Matt Burdan

+1 (415) 542 6132
burdz@burdz.net
@burdzwastaken
https://www.linkedin.com/in/burdz/
https://github.com/burdzwastaken
Last Updated: June 24, 2021

Summary

Senior Platform and Security engineer with a huge passion for open-source who specializes in deploying, maintaining, monitoring and operating software on CI/CD architecture for on premise and multi-cloud infrastructure using legacy deployment tools, cloud tooling and container orchestration. Experienced in administration, installation, configuration, tuning and upgrades in all flavours of Linux. Strong background in cloud security tooling, digital forensics, and network security having studied, deployed, monitored and designed rulesets for multiple different security tooling monitoring thousands of endpoints and helped achieve FedRAMP compliance within large enterprises.

Skills

Operating Systems

: Linux BSD Windows OSX

Languages

: Golang Python Bash Groovy Ruby Perl

Technologies

: AWS GCE GKE Azure Kubernetes Helm Docker OCI Harbor Istio Service Brokers Spinnaker Chef Terraform Ansible Saltstack Consul git Packer Jenkins Concourse Cerberus Vault Splunk SumoLogic Phantom DataDog osquery kolide OSSEC auditd SeLinux PKI EnCase TheSleuthKit GRR Nexpose Qualys Nessus Nmap Wireshark Bro tcpdump sops DNS

Education

2012-2014 Bachelor of Science; Cyber Forensics, Information Security Management and Business Information Systems; Murdoch University
2011-2012 Diploma; Information Technology; Kaplan Singapore
2005-2009 Guildford Grammar School

Experience

MuleSoft

Senior Platform Engineer San Francisco, CA August 2017 - Current

- Operated the entire lifecycle and management of Harbor, our internal OCI registry. The registry was deployed via Helm to Kubernetes, Configured with Terraform and utilizing all features including centralized authentication, replication to ECR and security scanning of all images using Clair
- Extended Kubernetes using CRDs and service catalog API to provide extended functionality such as IAM credentials to pods, Public cloud infrastructure provisioning and service mesh injection
- Automated the entire incident process including alerting, documenting and recording of all incidents using Slack, Pagerduty, Jira and NewRelic
- Own the reliability of production systems across development and production environments in US, EU and AWS GovCloud
- Integrated Terraform, Ansible, Packer to create and version the AWS Infrastructure, designing, automating, implementing and sustainment of Amazon machine images (AMI) across the cloud environments
- Lead the implementation of secure cloud architecture best practices & Pioneered Infrastructure-As-Code wherever possible
- Integrated NewRelic as an automated, unified monitoring platform and reduce MTTR
- Architected, deployed and operated high traffic micro-services on multi region large scale deployments to manage over sixty thousand runtimes by operating the core platform to ensure consistency, availability and reliability using tooling such as Kubernetes, Spinnaker and Jenkins
- Automated monitoring and observability for all critical Core Platform services
- Actively involved and hands-on in writing infrastructure tools and services for internal teams in Go, Python, and Bash
- Developed and maintained automation to manage our cluster automation to securely upgrade our running clusters both in-place and through a multi cluster model with DNS based cut overs for zero downtime to our internal and external customers

Lookout, Inc

Senior Security Engineer San Francisco, CA January 2015 - August 2017

- Produced weekly hardened AMIs for multiple flavours of Linux which all of Lookout Infrastructure is deployed on. This was achieved using packer and debian packages deployed through Spinnaker. This allowed us to achieve federal compliance
- Deployed and responsible for Cerberus - an opensource tool for Secrets management. This has been integrated with our CI/CD pipeline along with being used by all services for secure transportation of secrets
- Deployed and maintained infosec Kubernetes clusters running CoreOS. All security microservices were migrated to this cluster

- Created and managed entire PKI infrastructure including multiple offline Certificate and Validation Authorities, OCSP responders and our public facing certificates
- Architected completely automated vulnerability management system using Nexpose and Nessus deployed with terraform and chef within AWS
- Managed the Intrusion Detection System (IDS) infrastructure and responded to all suspicious traffic alerts with all office and datacenter networks
- Secured all Lookout AWS accounts using a mix of open source and in house tool hosted in containers and AWS lambda
- Architected the deployment of all security monitoring tools at Lookout. This included osquery, ossec auditd, GRR agent, scout2, security monkey and developed the process of responding to all alerts triggered
- Migrated all security tools from the DataCenter to AWS including internal PKI infrastructure
- Created environments for contractors to securely connect to our infrastructure. This included bastion hosts which are monitored, have secure key exchanges, fine grained policies that only allow for them to access the resources that are necessary
- Developed automated process to securely erased all sensitive PII data on our physical hardware during the migration to AWS
- Held company wide phishing campaigns using the tool GoPhish and custom templates. This allowed InfoSec to teach and promote security awareness throughout the organisation. This was deployed using Kubernetes and docker
- Member of the Principal working group for AWS best practices
- Member of the AppSec Champions initiative to promote security best practices across the engineering organisation
- Participated in the Lookout migration to AWS which allowed for our consumer product to have zero downtime and function within the cloud
- Developed a code review pipeline for AWS IAM policies in production. This allowed for a source of truth for all policies and the tightening of permissions within production
- Provided DFIR analysis to all potentially infected machines within all Lookout network's
- Created a tool (in golang) that allowed secure bootstrapping of systems from s3. This meant we were able to keep secrets out of plaintext repositories and into s3 buckets protected by IAM / bucket policies
- Developed an osquery table extension that allowed the collection of AWS tags through the use of a role. This allowed our AWS tags to be ingested into our security event system
- Developed multiple bots using AWS lambda functions with API gateways for various different functions
- Developed processes and procedures for offboarding users. Often was responsible for offboarding employees with production access
- Helped remediate issues and communication with researches through our bug bounty program with HackerOne

Ultimatum, Inc

CSO, CIO San Francisco, CA 2015 - 2018

- Architected and deployed secure CI/CD infrastructure
- Automated all backend architecture for creation of new environments
- Maintained and updated all clusters that the Ultimatum platform runs on
- Created monitoring for all microservices within the Ultimatum platform
- Implemented a secure way of handling all company and environment secrets that allowed version control for audits

Newedge - Societe Generale

Onboarding Analyst Singapore August 2014 - December 2014

- Managed the implementation and onboarding of new client accounts
- Perform initial sanity checks on documentation packages ensuring all activities are captured, accurately reviewed and processed in a timely fashion
- Dealing with customers' requests concerning different changes on their accounts
- Automated communication required to advise customers on changes to their accounts

Self Employed

Swimming Instructor Singapore 2009 - 2014

- Created lesson plans for all students
- Facilitated the certification process within the swimming lesson
- Handled all finances and scheduling management

Perth Duty Free

Warehouse Operations Perth 2010 - 2012

- Preparing and completing orders for delivery or pickup according to schedule
- Receiving and processing warehouse stock products
- Performing inventory controls and keeping quality standards high for audits

Dimension Data

Work Experience Perth 2009

- Configuring and deploying Cisco routers

References

will provide at request

will provide at request