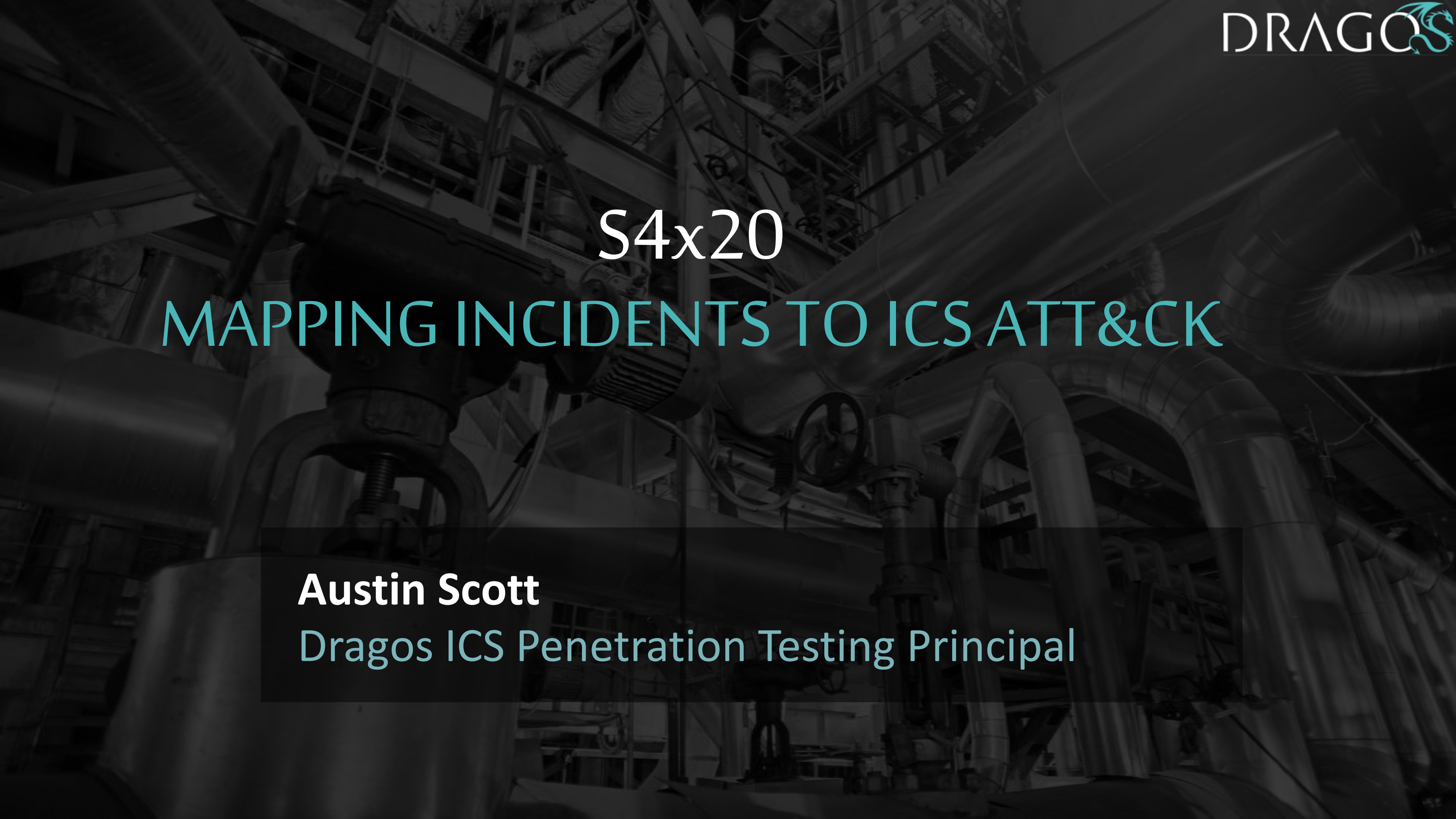


DRAGOS

# S4x20

# MAPPING INCIDENTS TO ICS ATT&CK

**Austin Scott**

Dragos ICS Penetration Testing Principal

# FOCUS ON THREAT BEHAVIOR IN 2020

