RSAConference2020
Asia Pacific & Japan
A Virtual Learning Experience | 15–17 July

SESSION ID: **SAO-F03V**

Forced Digital Transformation and the Realities to ICS/OT Cybersecurity

ROBERT M. LEE
CEO & Founder
Dragos, Inc.
@RobertMLee

DRAGOS
SAFEGUARDING CIVILIZATION

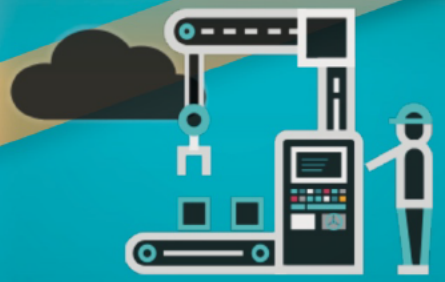
THE TREND OF ICS/OT

RISK

STANDARDIZATION

STAND-ALONE

3rd Industrial Revolution



LOOSELY CONNECTED

DCS SCADA

HIGHLY CONNECTED

4th Industrial Revolution

DRAGOS

WHAT IS THE INDUSTRIAL DIGITAL TRANSFORMATION?

DRAGOS

WHAT IS THE INDUSTRIAL DIGITAL TRANSFORMATION?

Definition

"A radical rethinking of how an organization uses technology, people, and processes to fundamentally change business performance"

George Westerman, MIT scientist and author of *Leading Digital: Turning Technology Into Business Transformation*

Technologies

- Analytics
- Cloud
- Process control, Sensors
- AI/ML

DRAGOS

DIGITAL TRANSFORMATION CASE STUDY—

Profile: Electric utility headquartered in Atlanta, Georgia

Customers: 2.5 million; 40% residential, 52% commercial/industrial

Use case: Monitoring transformers in distribution grid

Problem:

- 1,000's of transformers in distribution grid
- Transformer failures are costly, cause human injury

Solution:

- Continuous remote monitoring of transformers via connected sensors
- Automatic analysis of dissolved gas levels
- Automatic alerts

Benefit:

- Saved over $8 million in assets by predicting transformer failures
- Avoid downtime
- Safety improved

DRAGOS

https://www.ge.com/reports/digital-transformation-data-helping-100-year-old-utility-keep-customers-lights/

DIGITAL TRANSFORMATION CASE STUDY—

PETROCHEMICAL

Profile: Offshore oil and gas operations

Use case: Data analytics for predictive maintenance

Problem:

- Oil and gas organizations experience on average $49 million in losses annually due to unplanned downtime
- Predictive analytics require control networks to push data to sites for 3rd-party access
- Traditional IT security requires least-privilege access, layered segmentation, and restricts running scripts in the control network causing delays and increased expense

Solution:

- Implement compensating controls for a robust threat monitoring and response program
- Segmentation of safety sub-systems for additional compensating control

Benefit:

- $17M annual savings, a 36% reduction in unplanned downtime
- Data-based, predictive approach to maintenance

