RSAConference2019

San Francisco | March 4–8 | Moscone Center

BETTER.

SESSION ID: TECH-F02

Intelligence-Driven Industrial Security with Case Studies in ICS Attacks

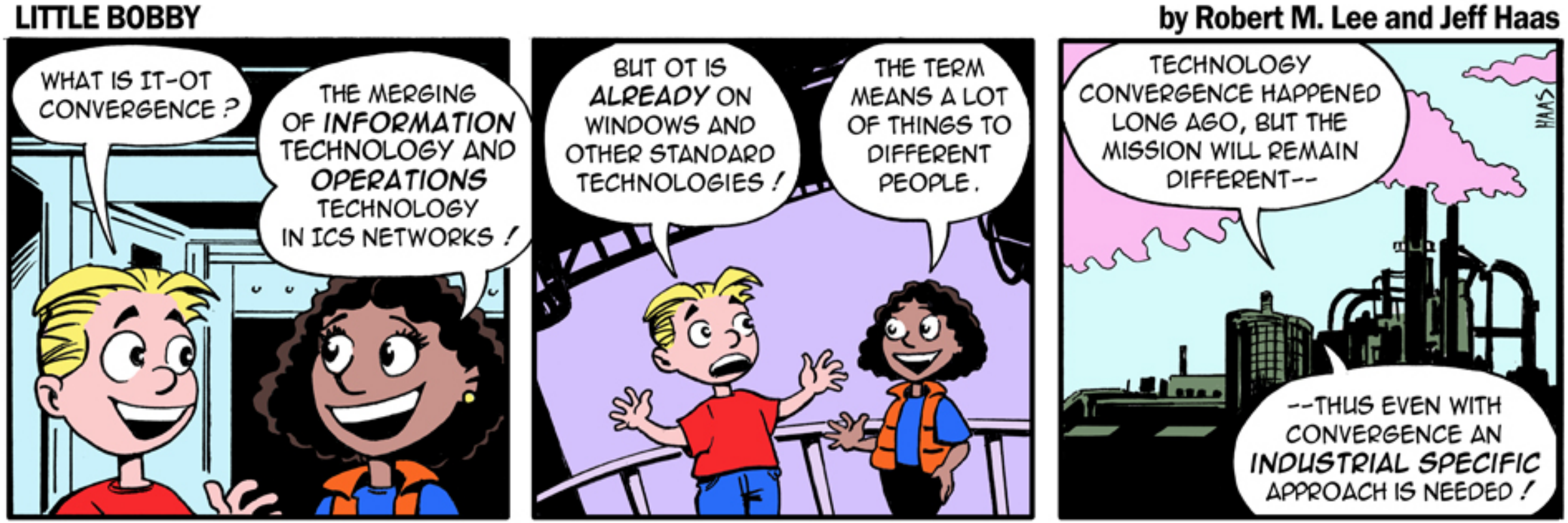
Robert M. Lee

CEO and Founder
Dragos, Inc.
@RobertMLee

About Me

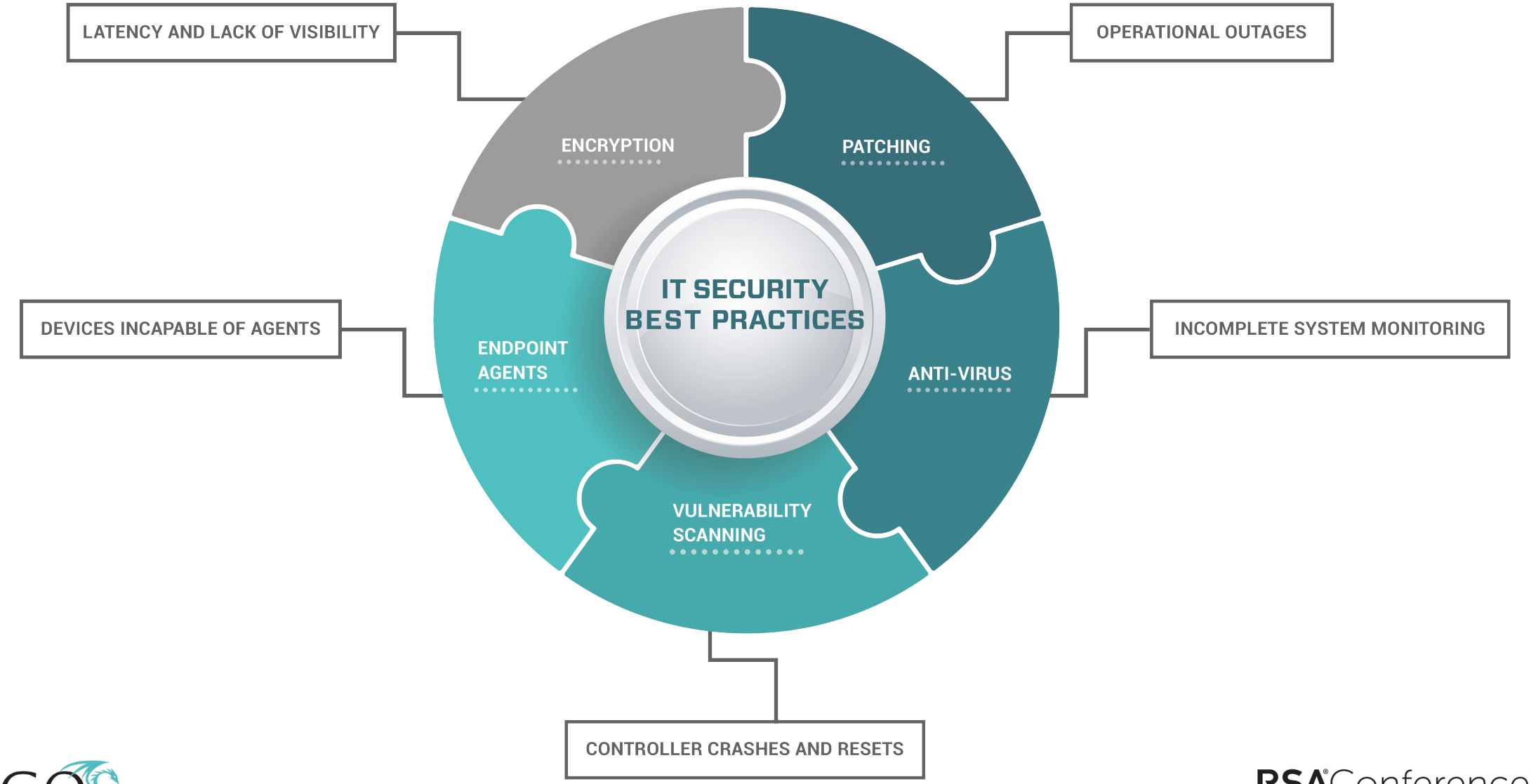
- CEO and Founder of Dragos, Inc
- Started career as a U.S. Air Force Cyber Warfare Operations Officer serving in the National Security Agency
  - Built a first-of-its-kind industrial control system (ICS) threat intel/discovery mission
- SANS Certified Instructor and Course Author
  - FOR578 – Cyber Threat Intelligence
  - ICS515 – ICS Active Defense & Incident Response

