APPLIED PURPLE TEAMING

Infrastructure
Threat Optics
Continuous Improvement

ISACA®
Trust in, and value from, information systems
Denver Chapter

DEFENSIVE ORIGINS

BLACK HILLS
Information Security
• 2008 •

Instructors

Jordan Drysdale
@Rev10D
ISACA# 1317214

Kent Ickler
@Krelkci
ISACA# 1317214

`$night_gig` = **Defensive Origins**

Founded by Jordan and Kent in January 2020

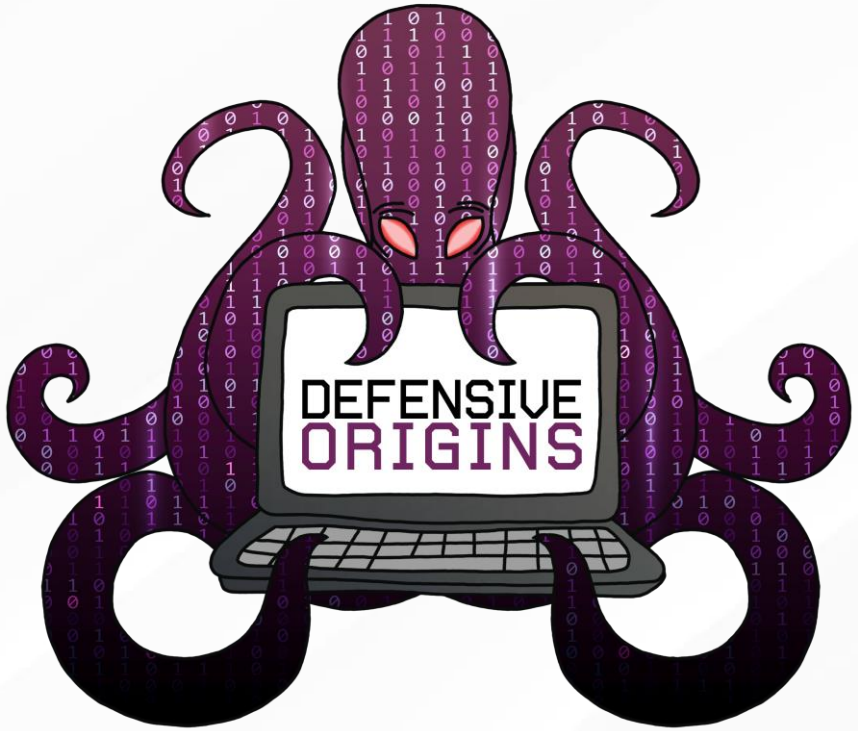
- Both hackers with business degrees
  - 30+ industry certs over last 15 years
- ***Ethos***: Make The World a Better Place
- Building a Better Defense

Fully supported by:

- Black Hills Information Security
- Our families

Intended to cover a growing niche in InfoSec:

- Purple Teaming
  - A blend of Business Operations
  - HR / Marketing / CISO / Red / Blue
  - Policy / Procedure
  - A path forward toward better optics



`$day_jobs` = **Black Hills Information Security**

Founded by John Strand in 2008

- 50ish Employees
- Coverage On Multiple Continents
- Penetration Testing
- Defensive Services
- Audits and Compliance
- Threat Hunting
- Training and Education

An incubator for dozens of other companies and open-sources projects!

Want a customized IT security review?
consulting@blackhillsinfosec.com

defensiveorigins.com

Workshop Objectives

- This slide deck. Intro materials. (45 min)
- Lab deployment demo on Azure. Couple clicks, viola, three system hunt lab (30 min)
- Post deployment optics build scripts. Deploy winAudPol, sysmon, wec, wef, etc (30 min)
- Hunt lab lifecycle operations:
- Executing SILENTTRINITY as a C2 and catching it all some of the ways (30 min + 30 min Lab)
- Executing an LNK hijack and relay and catching pass the hash in near time (30 min + 30 min Lab)

Websites and Contact Info

Defensive Origins
https://DefensiveOrigins.com
https://github.com/DefensiveOrigins

Black Hills Information Security
https://BlackHillsInfoSec.com
https://ActiveCounterMeasures.com

Emails
jordan@defensiveorigins.com
kent@defensiveorigins.com

If you want to thank John for our time today - john@blackhillsinfosec.com

