RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: **KEY-R01S**

The Industrial Cyberthreat Landscape: 2019 Year in Review

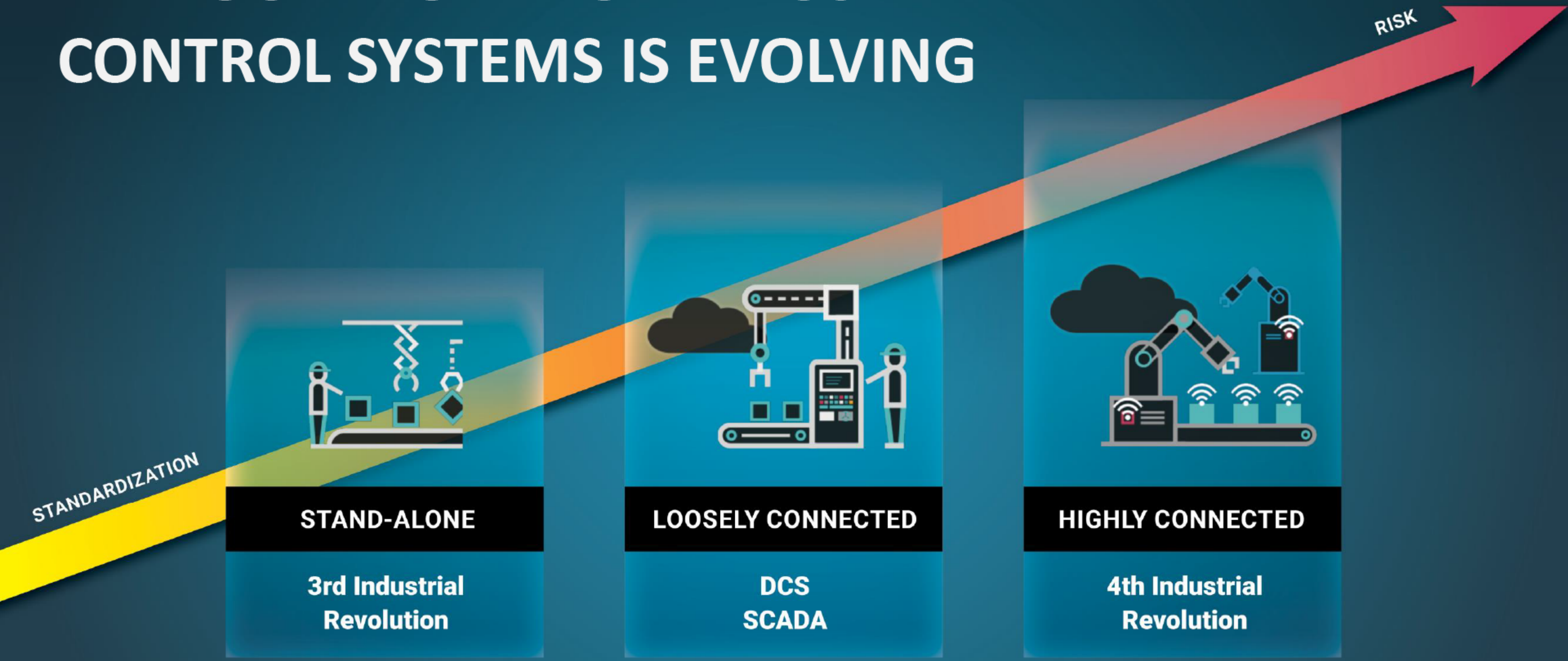
Robert M. Lee

CEO & Founder
Dragos, Inc.
@RobertMLee

#RSAC

OUR WORLD IS INDUSTRIAL

AND OUR WORLD OF INDUSTRIAL CONTROL SYSTEMS IS EVOLVING



STAND-ALONE

3rd Industrial Revolution

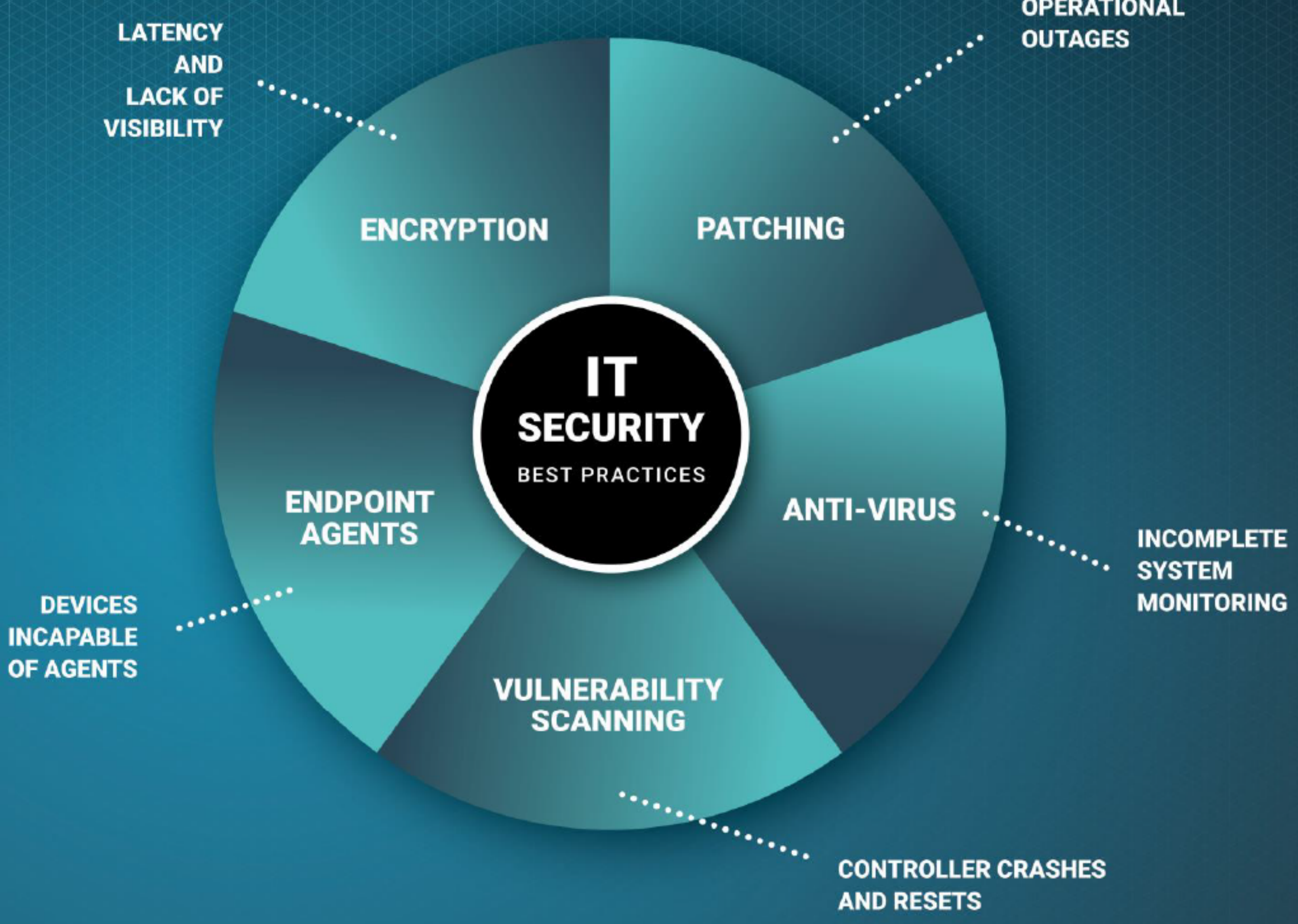