The Problem – IT Security is Different than ICS Security



Common IT Security Best Practices

Common Issues with IT Best Practices in ICS

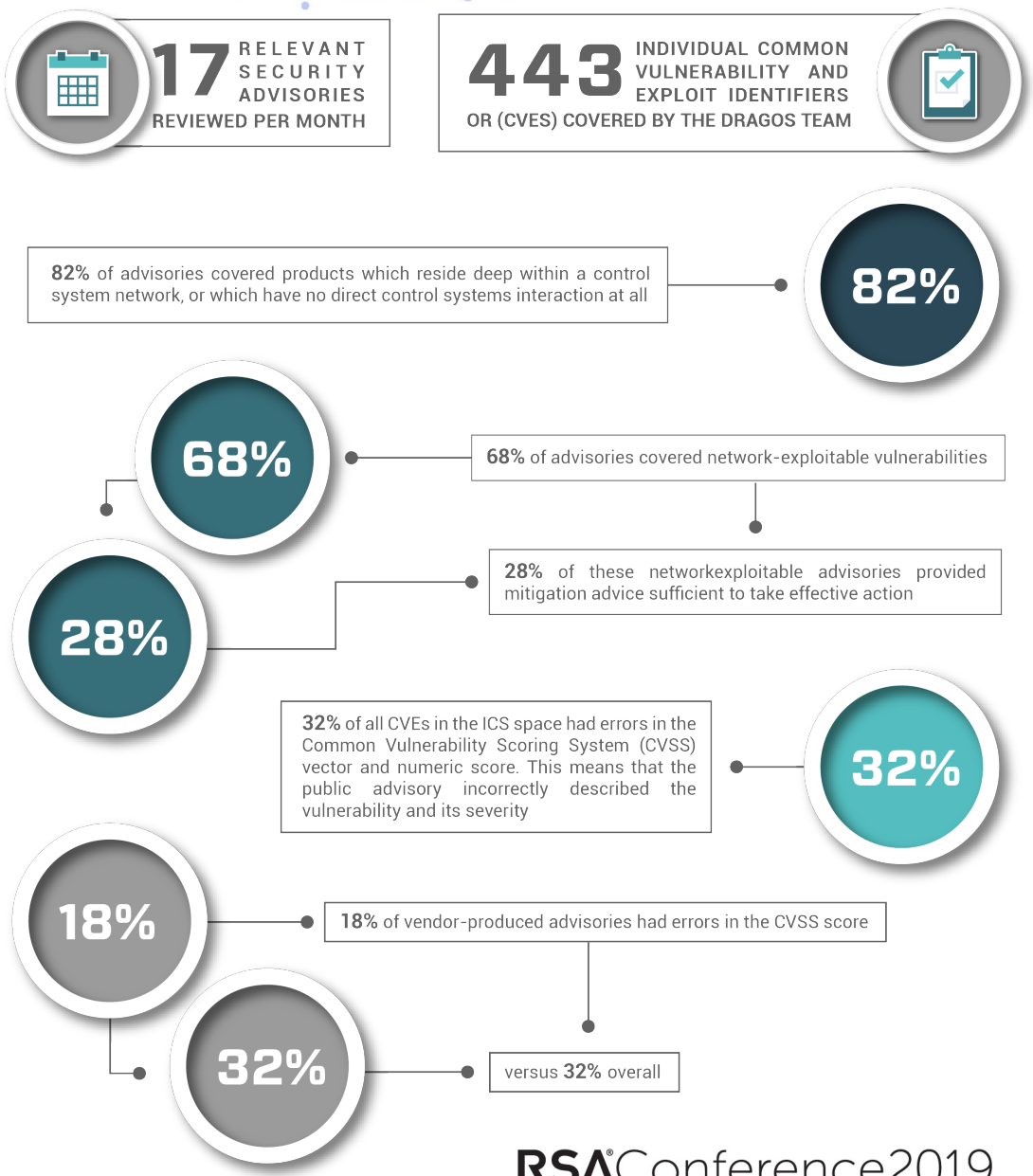


2018 Research on ICS Vulnerabilities

- Dragos' 2017 in Review reports revealed that for ICS vulnerabilities:
  - 64% of all vulns didn't eliminate the risk
  - 72% provided no alternate mitigation to the patch
  - Only 15% could be leveraged to gain initial access

2019 Research on ICS Intrusions

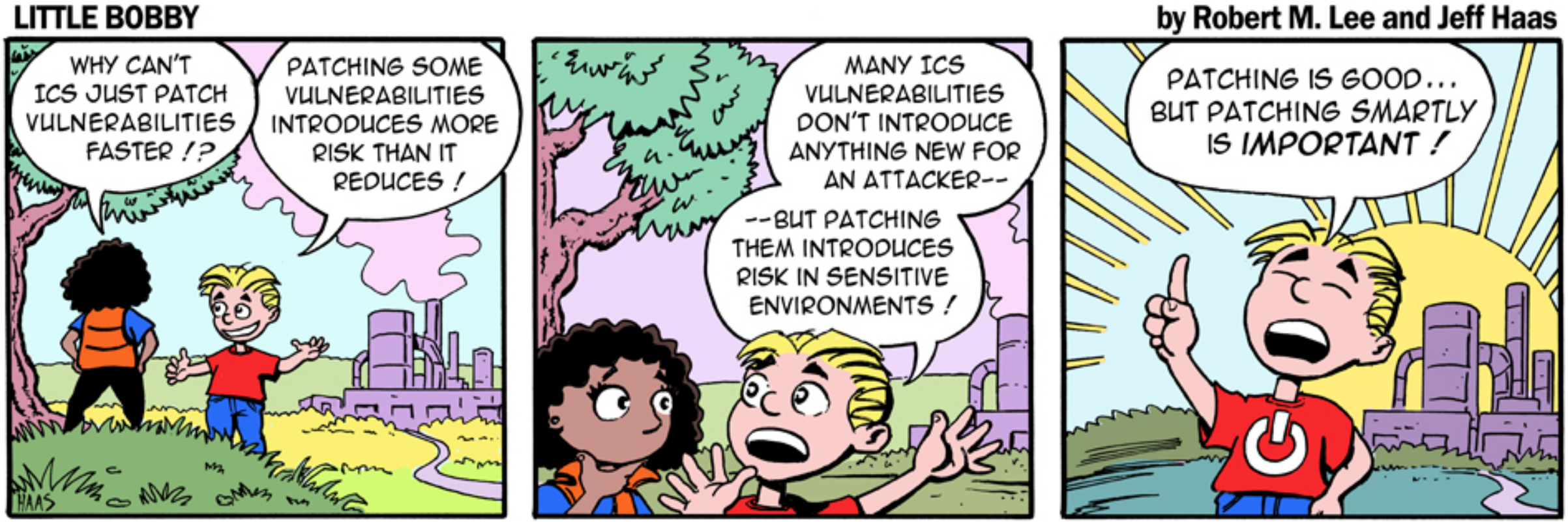
- Only 28% of network-exploitable advisories provided sufficient mitigation advice
- 32% of all CVEs in ICS had errors in the CVSS vector and score
- Nearly 72% of advisories cover HMI, EWS, and Field Device components yet nearly all of the vulnerabilities did not require the vulnerability to achieve the same functionality or impact



