sharing about principles and best practices in security and infrastructure.
- Served as the security engineering subject matter effort on a team that brought a group of legacy systems into being HIPAA compliant.
- Created tooling to provide engineers with automated mechanisms to simplify management of Hashicorp Vault, such as internal TLS certificate management.
- Improved scalability of operations teams by leading an effort to migrate from manual user/group management of a COTS piece of software (Looker) to instead be backed by Active Directory groups.
- Provided security engineering perspectives on new technologies being considered by application teams.
- Managed multiple 3rd party penetration tests of Nuna's infrastructure, followed all the way through to remediation of vulnerabilities. Managed relationships with multiple 3rd party COTS vendors providing various security products (tCell, Immunio, Komand).

- Improved scalability of Nuna's corporate security team by leading the effort to roll out an internally managed endpoint trust management system (Duo Beyond), as well the integrated single sign on system (Duo Access Gateway).
- Designed and implemented a deployment architecture for a highly available security ChatOps COTS application (Komand), using continuous integration principles as the foundation for development and deployment.
- Lead the Security team in architecting and implementing a redeployable Nessus setup, which was used to scan Nuna's entire commercial AWS infrastructure.

Cigital (remote) • Jun 2014 - Aug 2016

Senior Security Consultant • Oct 2015 - Aug 2016

- Designed/implemented a hardened Active Directory deployment within AWS for a client.
- Built an automated blue/green server deployment infrastructure for a client using Chef.
- Provided technical review and oversight for both internal and client-facing projects.
- Contributed to emerging internal security consulting practices, expanding the scalable value that could be delivered to future clients by Cigital.

Security Consultant • Jun 2014 - Oct 2015

- Increased scalability of consultants by automating internal processes with custom tooling.
- Contributed to increased sales by scoping projects and providing technical insight as part of sales pipelines.
- Improved the security posture of clients by conducting security assessments (red team, thick client, web app, network, source code review, and information security analysis reviews) and delivering detailed reports including findings, evidence, risk analysis, and remediation recommendations.

BeyondTrust (formerly eEye Digital Security) (Irvine & Aliso Viejo, CA) • Feb 2010 - May 2014

Security Research Engineer • Jun 2011 - May 2014

- Delivered executive analysis of over 100 Microsoft security patches to customers through the use of a combination of write-ups from the Microsoft MAPP program, as well as through the use of tools such as IDA Pro, DarunGrim, and ILSpy (sample).
- Generated marketing leads by co-leading over 30 monthly webinars discussing Microsoft security bulletins and recent security news.
- Delivered exploit and vulnerability details to our customers for 15-20 exploit toolkits on an ongoing basis. Details were sent via product data streams (Retina CS).
- Produced an exploit metadata importing utility in C# that pulled info from Metasploit and supplied the data via our customer-facing product, Retina.
- Delivered internal and external network penetration tests using Retina, Nessus, Metasploit, and Core Impact.

Security Research Intern • Feb 2010 - Jun 2011

- Analyzed 5-10 Microsoft security bulletins monthly, providing practical mitigation strategies to clients in the form of executive reports.

Canon Development Americas, Inc • Jun 2009 - Jan 2010

Security Research Intern

- Wrote a proof of concept to trigger a vulnerability in a Java application embedded in printers, documented analysis techniques, and shared reports internally.

Education

University of California: Irvine • Irvine, CA • 2011 • Bachelor of Science in Computer Science

Projects and keywords

github.com/carterjones/infrastructure • github.com/carterjones/nix-config • github.com/carterjones/signalr

DevSecOps • Infrastructure as Code • Infrastructure Security • Application Security • Security Automation • Continuous Integration • Configuration as Code • Secure Code Review • Terraform • Docker • Packer • Vault • AWS • IAM • EC2 • Route53 • RDS • CloudFormation • Config • Python • Golang • Bash • C# • C • C++ • HTML • JavaScript • Java