**Carter Jones**
resume.carterjones.info

**Summary**
Product security researcher and engineer with experience an individual contributor, technical lead, mentor, and manager. I performed deep dive product vulnerability analysis across numerous product lines and subsequently managed a team of product security researchers doing the same as a part of the Palo Alto Networks Product Security Incident Response Team (PSIRT). As a Product security engineer, I improved the security posture of AWS accounts across multiple clients and projects through direct action, as well as influenced key stakeholders to re-align their own goals to meet organizational security needs. With a background that spans endpoint and hosted product security, cloud infrastructure security, security engineering, offensive security, security research, and automation of all kinds, I will help expand your organization's security capacity, scalability, and maintainability.

**Employment experience**

**Palo Alto Networks (remote) • May 2022 – Present**
*Senior Manager, Vulnerability Discovery and Disclosures • Nov 2024 – Present*
- Published and managed high profile advisories on the Palo Alto Networks Security Advisory website.

*Manager, Vulnerability Discovery and Disclosures • Feb 2024 – Nov 2024*
- Performed deep dive analysis of numerous product vulnerability reports, identified root causes (both functionally and specific lines of code), guided product engineering to ultimate solutions, and verified the efficacy of fixes.
- Facilitated the resolution of customer security concerns by working directly with customers, product management, and engineers. Provided clear guidelines to the product team to ensure remediations were effective and complete.
- Drove visibility of SLA misses for remediation efforts by creating simple and effective self-service portals for multiple audiences (product management, InfoSec management, technical product management).
- Published and managed numerous high profile advisories on the Palo Alto Networks Security Advisory website.
- Onboarded, mentored, and managed a team of product vulnerability researchers who performed the core responsibilities of PSIRT. Drove career growth through frequent 1:1s and collaboration sessions, followed by more formal performance reviews on a 6-month basis.

*Senior Staff Product Security Researcher • May 2022 – Feb 2024*
- Performed deep dive analysis of numerous product vulnerability reports, identified root causes (both functionally and specific lines of code), guided product engineering to ultimate solutions, and verified the efficacy of fixes.
- Developed proof of concept exploits to demonstrate the specific mechanisms of vulnerabilities to the product teams, which could be used to demonstrate the severity and practicality of vulnerabilities, as well as verify the efficacy of fixes.
- Lead the remediation process for numerous Palo Alto Networks product vulnerability reports, from initial report triage, to collaborating with the engineering team to provide guidance and assist with reproduction when needed, and ultimately publishing advisories on https://security.paloaltonetworks.com.
- Ensured clear communication, set expectations, and facilitated information flow with reporters (customers, researchers, partners, etc.) by serving as the face of InfoSec over written communications.
- Reenforced team resilience by documenting numerous procedures only shared through tribal knowledge.
- Established robust automations and infrastructure as code by migrating multiple hand-crafted systems used to support the team's efforts to systems automatically built by Docker and Packer, that were entirely deployed via Terraform.
- Significantly improved the team's efficiency by refining our existing tooling, so we could apply our focus toward technical analysis, rather than spending time on automatable tasks.

**Truss (remote) • Oct 2020 - May 2022**
*Senior Infrastructure Security Engineer • Oct 2020 – May 2022*
- Improved the network defense and compliance of an AWS-based web application by leading the design and implementation of a network connection to and through NIPRNet, a secure DoD-managed network.
- Mentored team members on infrastructure security via pair programming.
- Lead the technical evaluation of a system's adherence to PostgreSQL STIG requirements.
- Minimized the risk exposure of an RDS-based PostgreSQL database by re-architecting the database connections to follow the principle of least privileges; modified unit tests to verify the new architecture design.
- Reduced technical debt and overall system complexity by combining Terraform modules.

**Nuna (remote) • Aug 2016 - Oct 2020**

*Staff Security Engineer • Mar 2018 - Oct 2020*

- Improved the foundational security of multiple 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).
- Developed cross-functional alignment through transparent and clear communication in multiple high impact commercial and government projects.
- Influenced key stakeholders (Product Owners, ISSO) to prioritize making risk-based decisions based on practical business and technical risks rather than focusing on strict adherence to compliance checklists, while still meeting mandatory compliance standards.
- Crystallized and amplified the highest impact goals of key stakeholders within multiple cross-functional teams.
- Decreased maintenance overhead shared by multiple teams as both a voice of influence and as an individual contributor by prioritizing highly impactful tech debt removal efforts, inspiring members of the organization to target similar tech debt reduction opportunities.
- 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 burdens and risks 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.
- Championed the DevOps concepts of continuous improvement on a daily basis in both a cross-functional team leadership capacity and as an individual contributor.
- Increased visibility into security deficiencies in multiple projects by implementing open source utilities into CI pipelines, utilizing internal tooling that controlled COTS vulnerability scanners, as well as created custom tooling where open source and COTS solutions were unavailable.