LOOSELY CONNECTED

DCS
SCADA

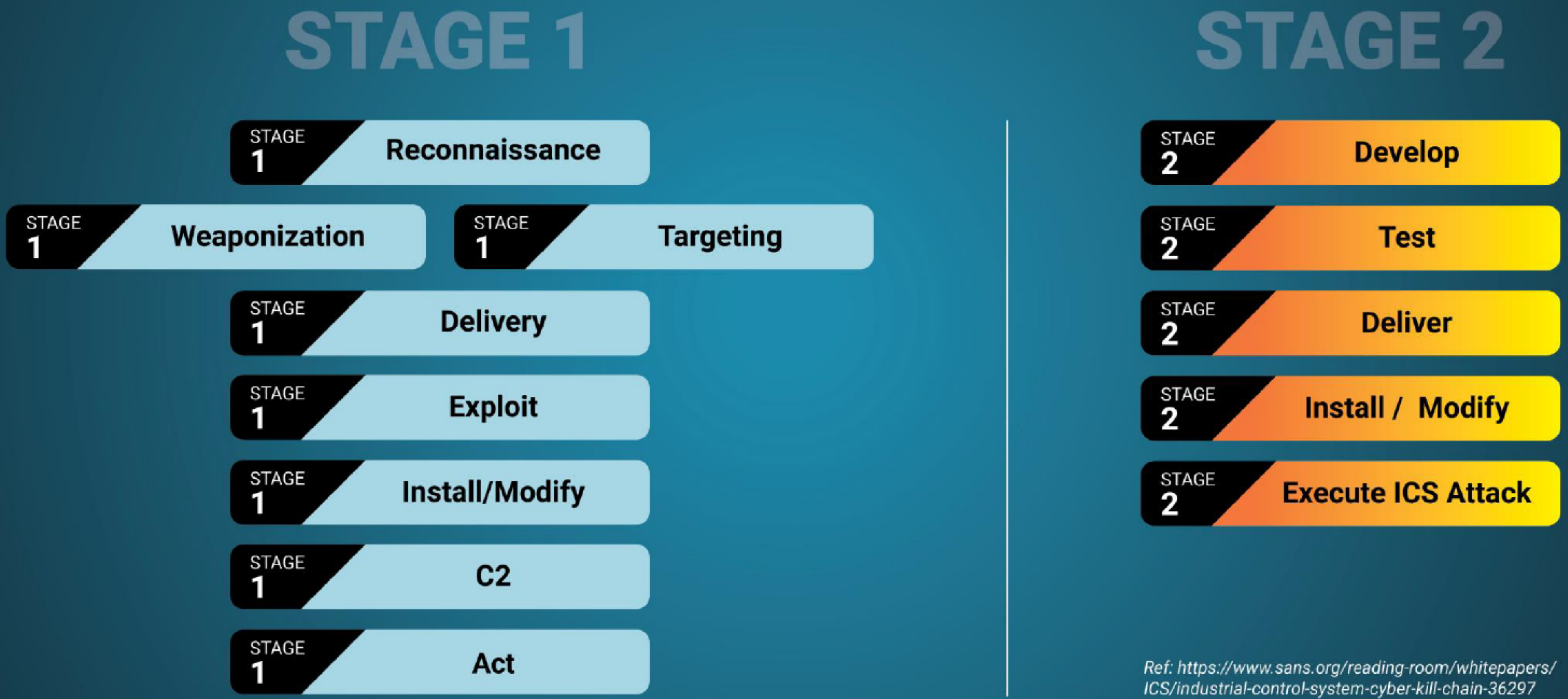
HIGHLY CONNECTED

4th Industrial Revolution

OPERATIONS TECHNOLOGY (OT) SECURITY IS DIFFERENT


IT
SECURITY
BEST PRACTICES
ENCRYPTION
PATCHING
ANTI-VIRUS
VULNERABILITY SCANNING
ENDPOINT AGENTS
LATENCY AND LACK OF VISIBILITY
OPERATIONAL OUTAGES
INCOMPLETE SYSTEM MONITORING
CONTROLLER CRASHES AND RESETS
DEVICES INCAPABLE OF AGENTS

