Explore the Real-World Implications of the MITRE ATT&CK Framework

Austin Scott – Dragos
Douglas Brush – Splunk
Chris Duffey - Splunk

Introductions

POLL 1:

How familiar are you with MITRE ATT&CK?

What is the MITRE ATT&CK Framework?

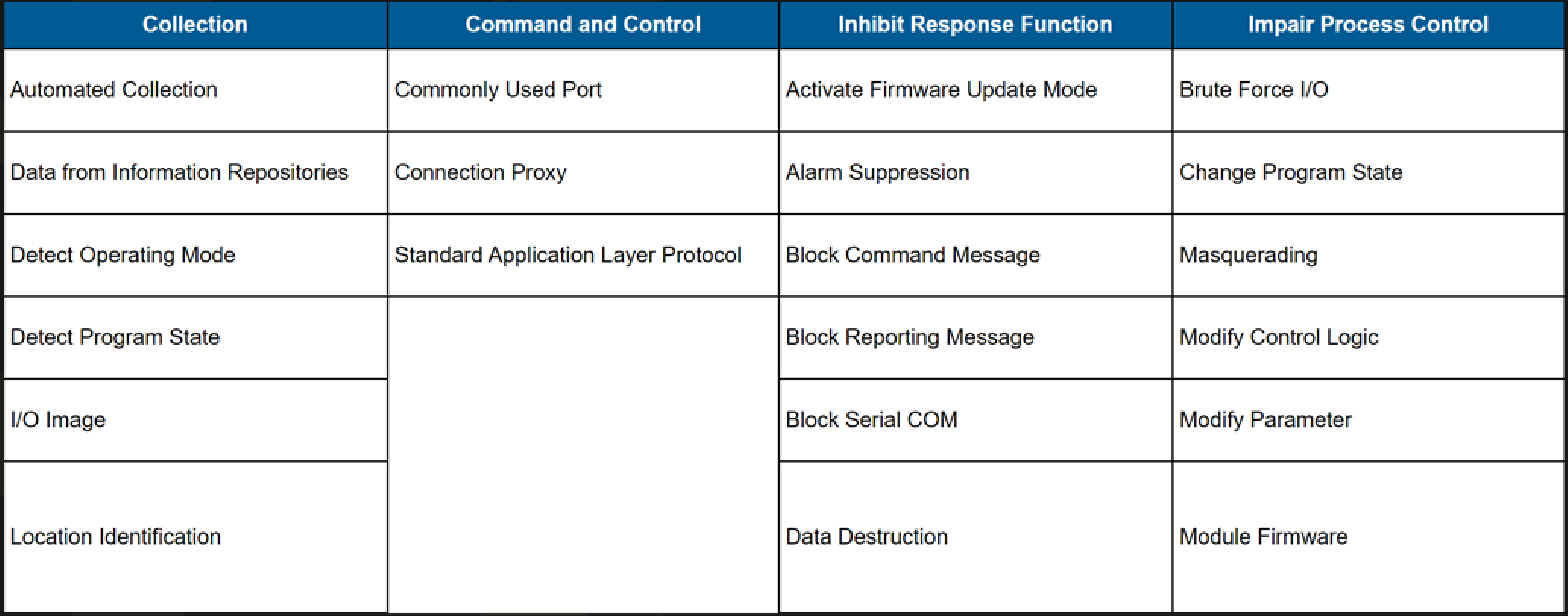
WHAT IS ATT&CK FOR ICS?

ATT&CK for ICS is an encyclopedia of ICS threat behaviors.

