Ian Norden

Remote, Colorado
inorco@proton.me
https://iancnorden.com

Employment History

Jan 2024 – Present | Intercontinental Exchange

Lead — Cybersecurity Engineering

- Transferred to Cybersecurity Engineering due to elimination of remote managers across ICE
- Procured new posture management, container security services, and DFIR CDR tooling
- Leading POCs across Cloud Detection & Response vendors, bringing in training for DFIR team
- Working closely with DFIR and Threat Intel teams to overhaul playbooks and teach Cloud
- Lead for all Architecture Reviews for systems both hosted on-prem and in AWS, Azure, & GCP
- Lead InfoSec resource for all Cloud development efforts, introducing IAC requirements and policy

Mar 2020 – Jan 2024 | Intercontinental Exchange

Manager — Cloud Security

- Automation focused posture management, container security services, and IAC scanning tools
- Responsible for training regimen, talent acquisition, managing a team of four engineers
  - *Additionally Interim manager AppSec in addition to CloudSec, (team of nine) July 2021 – Dec 2021*
- Standardized account vending and cloud controls alignment for logging, access, & tools integration
- InfoSec lead for Secret Storage projects, continuing SME in crypto (at rest, in transit, pw hashing)
- Eliminated TLS1.0/1.1/SSL3, coordinating change adoption across 100s of apps using Ops teams
- Lead architecture reviews for cloud acquisitions, coordinated day01 proactive conversations

Sep 2018 – Mar 2020 | Intercontinental Exchange

Senior Security Engineer — Application Security

- Leading new Cloud initiatives across dozens of apps, backfill for extended AppSec resource gap
  - Managed training coordination plan, and resourcing support handoff plan during transfer
- Lead Cloud Security pentests, developed new controls for AppSec in AWS & Azure adoption effort
- InfoSec lead for Secrets Storage design working closely with Systems Engineering architects
- Custody solution lead, cold & hot wallet storage, HSM operations, key sharding, and key vaulting
- Lead for Cloud design reviews for App Devs, their supporting infra, and lead AppSec M&A process
- AppSec SME for appx. 120 internal apps, responsible for tooling integration and findings pipeline

May 2016 – Sep 2018 | Intercontinental Exchange

Senior Security Engineer — Red Team

- Founding member of the ICE Red Team, built out social engineering, C2, and various attack tools
- Executed and hosted wide range of pentests against portfolio of critical applications and systems
- Eliminated two way trusts across our active domain infrastructure after discovering critical findings
- Built majority of reports and lead debriefs from internal and external Red Team engagements
- Teach and guide new InfoSec team members through hosting pentest workshops

Mar 2015 – May 2016 | Intercontinental Exchange

Security Analyst & Engineer — Application Security

- Responsible for success of vuln scanning fleet at ICE, became SME on Rapid7's Nexpose
- Coordinated and conducted half of all ICE pentests included RegSCI and other sensitive systems
- Took responsibility for team workflow, improving controls, app tracking, and pentest documents
- Introduced ICE to the concept of bug bounties, manged POC, implemented BugCrowd testing
- Design and deploy initial AppSec dedicated cloud tool sets, from scanners to c2 endpoints
- SME for vuln scanning, encryption in transit & at rest, password hashing, and misc crypto

Nov 2014 – Mar 2015 | EarthLink Inc.

Senior Security Engineer — Professional Services

- Rose to lead the Security arm of EarthLink's Pro Services offering, lead Sales Engineer
- Conducts vuln assessments and penetration testing customer engagements
- Provides mitigation guidance based on architectural analysis, threat modeling, and research
- Created EarthLink's attack and penetration testing methodology standards docs
- Architects and engineers Professional Service's team's tools and C2 infrastructure

Jan 2012 – Nov 2014 | EarthLink Inc.

Security Analyst I & II — Enterprise Information Security

- Manage and engineer vuln scanning infrastructure, SME for Tripwire IP360 scanners
- Primary resource for annual penetration testing delivery, coordination of NCC Group resources
- Designed and implemented risk assessment standards check leveraging dev-projects and IP360
- Incident response escalation point for forensics collection coordination with on-call rotation
- Regular mentoring and training of new analysts within the Security Operations team (Analyst II)

Education

Dec 2011 | **Georgia Southern University**

Bachelor's Degree, Information Technology

- Specialization: Networking and Data Center Administration
- Minor: Information Systems

Projects & Contributions

- Homelab, self hosted, on-premise;
  - Proxmox, TrueNAS, PiHole/AdGuard, misc. SDLC resources, tested backups, wireguard VPN
- Resume Home, git, Digital Ocean, CloudFlare DNS, etc; https://iancnorden.com
- Probable Word-lists contributor – https://github.com/berzerk0/Probable-Wordlists
- Discover Scripts contributor - https://github.com/leebaird/discover
- Awesome Security Talks contributor - https://github.com/PaulSec/awesome-sec-talks

Organizations

- OWASP Lifetime Member
- Linux Foundation Member
- EFF Annual Member
- FIRE Annual Member