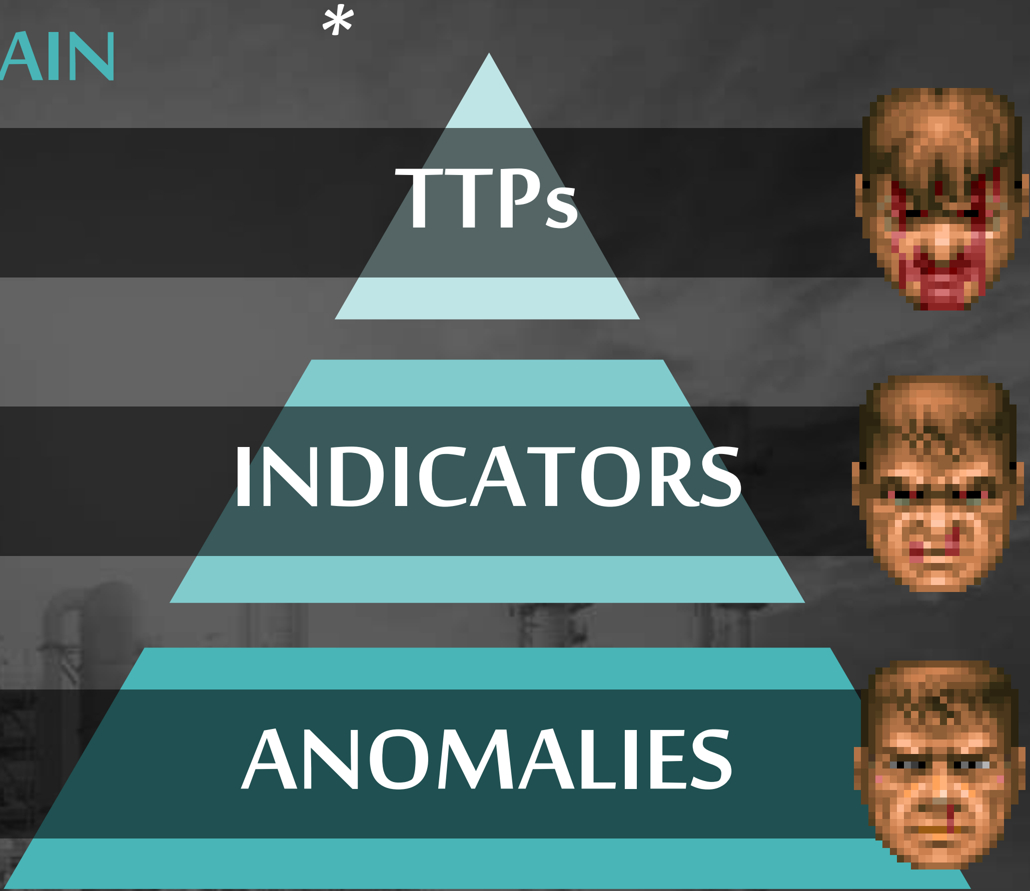
To protect against industrial adversaries, network defenders MUST focus on threat behaviors.

# ICS THREAT PYRAMID OF PAIN

Threat Behaviors (ATT&CK)

