Security Operations Center (SOC) Certification Overview

What is GIAC?

- Global Information Assurance Certification

- Focus on real-world, hands-on skills

- Award-winning, high-quality information security certifications

Typical GIAC Exam Configuration

- 115 Questions (100 scored / 15 un-scored), open book / open notes
- 3 hour time limit
- Renewable every four years via exam or Certification Maintenance Units (CMUs)
- No Experience Requirement
- No Training Requirement
- Cert Objectives Posted on Public Web Site

The State of SOCs

- Many SOCs are new (<5 years old)
- Our research shows SOCs have common traits across roles, but standard job descriptions or requirements are still in contention
- The industry is struggling to recruit qualified SOC staff

Current State of SOC Training

- Create a development and assessment plan aligned with SOC job descriptions

- Currently, there are resources helpful in training SOC staff – but few developed specifically to train or assess SOCs or SOC staff
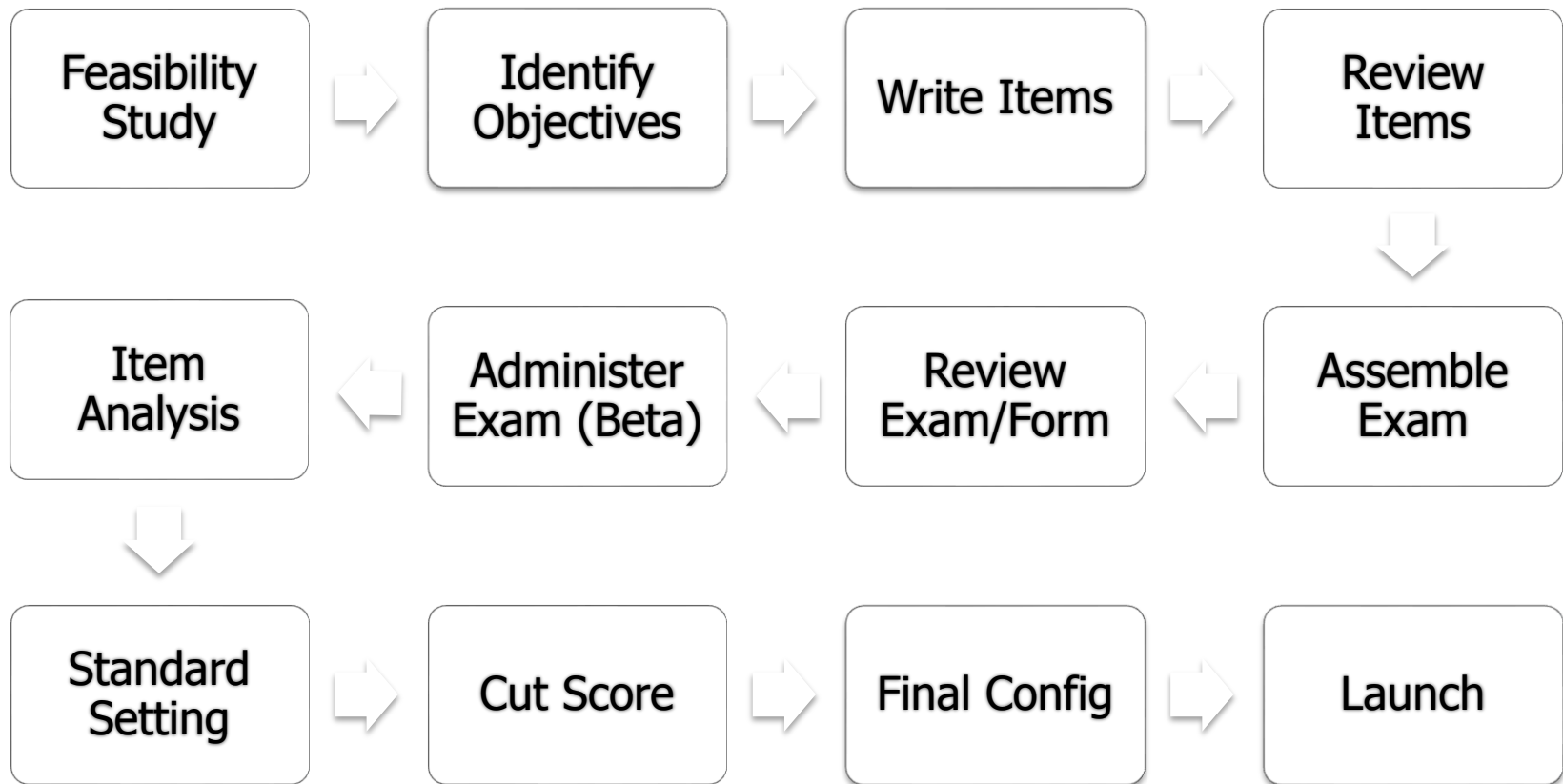
A Vision for SOC Certification
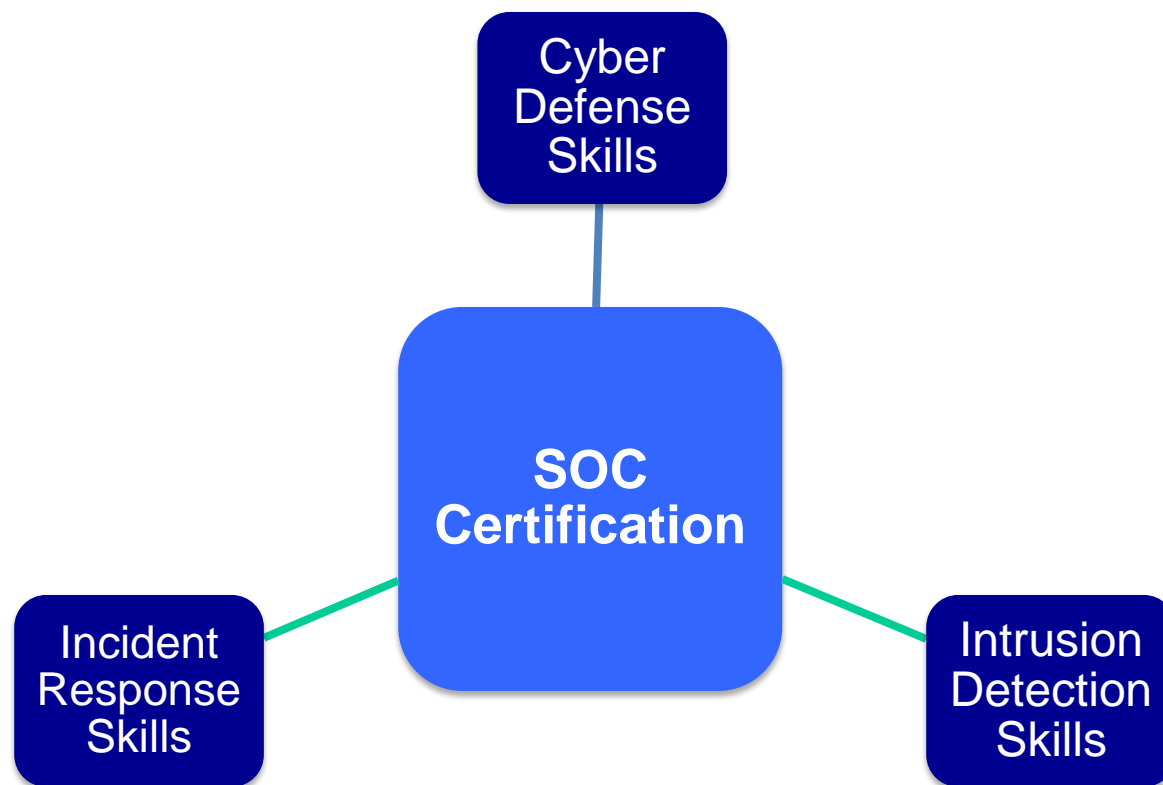
The "Elevator Pitch"

*"What is the **<u>minimum</u>** a technical professional should know (i.e. a 'common starting point - security knowledge, skills and abilities') to undertake security work in a Security Operations Center?"*

Cert Development Guidance

- Follow industry standard processes
- Bring in "real world" expertise to keep it relevant
- Alignment with SANS Curriculum
- Get it right the first time

Certification Development Process

Feasibility Study	→	Identify Objectives	→	Write Items	→	Review Items

Item Analysis	←	Administer Exam (Beta)	←	Review Exam/Form	←	Assemble Exam

Standard Setting	→	Cut Score	→	Final Config	→	Launch

Opportunities to Work Together

- Partner with organizations to continue feasibility discussions and define content/mission.

- Job Task Analysis – get the word out

- Item writing – exam questions

- Beta and pre-beta exams (need feedback)

- Live Beta Exam Participation

- Standard Setting SMEs (Cut Score)

We want you to tell us…

Would you want a SOC-specific certification?

What kind of value would it bring to your organization?

How would you use it, or who would you use it for?

Why would someone working in this realm pass this over?

Get involved!

Email me: cimbert@giac.org
or... jpike@giac.org
or... info@giac.org

Thank you!