Building the Next Generation of Security Talent

Operational Training and Security Internships

Black Hat USA 2019

William Peteroy | Security Chief Technology Officer, Gigamon
Alex Sirr | Security Engineer, Applied Threat Research, Gigamon

William Peteroy

Chief Technology Officer – Security at Gigamon

- Chief Technology Officer, Security of Gigamon, leading security strategy and innovation efforts
- Founder and CEO of ICEBRG (acquired by Gigamon in 2018)
- Previously in several business and technical leadership positions in the technology and software space
- Security Strategist at Microsoft's Security Response Center (MSRC) and managed product security for Windows and Internet Explorer
- Technical Director and Subject Matter Expert at the Department of Defense (DoD)
- Instructor at the National Cryptologic School at Fort Meade and researcher at Dartmouth

@wepiv

Gigamon

Alex Sirr

Security Engineer – Gigamon Applied Threat Research

- Security Engineer, Gigamon ATR
  - Focus: Detection research
- Former ICEBRG intern and Security Engineer
- Graduated from the University of Washington in 2018 with a degree in Informatics
- Black Hat EU 2018 speaker
  - Detecting DCOM lateral movement
  - Contributed DCOM parsers to Wireshark

@DarkAl3x1s

Gigamon®

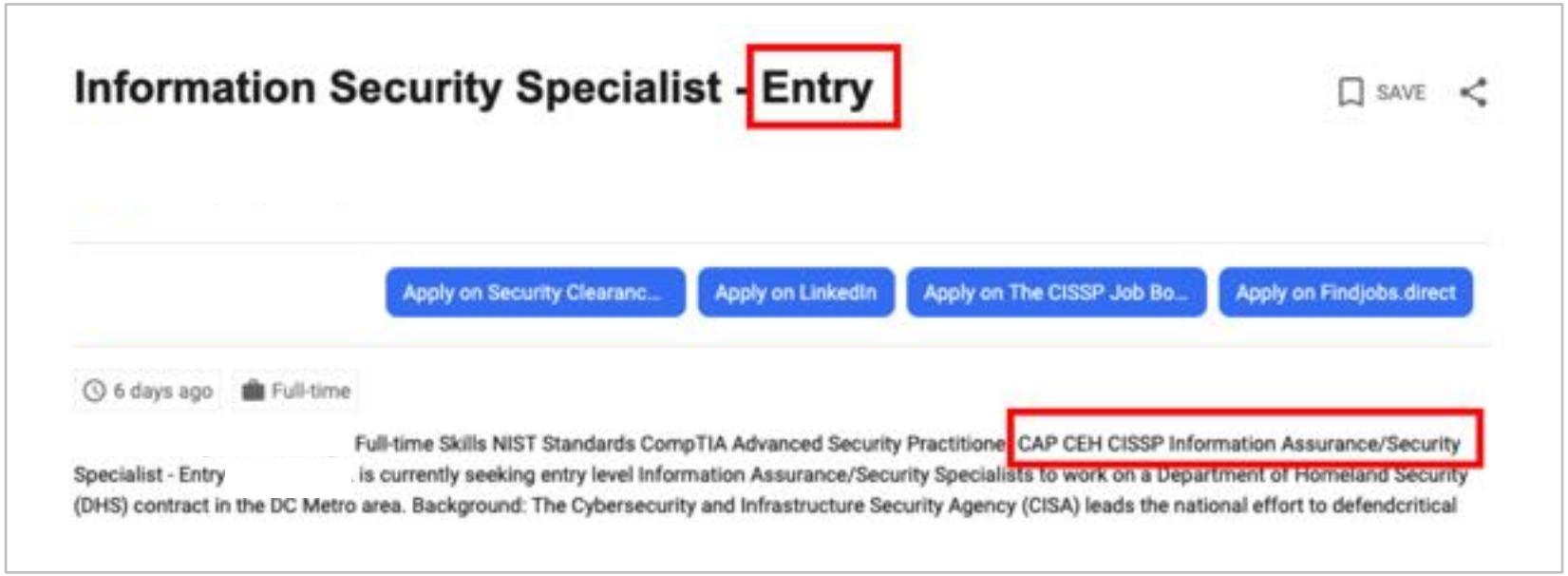
Let’s talk about training

Current State of Training in Information Security

Gigamon

Current State

Job Description



Doesn't take long to find entry-level jobs that have requirements that do not make sense

