RSAConference2019
Asia Pacific & Japan
Singapore | 16–18 July | Marina Bay Sands

SESSION ID: GPS-W09

Industrial Cyberthreats: Countering Those Who Target Our Civilization

Robert M. Lee

CEO and Co-Founder
Dragos, Inc.
@RobertMLee

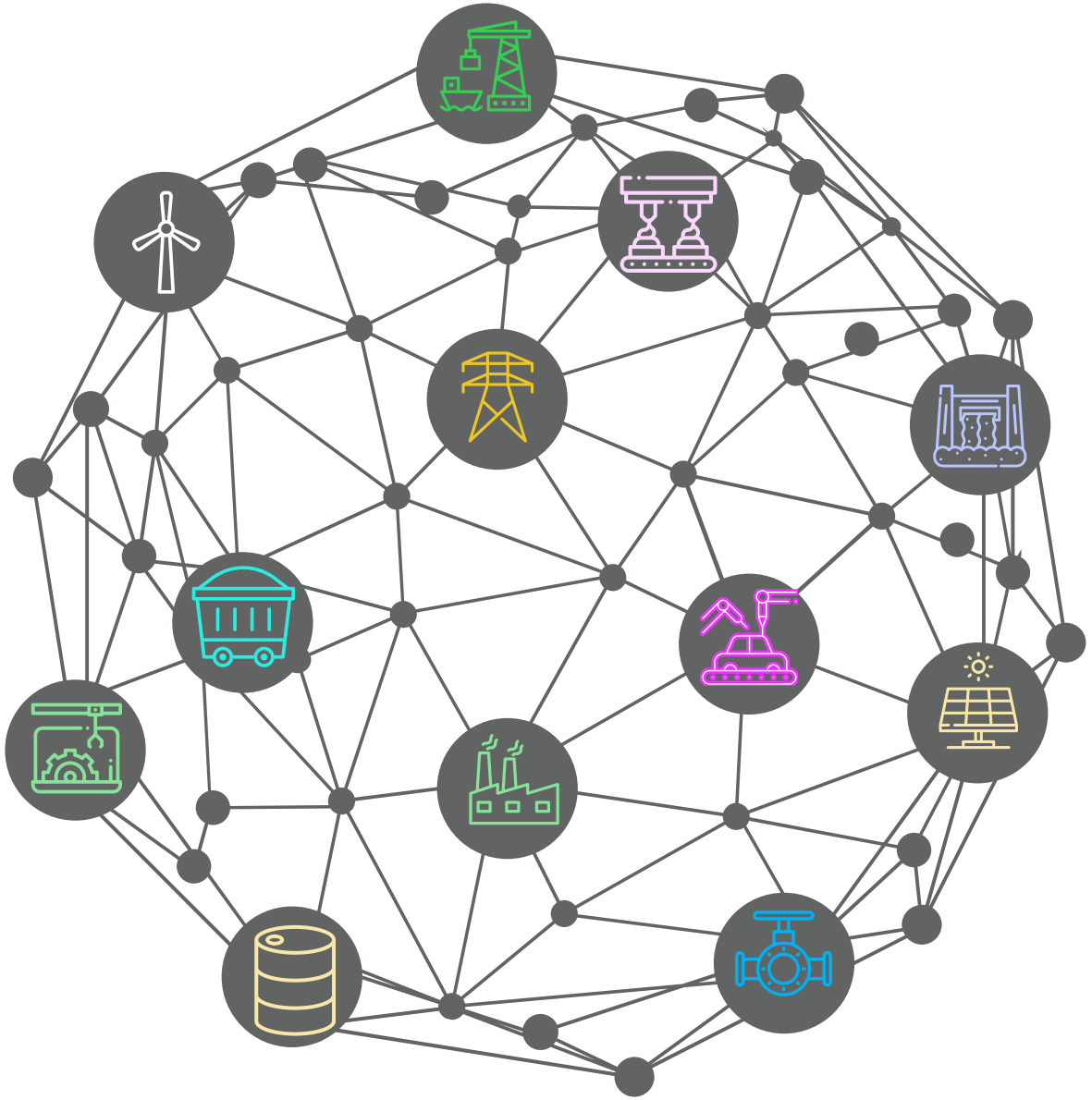
About Me

- 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

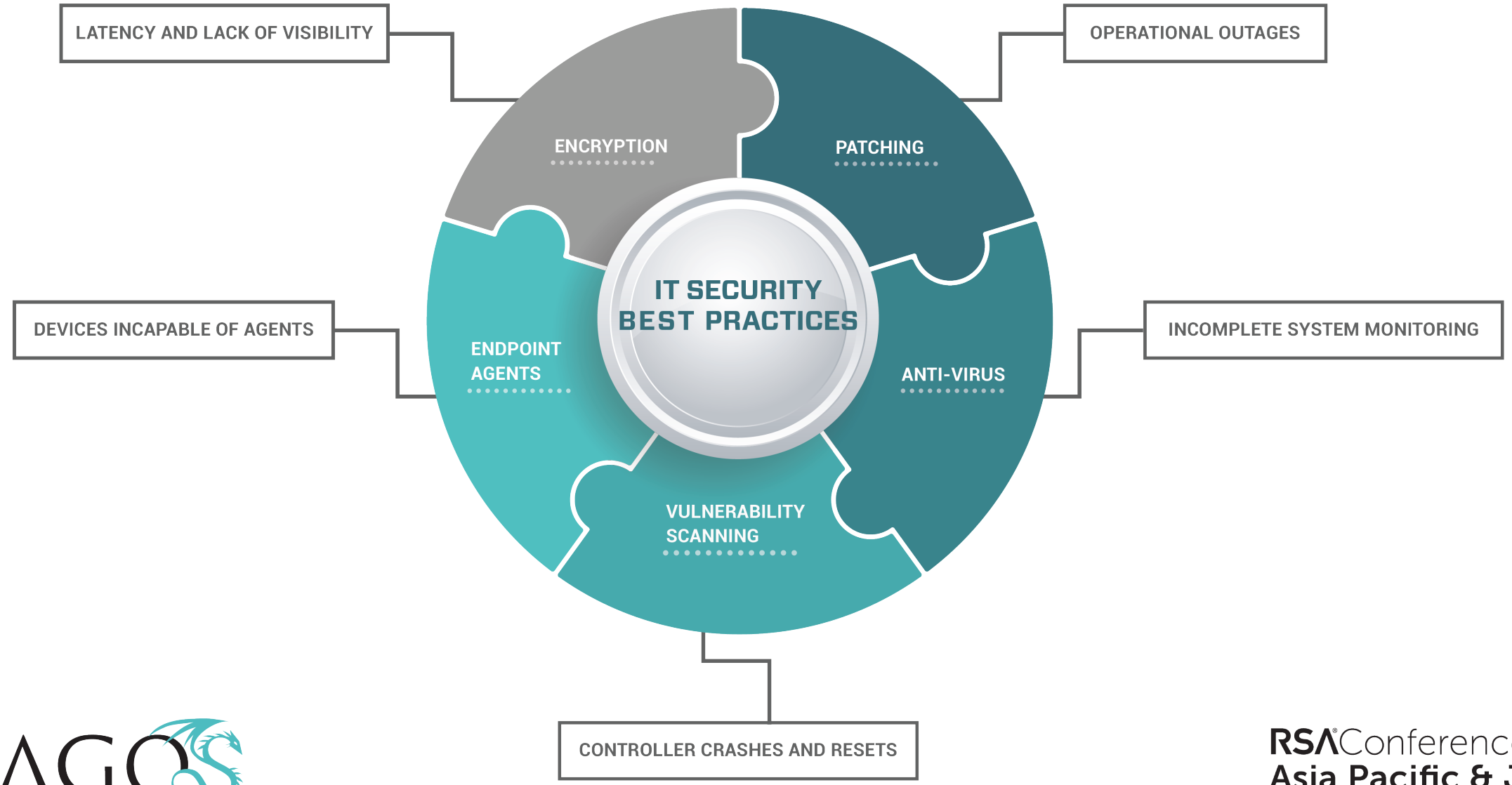
The Takeaways

- There are industrial specific cyber threats with unique tradecraft
- Most organizations have invested very little in industrial security
- Successful security strategies will prioritize what we've learned
- Tradecraft overlaps lends to highly successful detection strategy
- There are already key best practices to apply immediately