Configuration, Hashes, Tools

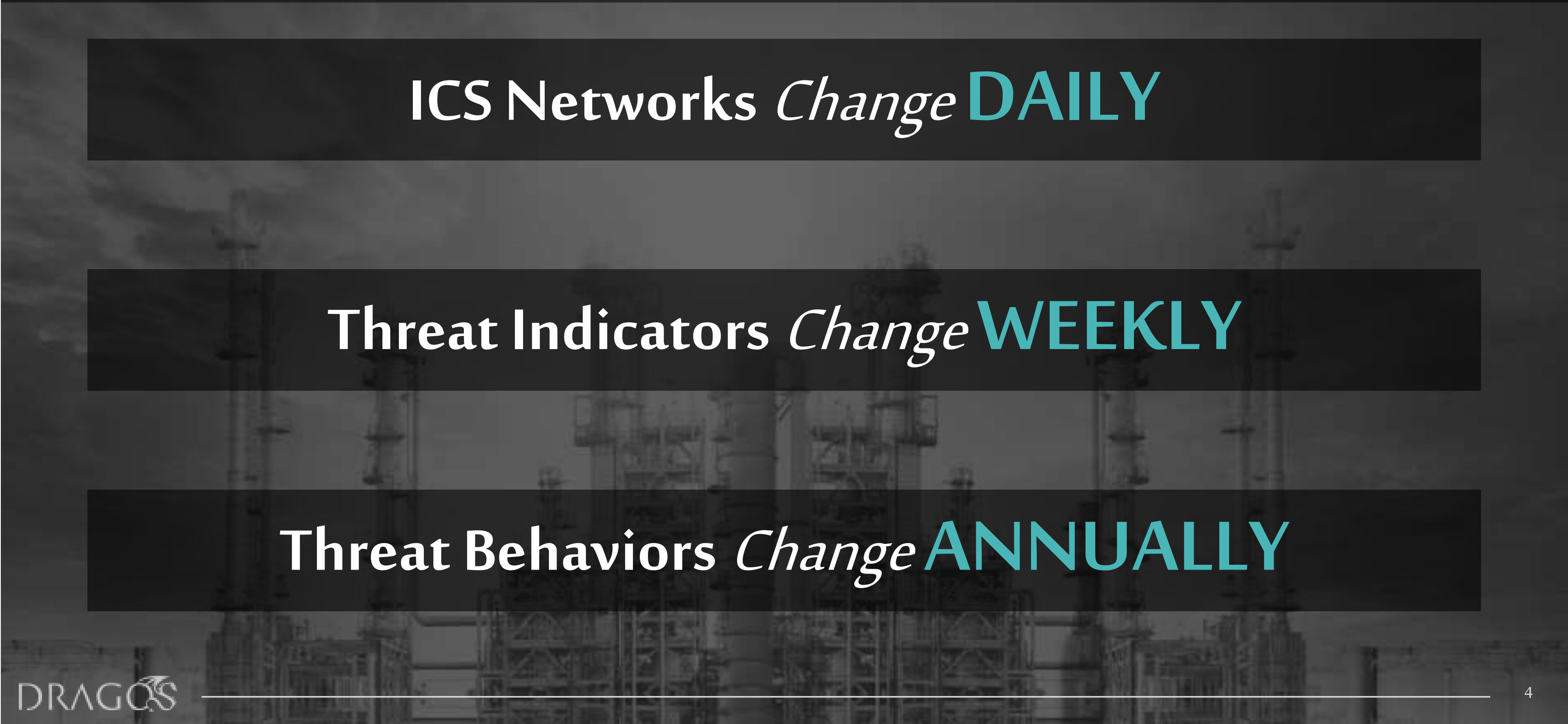
Network Changes



*Adversary pain when they are forced to adapt.*

DRAGOS

# TTP BASED DETECTIONS ARE RESILIENT



ICS Networks *Change* DAILY

Threat Indicators *Change* WEEKLY

Threat Behaviors *Change* ANNUALLY

# WHAT IS ATT&CK FOR ICS?

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