DRAGOS

RSAConference2019

One Approach – Intelligence-Driven ICS Security

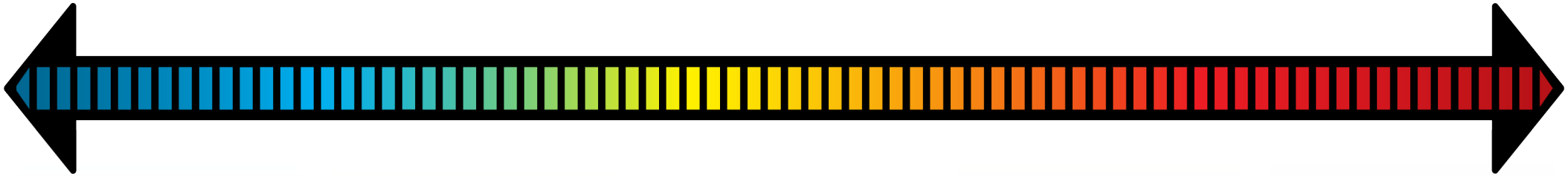


ICS Cyber Kill Chain

- Two Phase Kill Chain
- Adversary must understand the physical process and safeguards
- Takes more steps to do the type of attacks we're most concerned with

Ref: https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297

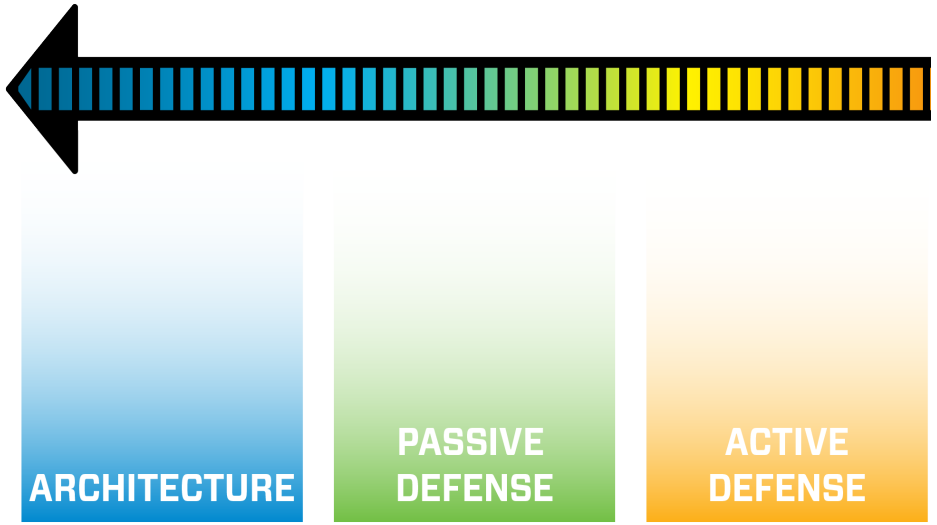
The Sliding Scale of Cybersecurity



ARCHITECTURE	PASSIVE DEFENSE	ACTIVE DEFENSE	INTELLIGENCE	OFFENSE
The planning, establishing, and upkeep of systems with security in mind	Systems added to the Architecture to provide reliable defense or insight against threats without consistent human interaction	The process of analysts monitoring for, responding to, and learning from adversaries internal to the network	Collecting data, exploiting it into information, and producing Intelligence	Legal countermeasures and self-defense actions against an adversary