Our World is Industrial



Industrial Control Systems (ICS) Security is Different



RSAConference2019
Asia Pacific & Japan

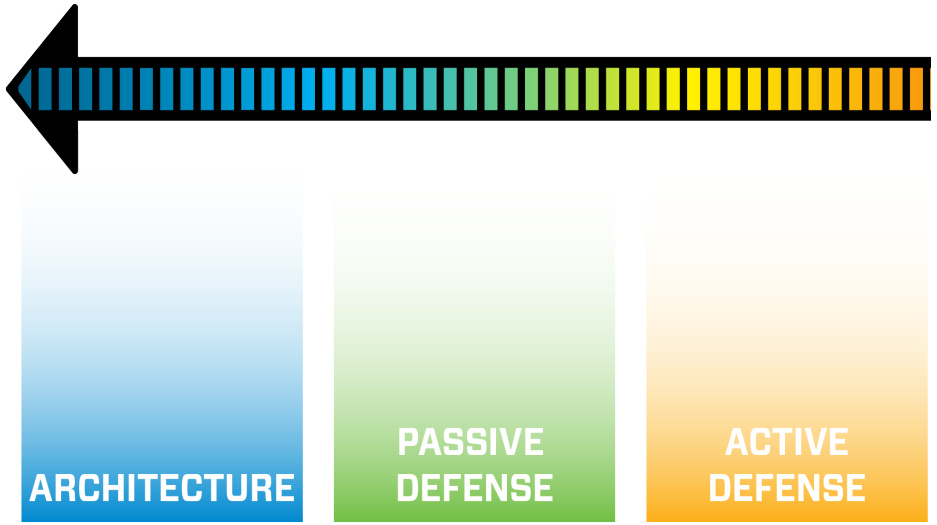
Taking an Intelligence-Driven Approach

Defense is Doable

Understanding ICS Cyber Attacks

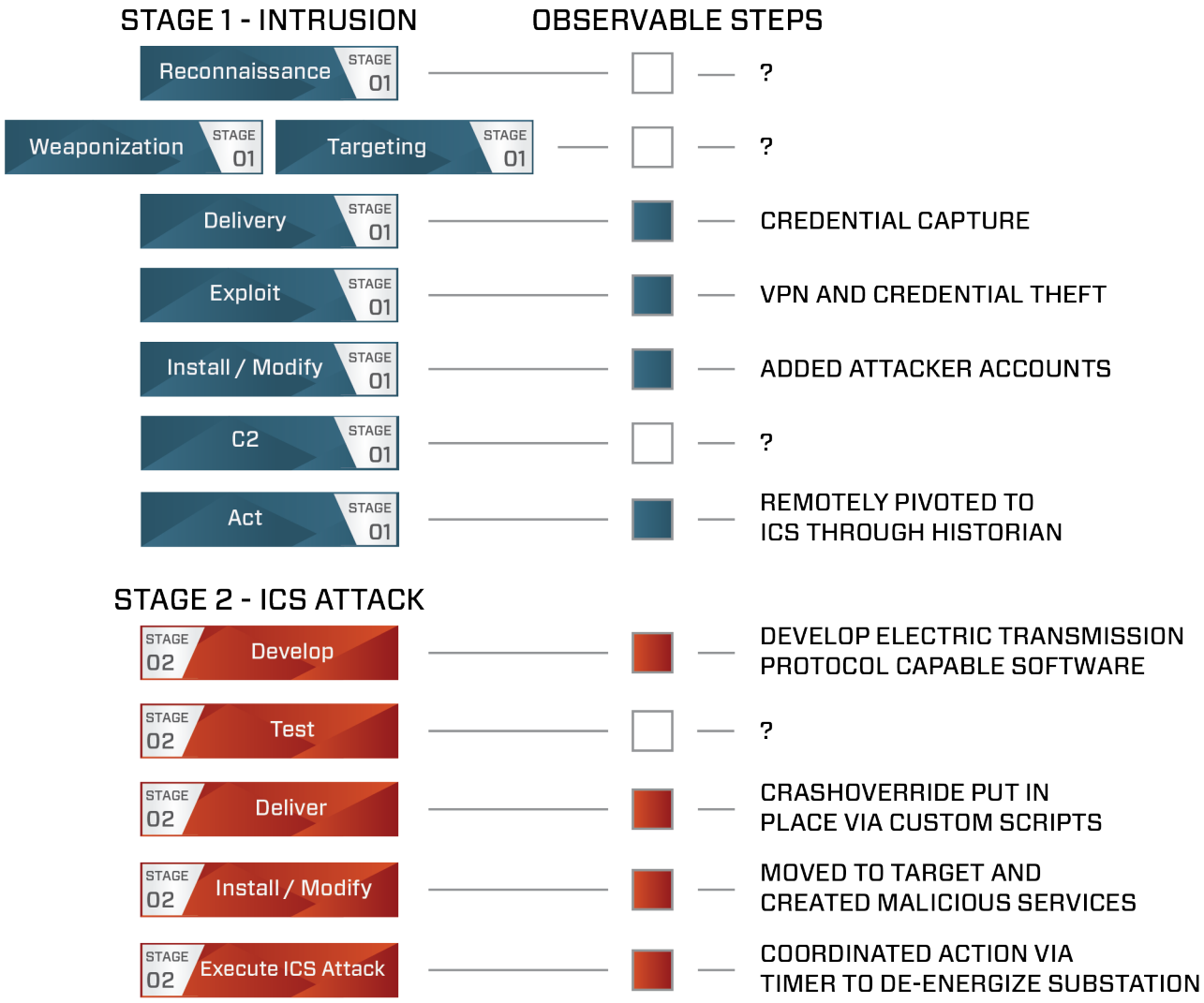
- Two Phase Kill Chain
- Adversary must understand the physical process and safeguards
- Takes more steps to do the type of attacks we're most concerned with

Achieving an Intelligence-Driven Approach



- 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 "CRASHOVERRIDE" Attack 2016

