

EMAIL james@jameshale.net

WEB jameshale.net

JAMES HALE

INFRASTRUCTURE SECURITY ENGINEER

Security engineer with over eight 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, VMware, networking, automation and security.

EDUCATION/CERTIFICATIONS

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

AWS Certified Solutions Architect - Professional - 2017

SKILLS

Information Security	Nessus, OSSEC, Nmap, Kali Linux, Metasploit, Snort, Burp Suite
Languages:	Python, Golang, Ruby, Groovy, PHP, Perl, YAML, JSON
Configuration Management:	Puppet, Chef, Ansible, SaltStack.
IaaS Platforms:	AWS, VMware, Google Compute Engine, OpenStack
Container technologies:	Docker, Kubernetes, Mesos, AWS ECS

- Primarily focused on deploying fault-tolerant, highly-available, and secure systems across a multitude of platforms
- Expertise with cloud and on-premises infrastructure platforms, IaaS/PaaS, 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 configuration management platforms.
- Knowledge of Datacenter and NOC operations.

WORK

Senior Systems Security Engineer

April 2018 – Present

Salesforce.com, Herndon, VA

- Maintain AAA (Authentication, Authorization and Accounting) infrastructure for Salesforce's core product.
- 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.
- Use 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*

November 2016 – April 2018

Blackboard, Washington, D.C.

- Research, design, develop, document and implement solutions for fault tolerance, performance, capacity, and configuration management for various data center operations.
- Define, plan, design, and evaluate information security systems.
- Design, implement, and maintain security infrastructure.
- Lead a team of security automation engineers to identify platform vulnerabilities, help design and implement security solutions.
- Contribute to and maintain security posture of the platform.
- Serve as a mentor to other Security and DevOps engineers.
- Design, develop and implement documentation or tools to facilitate Technical Support team responsibilities.
- Identify and drive opportunities to improve automation for deployment, management, and tooling, using Python, Ruby and Groovy, among other languages.
- Support and improve a highly available and fault tolerant SaaS offering.

Senior Infrastructure Engineer

January 2015 – November 2016

The Washington Post, Washington, D.C.

- Implement ephemeral, long-lived and immutable infrastructure as code, using AWS CloudFormation and internally-built solutions.
- Maintain infrastructure resources in an auditable and repeatable fashion using configuration management platforms and version control systems.
- Responsible for designing and implementing robust network and security architectures.
- Help to maintain a strong information security posture for data in transit and data at rest.
- Provide expertise to software developers on AWS services and best practices, such as EC2 (incl. EBS, ASG, ELB), VPC/Direct Connect, Route53, S3, IAM/KMS, RDS, SNS, SQS, SES, and CloudWatch.
- Contribute to internal software projects, centered around the orchestration of infrastructure resources and the continuous deployment of containerized applications to test and production environments.

Unix Systems Engineer

December 2011 – January 2015

The Washington Post, Washington, D.C.

- Managed physical and cloud-based infrastructure for the print, mobile, and web properties of Washington Post Media
- Supported content management systems and applications utilizing Apache, Nginx, Tomcat, and dynamic Java applications deployed on Glassfish and WebLogic application servers.
- Maintained Unix production, stage, and test environments, utilizing RedHat 5/6/7, CentOS 5/6/7, Solaris 9 & 10, AIX 5.3, HP-UX and Mac OS X Server
- Performed code deployments for development teams
- Carried out system maintenance and upgrades as needed, including backups and restorations
- Participated in 24x7 on-call rotation
- Assisted with a major data center relocation

Client Systems Engineer

September 2010 – December 2011

The Washington Post, Washington, D.C.

- Developed and maintained Windows and Mac desktop images, software deployments, and application patching while also identifying and resolving desktop security issues.
- Provided technical expertise to assist with implementation of desktop technologies: Windows and Mac desktops and laptops and their operating systems, desktop applications, management systems, and tools
- Created and supported desktop management related technical policies and procedures; helped to create and maintain related documentation.
- Administered and assisted in deploying LANDesk 8.8 & 9 environments and Symantec Endpoint Protection for a client base of 3000+ machines.
- Deployed regularly scheduled and out of band security/OS patches and updates via LANDesk and other mechanisms.
- Co-developed an asset management system to track physical assets via barcode scanning devices.

System Support Analyst

July 2009 – September 2010

Washingtonpost.Newsweek Interactive, Arlington, VA

- Actively monitored an extensive production environment for washingtonpost.com and other high-traffic Post properties
- Acted as a liaison between coworkers and the development and infrastructure technology teams
- Provisioned, integrated, diagnosed, and maintained PC and Macintosh clients in an Active Directory environment