- "Active secret or higher clearance (Required)"
- CISSP requires 5 years of professional experience
- This role pays $56,000 / year in Washington DC Metro

Gigamon

Training Starts with Entry-Level Personnel

- Entry-level personnel have the greatest need
- Training can establish more than technical knowledge
- Good training programs help set the baseline for company culture and work ethic

Training is More Than Knowledge

Support the growth of new employees

Bring new perspective

Enable true job effectiveness

Gigamon®

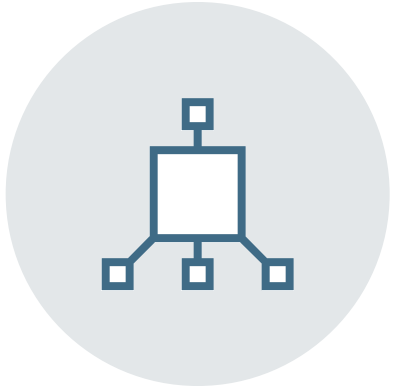
Gigamon®

Developing entry-level personnel

Developing Entry-Level Personnel

Commercial Training Options

Cyber Schoolhouse



On-the-Job Training

Commerical Courses

Pros and cons of current options

TARGETED:

INVESTMENT:

- Pros
  - Built and maintained by professionals*
  - Curriculum that can be leveraged for multi-stage training
  - Extensive options for content
  - Does not require internal resources to update
- Cons
  - Expensive
  - Few “big training vendors”
  - Classes are orphaned by original instructors
  - Content is often dated
  - Content is general purpose and not specific to roles needs
  - Courses assume a level of subject matter familiarity

* many courses struggle to stay up-to-date in information security

Gigamon

Cyber Schoolhouse

Pros and cons of current options

TARGETED:

INVESTMENT:

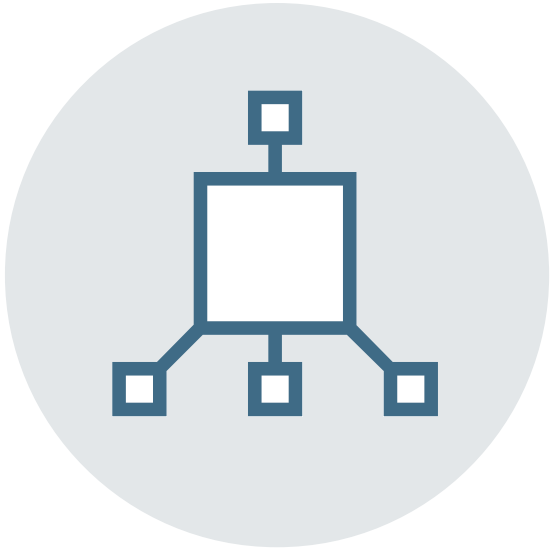
- **Pros**
  - Coverage of breadth of an area
  - Technical school for US Armed Forces (Joint Cyber Analysis Course)
- **Cons**
  - No well-recognized commercial options
  - Lose new employees for six months during basic skill training
  - Even at 6 months this course is a “firehose”
  - Content may not be applicable for any particular trainee

On-the-Job Training

Pros and cons of current options

TARGETED:

INVESTMENT:



- **Pros**
  - 100% of the content is applicable for the trainee's job role
  - Cash inexpensive
- **Cons**
  - Requires senior personnel to train junior folks
  - Takes resources to stand up and maintain program (will get stale)
  - Limited in the commercial sector to "internships", which vary widely in what you will learn from them