OUR THREATS ARE DIFFERENT



STAGE 1

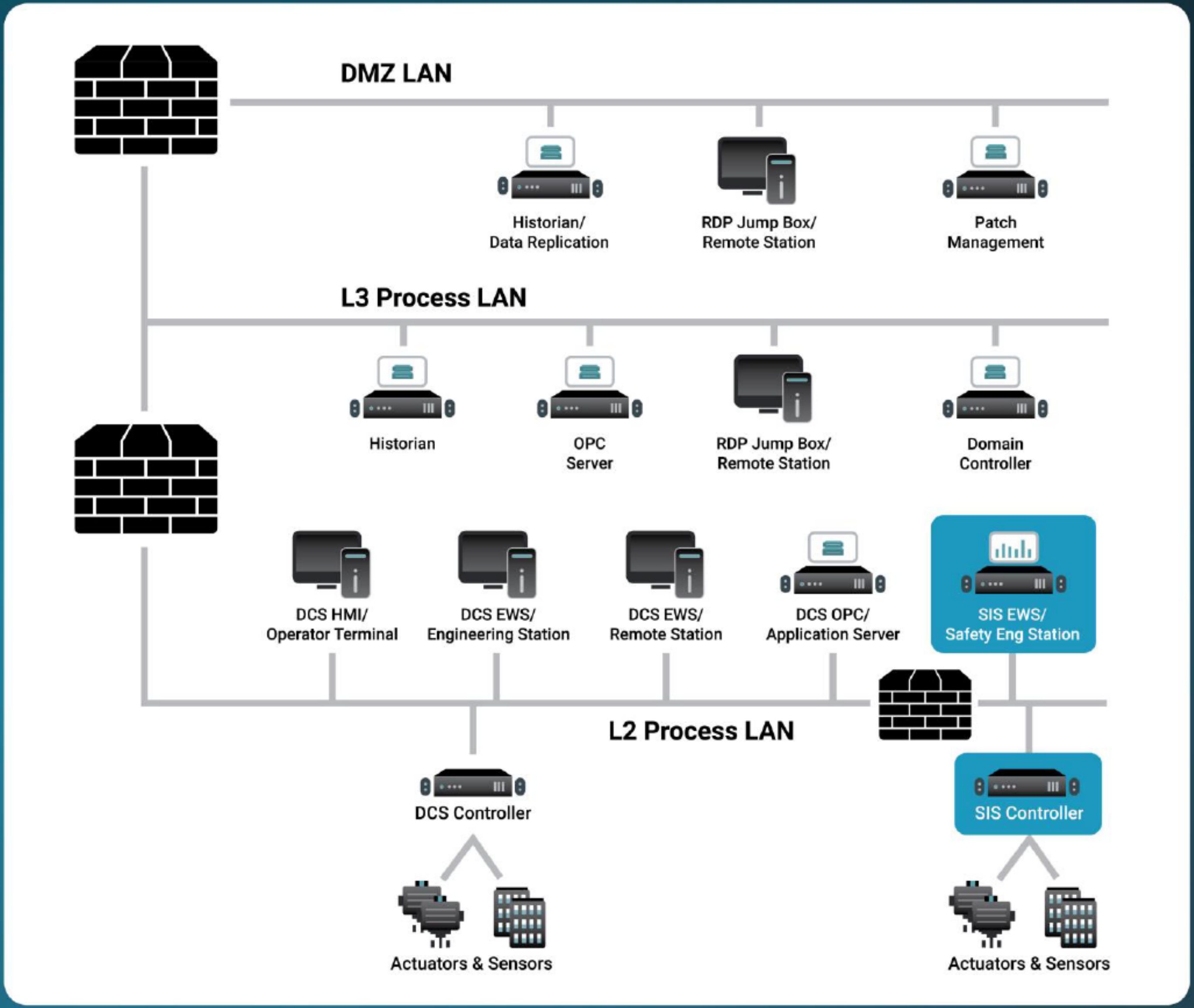
- STAGE 1 Reconnaissance
- STAGE 1 Weaponization
- STAGE 1 Targeting
- STAGE 1 Delivery
- STAGE 1 Exploit
- STAGE 1 Install/Modify
- STAGE 1 C2
- STAGE 1 Act

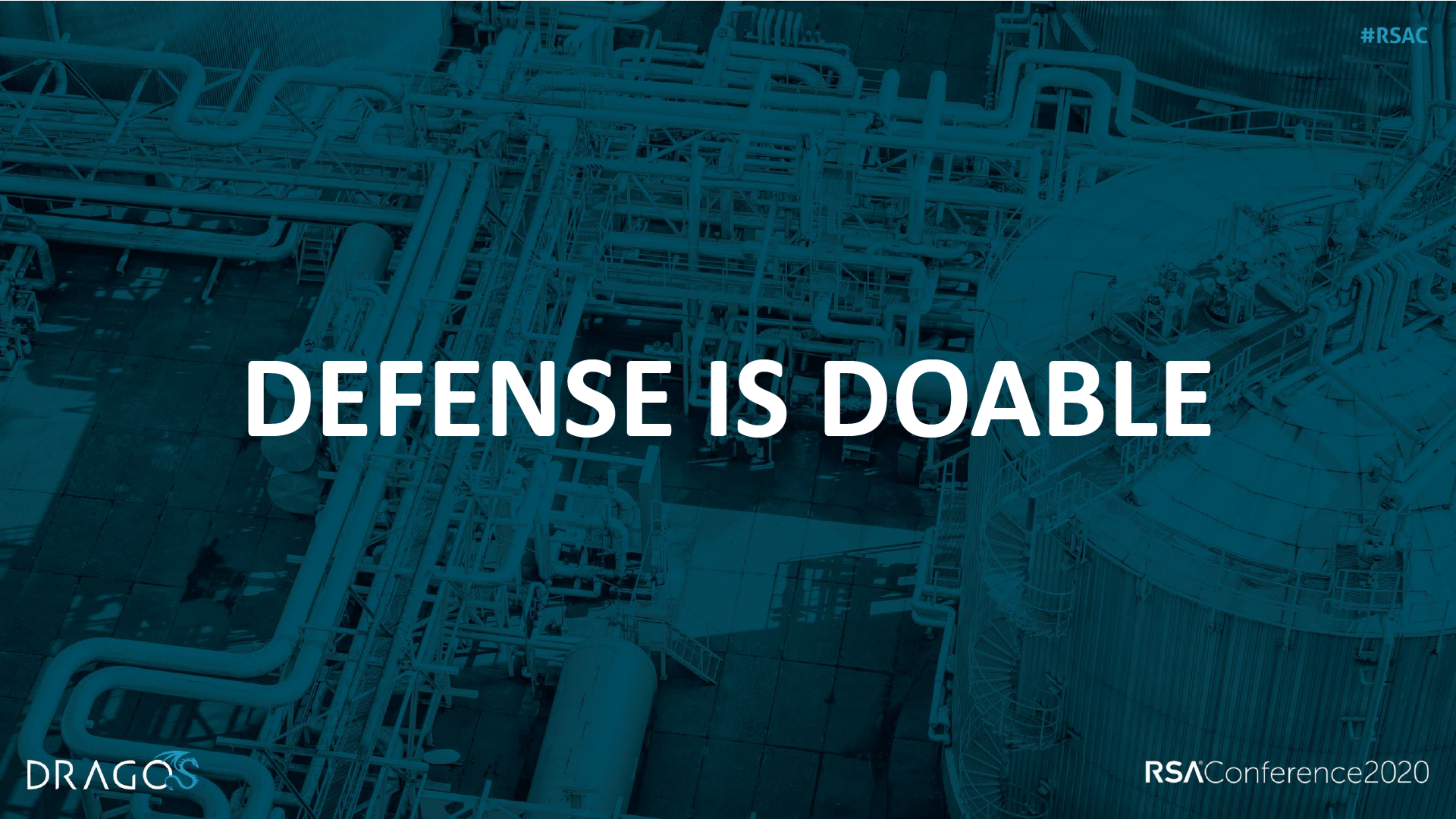
STAGE 2

- STAGE 2 Develop
- STAGE 2 Test
- STAGE 2 Deliver
- STAGE 2 Install / Modify
- STAGE 2 Execute ICS Attack

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

SAUDI ARABIA 2017 - TRISIS


DMZ LAN
Historian/ Data Replication
RDP Jump Box/ Remote Station
Patch Management
L3 Process LAN
Historian
OPC Server
RDP Jump Box/ Remote Station
Domain Controller
DCS HMI/ Operator Terminal
DCS EWS/ Engineering Station
DCS EWS/ Remote Station
DCS OPC/ Application Server
SIS EWS/ Safety Eng Station
L2 Process LAN
DCS Controller
SIS Controller
Actuators & Sensors
Actuators & Sensors