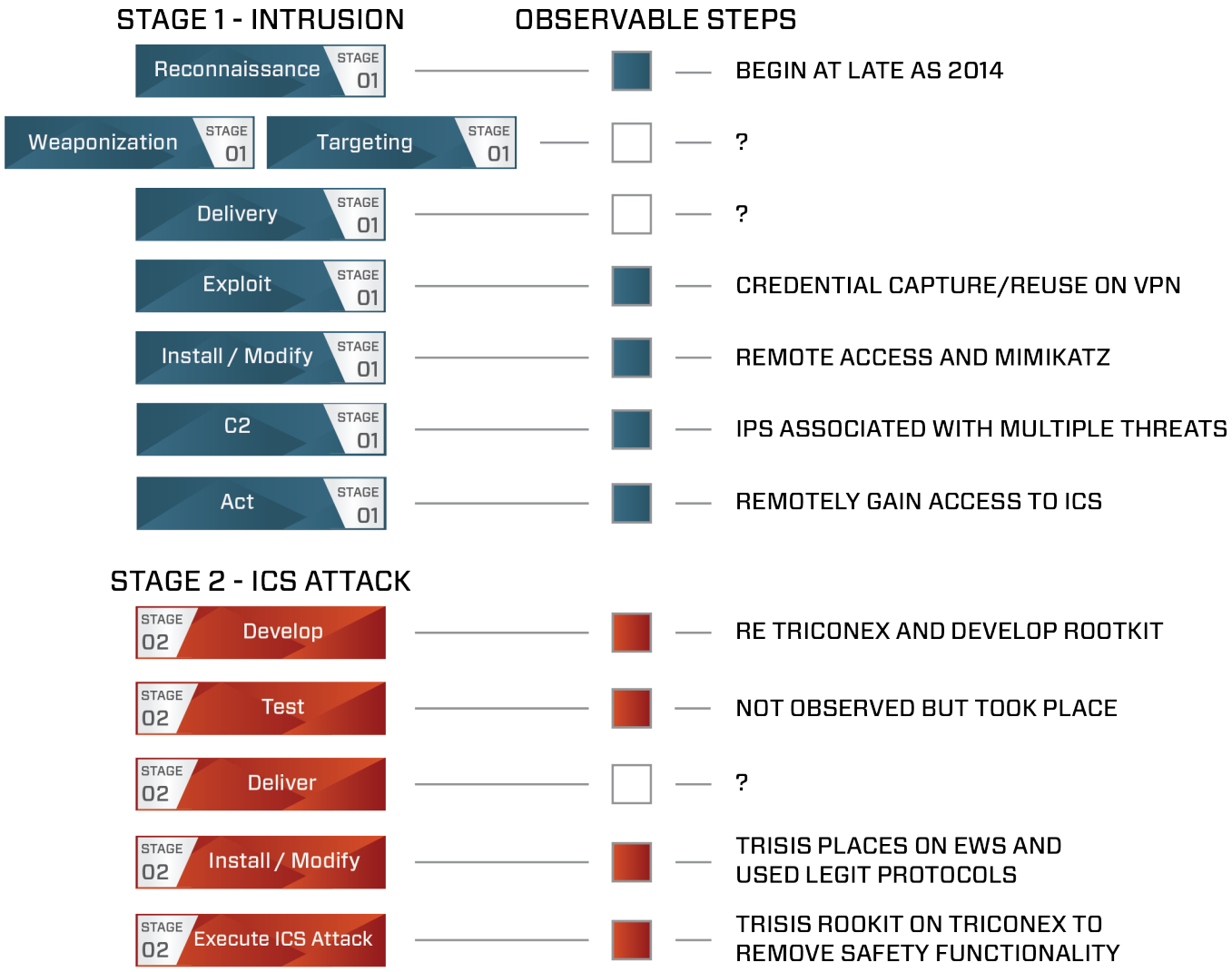


- Today: (whatever you have)

