RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: SBX1-W16

Cyber Situational Awareness in ICS/SCADA Networks

Jonathan Lavender

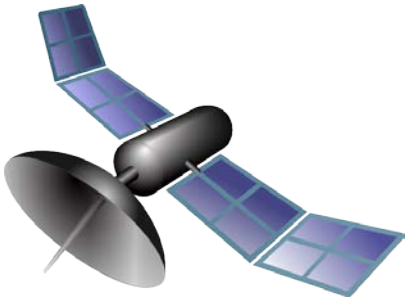
Chief Technology Officer
Dragos Security, LLC
@jonlavender

Special Thanks to @robertmlee

#RSAC

Controls Systems - IoT

Internet of Things

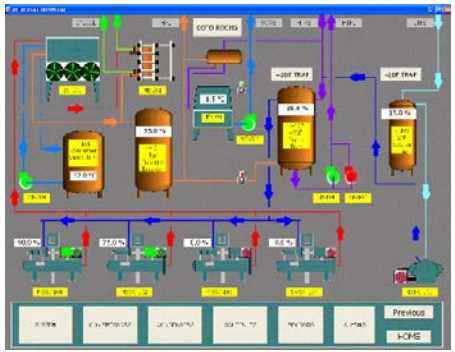


DRAGOS SECURITY™

Controls Systems - Industrial

Controls Systems - Industrial

Industrial



Fake vs Real Threats

2008 Turkey Pipeline Explosion

Fake vs Real Threats

Israel Electric Authority
Cyber Attack

Fake vs Real Threats

Ukraine Power Grid
Cyber Attack

