Ian Norden

Relocating to Colorado (Remote)
Iancnorden@protonmail.com
https://iancnorden.com

Employment History

Mar 2020 – Present | Intercontinental Exchange
Manager — Cloud Security

- Responsible for building roles and hiring acquiring talent for a team of three
  - *Interim manager AppSec in addition to CloudSec, (team of nine) July 2021 onward*
- Lead team effort to standardize account vending, standardize cloud-based InfoSec controls
- Delivered workshops and training solutions for nascent cloud knowledge across variety of partnered teams in release engineering, incident response, systems engineering, etc
- InfoSec lead for Secret Storage project, leveraging Thales HSM and Hashicorp Vault
- Design and lead container security strategy, building team resources supporting implementation of AquaSec toolsets
- Eliminated TLS1.0/1.1 use in edge networks, coordinating adoption across 100s of apps
- Lead architecture reviews for cloud acquisitions, aligning team resources and capabilities

Sep 2018 – Mar 2020 | Intercontinental Exchange
Senior Security Engineer — Application Security

- Returned to AppSec as a Senior resource to solve department resourcing gaps
- Lead Cloud Security assessments and controls alignment in AWS & Azure adoption effort
- Conducted crypto risk assessments to lead adoption of Enterprise Secrets Storage project
- Crypto 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
- 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 in Python
- Started the InfoSec dashboard initiative, Django/Python dashboard automation system
- 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

- Architect and implement AppSec tool sets including out of band assessment implementations.
- 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

- Manages and executes annual penetration tests against wide portfolio of critical applications
- Improve and maintain the groups testing methodology, acquiring new tools such as Burp and building Linux test infrastructure for SQLMap and similar toolsets
- Overhaul team documentation to provide knowledge base for AppSec task and app tracking
- SME for application retesting, triaging vulnerabilities and providing video/screenshot proof for ticket remediation coordination
- Complete ownership of a net-new vulnerability scanning infrastructure builds with Nexpose, deploying 108 scanners in 2015, reaching >92% coverage of hosts

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 and coordination
- Designed and implemented risk assessment processes for new infrastructure builds
- SIEM investigation & tuning of Q1Radar implementation
- Primary incident response escalation point and forensics coordination
- Regular mentoring and training of new analysts within the Security Operations team

Education

Dec 2011 | **Georgia Southern University**

Bachelor's Degree, Information Technology

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

Projects & Contributions

- Homelab – Vsphere & Proxmox hosts, Freenas, Pfsense, PiHole, Unifi, SIEM test hosts, pentest range, personal VPN, self-hosted Git repo for Python codebases
- Probable Word-lists – https://github.com/berzerk0/Probable-Wordlists: Attribution for early work on hosting, distribution of large datasets
- Discover Scripts - https://github.com/leebaird/discover - Trusted contributor to this OSINT and Pentest automation resource
- Awesome Security Talks - https://github.com/PaulSec/awesome-sec-talks

Organizations

- OWASP Lifetime Member
- Linux Foundation Member