THE ATT&CK FOR ICS MATRIX

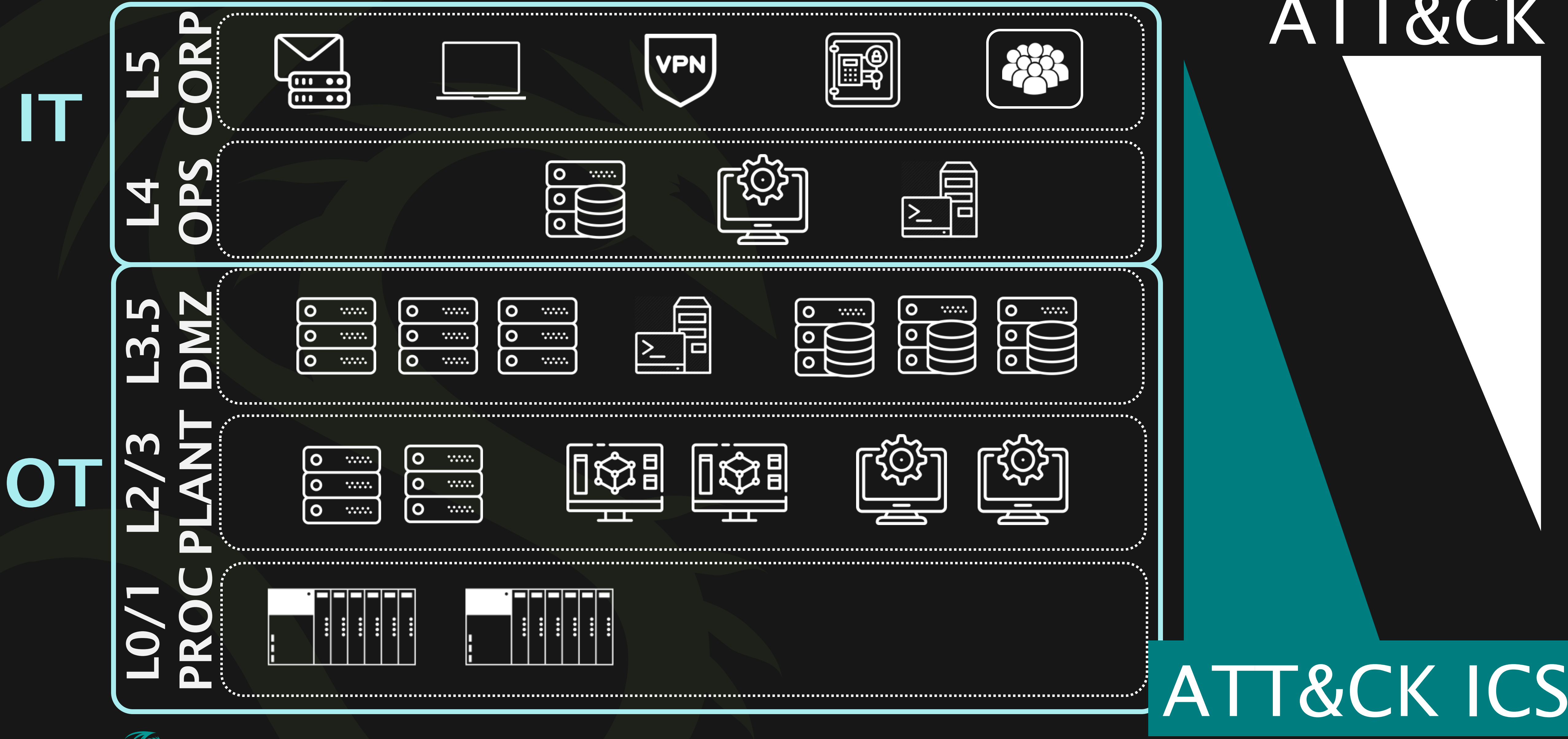
TACTICS
Technical Goals

TECHNIQUES
Achieve Goals



Collection	Command and Control	Inhibit Response Function	Impair Process Control
Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O
Data from Information Repositories	Connection Proxy	Alarm Suppression	Change Program State
Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Masquerading
Detect Program State		Block Reporting Message	Modify Control Logic
I/O Image		Block Serial COM	Modify Parameter
Location Identification		Data Destruction	Module Firmware

ATT&CK FOR ENTERPRISE VS. ATT&CK FOR ICS



WHO USES ATT&CK FOR ICS?