Concerns with ICS

Loss of View

Denial of View

Manipulation of Safety

Loss of Control

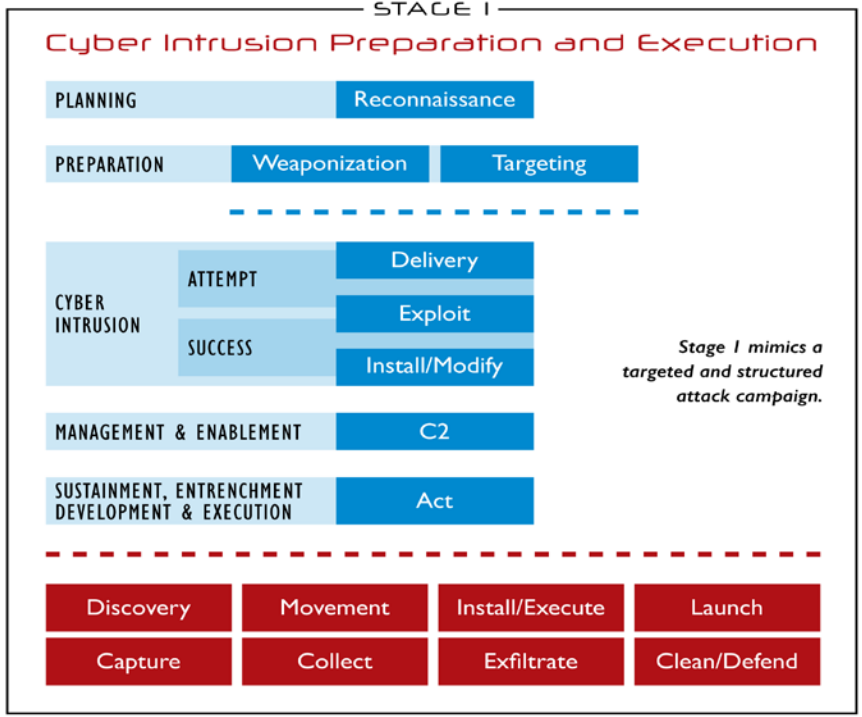
Manipulation of View

Manipulation of Sensors

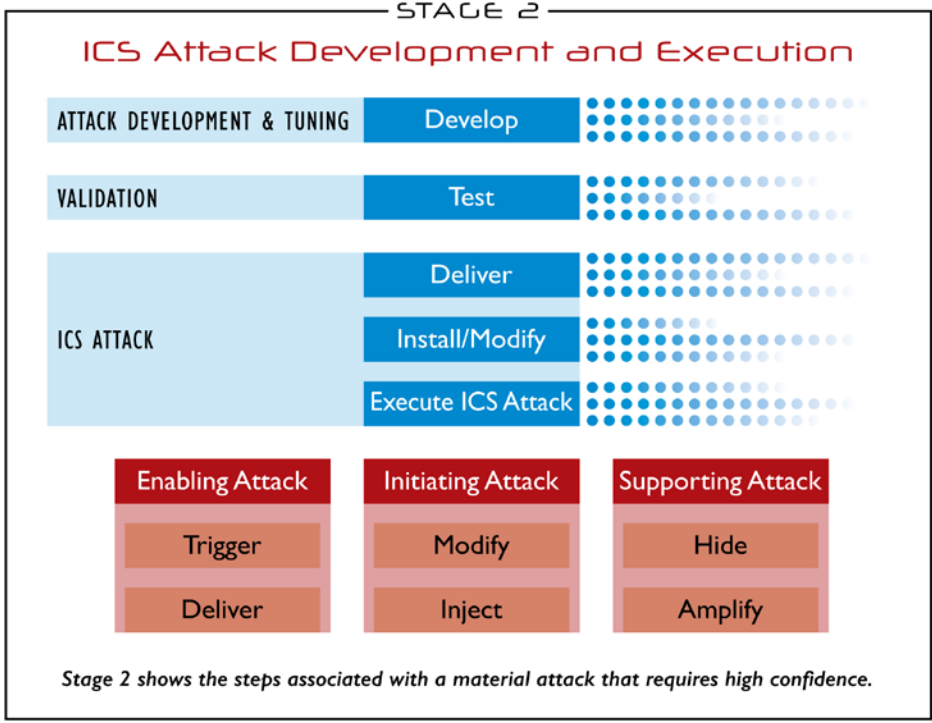
Denial of Control

Manipulation of Control

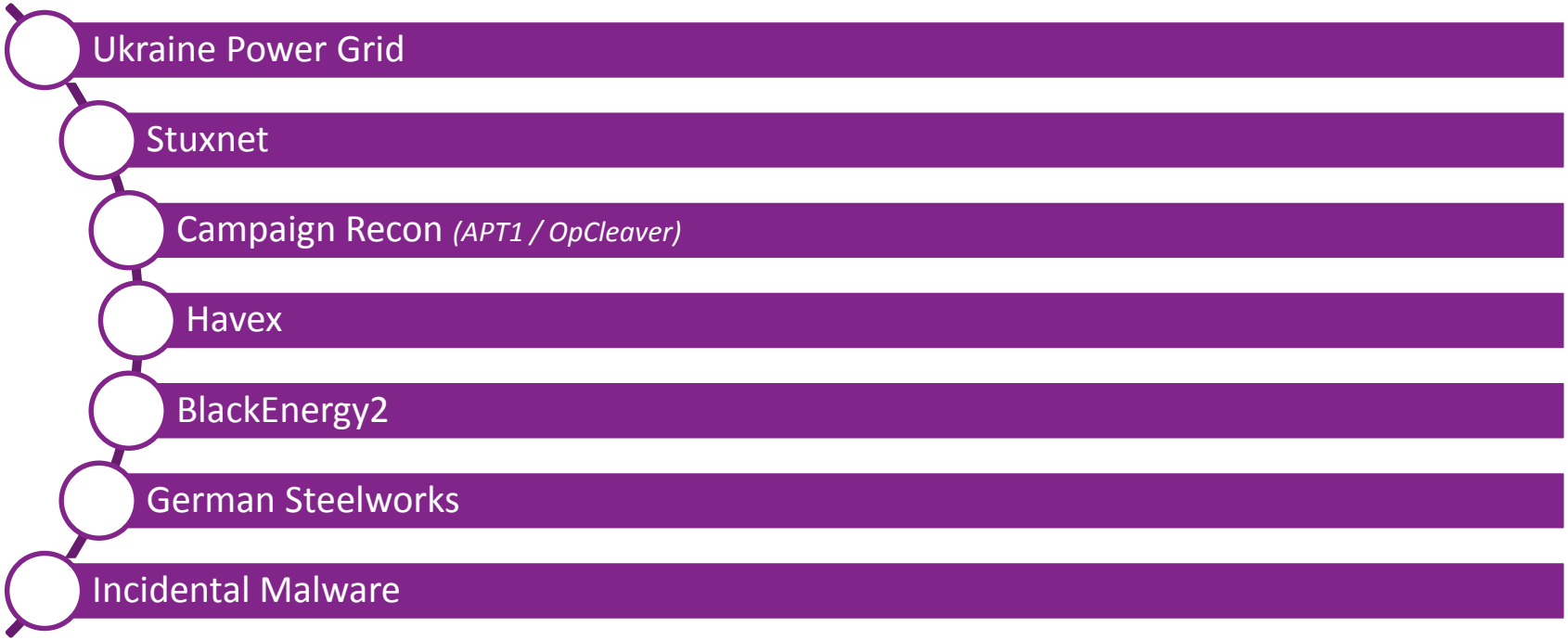
Denial of Safety



Based on the Cyber Kill Chain® model from Lockheed Martin



Real ICS Threats



Sliding Scale of Cyber Security

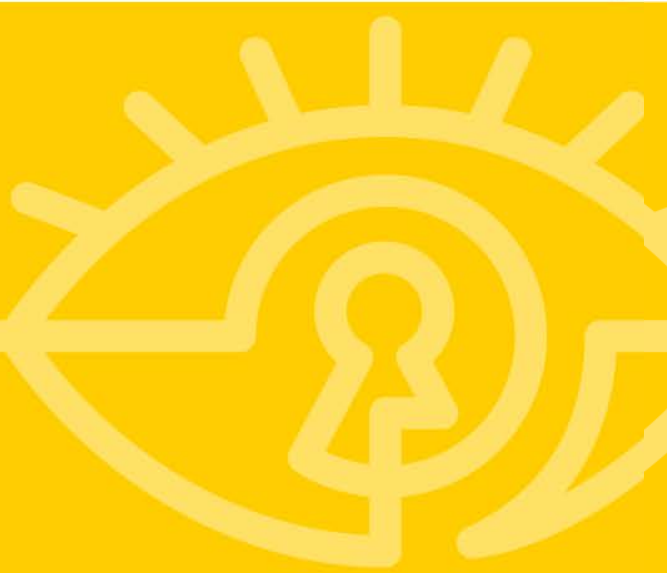
Architecture
Supply Chain, Architecting the network, maintaining/patching

Active Defense
Analysts monitor for, respond to, and learn from adversaries internal to the network

Offense
Legal countermeasures, "hack-back", etc.

Passive Defense
Provide protection without constant human interaction Firewalls, IPS, AV, etc.

Intelligence
Collecting data, exploiting it into information, and producing Intelligence



Cyber Situational Awareness

Subhead if needed

Situational Awareness Is…

Cyber situational awareness is the concept of understanding and visualizing the networked environment and its individual elements to identify changes across time

Situational Awareness Is NOT…

Why Defenders Fail

- How can you protect what you don't know you have?