- 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

DRAGOS

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

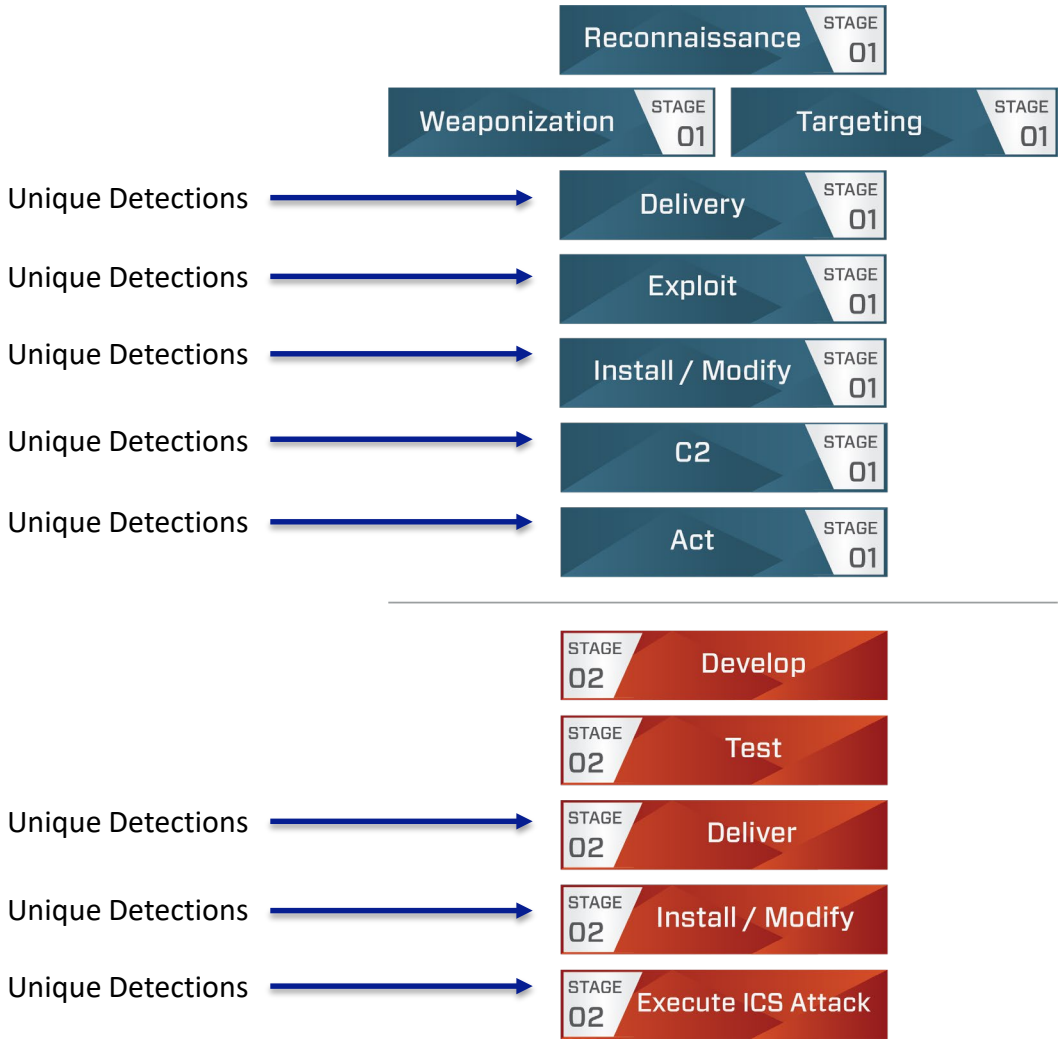
DRAGOS

RSAConference2019
Asia Pacific & Japan

Countering the Current Threats

The Best Defense is Defense

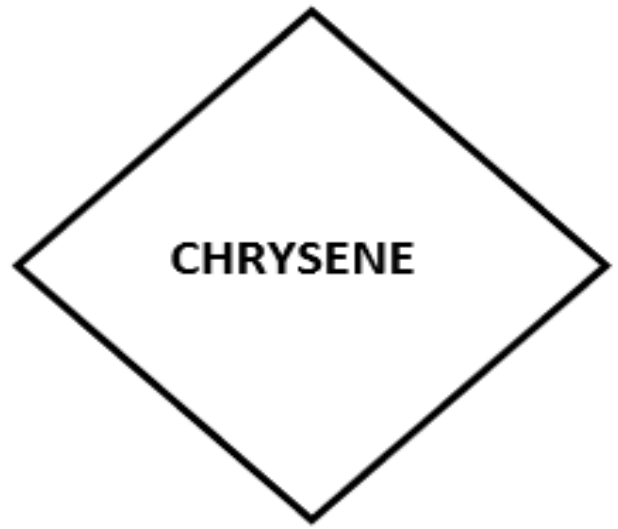
Analytical Coverage – Tradecraft Overlaps



- Have a detection strategy that allows you to not detect it all
- Analytical coverage across kill chain means higher chance of detecting adversary and overlaps
- Overlapping tradecraft is common; adversaries may do something novel but not every step is novel

ADVERSARY:
- Evolution of “Greenbug” activity.
- Possible links with Shamoon, StoneDrill as initial access team for destructive attacks.

INFRASTRUCTURE:
- Registers domains that look like legitimate IT services.
- Create and manage specific name servers for domains to provide required DNS response for C2.



CAPABILITIES:
- 64-bit malware is current toolset, older toolset has overlap with “OilRig” malware.
- Extensive use of DNS for covert communications.
- Possible use of watering hole attacks on ICS-related websites.

VICTIM:
- Oil and gas, electric generation, and petrochemical industries.
- Targeting observed in Saudi Arabia, UK, Israel, Pakistan. Possible activity in North America.

ADVERSARY:

- Espionage group with ICS industry focus.
- Associated with APT 33.

INFRASTRUCTURE:

- Registers own infrastructure.
- Spoofs victim organizations and generic IT themes.

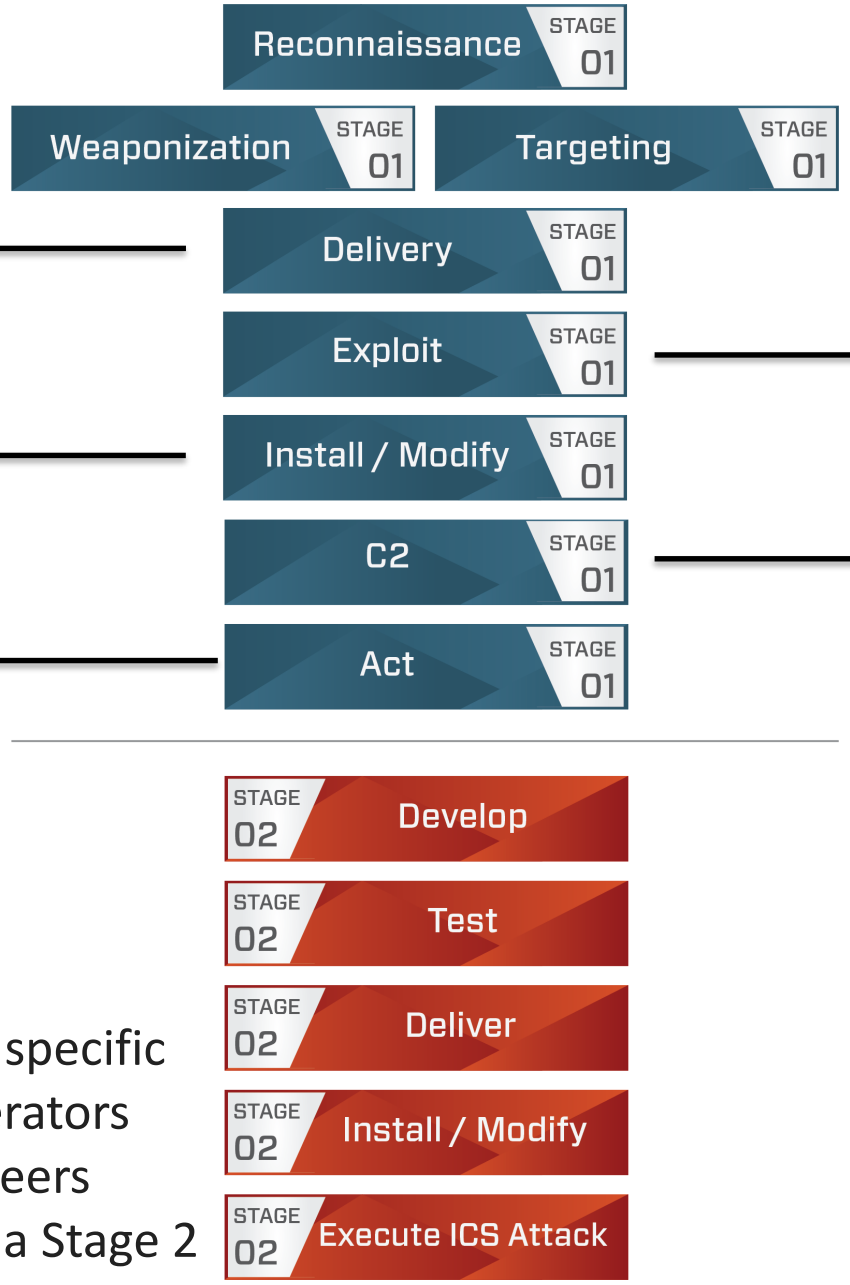
CAPABILITIES:

- Espionage toolkit including a non-destructive variant of StoneDrill malware. Shifted to PowerShell for post-exploitation in 2018.
- No ICS-specific capability observed.

VICTIM:

- All victims either Saudi Arabian organizations, or companies with joint ventures with Saudi businesses.
- Focus on petrochemical and aerospace sectors.

HEXANE



Malicious Microsoft Office documents containing embedded binaries

Construct and install binary through Visual Basic for Application code in document. Built-in system functions for code execution

Writes malware to "Users\Public" folder, compiles and executes additional code in memory to evade detection/forensics

Uses a combination of HTTP and DNS tunneling for command and control traffic. Identified infrastructure are adversary-owned Virtual Private Server (VPS) instances

Attempts to retrieve a 3rd-stage script object from C2 for further execution, but unable to determine function or intent at this time

Activity is specific to ICS operators and engineers hinting at a Stage 2

DRAGOS

Tradecraft Overlaps Mapped

- *Specific method to evade detection in memory with unique processes*
- Waterhole of specific type of ICS websites
- *Complex C2 over DNS schema to adversary owned infrastructure*
- Ismdoor malware; relation to “Greenbug”

- *Specific method to evade detection in memory with unique processes*
- Phishing using ICS jobs
- *Complex C2 over DNS schema to adversary owned infrastructure*
- TURNEDUP, Stonedrill and later Powershell; relation to “APT33”

- *Specific method to evade detection in memory with unique processes*
- Complex malicious docs targeted towards ICS Ops
- *Complex C2 over DNS schema to adversary owned infrastructure*
- Scripting called from Office; no known links

RSAConference2019
Asia Pacific & Japan

Tips for a Successful ICS Security Strategy

Start Now, Have an End Goal, Be Flexible

Develop a 2-5 Year Strategy

Choose a Framework

- Choose something recognizable such as NIST CSF and then adapt it based on your environment
- Determine consequence driven risk
- Determine intelligence-driven risk and develop a threat model
- Gain approval from stakeholders

Assess

- Take 1-2 sites and do self-assessment
- Identify gaps in the framework, the sites, the culture, and your skills
- Do 5-10 sites with outside experts side saddled
- Develop requirements for the right people and technology