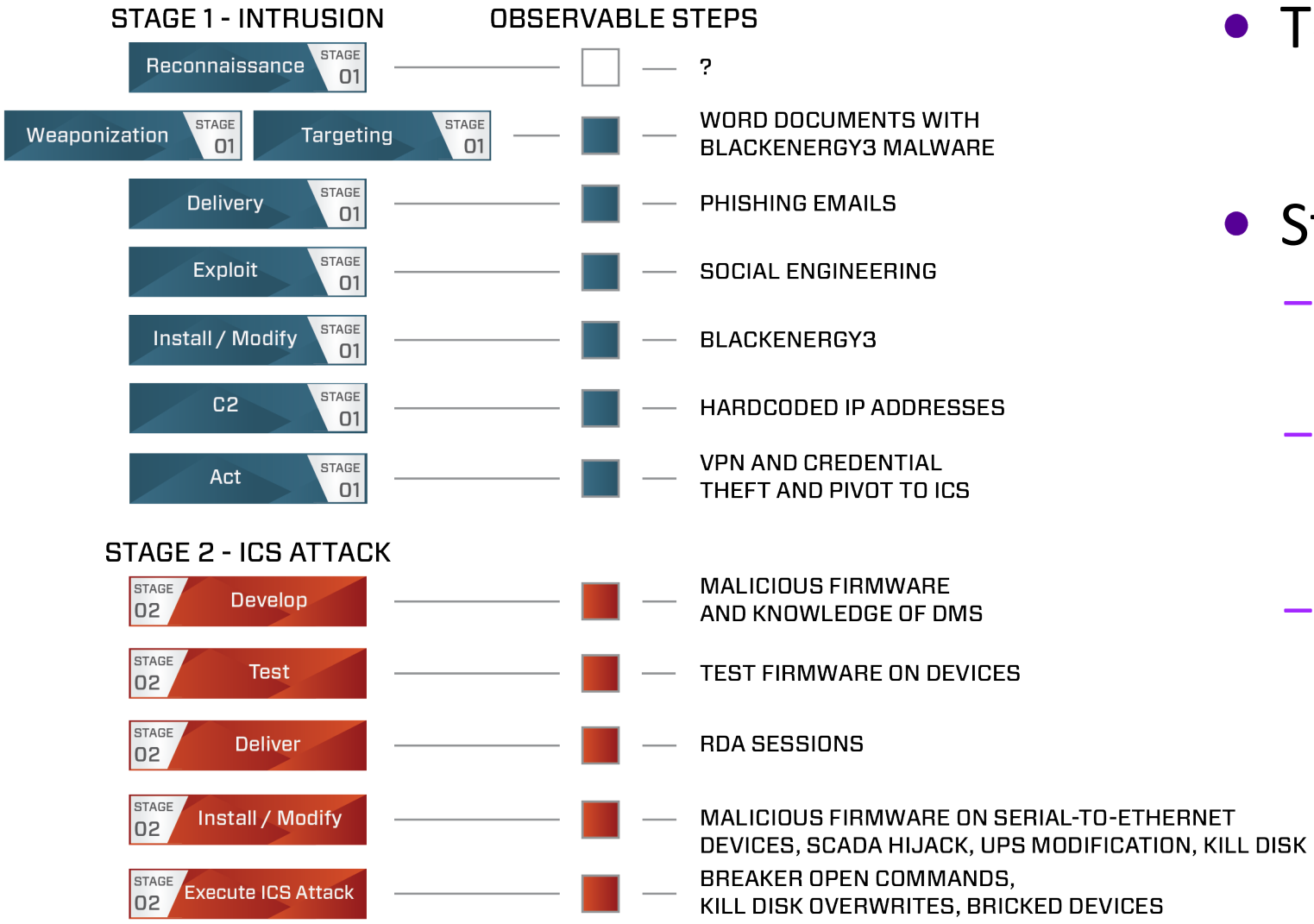
Ref: https://www.sans.org/reading-room/whitepapers/ActiveDefense/sliding-scale-cyber-security-36240

Map the Models Together



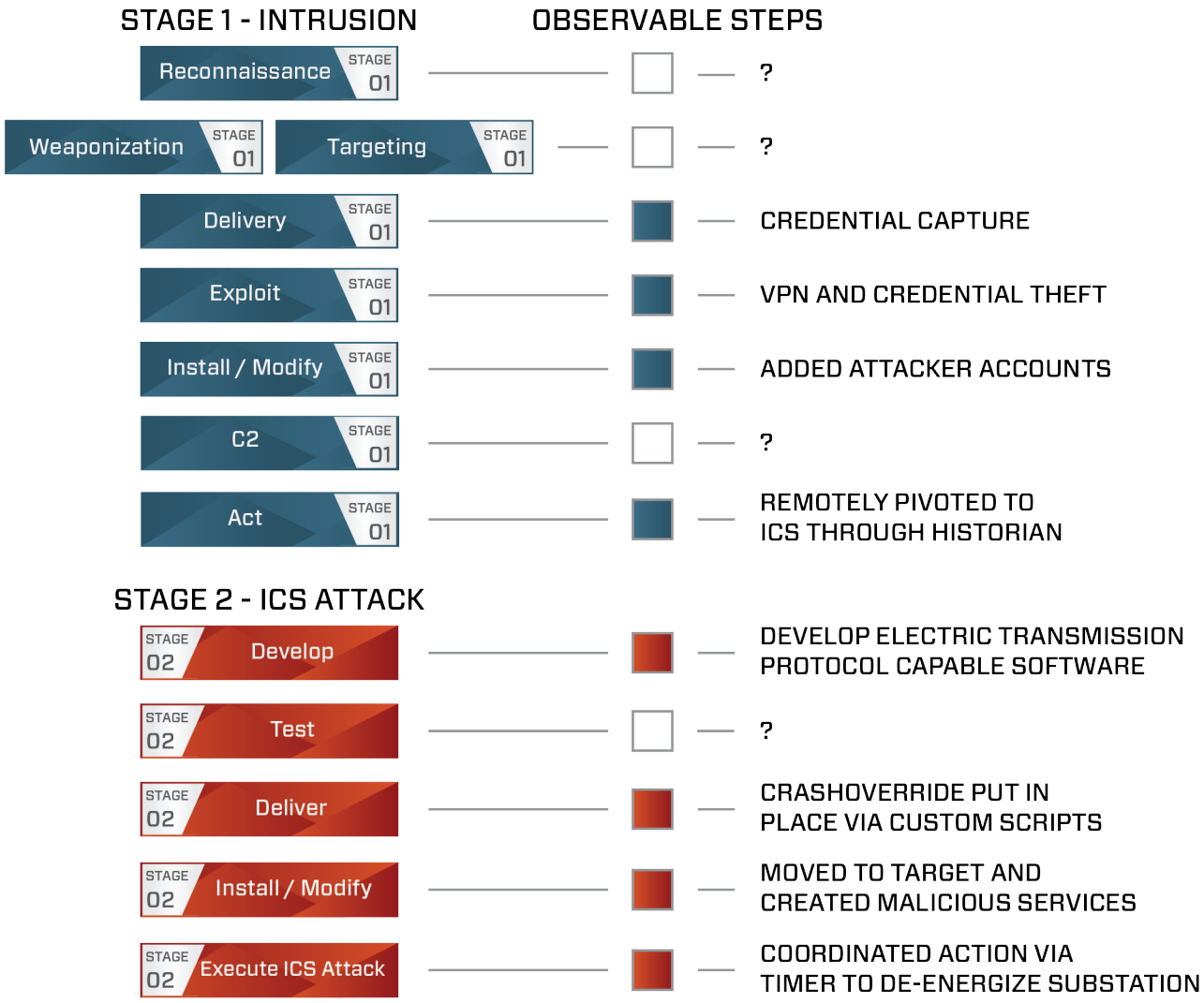
- For every observable step on Architecture, Passive Defense, and Active Defense note what is in place today and proposed for later
- Take the top few controls across the total of your intrusions for ~6 months – 1 year and those are *your* best practices off of *your* industrial threat landscape