ANALYSTS

- Standardize Language
- Training
- OT SOC

IR/THREAT HUNTERS

- ICS Specific Tradecraft
- ICS Specific IR Playbooks

PEN TESTERS

- Adversary Emulation
- Crown Jewels

MITRE ATT&CK MATRIX
SO HOT RIGHT NOW
imgflip.com

Ummm…whut?

You want me to present this to …. Who?

TL;DR

Oh, ok!

STOP BAD PEOPLE FROM DOING BAD THINGS IN MY ENVIRONMENT,

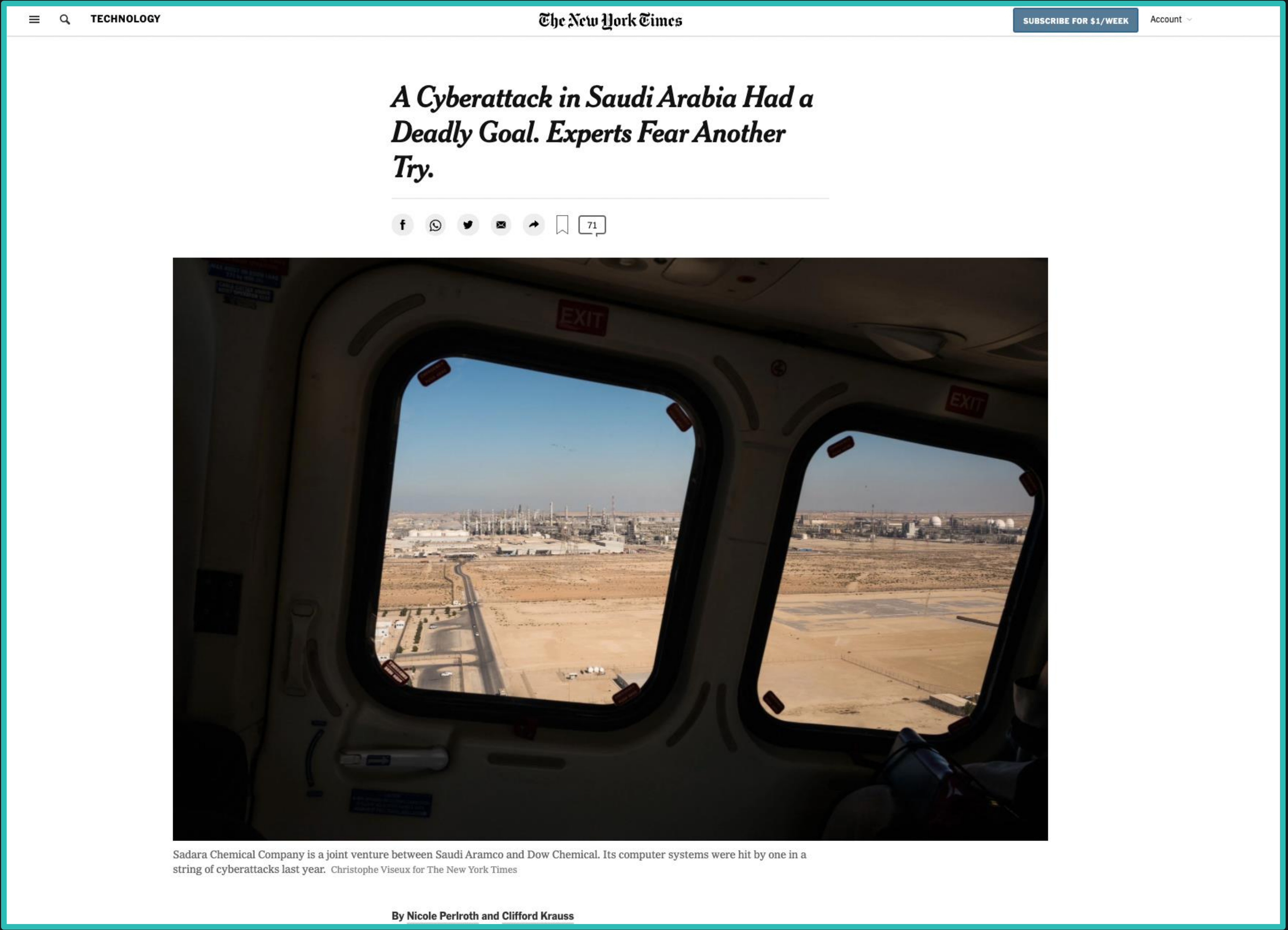
FASTER,

BASED ON COMMON PATTERNS

POLL 2:

What is your comfort level in understanding how to deploy the MITRE ATT&CK framework?