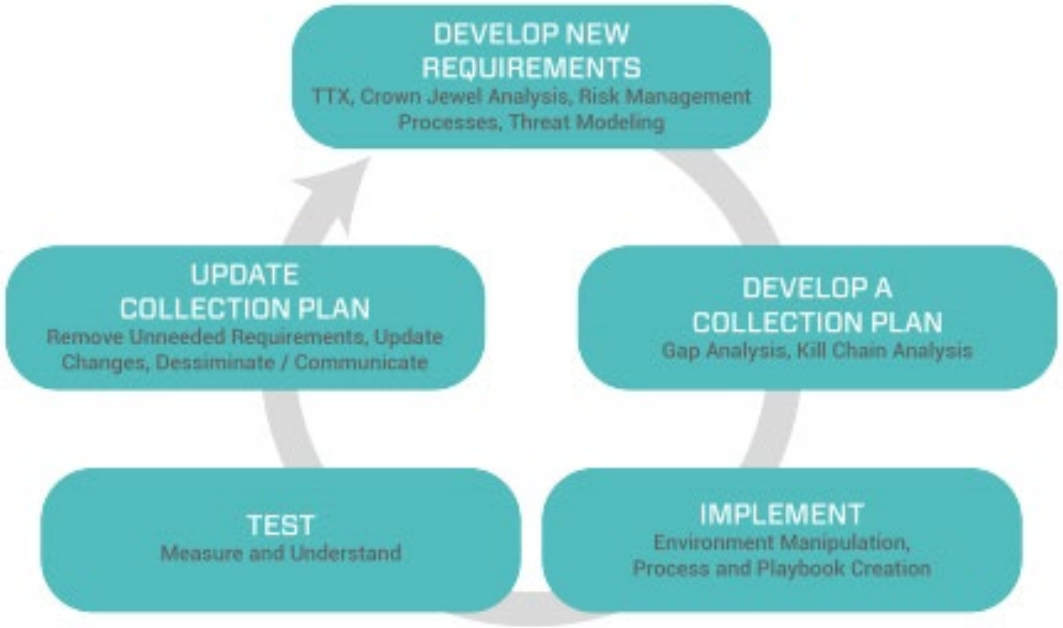
People, Process, and Technology

- Hire/train appropriate staff for your requirements
- Select technology off of your requirements
- Deploy tech at the 5-10 assessed sites
- Capture lessons learned

Rinse and Repeat

- Tailor requirements, framework, and resourcing as required
- Assess and deploy technology to next 10-25% of sites
- Keep doing in 10-25% batches until done

Choose the Right Collection Strategy



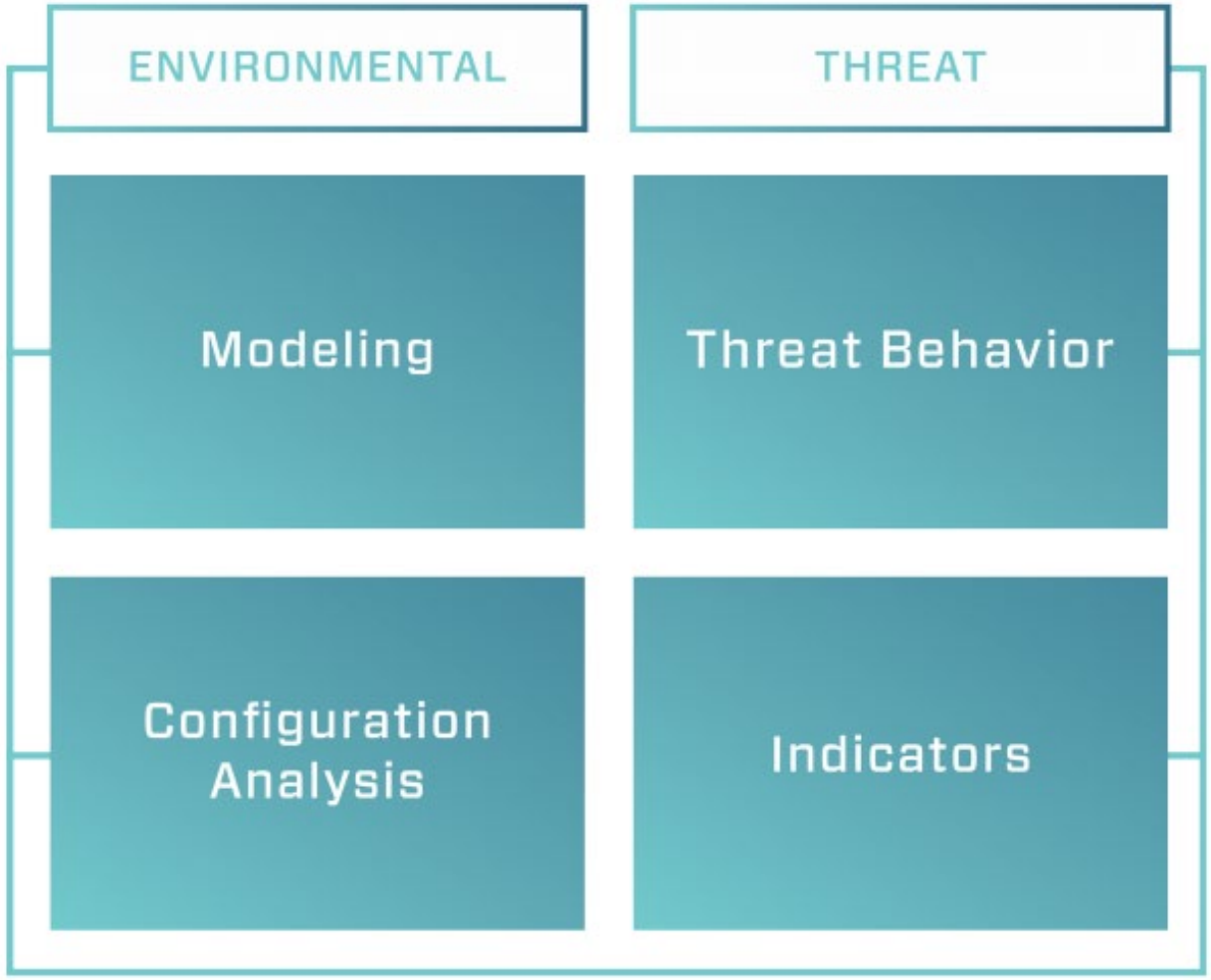
	CONTROL CENTER	CONTROL CENTER	CONTROL CENTER	TRANSMISSION SUBSTATION	TRANSMISSION SUBSTATION
ASSET TYPE	Windows Human Machine Interface	Data Historian	Network Monitoring Appliance	Windows Human Machine Interface	Remote Terminal Units
DATA TYPE	Windows Event Logs	Alarms	Alerts	Windows Event Logs	Syslog
QUESTION TYPE (KILL CHAIN PHASES)	Exploration, Installation, Actions on Objectives	Actions on Objectives	Internal Reconnaissance, Command and Control, Delivery, Actions on Objectives	Exploitation, Installation, Actions on Objectives	Installation, Actions on Objectives
FOLLOW-ON COLLECTION	Registry Keys	Set Points and Tags	Packet Capture	Registry Keys	Controller Logic
DATA STORAGE LOCATION	Enterprise SIEM	Local	Enterprise SIEM	Local	Local
DATA STORAGE TIME	60 Days	120 Days	30 Days	30 Days	7 Days