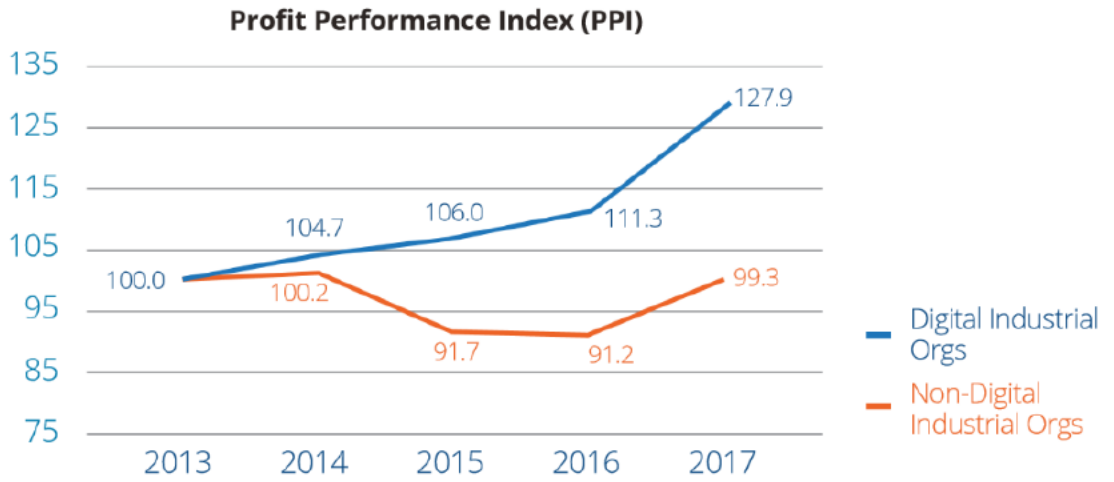
DRAGOS

https://www.dragos.com/wp-content/uploads/SecIndSys_Purdue_GEDragos.pdf

BENEFITS OF INDUSTRIAL DIGITAL TRANSFORMATION

HIGHER EFFICIENCY, QUALITY, PROFITABILITY

"The opportunity for industrial organizations is higher than many other segments, representing more than $4.5 trillion in annual value."