SO WHAT?
WHAT'S IN IT FOR ME?
memegenerator.net

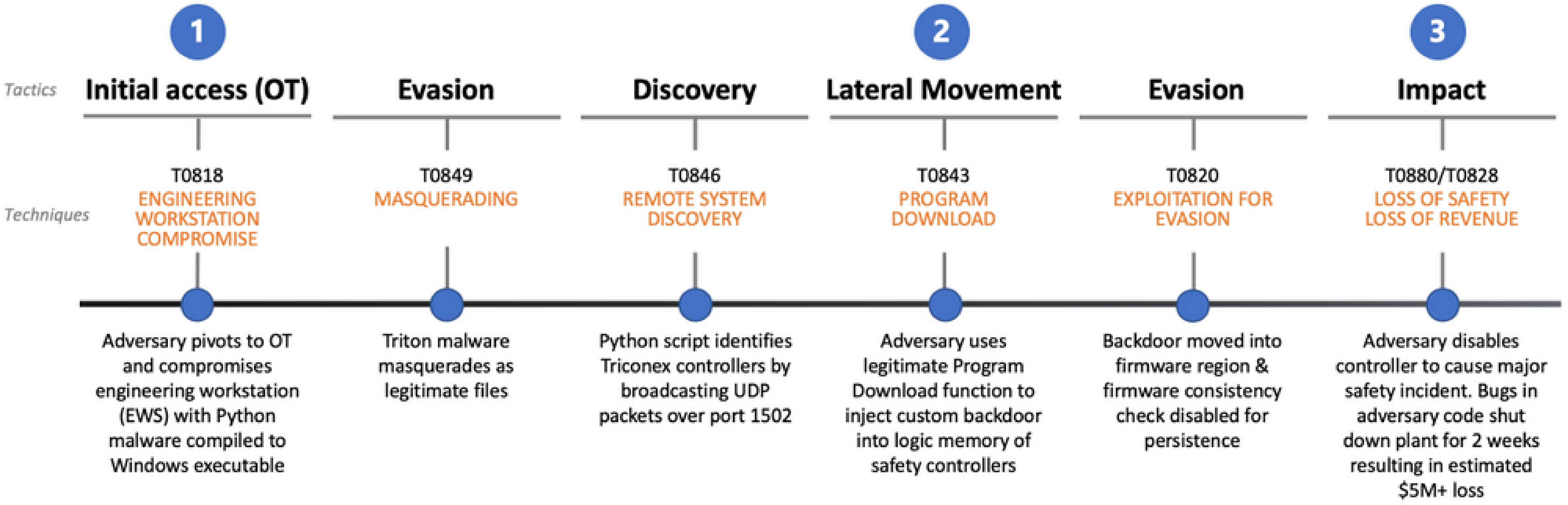


A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try.

Sadara Chemical Company is a joint venture between Saudi Aramco and Dow Chemical. Its computer systems were hit by one in a string of cyberattacks last year. Christophe Viseux for The New York Times