Gigamon

Internships and On-the-Job Training

- In commercial industry, getting training dollars can be a challenging and frustrating experience
- On-the-Job Training (OJT) provides us the most targeted training with the lowest overall cost
- We’re going to focus on getting the most out of on-the-job training and how to leverage it to make interns and entry-level employees successful

Gigamon®

Developing a Training Program

Internship Programs

Revisiting On-the-Job Training Challenges

Challenges

Time investment from senior personnel

Justify ongoing resources invested in continual improvement of the program

Make sure that internships are more than “learning coffee orders”

Requirements

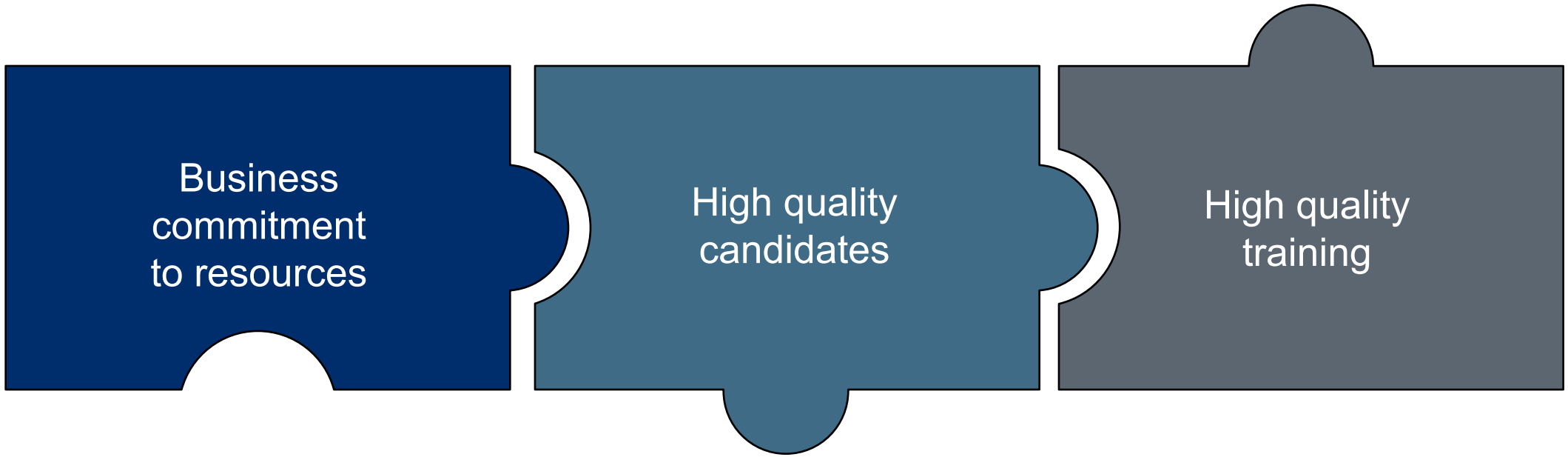
Domain expertise
(from our senior personnel)

Scope

Structure

Feedback Loops

Building High Performing Personnel



Business Commitment Resources

- To enable the program we need to talk to the business and secure resources
- Part-time commitment of multiple senior personnel to help build requirements and understanding of what skills the interns need to develop during their internship
- One part-time senior FTE to oversee the program and:
  - Track progression through the program
  - Mentor interns and help them ask/answer questions

High Quality Candidates

- Critical to establish a pipeline of high-quality candidates
- Good candidates are:
  - Intelligent
  - Articulate
  - Driven
- We start screening for FTE employment before internships to maximize chance of hiring as FTE

High Quality Training

- Scope training around job role and operational requirements
- Start with the basics as a foundation
- Foundations enable a baselined training experience

High Quality Personnel

- A great training pipeline will generate great people
- Great people need room to grow and demonstrate new skills
- Do this by giving interns opportunities to demonstrate that they are:
  - Intelligent
  - Articulate
  - Driven

Gigamon®

Security Internship Programs in the Real World

Objections, Challenges, Experiences and Outcomes

Early Challenges

We faced lots of questions and objections

- Why would we have an intern program?
- Interns won’t be able to do real work.
- This will be a drain on our FTE personnel.
- College kids are distracting and hard to manage.
- Do they know anything coming out of college?

