Lessons Learned from Teaching CTI All Over the World

Jess Garcia

www.sans.org

www.one-esecurity.com

Jess Garcia - Background

Hat 1: One eSecurity - Active DFIR/CTI Practitioner & Consultant

- One eSecurity Founder/Owner
  - 20 employees, DFIR/CTI focus
- 23+ years in Cybersecurity, mainly DFIR/CTI
  - Government 10 years / Private 13 years
- DFIR/CTI Investigations & Consulting for Top Global Organizations
- Trans-national Investigations World Wide

Hat 2: SANS Institute - Principal SANS DFIR/CTI Instructor

- 15+ years (since 2002)
- Lead DFIR/CTI Instructor EMEA
- 9 different courses taught (7 DFIR/CTI)
- 15+ courses taught per year internationally

“Research” Context

〉[Hat 1] DFIR Investigations & Consulting:

- Dozens of APT / Cybercrime Investigations
- Multiple consulting sessions helping organizations establish CTI capabilities

〉[Hat 2] Training:

- 10+ SANS FOR578 CTI courses taught in 2016-7
- Locations: Europe, Middle East, Asia, Australia

SANS FOR578 Syllabus

- *5 day* course
- **Content**
  - CTI Overview
    - Intelligence
    - Lexicon and Definitions
    - Traditional Intelligence Cycle
    - Threat & Risk
  - Tactical CTI
    - Kill Chain
    - Diamond Model
    - Handling Multiple Kill Chains
    - Pivoting OSINT
  - Operational CTI
    - Intelligence Aggregation & Data Visualization
    - Campaigns
    - Storing & Sharing Threat Intelligence
  - Strategic CTI
    - Psychology of Intelligence Analysis
    - Analysis of Competing Hypotheses
    - Attribution

What is the Students Organizational Background?

- Orgs with already existing CTI Capabilities
- Organizational Backgrounds

What is YOUR Organizational Background?

What is the Students Professional Background?

- Professional Background
- Roles

What is YOUR Professional Background?

What Are Students Looking For?

- Consumers / Producers
- Most students unaware of the Tactical / Operational / Strategic layers
- Initially most students only interested in Tactical
- Very little interest (initially) in Operational, Strategic
- Most students confess that Management does not understand the Strategic Value of CTI

What are YOU Looking For?

What Are Students Most Common Questions?

- Tools
  - What are the best tools?
  - Is Open Source ok?
  - What commercial tools are available?
- Feeds
  - Which ones should I use?
  - Which feeds should I use?
  - How many indicators are enough?
  - When is it ok to pay?

What Are YOUR Questions?

What Are Students Most Common Complains / Needs?

- Sharing
  - Challenges:
    - Limited visibility of threats at the Strategic Level
  - Need of Strategic Sharing inside communities
- Awareness
  - At the highest organizational layers
  - Why CTI
    - Many students don't really know what they want
  - Consumer / Producer
  - The Million-IOC problem

What are YOUR Complains / Needs?

What Do Students Value Most from the Training?

- Operational & Strategic
- Team Work
- Discussions

What do YOU value most?

Jess Garcia

jess.garcia@one-esecurity.com
Twitter: @j3ssgarcia

www.sans.org
info@sans.org

www.one-esecurity.com
info@one-esecurity.com
+44 20 8123 5211