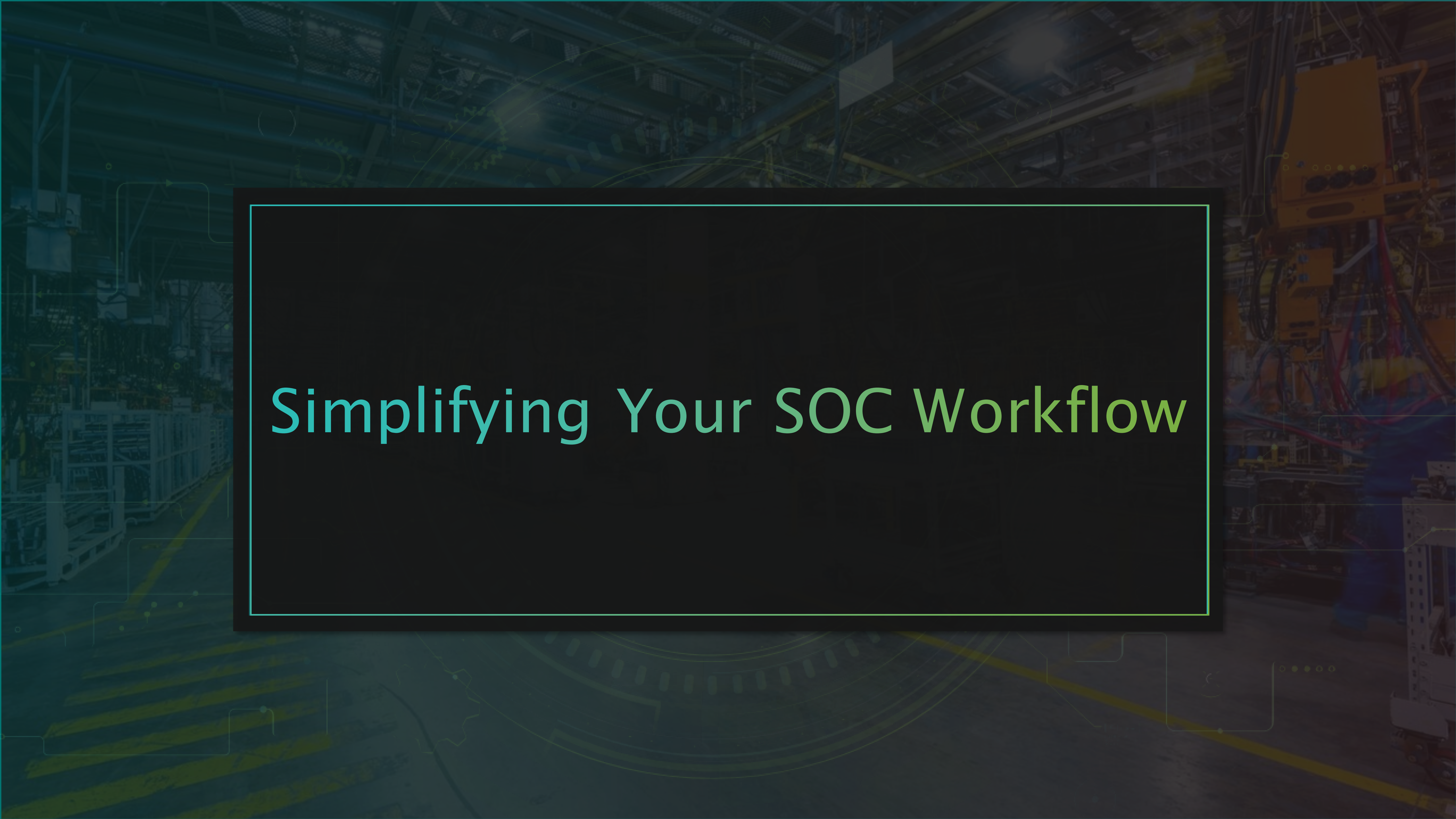
By Nicole Perlroth and Clifford Krauss

Mapping the TRITON kill-chain to MITRE ATT&CK for ICS



	1			2		3
Tactics	Initial access (OT)	Evasion	Discovery	Lateral Movement	Evasion	Impact
Techniques	T0818 ENGINEERING WORKSTATION COMPROMISE	T0849 MASQUERADING	T0846 REMOTE SYSTEM DISCOVERY	T0843 PROGRAM DOWNLOAD	T0820 EXPLOITATION FOR EVASION	T0880/T0828 LOSS OF SAFETY LOSS OF REVENUE
	Adversary pivots to OT and compromises engineering workstation (EWS) with Python malware compiled to Windows executable	Triton malware masquerades as legitimate files	Python script identifies Triconex controllers by broadcasting UDP packets over port 1502	Adversary uses legitimate Program Download function to inject custom backdoor into logic memory of safety controllers	Backdoor moved into firmware region & firmware consistency check disabled for persistence	Adversary disables controller to cause major safety incident. Bugs in adversary code shut down plant for 2 weeks resulting in estimated $5M+ loss