Initial Approach

Pros

Incredible energy, attitude, and approach to work

Blank slate for training

Low salary expense

Cons

On-the-job training takes resources from senior personnel

Maturity and work experience

Low initial productivity

Practical approach

Practical screening

Provide structure for interns

Leverage self-directed training

Program Establishment

Understand your local university

- Engage with faculty
- Engage with program coordinators
- Track down where students and clubs that are interested in information security are (CTF / CCDC / etc.)

Support your local university

- Ask if there's anything that you can do
- Make your executives and SMEs available to talk to students

Advertise the program and process

Build structure for your incoming interns

Program Establishment - continued
(cont'd)

Leverage your Subject Matter Experts (SMEs)

- What do we need our employees to know?

Build training structure

- JQR – Job Qualification Requirement
  - Knowledge Requirements
  - Practical Requirements
  - Signers

Build a schedule

- Self-paced training needs some loose timelines and structure

Onboard interns

- Be inclusive – make them a part of the team

Gigamon

Gigamon®

Developing On-The-Job Training and OpenJQR

Structured On-The-Job Training

A Job Qualification Requirement (JQR) is a document that captures the knowledge and practical functions needed to perform in an operational job role.

On-the-Job Training – What's a JQR

JQRs have trainees and qualifiers

Trainees

Work through the JQR with qualified signers to show that they understand the requisite knowledge and can perform operational tasks for their role.

Qualifiers

Have completed the JQR and are qualified to train and certify new personnel on JQR items.

What's Special About a JQR?

- Tailored specifically to a job role
- Zero assumed knowledge
- Completed with a mentor
  - Experience in the role
  - Qualified to train and answer questions
- Emphasizes self-directed learning with peer support

Mapping the JQR to our OJT Challenges

Scope

- Build JQR content to job role
- Understand job functions, skills and knowledge for the specific job role

Training Consistency

- Qualified senior personnel
- Clear written guidelines (ex. no rote memorization)
- Limited list of “qualified signers”

Structure

- Clearly defined timeline
- Expectations
- Maintenance plan

Feedback Loops

- Intern interviews on completion
- Interns / trainees that have completed the training and are in role will continue to update and direct training

Gigamon®

OpenJQR

GOAL: Build community-validated JQRs based off of job roles in security

- OpenJQR Beta (releasing now)
  - Focus on one job role – Entry level SOC analyst
  - 39 Knowledge Areas
  - 12 Practical Skills

OpenJQR – SOC Analyst

Environment Basics

Available tools

Common network protocols

Endpoint basics

"What do I have access to?"

Search Techniques

Building queries in aggregation tools

“How do I get the data I need?”

OSINT Techniques

Introduction to public resources

Improving search engine queries

“What can I use to help confirm that X is malicious?”