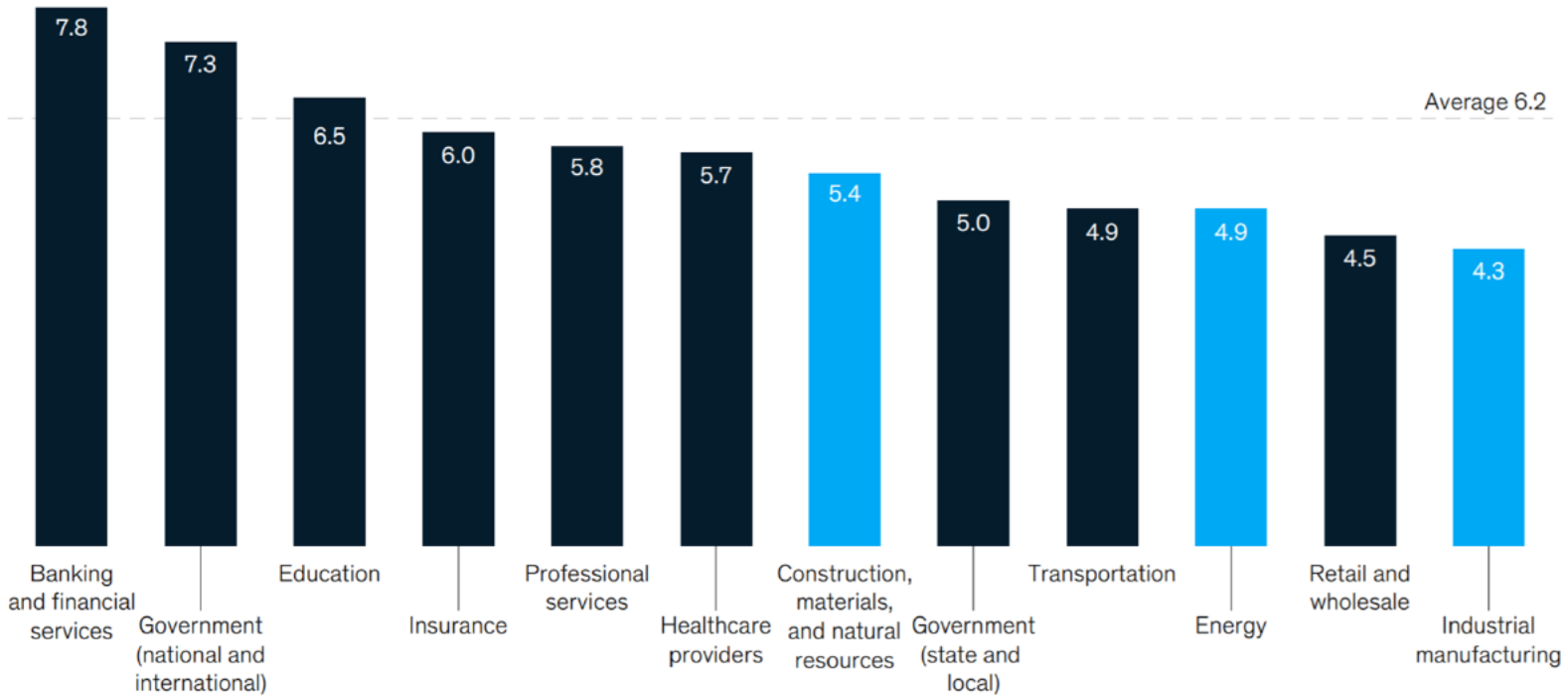


Source: IDC

HEAVY INDUSTRIAL AND ENERGY LAG IN CYBERSECURITY SPENDING

IT security spending as a % of all IT spending

Source: McKinsey 2018
Critical infrastructure companies and the global cybersecurity threat
https://www.mckinsey.com/business-functions/risk/our-insights/critical-infrastructure-companies-and-the-global-cybersecurity-threat

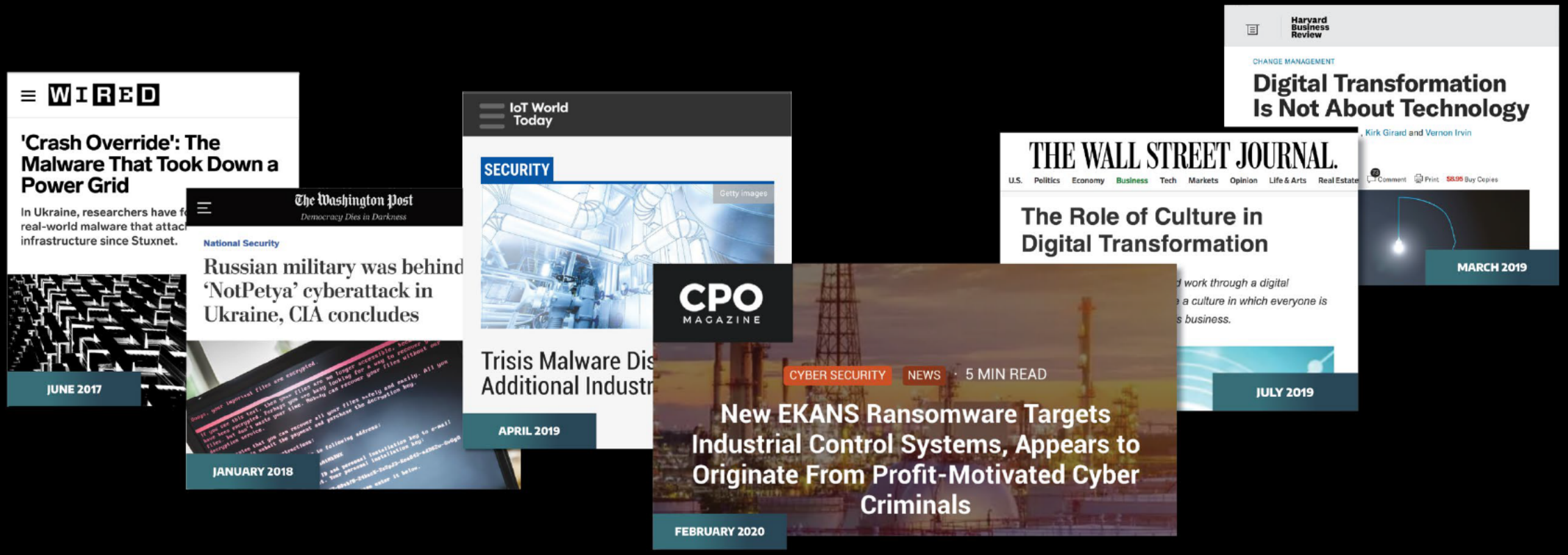


Source: IT Key Metrics Data 2018: Key IT Security Measures: By Industry, Gartner.com, 2018

DRAGOS

RSAConference2020 APJ
A Virtual Learning Experience

WHAT'S CHANGED, WHY NOW



Threats are increasing **AND** the landscape is changing.

