resume

jon spearheads technical projects spanning backend and frontend development, cybersecurity, machine learning, and mobile and desktop apps. as comfortable with legacy code as greenfield work, he can take a general customer need and shepherd it through r&d to production, fleshing out an idea to a complete backend and frontend stack that can perform at scale.

a self-taught programmer, jon got his start in open source, contributing massive core enhancements and significant improvements to handbrake, an award-winning project, where he received his first exposure to the practical use of deep neural nets for signal filtering.

he then worked on endpoint agents for the market research industry at nielsen, using low-latency kernel extensions and browser extensions in techniques he patented there to fingerprint user behavior based off of encrypted network traffic.

he also has years of experience in mobile development for commercial field operators at nitro mobile solutions, pushing the boundaries of the iphone and ipad to bring complex backend data systems to life within the resource and connectivity constraints of edge computing.

jon was a day zero hire for the core engineering team at threatwarrior, a cybersecurity startup that uses unsupervised deep learning to hunt for network threats. at threatwarrior, jon focused on machine learning and backend data processing pipelines, infrastructure as code, cloud technologies, data visualizations, and the network packet analysis stack. jon architected threatwarrior's anomaly detection machine learning models as well as their kubernetes-based training and deployment harness. he was also responsible for designing and implementing their device profiling user behavior tracking system and prototyped its distinctive user experience. jon's contributions to threatwarrior's infrastructure as code templating for their backend systems on gcp and customer cloud deployments in aws were critical to their ability to scale and adapt to meet customer needs. threatwarrior successfully closed a series-a round, during which jon served as a technical sme throughout investor discussions and due diligence.

jon codes primarily in go, python, typescript, and c, along with years of experience in swift and objective-c, and some dabbling in rust. he is deeply familiar with orchestration and deployment technologies like terraform, terragrunt, docker, kubernetes, and helm, as well as with the

gcp and aws restful apis. jon has spent years working with kafka and elasticsearch / opensearch for processing data. on the frontend, he is proficient with d3.js, react, and apple uikit. jon regularly uses a wide array of the google cloud (gcp) stack, including google dataflow / apache beam, google cloud run, google kubernetes engine, google pubsub, google bigtable, and google bigquery.

---

work

insane cyber -- director of engineering

sep 2024 -- present · san antonio, tx (remote)

balancing the needs of the rest of the insane cyber leadership team -- as well as those of our design partners and customers -- i direct the product roadmap, manage the engineering team, and make contributions to core platform functionality.

---

threatwarrior -- principal software engineer

jul 2018 -- sep 2024 · tampa, fl

- designed, implemented, and maintained machine learning pipelines for unsupervised deep autoencoders to perform anomaly detection on network traffic flows using python, kafka, typescript / node.js, google kubernetes engine, and helm.
- designed, implemented, and maintained serverless, distributed user and entity behavioral profiling and anomaly detection streaming pipelines, middleware, and frontend ui for tracking interactions over time across arbitrary data sources with mergeable, probabilistic data structures in a graph model to answer who communicated with whom, how much, and what about, using go, apache beam / google dataflow, google bigtable, google bigquery, python, typescript, d3.js, and react. served in production as a flagship feature and foundational technology for threatwarrior's xdr approach.
- led a cloud migration from bare metal servers in a colo datacenter, where processes ran in vms and communicated over inter-process communication (ipc), to containerized microservices running in google kubernetes engine and communicating over an apache kafka message bus, using typescript / node.js and helm. this involved writing a number of

custom typescript libraries for integrating application services and kafka with the node.js streams api.

- led a subsequent cloud initiative to embrace cloud-native idioms like serverless containers and infrastructure as code, rearchitecting the entire backend stack to deploy with terraform, terragrunt, google cloud run, and google pubsub. this enabled backend scalability and rapid provisioning of customers within minutes.
- researched applying generative ai techniques like transformer architectures to assembly code for anomaly detection on supply chain software updates, prototyping a hierarchical transformer model which learned to represent sequences of basic blocks of decompiled windows and linux binaries in ways that clustered vectors from similar binaries together using python, torch, huggingface, rizin, and ghidra.
- patched and integrated c libraries for network packet analysis and reporting, developing a dynamic plugin loading library on top of suricata to process results through a proxy that could safely and legally link to ndpi, a network traffic protocol detection library under a conflicting open source license, using zmq to deliver output results to a custom process.
- implemented and maintained a tool to discover and enumerate resources in cloud environments, unify them into a single data model across providers, structure them into a hierarchy, aggregate their network usage, and visualize them as graphs or sankey diagrams using python, javascript / node.js, the aws and gcp restful apis, gephi, and d3.js.
- implemented a flexible, turnkey system to deploy threatwarrior's network monitoring sensors and traffic mirroring infrastructure inside customer aws environments, using terraform and terragrunt. this was an extremely sophisticated infrastructure as code project, which required developing many custom modules deployed across multiple vpcs and accounts, making heavy use of mapping and looping within templates.
- developed a user-session tracking data pipeline to aggregate and report api audit events to slack using python, apache beam / google dataflow, google pubsub, and google bigquery.
- held devops responsibilities utilizing grafana, m3db, google cloud metrics, and google cloud trace / opentelemetry for dashboarding and alerting from elasticsearch / opensearch clusters, apache kafka clusters, google kubernetes engine clusters, and internal tooling.