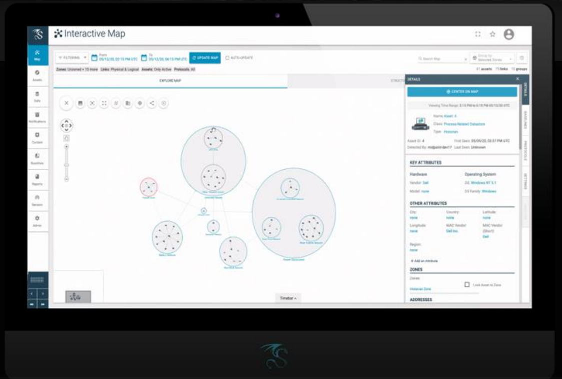
Example kill-chain from Microsoft



Simplifying Your SOC Workflow

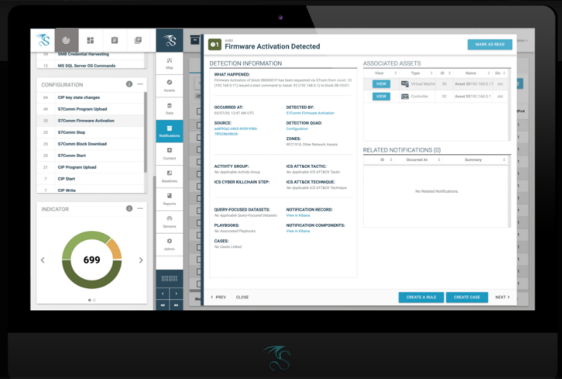
THE DRAGOS PLATFORM

COMPREHENSIVE ICS/OT TECHNOLOGY



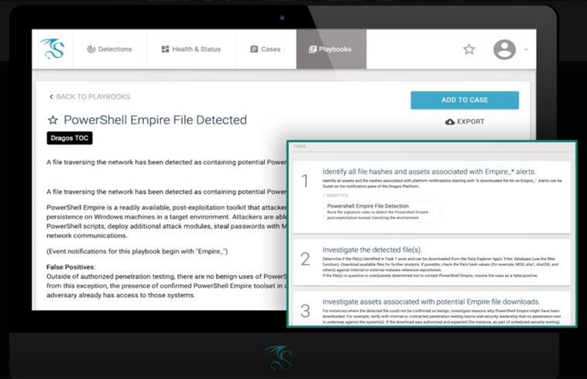
ASSET IDENTIFICATION & ANOMALY DETECTION

- ✓ See OT network traffic and assets
- ✓ Timeline and historical views
- ✓ Highly customizable zoning
- ✓ In-depth asset details including device type, vendor, firmware, model, and more



