EMAIL   james@hale.dev
WEB   hale.dev

JAMES HALE
SECURITY ENGINEERING LEADERSHIP

Security engineer with over twelve years of experience. Specializing in architecting and deploying secure and scalable systems with high availability, using cloud-based and on-premises infrastructure resources, including hybrid solutions.

DevOps and security-focused. Experienced in Agile methodologies, including Scrum and Kanban.
Leadership experience

Specialties include: AWS, Terraform, CI/CD, Identity mechanisms, and security automation.

EDUCATION/CERTIFICATIONS

University of Massachusetts Amherst - B.S. Computer Science (2009)

AWS Certified Solutions Architect - Professional (2017)
AWS Certified Security - Specialty (2019)
Certified Information Systems Security Professional (CISSP) (Feb. 2020)

SKILLS

Security Policy Tools	Open Policy Agent (OPA), Checkov
Identity Federation	SAML, OpenID Connect, Okta, Keycloak, AWS IAM
Coding	Python, Golang, Ruby, Groovy, PHP, Perl, YAML, JSON
Configuration Management	Terraform, Puppet, Chef, Ansible, SaltStack
IaaS Platforms	AWS, VMware, Google Compute Engine, OpenStack
Container technologies	Docker, Kubernetes, Mesos, AWS ECS and EKS
Other Security Tools	Nessus, OSSEC, Nmap, Kali Linux, Metasploit, Snort, Burp Suite

- Primarily focused on creating fault-tolerant, highly-available, and secure systems across a multitude of platforms
- Expertise with cloud and on-premises infrastructure (IaaS/PaaS) platforms, including designing and implementing hybrid solutions.
- Security-minded. Aim to identify, assess and remediate risk and vulnerabilities in platforms.
- Strive to provide infrastructure as a service to software developers and facilitate their deployment tasks without increasing risk exposure to the platform.
- Experience with automating deployment and administration tasks with Infrastructure-as-code, and configuration management solutions.
- Knowledge of data center, SOC, and NOC operations.

WORK

Senior Manager, Security Engineering
Salesforce

July 2021 – Present
Virginia

- Manage a team of 8 engineers. Drive career development discussions, talent reviews, and interview panels. Ensure members of the team are on the right track with engineering deliverables.
- Coordinate engineering resources with partner teams.
- Participate in security architecture discussions and provide input to key decision making. Taking the output of these discussions and delivering it to my team and other stakeholders as engineering deliverables.
- Provide technical leadership and guidance, mentor junior engineers, and participate in code reviews.

Lead Security Engineer
Salesforce

June 2020 – July 2021
Virginia

- Technical lead for a team of three engineers. Drove Agile development, acting in Product Owner and Scrum Master roles.
- Co-authored a project to implement Terraform static code analysis as part of the CI/CD pipeline, using Checkov, eventually scaling up to company-wide use.
- Responsible for design and implementation of security solutions using AWS native services in GovCloud.

Senior Systems Security Engineer
Salesforce

April 2018 – June 2020
Herndon, VA

- Maintained AAA (Authentication, Authorization and Accounting) infrastructure for Salesforce's core product used by public sector customers.
- Led effort to deploy Terraform across the Government Cloud infrastructure. Focused on AWS GovCloud Identity and Access Management.
- Designed federated authentication and centralized logging mechanisms in AWS GovCloud.
- Used Puppet and other configuration management frameworks to implement security controls for FedRAMP Moderate and High, and DISA IL4 compliance.

Senior DevOps Security Engineer
Team Lead, Security Automation Engineering
Blackboard

November 2016 – April 2018

Washington, D.C.

- Researched, designed, developed, documented and implemented solutions for fault tolerance, performance, capacity, and configuration management for various data center operations.
- Defined, planned, designed, and evaluated information security systems.
- Designed, implemented, and maintained security infrastructure.
- Led a team of security automation engineers to identify platform vulnerabilities, help design and implement security solutions.
- Contributed to and maintained security posture of the platform.
- Served as a mentor to other Security and DevOps engineers.
- Designed, developed and implemented documentation or tools to facilitate Technical Support team responsibilities.
- Identified and drove opportunities to improve automation for deployment, management, and tooling, using Python, Ruby and Groovy, among other languages.
- Supported and improved a highly available and fault tolerant SaaS offering.