[Graphic Here]

Why the Adversary Wins

Tipping the Scale in ICS

- Defenders should always understand their networks
- Adversaries should struggle to gain the same knowledge
- An ICS is typically smaller and more static than enterprise IT
- Networked OT devices/protocols less common to hackers

Benefits from Cyber-SA

- Baseline your network
  - Ports, Protocols, Assets, and Communication
- View your network over time
  - Recognize abnormalities
  - Gain insight into ing and understanding change is very important

Challenges

Challenges

- Shiny Object Syndrome
- Training, education, and experience
- Bridging the Gap, IT and OT
- Organizational Buy-in

Applying Cyber-SA

Architecture
Supply Chain, Architecting the network, maintaining/patching

Active Defense
Analysts monitor for, respond to, and learn from adversaries internal to the network

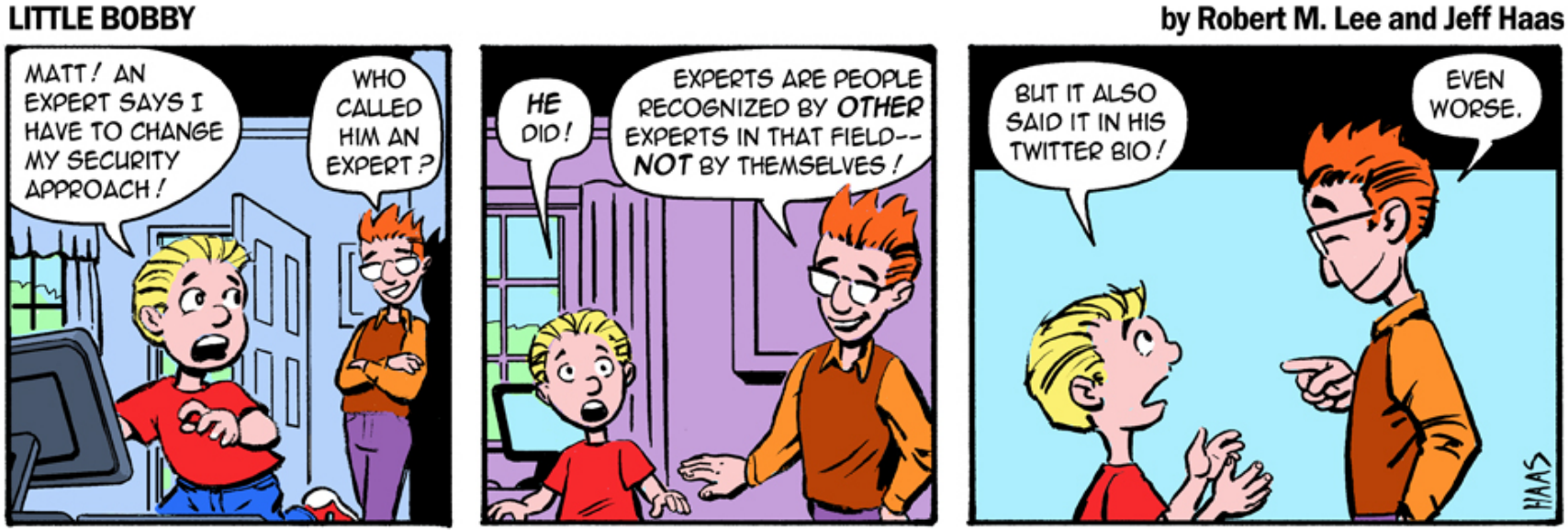
Offense
Legal countermeasures, “hack-back”, etc.

Passive Defense
Provide protection without constant human interaction Firewalls, IPS, AV, etc.

Intelligence
Collecting data, exploiting it into information, and producing Intelligence

DRAGOS SECURITY™

Questions


LITTLE BOBBY
by Robert M. Lee and Jeff Haas
MATT! AN EXPERT SAYS I HAVE TO CHANGE MY SECURITY APPROACH!
WHO CALLED HIM AN EXPERT?
HE DID!
EXPERTS ARE PEOPLE RECOGNIZED BY OTHER EXPERTS IN THAT FIELD-- NOT BY THEMSELVES!
BUT IT ALSO SAID IT IN HIS TWITTER BIO!
EVEN WORSE.
HAAS