DEFENSE IS DOABLE

DRAGOS 2019 YEAR IN REVIEW REPORTS

DRAGOS
SAFEGUARDING CIVILIZATION
YEAR IN REVIEW 2019
ICS ACTIVITY GROUPS AND THE THREAT LANDSCAPE
DRAGOS
SAFEGUARDING CIVILIZATION
YEAR IN REVIEW 2019
LESSONS LEARNED FROM THREAT HUNTING & RESPONDING TO INDUSTRIAL INTRUSIONS
DRAGOS
SAFEGUARDING CIVILIZATION
YEAR IN REVIEW 2019
INDUSTRIAL CONTROLS SYSTEM VULNERABILITIES

ICS Vulnerabilities

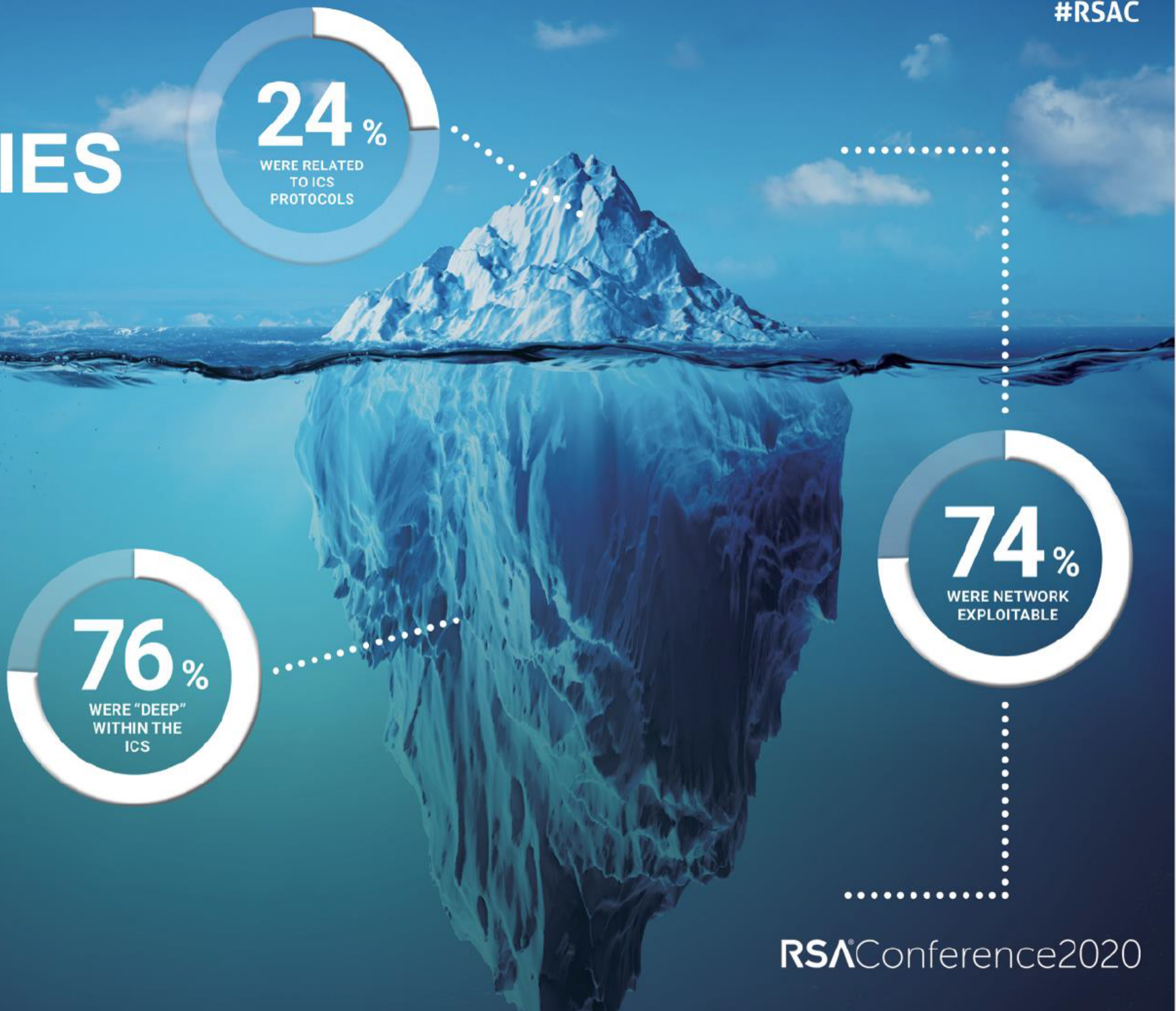
ICS Threat Landscape

Front-Line Lessons Learned

Insights and lessons learned from Dragos's first-hand experience tracking and combating (ICS) adversaries