THREAT PROLIFERATION: ACTIVITY GROUPS

100% of Activity Groups
use Remote Access

THREAT PROLIFERATION: ACTIVITY GROUPS

Three new activity groups identified in 2019 (now a total of 12):

- **HEXANE**
- **PARISITE**
- **WASSONITE**

HEXANE (since 2018)

Mode of operation: IT compromise and information gathering against ICS entities

Capabilities: Embedded binaries in documents, C2 via DNS and HTTP, evasion techniques

Victimology: Oil & Gas, Middle East, Central Asia, Africa

Links: None

PARISITE (since 2017)

Mode of operation: VPN Compromise of IT networks to conduct reconnaissance

Capabilities: Exploiting known VPN vulnerabilities, SSH.NET, MASSCAN, and dsniff hacking tools

Victimology: US, Middle East, Europe, Australia, Electric, Oil & Gas, Aerospace, Government

Links: MAGNALLIUM

WASSONITE (since 2018)

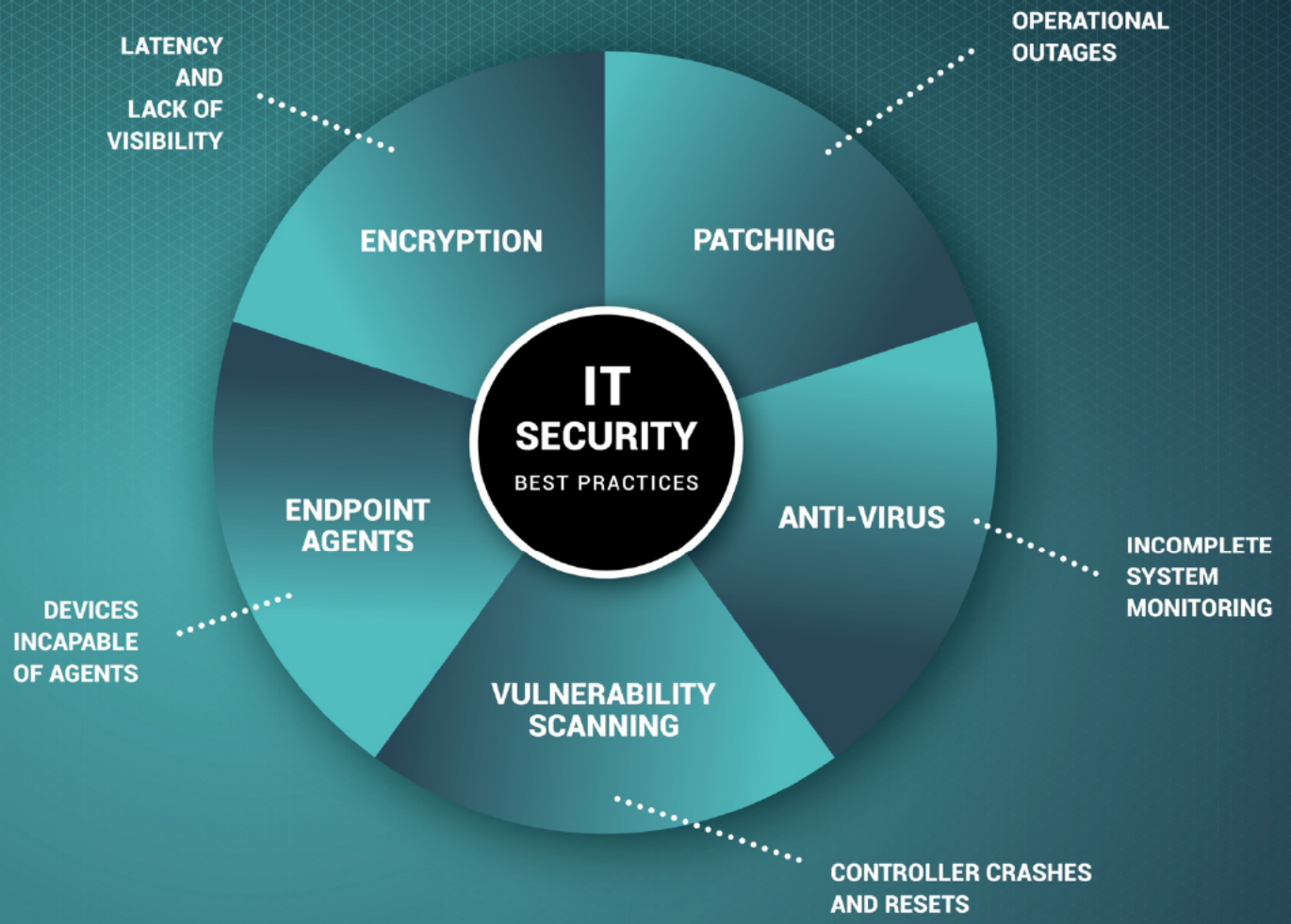
Mode of operation: IT compromise and information gathering