OpenJQR – Development Roadmap and Future Plans

Engage with the community

- More contributors
- More references

Map to NIST NICE

Expand the SOC JQR into multiple SOC specialty JQRs

- Network Analyst
- Endpoint Analyst
- Threat Intel Analyst

Gigamon

OpenJQR – Release

- https://github.com/alexsirr/OpenJQR
- Contact us at: openjqr@gmail.com

OpenJQR – Community Engagement

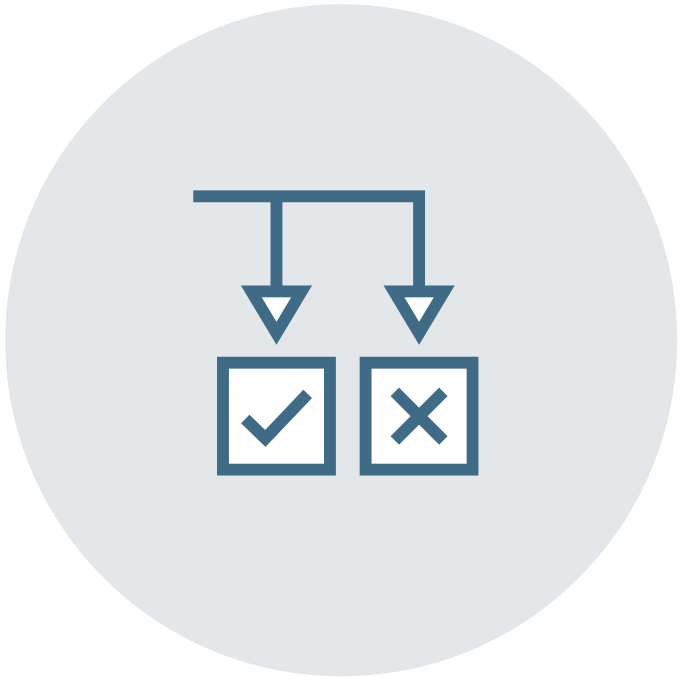
- Give organizations a foundation to build and customize their own JQRs to more easily hire new people
- Way to prepare interns and folks that are looking to enter the field
- Providing real-world structure but needs as much engagement as possible on tools and what analysts are doing
- Open Source model
  - Feedback on what works
  - Feedback on what doesn't work
- If you hire entry-level security analysts we are keen to engage with you for your feedback and input

Gigamon

Gigamon®

Lessons Learned

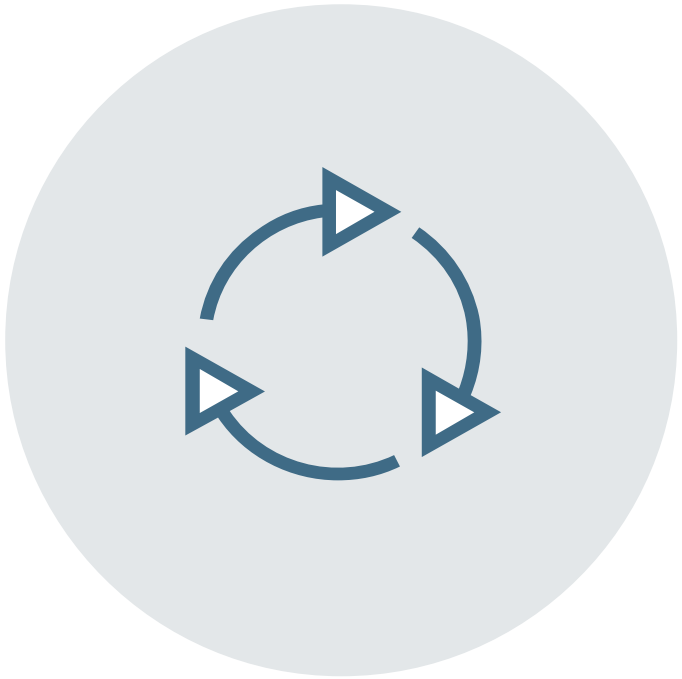
Lessons Learned



- Screen your interns
  - Practical challenges that encourage applicants
  - Require writing, self-directed research
  - Require a hard timeline
- Support your interns
  - Paid Internships
  - Give interns stock and ownership
  - Tier-1 Training opportunities
  - Structured growth opportunities
- Continually develop your training
- Final project
- Have clearly defined success criteria and timelines
- Don’t be afraid not to hire your interns