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

ICS CRITICAL VULNERABILITIES

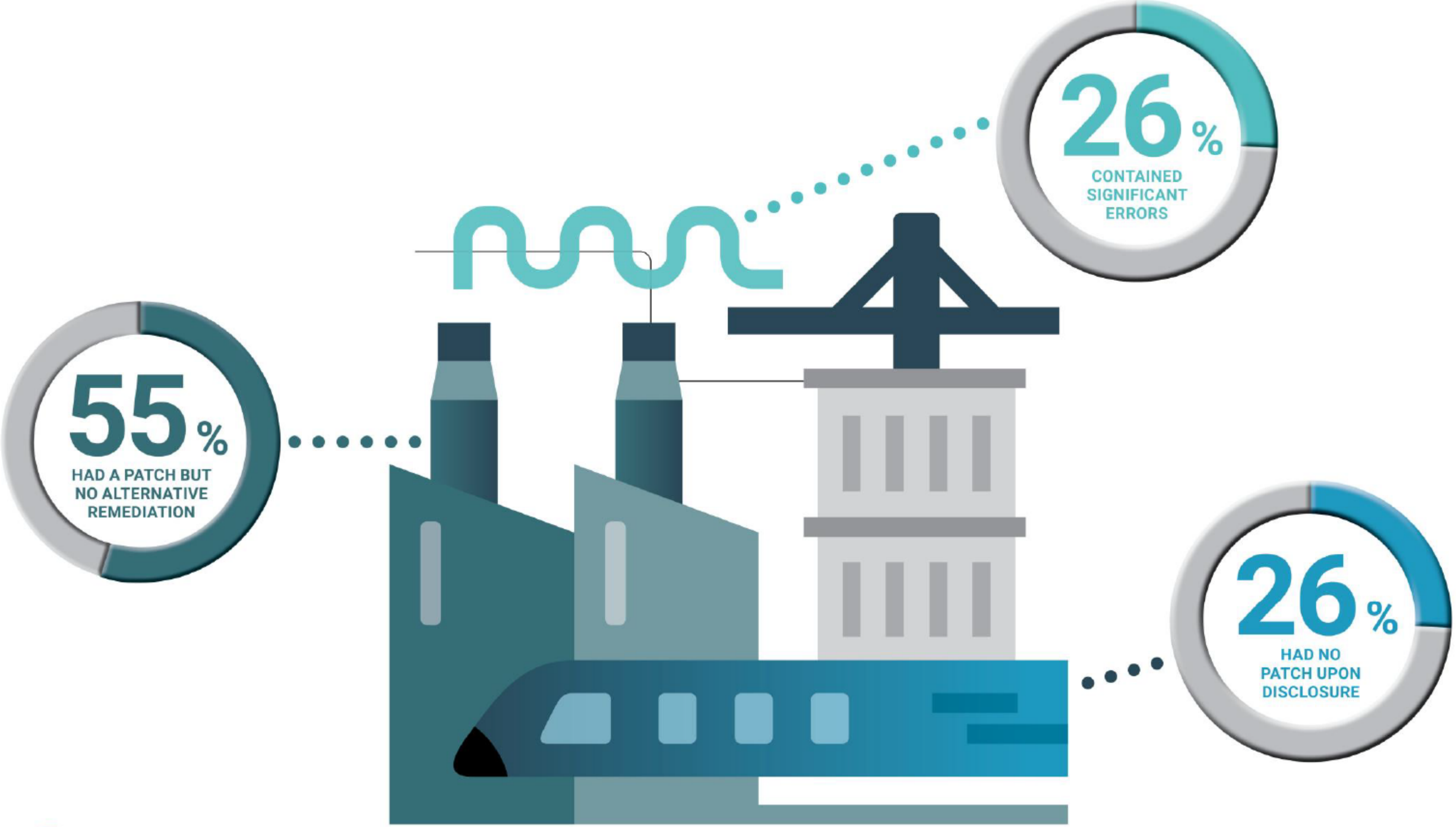


24 % WERE RELATED TO ICS PROTOCOLS

74 % WERE NETWORK EXPLOITABLE

76 % WERE "DEEP" WITHIN THE ICS

ICS CRITICAL VULNERABILITIES



26% CONTAINED SIGNIFICANT ERRORS

55% HAD A PATCH BUT NO ALTERNATIVE REMEDIATION

26% HAD NO PATCH UPON DISCLOSURE

THREAT PROLIFERATION: ACTIVITY GROUPS

THREAT PROLIFERATION: ACTIVITY GROUPS

Two new activity groups identified in 2019 (now a total of 11):

- ➢ **PARISITE**
- ➢ **WASSONITE**

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

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

THREAT PROLIFERATION: ACTIVITY GROUPS

7 activity groups operate across verticals:

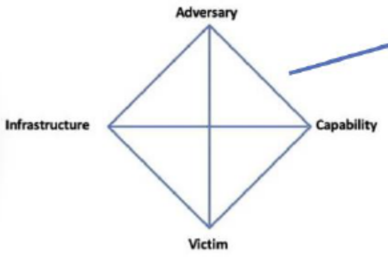
- **MAGNALIUM, PARISITE, HEXANE, CHRYSENE, XENOTIME, DYMALLOY, WASSONITE**

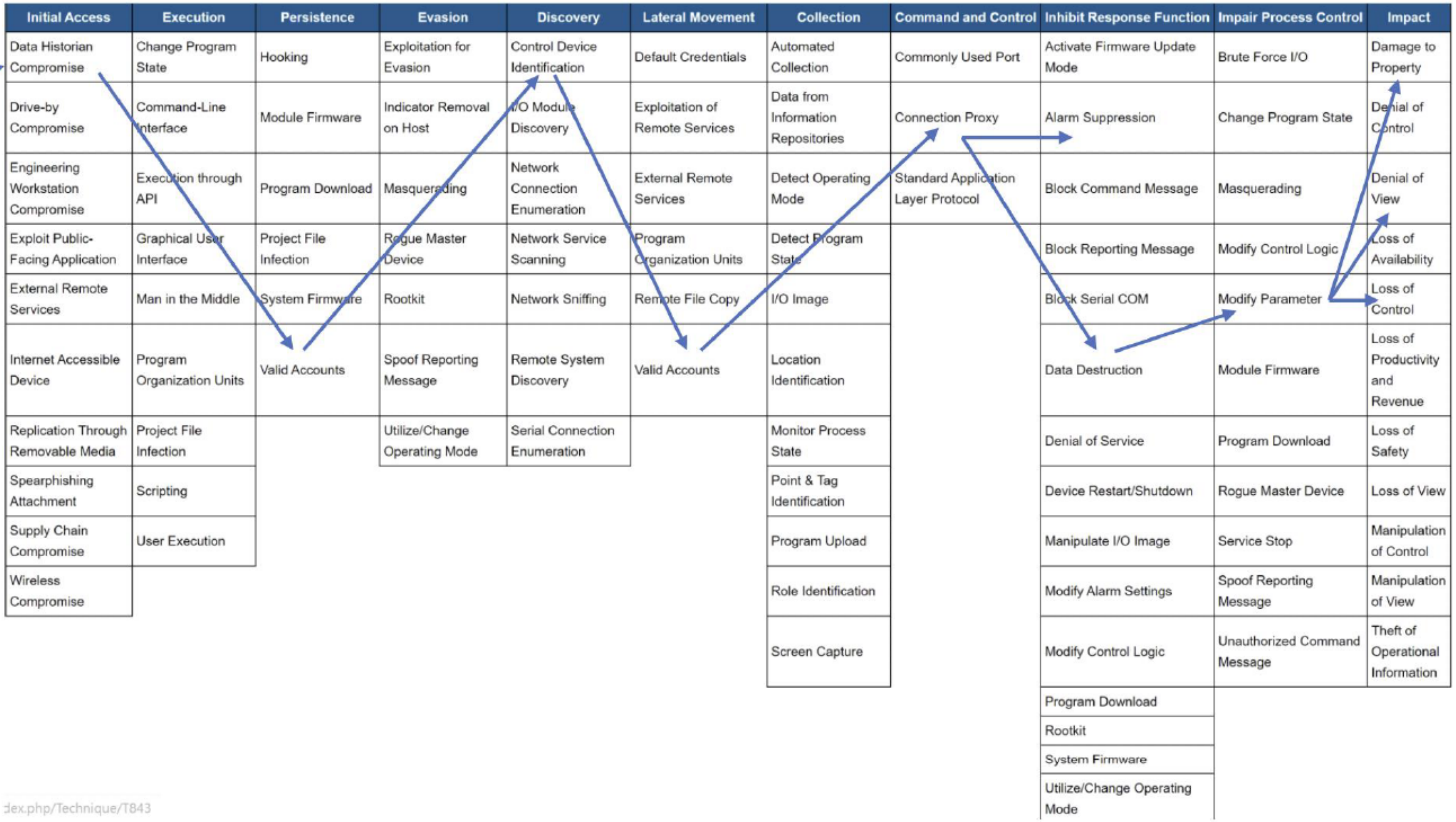
MITRE | ATT&CK™ FOR ICS

- A key milestone in ICS cybersecurity
- A globally-accessible knowledge base of adversary tactics and techniques based on intelligence-driven insights

