417 Thin Edge Rd.
Santa Cruz CA 95065

Andrew Yasinsky

(415) 341-6424
andrew@yasinsky.com

SUMMARY

Software engineer 15+ years of experience in Cybersecurity, data processing, DevOps. Cloud/VM/Bare metal.
US Citizen, MSEE
Looking for hands on Development, Data Eng, DevOps roles

- Last 10 years using data to make networks safer in real time
- Large scale telemetry Kafka, Go, kqlDB into ES, Clickhouse, InfluxDB, S3, Mongo and Logstash.
- L3 (ddos)/L7 (waf/bot) security BGP/GRE, cloud, metal
- Writing cloud native meshed micro services and Apis in Golang, AWS, Envoy.
- Writing Gitlab CI/CD tooling scripts to AWS ES anywhere.
- Capturing and enriching SLOW, IPFIX, SNMP, DNS queries, L3 IP blocks.
- Grocking syslog streams with Logstash/kConnect, overlaying with BGP network's configuration changes and dictionaries producing patterns for MLOps use.
- Developing and maintaining ETL and timeseries pipelines and data stores Goflow/Logstash/Go/kqlDb
- Design, migrations, capacity planning, modeling, indexing/mapping, upgrading data stores.
- PCI/Fedramp compliance.
- Good chunk of my time spent mentoring devs on edge and streaming technology.

SKILLS

- Linux, AWS ECS/EC2,Docker, Kvm, Kubernetes, Vagrant
- Go, C, Python, Bash, PHP, Java, Ruby
- Stream/Parallel/Multi-thread/process/Evented/Microservices/Mesh design patterns.
- Kafka ecosystem (Zoo, kconnect, kschemas, kqlDb)
- ES ecosystem, Kibana, Logstash
- Clickhouse, MongoDb, Redis, InfluxDB, Postgress, MySQL
- Prometheus, Superset, Ganglia, Elastiflow, Nagios, Grafana, Statsd
- Nginx,HAProxy, ZMQ, MQTT,Varnish, Envoy, Istio, RPC, Thrift
- Gitlab, Jira, Confluence, librenms
- TLS, X.509, Auth0,JWT security
- Sflow, netflow, ipfix, snmp, Otel, mqtt, http2/3
- IPv4, IPv6, TCP/UDP, DNS, GRE, BGP, Sflow, Ipfix, Snmp, wireshark, tcpdump
- http://andrew.yasinsky.com
- https://github.com/n0needt0
- https://www.linkedin.com/in/andrewyasinsky/

Professional Experience

Software Engineer Architect May 2017 to Present
Neustar (Acquired by TransUnion now vercara.com)

- Tech lead for observability/ML infosec project agile team
- Collect/normalize/enrich/augment TBs of streaming network data centers (Sflow/Ipfix/Snmp), security logs (Citrix/Arbor/CEF), Otel, WEB/DNS/Application logs, Security Exceptions, Blocked Ips.
- 15 multi-homed BGP routed data centers *5 AWC VPCs*
- Built services in Golang ported envoy proxies for WAF and DDOS mitigation
- Developed gQL and REST APIs.
- ES schema/mappings/object indexes/shard rotation and merge
- Timeseries ingestion tsdb/influxdb2 tables
- Clickhouse tables, aggregations and materialized views design
- Network router config changes parsing from router config files to MongoDB
- Agile team Working with PRDs and ERDs
- Monitoring and SLAs

417 Thin Edge Rd.
Santa Cruz CA 95065

Andrew Yasinsky

(415) 341-6424
andrew@yasinsky.com

Principal Software Engineer Oct 2014 to May 2017
Fortinet Inc
www.fortinet.com

Cloud performance team. Micro services monitoring and optimization in Public/Private environments on Debian, Kali, FortiOs and CoreOs via Docker, KVM.
Our group is small team of experienced engineers operating across Network/OS/Providers/Security and application boundaries striving to bring carrier grade performance to variety of internal and cloud facing services. We are “go to” group to release new or give legacy product some more time to live

FORTIDIRECTOR - Smart CDN BGP frontend DNS and HTTP rule engines
FDOS – Network and services monitoring & DDOS mitigation. Scale to support carriers DNS, HTTP, SMTP, SQL (about 20 protocols and service) monitoring anything that can be ddosed FDOS is FPGA based so we only work on stats collection via UDP-> Statsd->Whisper

FORTI SA – Attack surface monitoring, recon and intrusion monitoring product with REST API
A mesh of micro services integrating various test tools via REST and RPC in Kali Linux env.

My day consists of :

1. Attaching to production or creating test environments via Vagrant/Chef or lately Terraform in Cloud (we use AWS/Linode or local KVMs)
2. Writing custom network tools in GO , for instance if I need to simulate SYN DDOS flood @10G
3. Run long running timeseries stats into Statsd->InfluxDB->Graphite/Ganglia or to logs on Hdfs or Elastic
4. Identify problems: network, architecture, framework or language “features”, SQL or NoSQL problems
5. Working with developers on optimization from SQL indexes to JVM heap analysis.
6. Setup and break it again :)

Director Information Solutions May 2011 to Oct 2014
HelpPain Medical (acquired by Stanford Health)
www.helppain.net

High energy medical startup in chronic pain management and schedule 1 prescriptions.
Changing pain medicine through Integration, Big Data analysis ELK, mobile devices with real time outcomes and in constrains of HIPAA/DEA regulations. Hands on lead of small agile development team.
Go/ES/React/Nginx

Principal Software Engineer Dec 2009 to May 2011
3Crowd (aka XDN) Networks (acquired by Fortinet)
www.3crowd.com

- First engineering hire for this smart DNS/BGP CDN.
- Developed DNS rule engines, asset monitoring and alerting systems
- OpenDNS, Mysql, C, PHP, Perl, Redis, Esper, Hadoop, JS GUI Libs.

Education: 1991 MSEE Saint Petersburg, Russia