Capabilities: DTrack RAT, Mimkkatz, system tools for file transfer and lateral movement

Victimology: India, South Korea, Japan, Electric, Nuclear, Oil & Gas, Manufacturing, Research

Links: COVELLITE

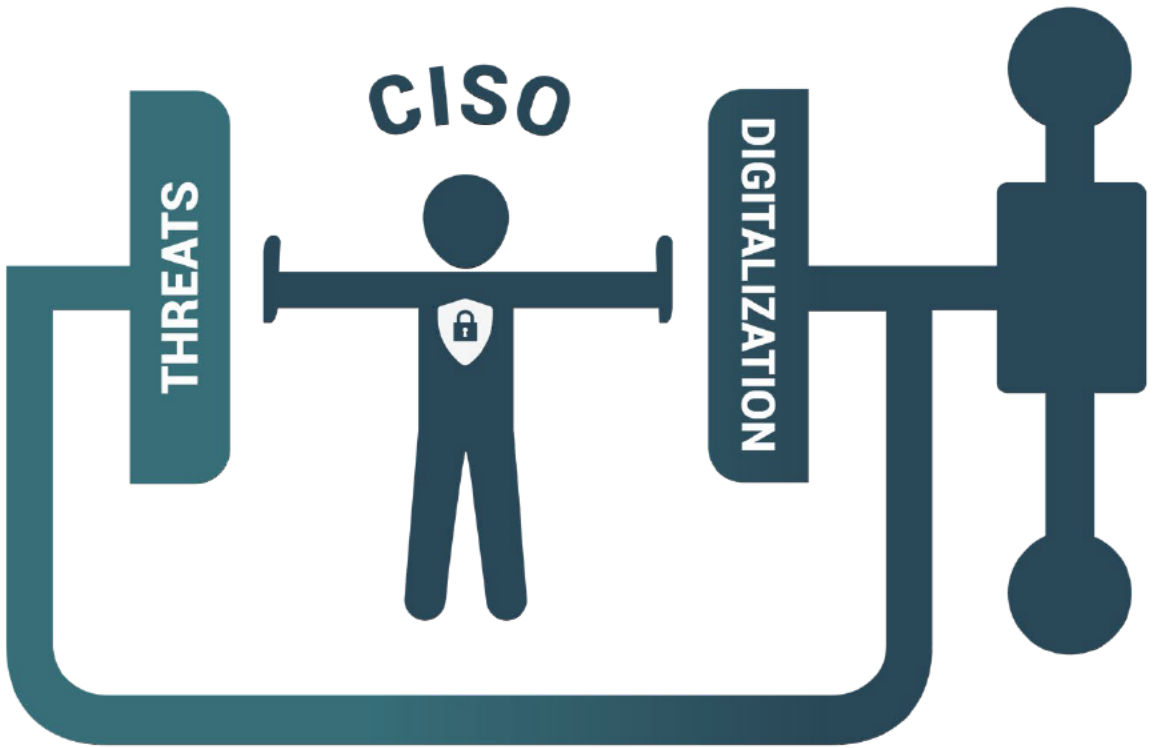
