Building and Retaining an ICS Cybersecurity Workforce

Robert M. Lee,
CEO & Founder,
Dragos

Steve Livingston
Principal
Deloitte & Touche LLP

IT compared to OT

It’s not IT vs. OT

- OT is essentially mission critical IT but, critically, they are an important part of the ICS
- Different systems, network protocols, data sources, etc. all exist but that’s not the point
  - ICS security is a system of systems security with a much different mission and impact
  - Safety, environmental impact, process availability, and intellectual property are key
  - The point isn’t the Operating System, yes, we have Windows too
- In a simplistic way think of OT as IT + Physics
  - The physics piece is the hard part
- Many of the basics of IT security simply do not apply (e.g. vulnerability patching’s value)
- Different mission, different systems, different threats, and different impact = don’t copy/paste your Enterprise security strategy into the ICS

Embrace and Work with HR

Common Mistakes

- “Cybersecurity Job Shortage”
- College Degrees
- Years of Experience
- Re-classifying IT as Cybersecurity

Common Opportunities

- “How it’s Made”
- Training and Retention
- Empowerment
- Career Development
- Mission

OT Skill Shortage

Hard to get access to industrial environments and training

Industrial ranges can come close but are often extremely costly with very little virtualization

Try to engage the operations side of the house at your company; take interest in the mission and leave out the “security checklist”

Engage the Community

Dragos' ICS Roadshow:
https://www.dragos.com/dragos-ics-roadshow/

Dragos Industrial Security Conf:
http://dragos.com/disc

SANS ICS Summit
https://ics.sans.org/events

GridSecCon

S4
https://s4xevents.com/

ICSJWG

One Possible Path

There is no set or defined path

- https://www.robertmlee.org/a-collection-of-resources-for-getting-started-in-icsscada-cybersecurity/
  - Learn the Language (physical process videos)
  - ICS Cyber Kill Chain
  - Reports on STUXNET, Ukraine 2015, Ukraine 2016, TRISIS, and Dragos Year in Review Reports

- https://www.networkdefense.co/
  - Investigation Theory
  - Building Virtual Labs
  - Practical Packet Analysis
  - ELK For Security Analysis
  - Effective Information Security Writing

- SANS ICS
  - SANS ICS410
  - SANS ICS515
  - SANS ICS612

- Dragos 5 Day Class

- Doughnuts, drinks, operations staff

Recommended Reading and Courses

Recommended Reading

My Reading List:

https://www.robertmlee.org/a-collection-of-resources-for-getting-started-in-icsscada-cybersecurity/

Dragos' Reading List

https://dragos.com/blog/industry-news/a-dragos-industrial-control-system-security-reading-list/

Dragos' Year in Review Reports

https://dragos.com/year-in-review/

Recommended Courses

US-CERT Red vs. Blue (Free)

https://www.us-cert.gov/ics/Training-Available-Through-ICS-CERT

SANS ICS

https://ics.sans.org/training/courses

Dragos' 5 Day Course

https://dragos.com/training/

Recommended Approach

Engage Operations

A box of doughnuts and a case of beverages go along way

Go On a Hunt

Be proactive in your environment not looking just for vulnerabilities and access control but search for threats and identify collection gaps

Get Knowledge Transfer

Bring in external teams such as Dragos or Deloitte to do assessments but don't just get a report; ride along and ask questions