Ukraine 2015



- Today: (whatever you have)
- Stage 2 Deliver Proposed:
  - Architecture:
    - 2 form authentication on access into ICS
  - Passive Defense:
    - ICS network visibility and analysis tool with VPN and RDA log ingest
  - Active Defense:
    - Analysts familiarize themselves with maintenance, integrator, and OEM accesses into ICS and what normal operations looks like

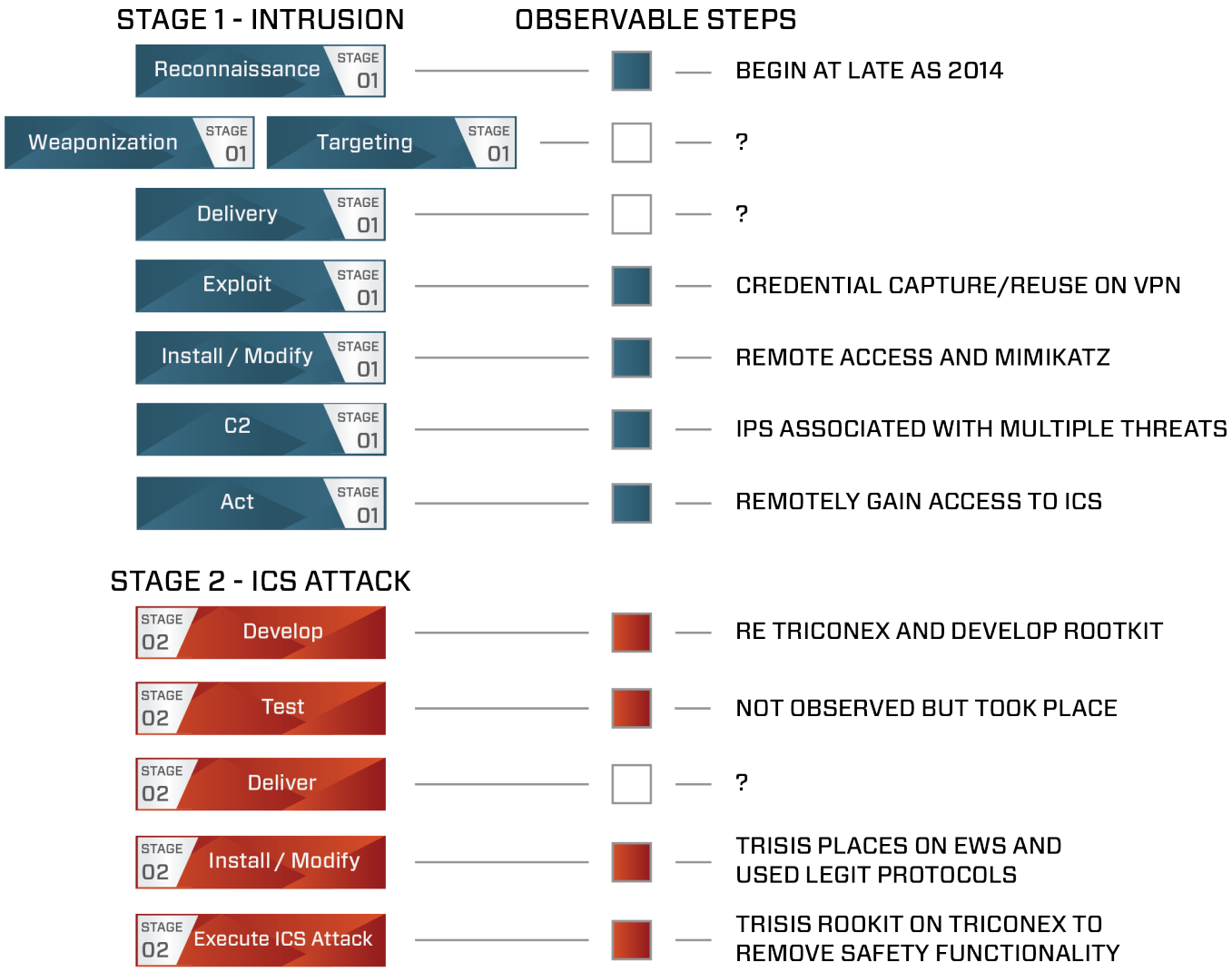
Ukraine "CRASHOVERRIDE" Attack 2016



- Today: (whatever you have)

- Stage 2 Install Proposed:
  - Architecture:
    - Host based logging on OT (HMI/EWS) to be able to identify new processes outside maintenance windows
  - Passive Defense:
    - Network visibility tool to consume host based logs and trigger on new HMI Master's (IEC-104 master)
  - Active Defense:
    - Analysts should learn (and then move into a playbook) new IEC-104 master processes, how to validate, and how to safely remove with operations

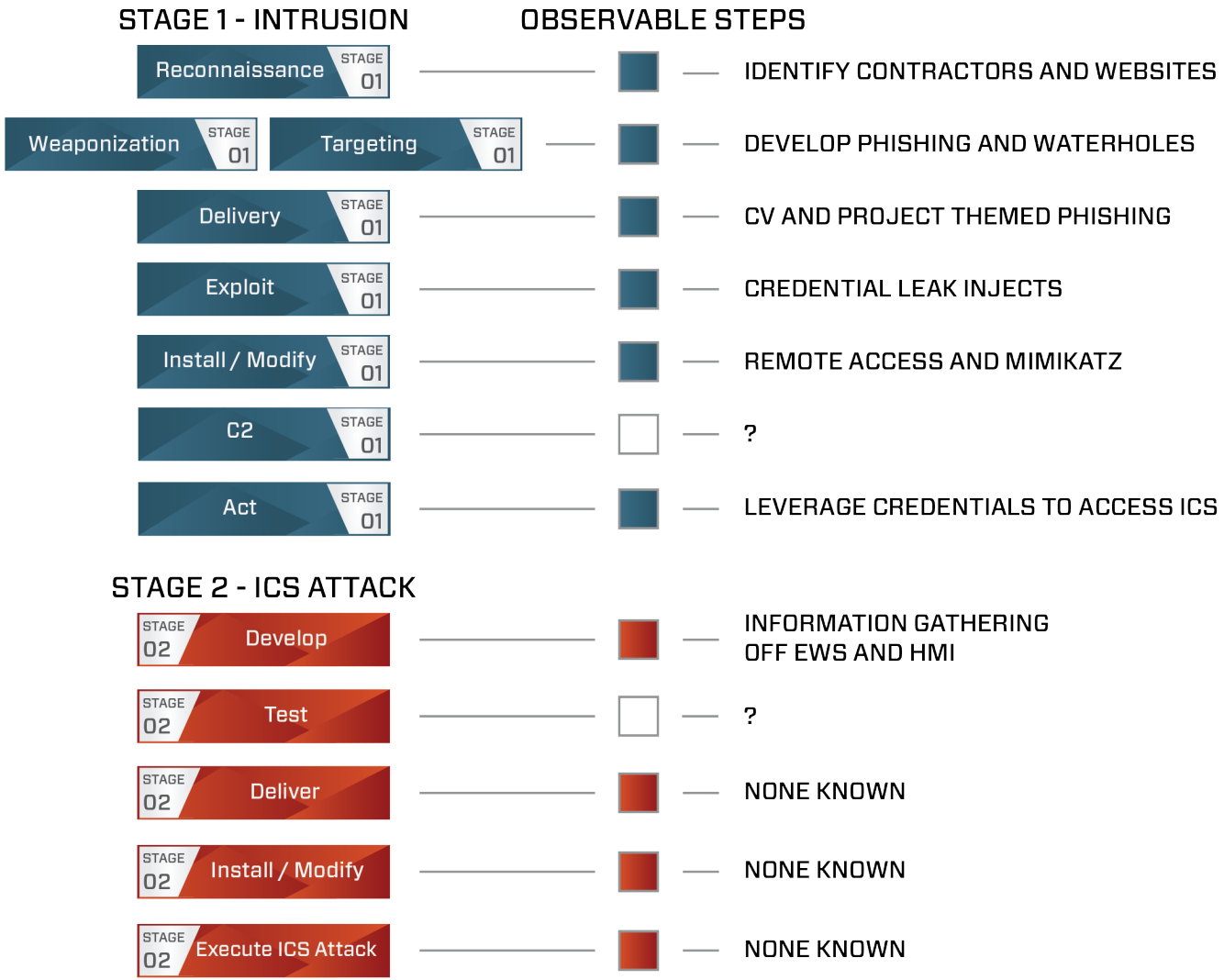
Saudi Arabia "TRISIS" Attack 2017



- Today: (whatever you have)