https://attack.mitre.org/ics

ACTIVITY GROUPS





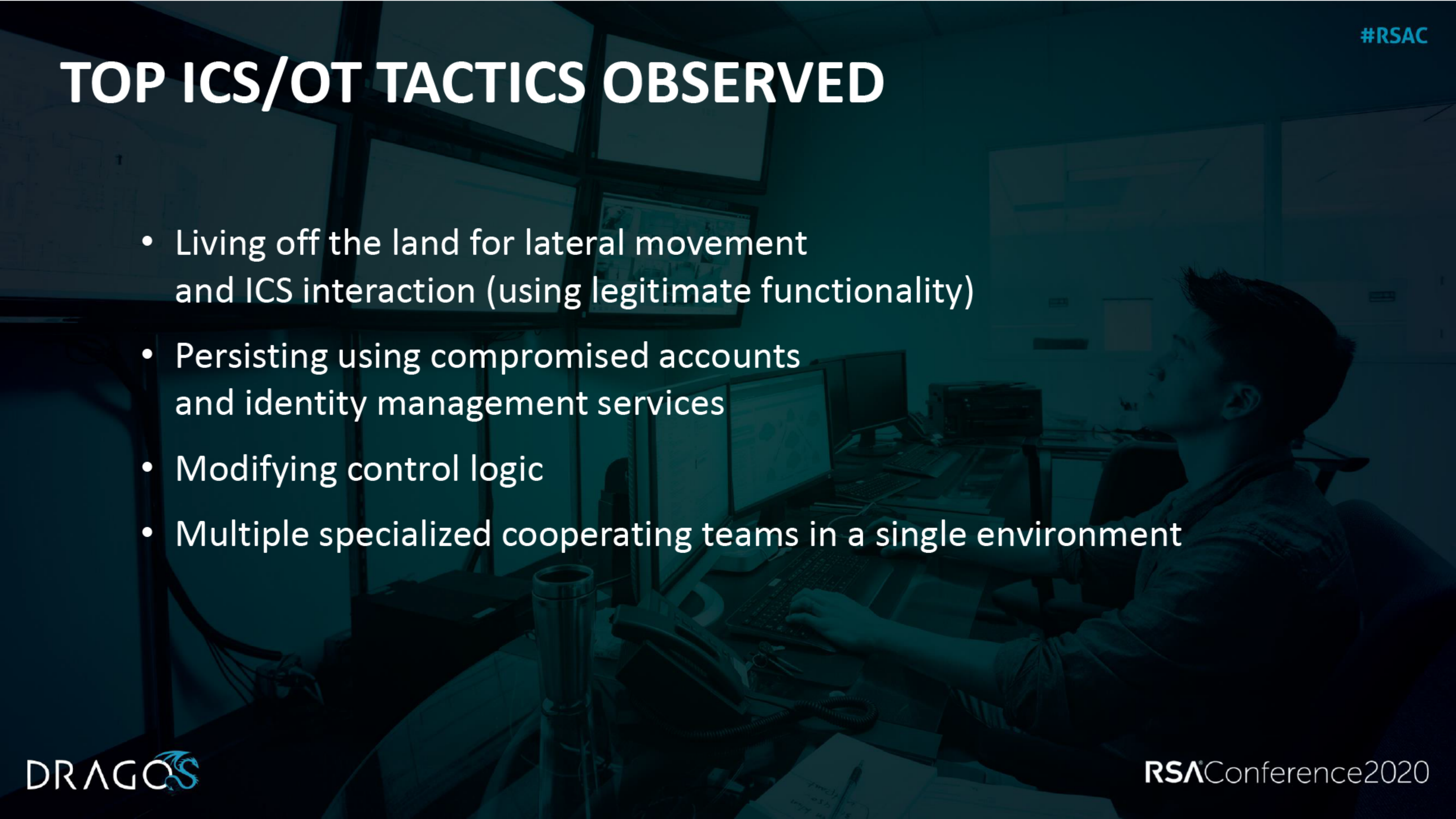
Initial Access	Execution	Persistence	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Data Historian Compromise	Change Program State	Hooking	Exploitation for Evasion	Control Device Identification	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Drive-by Compromise	Command-Line Interface	Module Firmware	Indicator Removal on Host	I/O Module Discovery	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Change Program State	Denial of Control
Engineering Workstation Compromise	Execution through API	Program Download	Masquerading	Network Connection Enumeration	External Remote Services	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Masquerading	Denial of View
Exploit Public-Facing Application	Graphical User Interface	Project File Infection	Rogue Master Device	Network Service Scanning	Program Organization Units	Detect Program State		Block Reporting Message	Modify Control Logic	Loss of Availability
External Remote Services	Man in the Middle	System Firmware	Rootkit	Network Sniffing	Remote File Copy	I/O Image		Block Serial COM	Modify Parameter	Loss of Control
Internet Accessible Device	Program Organization Units	Valid Accounts	Spoof Reporting Message	Remote System Discovery	Valid Accounts	Location Identification		Data Destruction	Module Firmware	Loss of Productivity and Revenue
Replication Through Removable Media	Project File Infection		Utilize/Change Operating Mode	Serial Connection Enumeration		Monitor Process State		Denial of Service	Program Download	Loss of Safety
Spearphishing Attachment	Scripting					Point & Tag Identification		Device Restart/Shutdown	Rogue Master Device	Loss of View
Supply Chain Compromise	User Execution					Program Upload		Manipulate I/O Image	Service Stop	Manipulation of Control
Wireless Compromise						Role Identification		Modify Alarm Settings	Spoof Reporting Message	Manipulation of View
						Screen Capture		Modify Control Logic	Unauthorized Command Message	Theft of Operational Information
								Program Download		
								Rootkit		
								System Firmware		
								Utilize/Change Operating Mode		

dex.php/Technique/T843

MAPPING ACTIVITY GROUPS TO MITRE ATT&CK™ ICS

Activity Group	Common Tactic	Mitre ATT&CK ICS Designation Number
ALLANITE	Point and Tag Identification for Collection	**T852**
CHRYSENE	Scripting for Execution	**T853**
COVELLITE	Spearphishing Attachments for Initial Access	**T865**
DYMALLOY	Screen Capture for Collection	**T852**
ELECTRUM	Wiper to Inhibit Response Function	**T809**
HEXANE	User Interaction for Execution	**T863**
MAGNALIUM	Loss of View	**T829**
PARISITE	Exploitation of Remote Services	**T866**
RASPITE	Drive-by Compromise for Initial Access	**T817**
WASSONITE	Valid Accounts for Persistence	**T859**
XENOTIME	Safety Engineering Workstation Compromise	**T818**

TOP ICS/OT TACTICS OBSERVED



- Living off the land for lateral movement and ICS interaction (using legitimate functionality)
- Persisting using compromised accounts and identity management services
- Modifying control logic
- Multiple specialized cooperating teams in a single environment

MOST DANGEROUS ICS/OT TACTICS

- Safety System Compromise
- Engineering destructive events triggered during recovery process
- Increased development of wiper capabilities and wipers disguised as ransomware
- OSINT collection and analysis of regulatory mandated information release

KEY LESSONS FROM INCIDENT RESPONSE

Weak Perimeters

100% adversary accessed direct from the internet.

