Ian Norden

Remote, Colorado
Iancnorden@protonmail.com
https://iancnorden.com

Employment History

Mar 2020 – Present | Intercontinental Exchange

Manager — Cloud Security

- Created CloudSec team; automation focused posture management, container security services, and IAC scanning
- Responsible for building training regimen and acquiring talent for a team of four engineers with limited budget
  - *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, etc
- InfoSec lead for Secret Storage projects, regular SME for cryptographic based systems or controls
- Eliminated TLS1.0/1.1 use in edge networks, coordinating adoption across 100s of apps driven through Ops teams
- Lead architecture reviews for cloud acquisitions, aligning onboarding and proactive day1-30 discussions

Sep 2018 – Mar 2020 | Intercontinental Exchange

Senior Security Engineer — Application Security

- Backfill transer for an extended AppSec resource gap, lead for new initiatives within InfoSec
  - Managed own successful training coordination plan, and resourcing support handoff plan
- Lead Cloud Security assessments and controls alignment in AWS & Azure adoption effort
- Coordinated crypto risk assessments between Dev, AppSec, and GRC to drive need for Secrets Storage/PKI
  - InfoSec liasion with Enterprise Architecture teams for requirements, proof of concepts, and general design
- Co-lead for Bakkt custody solution, consulted on key signing ceremonies, cold / hot wallet storage, HSM operations, key sharding, and key vault distribution
- SME leading architecture design reviews for AppSec supporting system M&A process for ICE
- AppSec SME for 120+ internal apps, liaising with AppDev teams for application testing

May 2016 – Sep 2018 | Intercontinental Exchange

Senior Security Engineer — Red Team

- Founding, initial member of Red Team to build out the tools and capability playbooks
- Earned Senior Engineer role, Mar 2017, managed changeover of 3rd party bug bounty vendors
- Executes penetration tests against wide portfolio of critical applications and systems
- Builds reports and leads debriefs from internal and external Red Team engagements
- Design vulnerability scanning, social engineering, and Red Team C2 infrastructure
- Automate manual remediation-reporting processes via Python scripting
- Build and maintain internal virtual pentest practice range of vulnerable machines
- Teach and guide new InfoSec team members through brown bag's and pentest workshops
- Develop applicable POC exploits from frameworks such as Mitre's ATT&CK Matrix

Mar 2016 – May 2016 | Intercontinental Exchange

Security Engineer — Application Security

- Introduce, acquire, and manage 3rd party bug bounty programs, strategize testing rollouts, program rulesets
- Architect and deploy standardized AppSec tooling internal and externally to the organization, primarily in AWS
- Manages and executes annual penetration tests against wide portfolio of critical applications
- SME handling ICE TLS configuration standards and built automation for TLS / SSL attack surface assessments
- Subject matter expert and primary engineer for Nexpose vulnerability scanning infrastructure
- Produces company standards and guidelines documentation leveraging proven expertise

Mar 2015 – Mar 2016 | Intercontinental Exchange

Security Analyst — Application Security

- Owned strategy and responsible for implementing vuln scanning toolset, Nexpose
  - Deploying 108 distributed scanners in 2015, reaching >92% coverage of hosts based on CMDB with returned contributions
- Coordinated and conducted (appx. 50% split) annual pentests against wide portfolio of critical applications
- Iterated AppSec testing methodology, licensing Burpsuite and coordinating Kali infrastructure supporting whitebox
- Responsible for team's AppSec workflow, controls, app tracking, and pentest documentation
- Lead for triaging vulnerabilities and coordinating retests between development, GRC, and other teams
- Iterated evidence collection by standardizing video/screenshot capture workflows

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 vulnerability 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 infrastructure vulnerability assessment program, SME Tripwire IP360
- Primary resource for annual penetration testing delivery, coordination of NCC Group resources
- Designed and implemented risk assessment standards check leveraging dev-projects and IP360
- SIEM investigation & tuning of Q1Radar implementation
- Incident response escalation point for forensics collection coordination and regular with tier1 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 – Proxmox, Truenas, PiHole, Pentest range, Self-hosted git repos, Backups, Wireguard (vs. Tailscale)
- Homelab Decoms – Vsphere, Graphana, Alienvault, OpenVPN
- Probable Word-lists – https://github.com/berzerk0/Probable-Wordlists: Contributed time and help around repack, distribution, and cleanups
- Discover Scripts - https://github.com/leebaird/discover – PR based contributions to this OSINT resource
- Awesome Security Talks - https://github.com/PaulSec/awesome-sec-talks – PR contributor

Organizations

- OWASP Lifetime Member
- Linux Foundation Member