Visibility is key but what visibility determines what threat detection you do which determines how you respond which determines what you can prevent

DRAGOS

https://dragos.com/wp-content/uploads/CMF_For_ICS.pdf

Choose the Right Threat Detection Strategy



https://dragos.com/wp-content/uploads/The_Four_Types-of_Threat_Detection.pdf

- Each type of detection has unique characteristics
- Each have costs and benefits to consider

	TRANSPARENCY	DURABILITY	EASE OF IMPLEMENTATION	COVERAGE	ADAPTABILITY
CONFIGURATION	Moderate	Good	Moderate	Good	Poor
MODELING	Poor	Moderate	Poor	Good	Poor
INDICATORS	Good	Poor	Good	Poor	Moderate
THREAT BEHAVIOR	Good	Good	Moderate	Moderate	Good

	INVESTIGATIONS	NOVEL ATTACK DETECTION	SIMILAR THREAT DETECTION	SCOPING
CONFIGURATION	Poor	Good	Poor	Good
MODELING	Poor	Good	Poor	Poor
INDICATORS	Moderate	Poor	Moderate	Good
THREAT BEHAVIOR	Good	Moderate	Good	Moderate

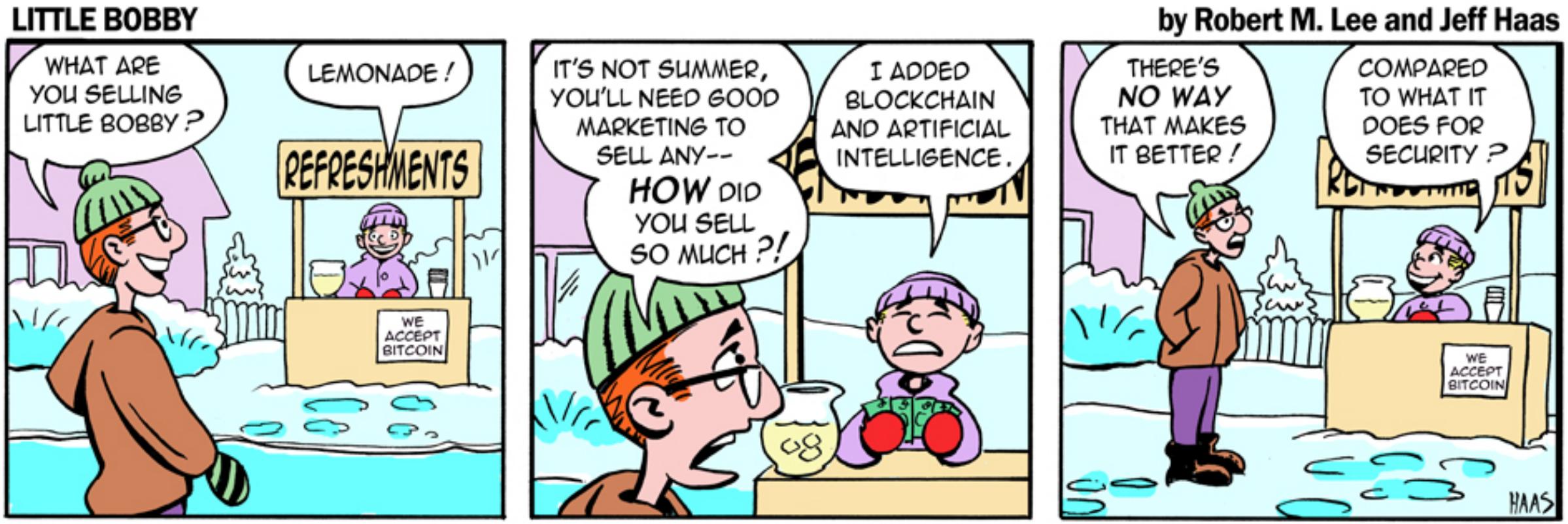
- Each detection can be used together but each has specific use-cases
- Threat Behavior excel for initial detection

Develop the Right Response Strategy

How to Apply This

- When You Get Back to Work:
  - Determine if your industrial networks have been assessed in the past 2 years and have more than segmentation and firewalls
- Within Six Months:
  - Perform assessments against the first couple of key sites
  - Develop a threat model and an understanding of what can go wrong
- Within Twelve to Eighteen Months:
  - Perform assessments on another 5-10 sites with help and build a CMF
  - Develop requirements to implement ICS specific people + process + technology
  - Leverage an intelligence-driven approach (threat behaviors) to detection to achieve analytical coverage
  - Develop Incident Response plans tailored to your threat model + detection strategy

Questions?



@RobertMLee
www.Dragos.com
@DragosInc