INACCURATE

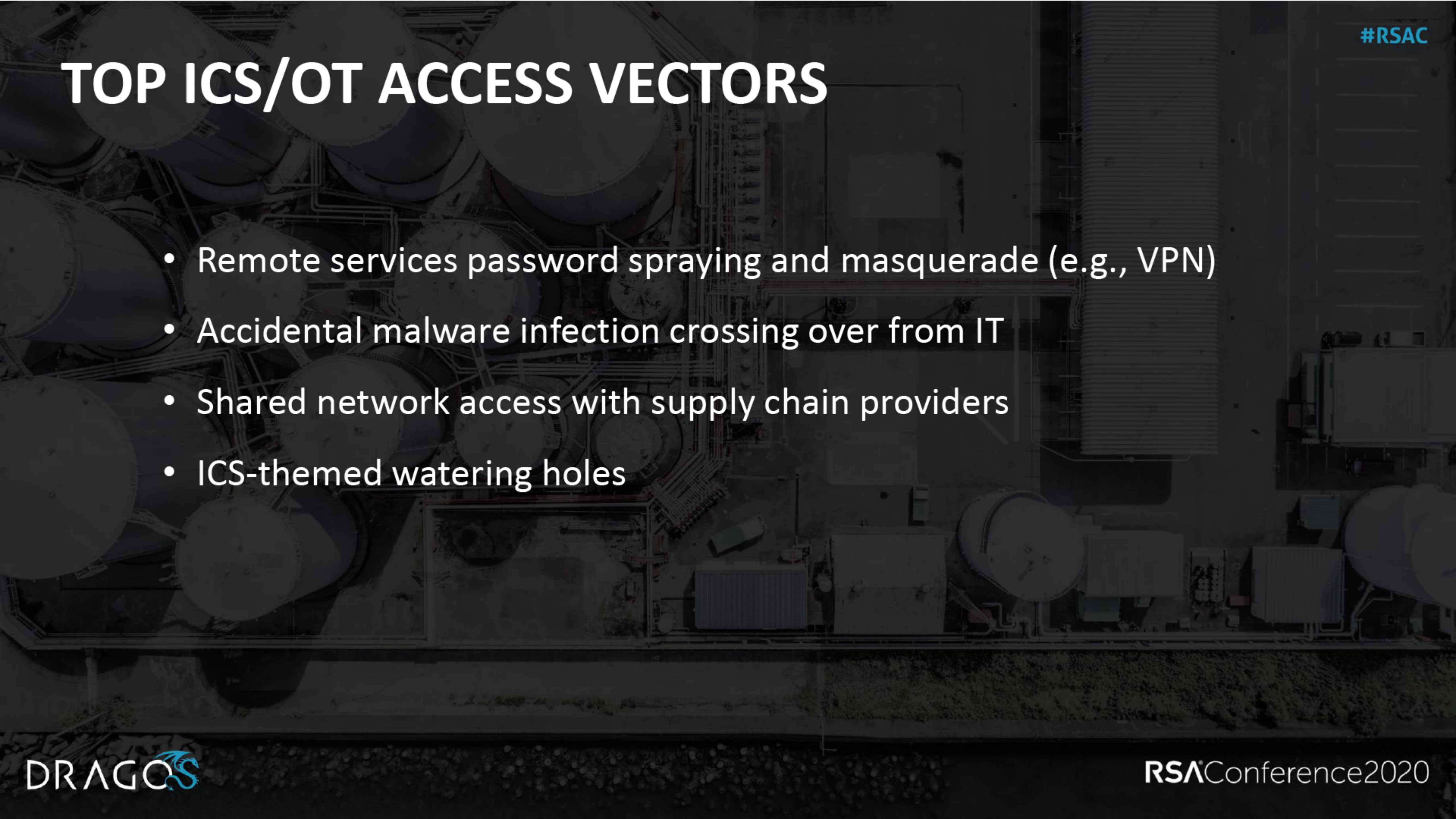
Wrong Information

51% of cases identified existing architecture diagrams were lacking or presented false information.

Poor Visibility

0% of IR cases were facilitated by aggregated logging or passive visibility into the ICS networks. Every case involved manual retrieval of logs and distributed analysis.

