

# Ian C Norden

---

Greater Atlanta Area

[iancnorden@gmail.com](mailto:iancnorden@gmail.com)

<https://iancnorden.com>

## Employment History

May 2016 – Present | **Intercontinental Exchange**

**Information Security Engineer — Red Team**

- Challenged as initial member of Red Team to build out the team and capability playbooks.
- Assess and build the Red Team testing platforms, tools, and infrastructure.
- Executes penetration tests against wide portfolio of critical applications and networks.
- Improve processes via automation engineering and coding.
- Maintain and improve upon the current Bug Bounty program.
- Engineer, maintain, and manage the Nexpose infrastructure vulnerability scanning platforms.

Mar 2016 – May 2016 | **Intercontinental Exchange**

**Information 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.
- Subject matter expertise in configuration and built automation around TLS / SSL 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**

**Information Security Analyst — Application Security**

- Manages and executes annual penetration tests against wide portfolio of critical applications.
- Improve and maintain the groups testing methodology and metrics.
- Overhaul documentation practices to provide robust knowledgebase previously lacking.
- Provide subject matter expertise showcasing proof of concept exploits against found vulnerabilities.
- Assess and build from ground up the vulnerability scanning infrastructure and platform.

Jan 2015 – Mar 2015 | **EarthLink Inc.**

**Sr. Security Engineer — Professional Services**

- Lead and execute vulnerability assessments and penetration testing customer engagements.
- Provides mitigation guidance based on technical architectural analysis, threat modeling, and research.
- Created EarthLink's attack and penetration testing methodology standards.
- Architects and engineers Professional Service's team's tools and infrastructure.

Nov 2014 – Jan 2015 | **EarthLink Inc.**

**Information Security Engineer - Professional Services**

- Assess, purchase and built penetration testing and assessment infrastructure.
- Leads and maintains penetration testing resources.
- Lead engineer for the creation of EarthLink's security professional services team.
- Provide sales engineering engagements based on client's needs.
- Engineer methodologies, sales engineering documentation, and tech spec sheets for team foundation.

Jan 2012 – Nov 2014 | **EarthLink Inc.**

## **Information Security Analyst I & II — Enterprise Information Security**

- Manage and engineer infrastructure vulnerability assessment program, subject matter expert Tripwire IP360.
- Primary resource for annual penetration testing services coordination.
- Built and maintained the risk assessment processes for new infrastructure builds.
- SIEM investigation and leveraging 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

## Certifications

- **CEH Certified** | EC-Council, Certification: ECC77822375901
- **SSCP Certified** | ISC2, Certification: 462645

## HomeLab

- **PFSense** Firewall deployment controlling ingress / egress.
- Snort deployed and sniffing ingress / egress.
- Segregated Ubiquiti Wifi.
- **OSSIM** deployed as a test bed for attacks and infrastructure
- Multiple development virtual machines for coding or git push / pulls.
- **Segregated Pentest Lab** housing a number of vulnerable virtual machines to prepare for OSCP against.
- Nessus / Nexpose deployed alongside **Kali as a Pentest firing range**.
- Security onion sniffing traffic in and out of the Pentest lab.

## Coding + Open Source Contributions

- Discover Scripts - <https://github.com/leeбайд/discover> - **Trusted contributor** to this OSINT and Pentest automation resource.
- Distroseed - <http://distroseed.github.io/distroseed/> - I co-founded this open source project which is an automated assistant for finding, downloading, and managing Linux Distributions, with a beautiful dashboard.
- Awesome Security Talks - <https://github.com/PaulSec/awesome-sec-talks> I regularly contribute to this well maintained security talks and conferences reference.
- SSLDash - Not yet open source - Beautiful dashboard for automated scanning, grading, and reporting on SSL / TLS strength for websites. Provides guidance to end users for hardening and configuration as well.

## Organizations

- **OWASP Lifetime Member** – Atlanta Chapter
- Linux Foundation Member
- InfraGard Atlanta Member