*Senior Security Engineer • Aug 2016 - Mar 2018*

- Worked shoulder to shoulder with other employees through constant pairing, mentoring, and knowledge sharing about principles and best practices in security and infrastructure.
- Was the security engineering subject matter expert on a team that made a group of legacy systems HIPAA compliant.
- Created internal tooling to simplify use of Hashicorp Vault, such as internal TLS certificate management tooling.
- 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 reviews of 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 security product vendors.
- Improved scalability of Nuna's corporate security team by leading the effort to roll out an internally managed endpoint trust management system, as well as an integrated single sign on system.
- Designed/implemented a CI deployment architecture for a highly available security ChatOps COTS application.
- Lead the Security team in architecting and implementing a redeployable Nessus setup that scanned Nuna's entire commercial AWS infrastructure.

**Cigital (remote) • Jun 2014 - Aug 2016**

*Senior Security Consultant • Oct 2015 - Aug 2016 (Security Consultant • Jun 2014 - Oct 2015)*

- Designed/implemented a hardened Active Directory deployment within AWS using a blue/green deployment model.
- Provided technical review and oversight for both internal and client-facing projects.
- Expanded the scalable value that could be delivered to future clients by Cigital by automating internal processes with custom tooling, as well as contributing to emerging internal security consulting practices.
- 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 (Security Research Intern • Feb 2010 - Jun 2011)*

- 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 reverse engineering tools (sample).
- Co-lead 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 paid product data streams.

- Designed and implemented an exploit metadata importing utility that pulled from Metasploit and supplied the data via our proprietary vulnerability scanner.
- Performed internal and external network penetration tests.

**Canon Development Americas, Inc (Irvine, CA) • 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 presented reports internally.

**Select blog posts from blog.carterjones.info**:
- CVE-2014-0301 Analysis: https://blog.carterjones.info/cve-2014-0301-analysis/ (Reddit post)
- Halo Hacking: https://blog.carterjones.info/halo-hacking/
- DarunGrim with Symbols: https://blog.carterjones.info/darungrim-with-symbols/
- XPDF Fuzzing: https://blog.carterjones.info/xpdf-fuzzing/

**Select projects from github.com/carterjones**:
- github.com/carterjones/nouzuru: a library for simple development of memory analysis software on Windows
- github.com/carterjones/halo-trainer: a game trainer for the PC version of Halo
- github.com/carterjones/infrastructure: my personal infrastructure as code (Terraform, Docker, CI)
- github.com/carterjones/nix-config: my personal *nix system configuration script used to configure MacOS and Linux
- github.com/carterjones/signalr: SignalR WebSocket client written in Golang used for cryptocurrency trading

**Technologies**
- GCP: VPC, IAM, CloudRun
- AWS: IAM, EC2, S3, ECS/Fargate, RDS, KMS, Config, CloudFormation, Route53, DirectConnect, VPN, NAT, VPC
- Languages: Go, Python, Bash, Terraform, C#, C, C++, HTML, JavaScript, Java
- Infrastructure Engineering: GitHub Actions, CircleCI, Jenkins, Docker, Packer, Vault, Chef
- Security engineering tools: Bandit, Prowler, s3tk, CS Suite, Duo Beyond, Duo Access Gateway
- Defensive security tools: tCell, Immunio, Komand
- Offensive security tools: OWASP ZAP, Burp Suite, Nessus, Metasploit, Core Impact, IDA Pro, DarunGrim, ILSpy

**Certifications:** CASP+, Security+
**Concepts:** Vulnerability Remediation, Responsible Coordinated Disclosure, DevOps, Infrastructure as Code, Infrastructure Security, Application Security, Security Automation, Continuous Integration, Configuration as Code, Secure Code Review
**Education**: University of California: Irvine • Irvine, CA • 2011 • Bachelor of Science in Computer Science

*Carter Jones*