OPERATIONS TECHNOLOGY (OT) SECURITY IS DIFFERENT



DRAGOS

RSAConference2020 APJ
A Virtual Learning Experience

COVID ADDED RISK AND SPEED



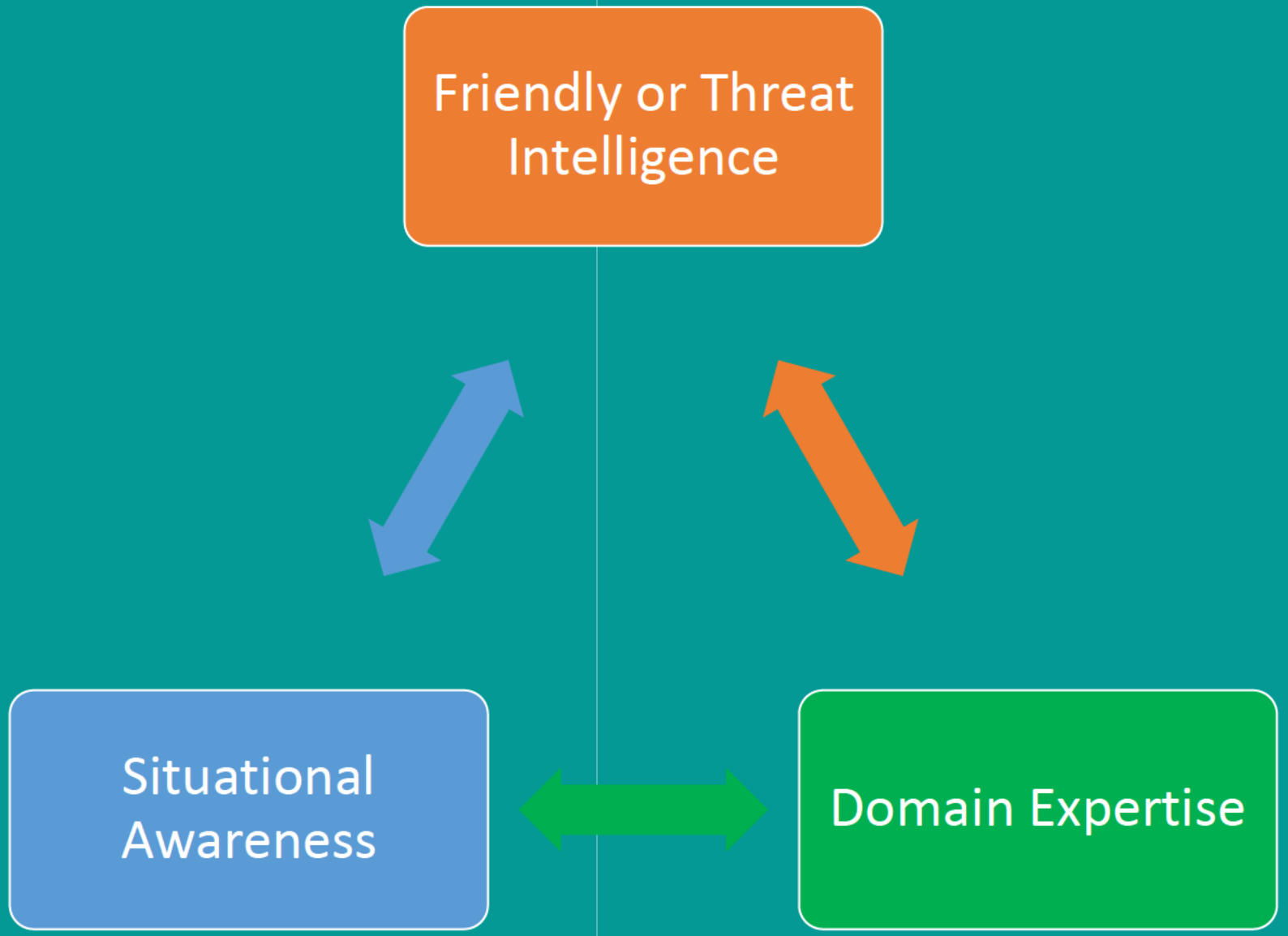
Increased dependency on digital technology, e.g., remote access