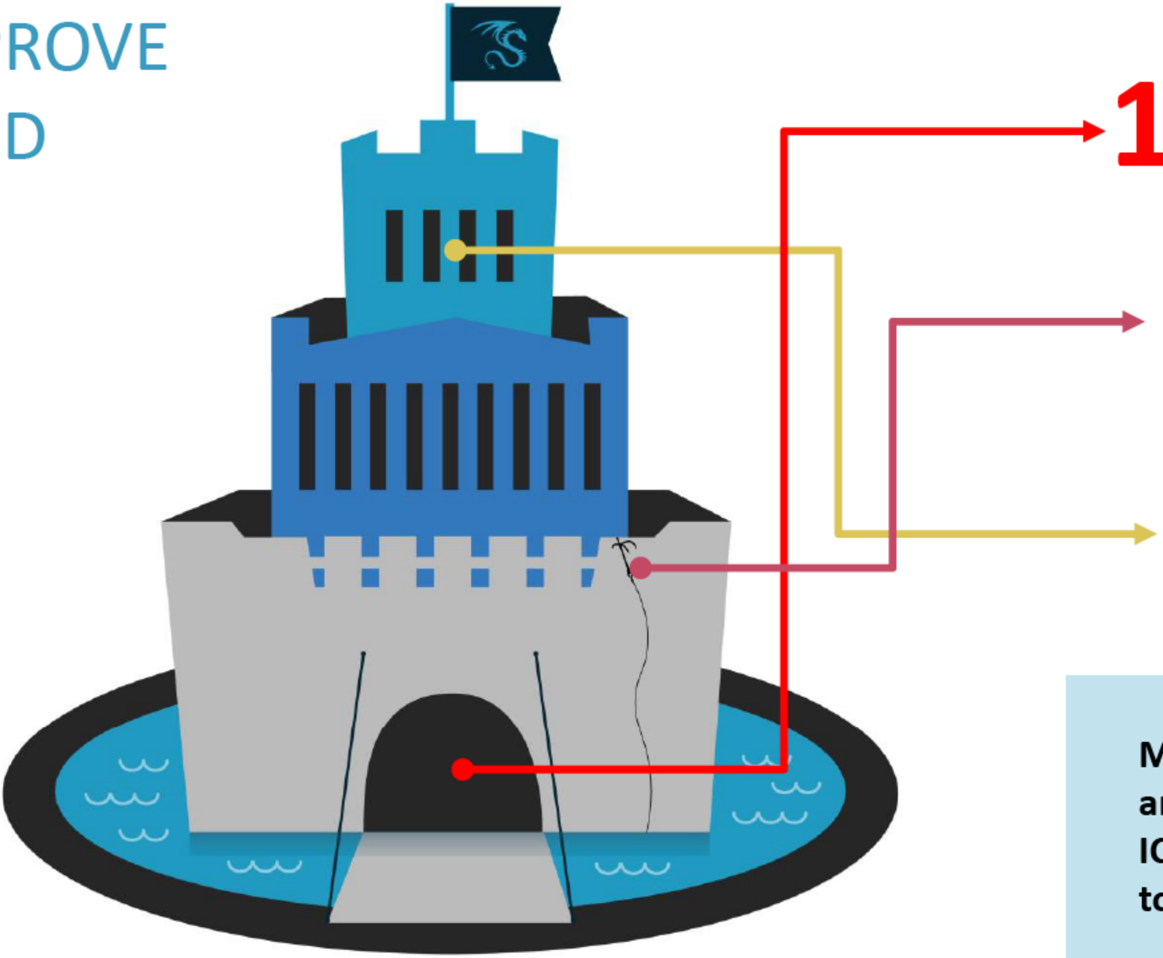
TOP ICS/OT ACCESS VECTORS



- Remote services password spraying and masquerade (e.g., VPN)
- Accidental malware infection crossing over from IT
- Shared network access with supply chain providers
- ICS-themed watering holes

KEY LESSONS FROM PROACTIVE ASSESSMENTS

NEED TO IMPROVE VISIBILITY AND DETECTION



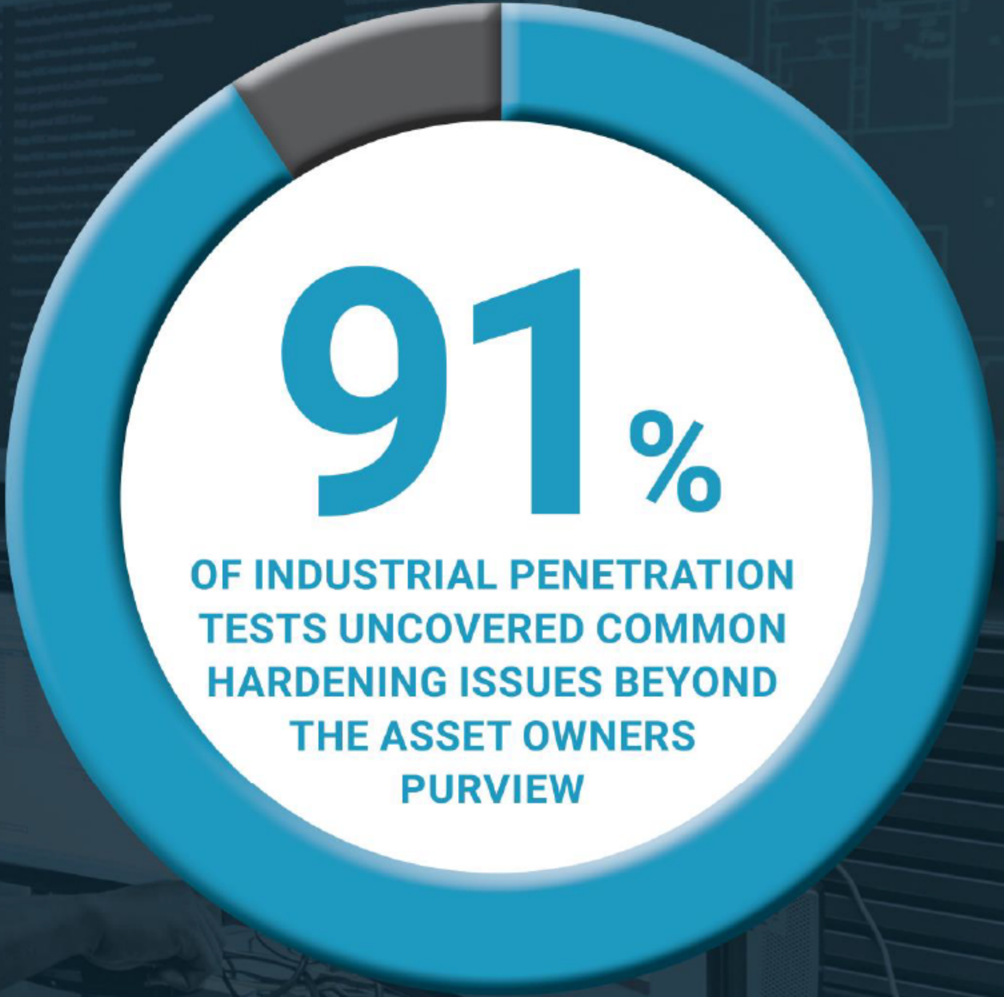
100% of network the client believed was 'air-gapped' was found with multiple routing points

76% of clients were not able to detect our red teams

71% of ICS assessments we were able to traverse into critical ICS networks

Most organizations either did not have an incident response plan for their ICS or thought they did but found it to be insufficient upon review.

CALL TO ARMS: OEMs



91%

OF INDUSTRIAL PENETRATION TESTS UNCOVERED COMMON HARDENING ISSUES BEYOND THE ASSET OWNERS PURVIEW

RECOMMENDED CONTROLS FROM THIS YEAR'S INSIGHTS

- ICS specific incident response plan with Tabletop Exercise
- ICS specific visibility and threat detection on key threat behaviors
- Multi Factor Authentication wherever possible for remote sessions
- Risk based approach to patching (vulnerabilities not a key priority)

HOW TO USE THIS INFORMATION AFTER THE CONFERENCE

- Days after the Conference:
  - 1-7: Rest and catch up on emails
  - 7-30: Pick 3-5 scenarios from Intel and Consequence
  - 30-60: Determine response to 3-5 scenarios; map your detection strategy and collection strategy to response
  - 60-90: Perform internal TTX against the top scenario
  - 90-120: Pick the top 5 critical sites and assess
  - 120-180: Determine People, Process, and Tech gaps

HOW TO GET STARTED IN THE ICS/OT COMMUNITY

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