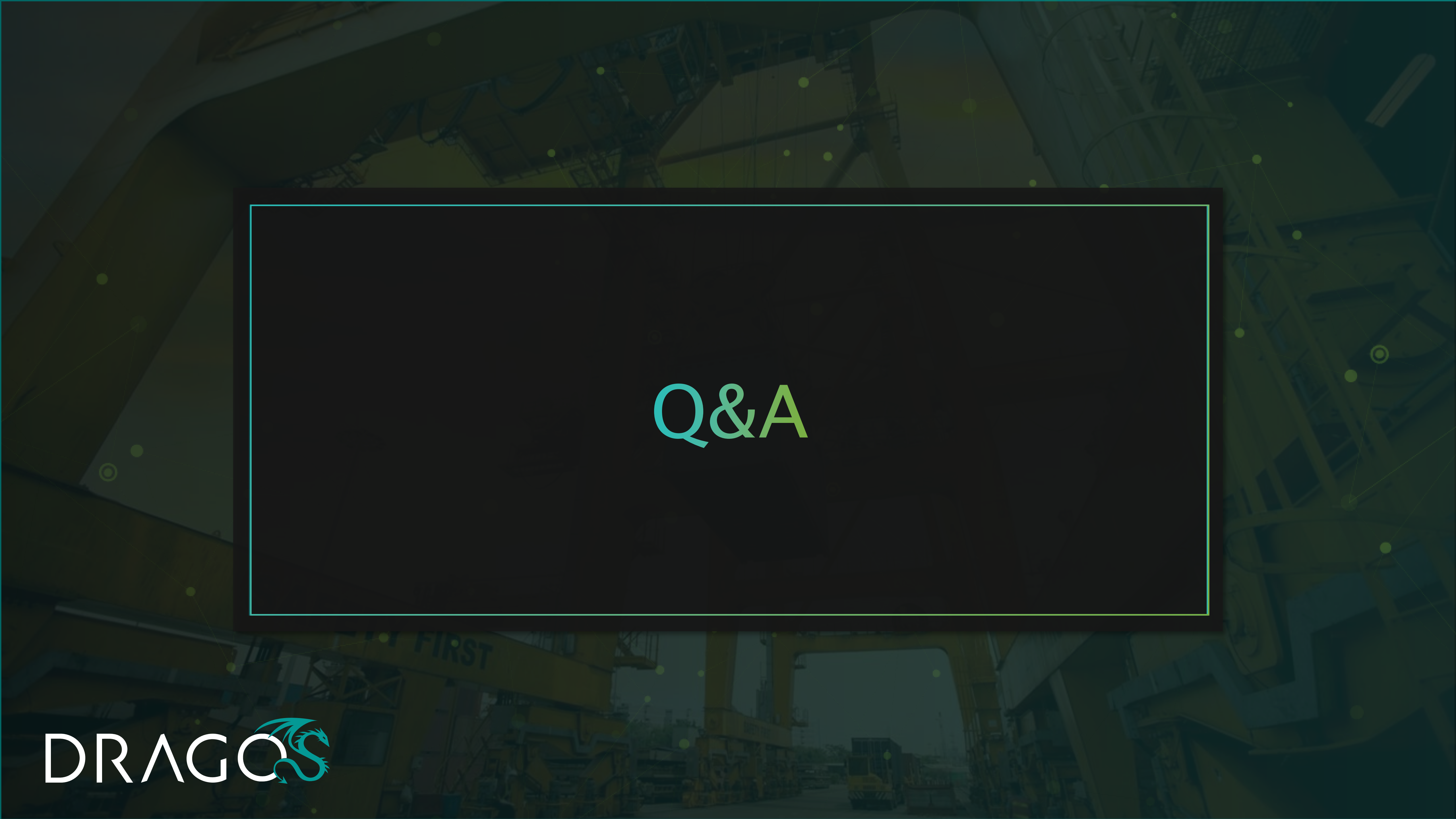
THREAT ANALYTICS MAPPED TO MITRE ATT&CK for ICS

- ✓ Continuous threat monitoring
- ✓ Context rich threat detection
- ✓ Mapped to MITRE ATT&CK for ICS
- ✓ Unique adversary TTPs and Indicators


Detections
Health & Status
Cases
Playbooks
BACK TO PLAYBOOKS
PowerShell Empire File Detected
Dragos TOC
ADD TO CASE
EXPORT
1 Identify all file hashes and assets associated with Empire_* alerts.
2 Investigate the detected file(s).
3 Investigate assets associated with potential Empire file downloads.

ANALYST WORKBENCH WITH INVESTIGATION PLAYBOOKS

- ✓ Case management and workbench
- ✓ Pre-made queries for alert triaging
- ✓ Step-by-step guides to investigations
- ✓ Playbooks for each threat analytic



Q&A

DRAGOS