Jordan Conard

jordan.conard3@gmail.com

Work Experience

May '20 - *Current* | Senior Detection Engineer - Spotify, New York City

- Lead the Security Incident Response program operating a 24/7/365 rotation across U.S. and European time-zones consisting of over 30 responders.
- Developed security threat detections to more quickly identify malicious behavior and alert notification pipelines which prompted users for confirmation to reduce the likelihood of a false positive alert.
- Created a Blue Team 'Capture The Flag' around an example intrusion into a GCP GKE cluster as a Kubernetes and investigation training exercise for two dozen Security Responders.
- Performed due diligence for the Chartable acquisition in coordination with Corporate and Infrastructure teams. Lead the Security on-boarding of Chartable into Spotify's security program and assisted them in increasing their incident response preparedness.
- Transitioned SIEM platforms from Splunk to Google Chronicle to better investigate security events and reduce response time.

Feb '18 - May '20 | Senior Security Operations Engineer - MailChimp, Atlanta

- Created and lead the Security Operations team of three people to oversee defensive security in the Operations department.
- Lead a year long project to revamp Secure Shell (SSH) access across the company using Okta Advanced Server Access (Okta ASA), an Okta-based zero-trust service.
- Implemented a security logging, monitoring, and alerting pipeline in GCP using Forseti, Cloud Security Command Center (CSCC), and other GCP managed services.
- Built a security information and event management (SIEM) platform using Elasticsearch (ES) Auditbeat to aggregate auditd, authentication, and network logs.

Jan '15 - Feb '18 | Systems Engineer - MailChimp, Atlanta

- Scaled infrastructure, monitoring and tooling to support a 10 million doubling of customers in just over three years.
- Lead a five person team to perform a risk analysis against Spectre/Meltdown, plan the mitigation strategy, and execute it across the entire company.

Skills

Languages:	Go, Python, Bash, Puppet, Terraform, Scala
Platforms:	CentOS, Ubuntu, GCP, Amazon Web Services (AWS)
Software:	Google Chronicle, Splunk, Elasticsearch (ES), Kubernetes, Github, Jira
Security Tools:	AWS CloudTrail and GuardDuty, GCP CSCC, Capsule8, OSQuery, auditd

Education

2009 - 2014	Bachelor of Science in Computer Engineering Georgia Institute of Technology, Atlanta