- Stage 2 Execute ICS Attack Proposed:
  - Architecture:
    - Segmentation of SIS
  - Passive Defense:
    - Detection capabilities that can inspect and analyze SIS protocols such as Tristation
  - Active Defense:
    - Incident responders should train and prepare for responding to an incident in an environment with unsafe conditions and no SIS

ALLANITE Activity Group 2016-2019



- Today: (whatever you have)

- Stage 2 Execute Develop:
  - Architecture:
    - 2 form authentication for connectivity into ICS from IT networks
  - Passive Defense:
    - Network visibility and detection on behaviors for HMI screenshot exfil
  - Active Defense:
    - Hunting tactics trained for behaviors associated with moving HMI/EWS information out of the ICS

ICS Threat Activity Groups

XENOTIME

RASPITE

ALLANITE

MAGNALLIUM

ELECTRUM

DYMALLOY

CHYRSENE

COVELLITE

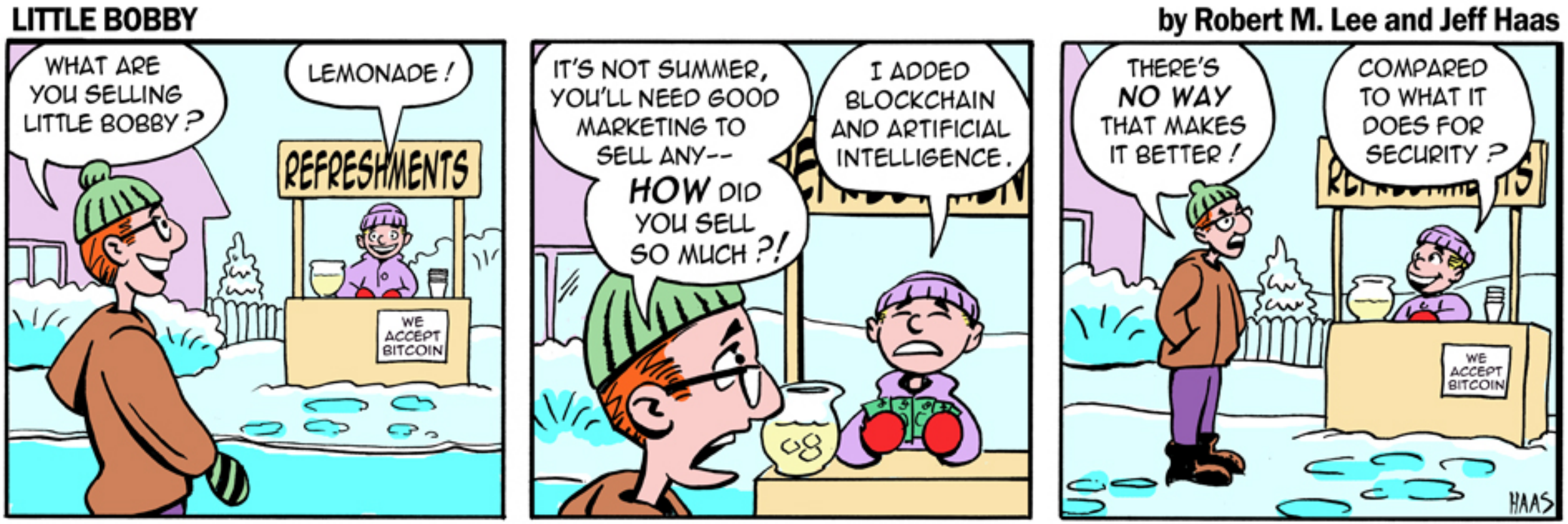
DRAGOS

RSAConference2019

Lessons to Apply Learned Across the Attacks

- Key Architecture Recommendations
  - Segmentation and chokepoints (not air gaps and diodes)
  - Enable logging not only from HMIs/EWS but also historians and controllers
  - Multi-factor authentication for accesses into the ICS
- Key Passive Defense Recommendations
  - Tools for ICS protocol dissection and network visibility
  - Tools for detection of adversary behaviors not just anomalies
- Key Active Defense Recommendations
  - Analysts trained on industrial operations including normal activity
  - Analysts empowered with investigation/response playbooks for ICS incidents
  - Analysts trained on industrial threat behaviors and ICS root cause analysis

Questions?



@RobertMLee
www.Dragos.com
@DragosInc