- shaped product roadmap, engineering hiring, costing and pricing, internal and external presentations, and technical discussions with investors as a key subject matter expert during due diligence for seed and a-round investment and merger and acquisition talks.
- worked closely with finance, providing monthly breakdowns and analyses of cloud costs across multiple vendors and cost centers.

---

nitro solutions -- senior software engineer

mar 2014 -- jul 2018 · tampa, fl

- led teams of offshore and onsite team members and collaborated directly with clients to gather requirements and estimate project complexity.
- developed an unsupervised facial recognition system using python, opencv, and dlib as part of an interactive 3d virtual receptionist product, which received media attention.
- performed exploratory data analysis and clustering of social graph data and document troves using python, sklearn / scikit-learn, javascript, and d3.js.
- designed, implemented, and enhanced ios apps and nitro's core ios libraries using swift and objective-c.
- designed and deployed a containerized infrastructure for nitro's server platform, nitroserver 6, on top of docker swarm mode using a custom-written node.js cli utility.
- developed automated build harnesses for native mobile apps on multiple platforms.
- crafted in-house tools for tasks like load testing backend servers, presenting (ipad) and controlling (iphone) an interactive scavenger hunt, and importing client data into backend systems.

in july 2018, nitro separated its cybersecurity business into an independent entity called kineticfuse.

---

nielsen -- lead software engineer

feb 2011 -- mar 2014 · oldsmar, fl

mac lead for a cross-platform user activity measurement tool, netsight, which powered many of nielsen's client reports, including netview.

- choreographed a suite of root daemons, user apps, and kernel extensions written in a mixture of c, c++, objective-c, and objective-c++ -- with a heavy dose of ported windows code.
- responded to security and hal changes as os x evolved, while preserving legacy support back to the 10.4 (i386) sdk.
- planned, estimated, and designed releases. assigned work to on-site colleagues and off-shore consultants.
- acted as integration manager, handling all branching, merging, and tagging.
- acted as a technical representative for the team in dealings with upstream and downstream groups at nielsen.
- contributed to nielsen's innovation program with white papers and patent applications.
- led the team's migration from cvs and svn to git, which was a pilot study for nielsen as the company considered certifying it as a "nielsen standard."
- ran the team's failure mode effects analysis (fmea) process.

---

handbrake -- lead developer

dec 2006 -- feb 2011

helped maintain the core library of the video transcoder: developed new features, isolated and fixed bugs, administered servers, moderated forums, wrote user and developer documentation, provided tech support, and organized public releases. focus was on developing new image filters to fix telecined and interlaced video -- first exposure to the practical use of deep neural nets for signal filtering. credited in the authors file with "massive core enhancements."

---

cf motion, inc. -- it intern

dec 2009 -- dec 2010

- prototyped a ruby on rails project tracking system to replace the company's manila folders.
- drafted curriculum for a network technology certification program.
- configured and troubleshot the deployment of a surveillance system for the veteran's administration.
- located invitation to bid opportunities in the government sector, wrote responses to requests for proposals, and priced out quotes for reselling technology equipment.
- interviewed job applicants to vet their technical skills.

---

patents

- **us 8914629** -- intercepting encrypted network traffic for internet usage monitoring (october 2014)
- **us 9516001** -- methods and apparatus to identify media distributed via a network (december 2016)
- **us 10810607b2** -- methods and apparatus to monitor media presentations (october 2020)

---

training

- black hat usa / def con 31 -- las vegas, august 2023
- black hat usa / def con 30 -- las vegas, august 2022
- wwdc 2013 -- san francisco
- wwdc 2012 -- san francisco

---

education

bachelor of applied science, technology management: business information systems st. petersburg college · 2009 -- 2010

associate of arts st. petersburg college · 2002 -- 2009

---

skills

languages: go, python, typescript, c, terraform

frameworks: node.js, d3.js, keras, tensorflow, pandas, huggingface, ndpi, react, protobuf, ddsketch, opentelemetry, zmq

tools: apache kafka, elasticsearch, opensearch, kubernetes, docker, apache beam, google dataflow, git, mongodb, m3db, grafana, helm, terragrunt, suricata, google cloud run, google pubsub, google bigtable, google bigquery

operating systems: macos, ios, linux