RECOMMENDATIONS: TAKING ADVANTAGE OF THE MOMENT, WISELY

- Identify the digital transformation strategy for your company
  - Advocate for a secure foundation, gain resources/budget
- Identify your critical sites/assets
- Determine your risk scenarios
- Determine the appropriate controls
- Compile, Assess, Deploy

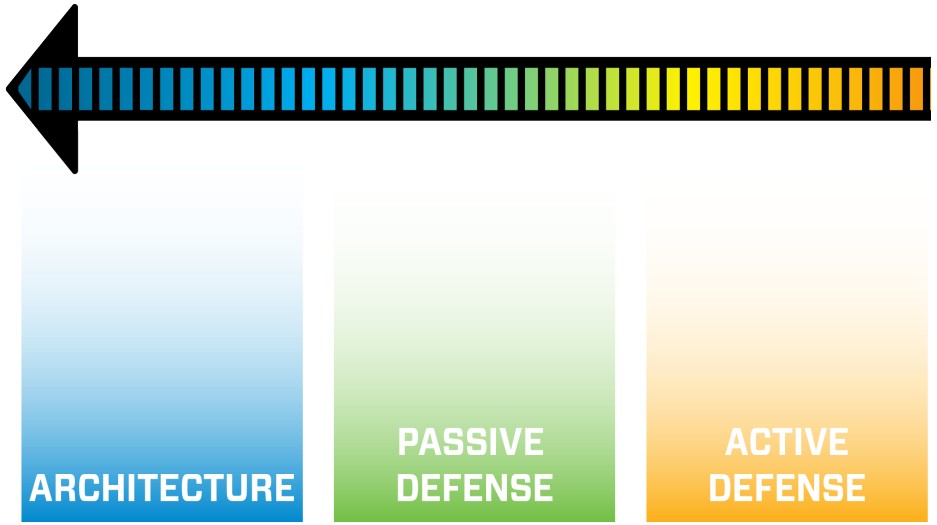
IDENTIFY YOUR CRITICAL SITES/ASSETS

RISK SCENARIO DEVELOPMENT



https://www.sans.org/reading-room/whitepapers/threats/paper/37172

DETERMINE THE APPROPRIATE CONTROLS

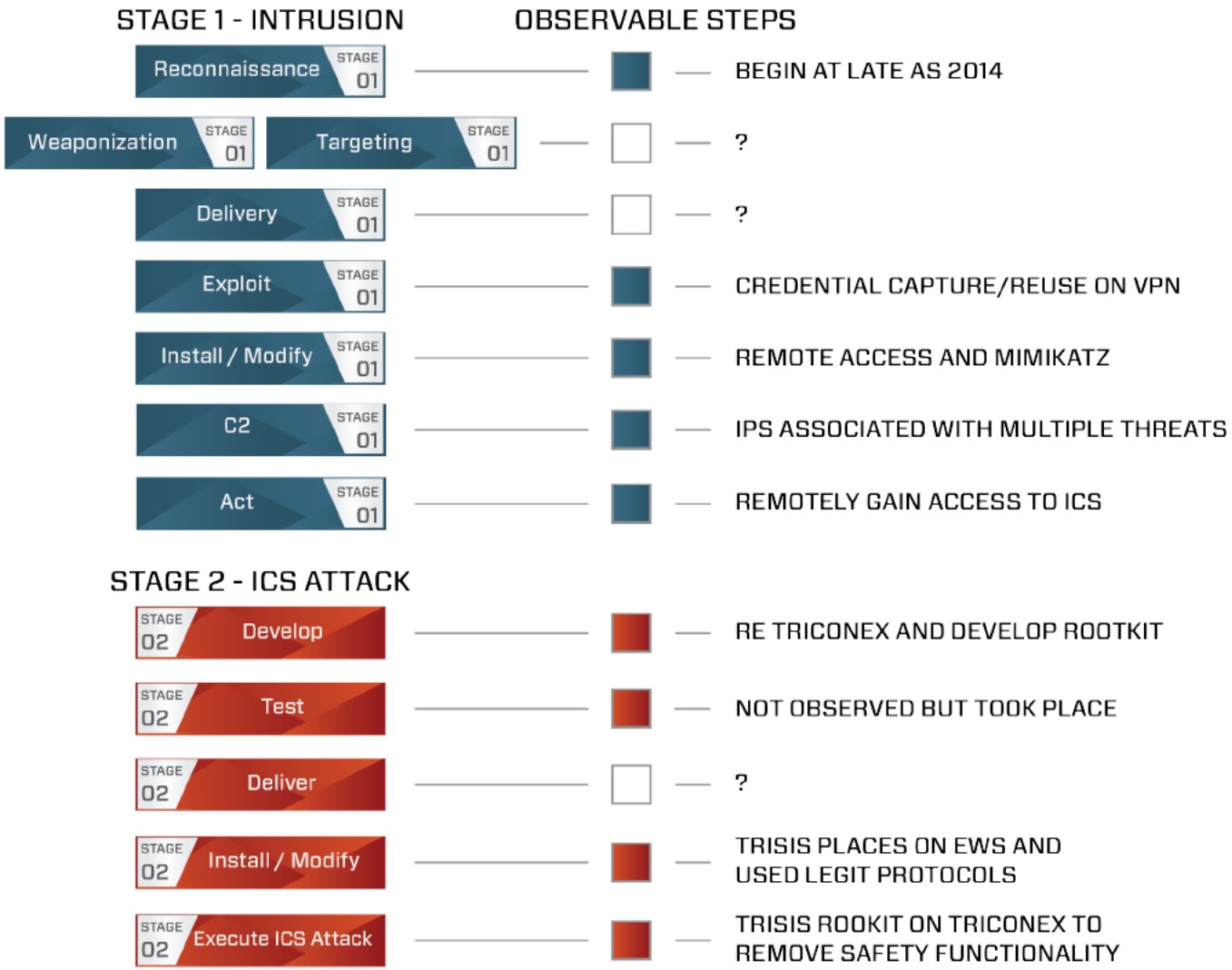


For every observable step on Architecture, Passive Defense, and Active Defense note what is in place today and proposed for later

https://www.sans.org/reading-room/whitepapers/ICS/paper/36297

https://www.sans.org/reading-room/whitepapers/ActiveDefense/paper/36240

EXAMPLE: XENOTIME (TRISIS)



- 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

COMPILE, ASSESS, AND DEPLOY

1. Take your ranked list, your security controls list for the end-to-end scenarios you developed and validate that you could roll these out at your top 10% of your Assets
2. If your work is validated, break your ranked list into an A, B, and C list
3. A class assets will have full coverage on your 3-5 scenarios
4. B class assets will have full coverage on your 1-2 top scenarios or partial coverage
5. C class assets will have at least a couple of the most important controls

   E.g. Incident Response plan and Segmentation

How many assets are in A, B, or C classes will depend on how many assets you have, what budget and resources you have, and how much time you need. Generally A class is 10-15% of the environment, B class are 16-50%, and C class is all else

https://www.dragos.com/resource/developing-a-strategic-ics-ot-cybersecurity-roadmap/

HOW TO USE THIS INFORMATION AFTER THE CONFERENCE

Days after the Conference:

- 1-7: Rest and catch up on emails
- 7-30: Identify the digital transformation stakeholders and strategy (e.g. Digital Transformation Officer)
- 30-60: Develop the critical site/asset list and the risk scenarios
- 60-120: Safety permitting assess the most critical sites for what's being done today with remote connectivity in COVID
- 120-180: Complete the "A Class" plan and begin delivery