Gigamon

Feedback Loops are Critical



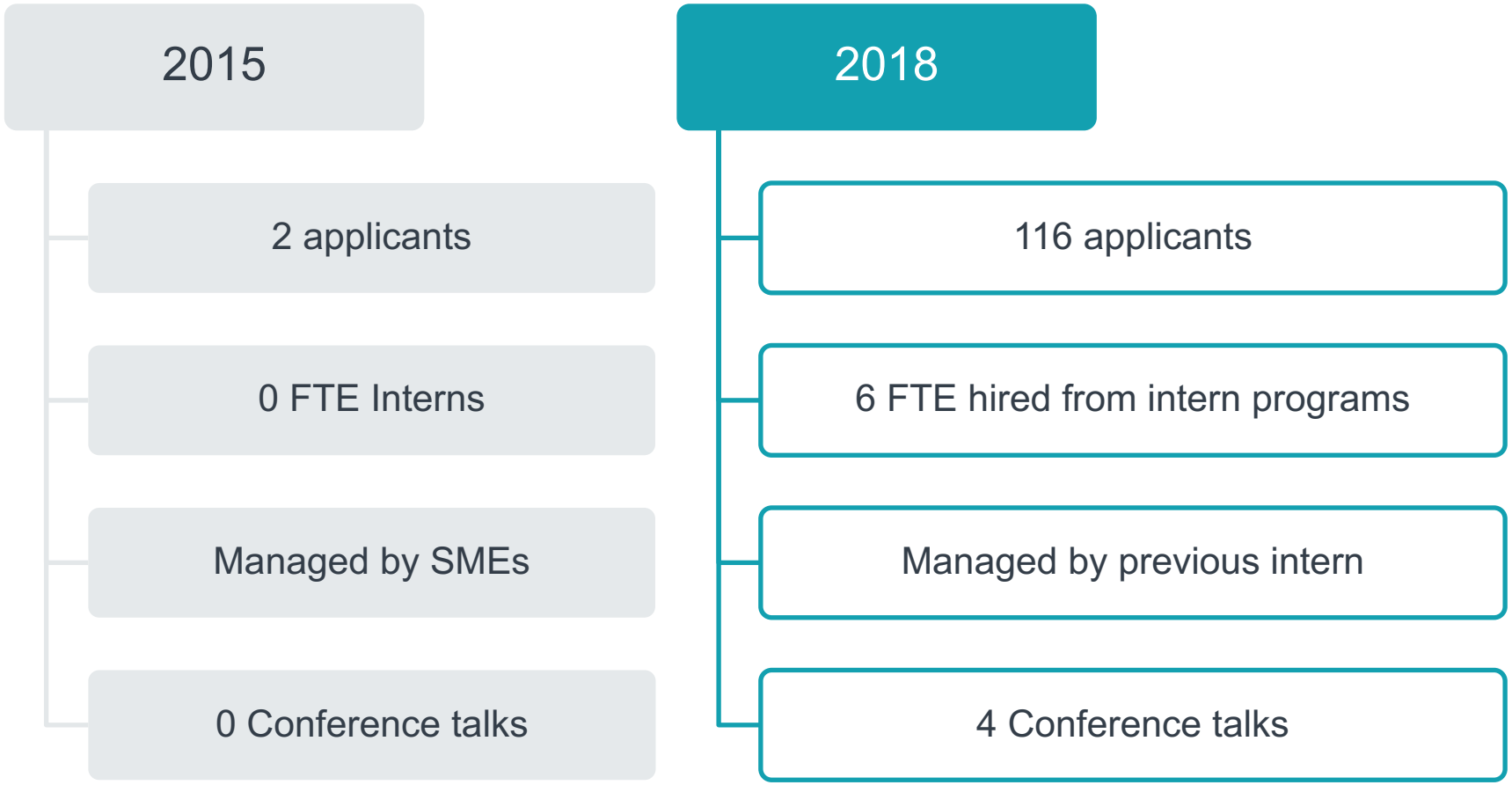
- InfoSec is a fast moving space
- Skills are perishable
- Your internal tools and tasks are changing
- The people you're training are then doing the work
- Leverage their experience at work to build better training
- The trainees must become the trainers

JQR Evolution Over Time

2015	2018
✓ 103 questions	✓ 54 questions
✓ Networking and Protocols	✓ Company background
✓ Security Investigations	✓ IQL
	✓ Attack Chain
	✓ Detections
	✓ Capstone

Gigamon

Intern Program Evolution



Intern Experience

Assimilated into the team

Work was not purely grunt labor

Worked closely with a fellow interns

FTE offer at the end

Questions?

Thank you