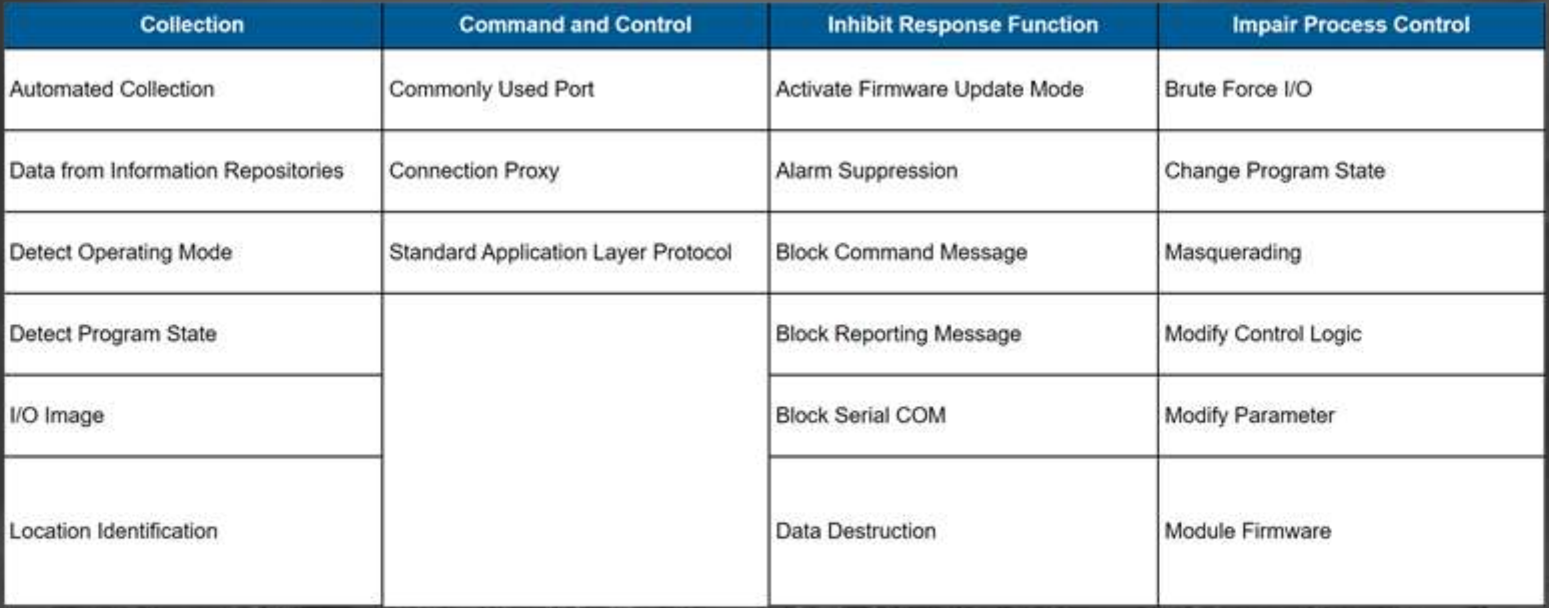
# THE ATT&CK FOR ICS MATRIX

## 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 ICS - BY THE NUMBERS

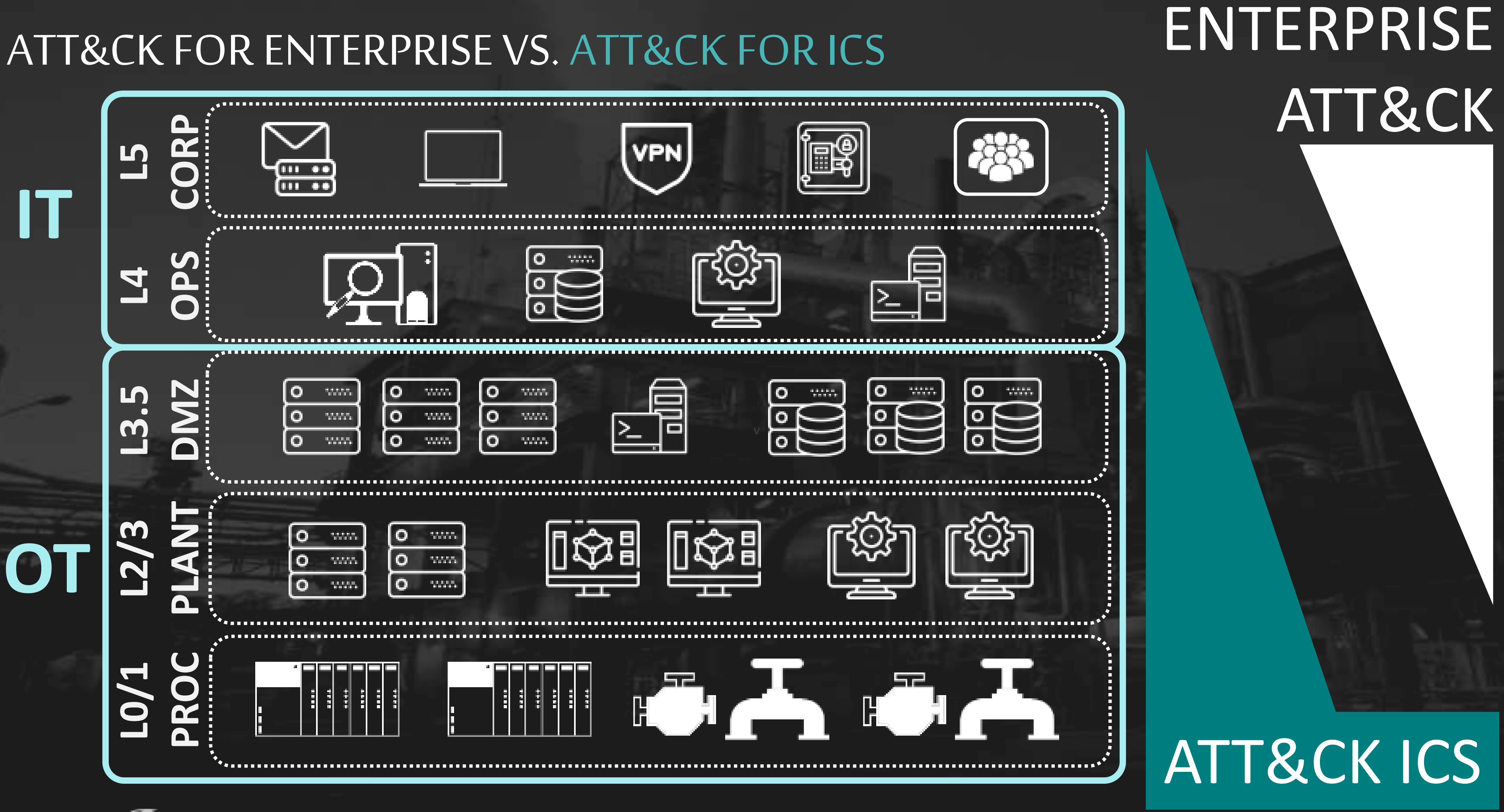
475 ICS Tradecraft Citations

11 ICS Tactics

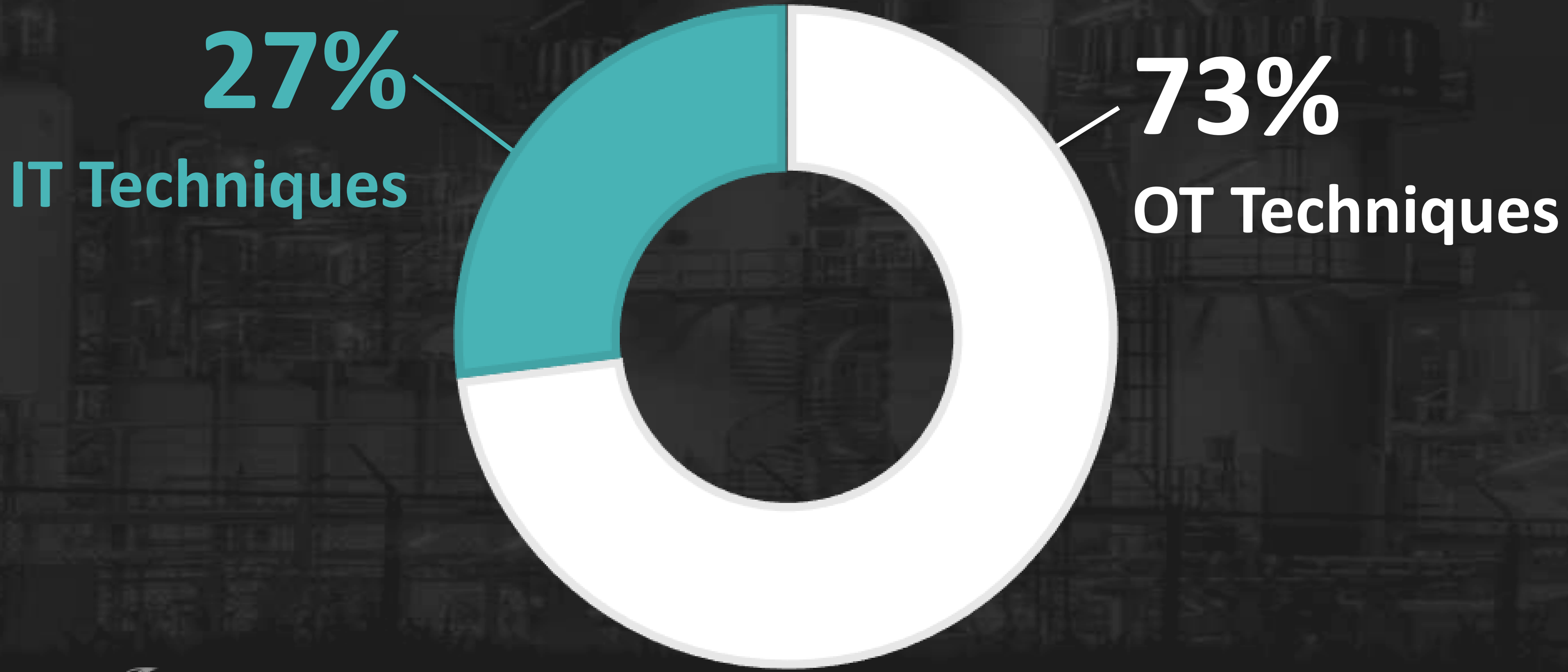
81 ICS Techniques

17 ICS Software Malware Tools

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



# IT VS. OT TECHNIQUES



# TACTIC

# %

# OT ONLY

# TECHNIQUES

| | | |
|---|---|---|
| Command and Control | 0% | IT |
| Lateral Movement | 17% | |
| Initial Access | 40% | |
| Discovery | 43% | |
| Execution | 67% | |
| Persistence | 67% | |
| Evasion | 71% | |
| Collection | 91% | |
| Inhibit Response Function | 100% | |
| Impair Process Control | 100% | OT |
| Impact Process | 100% | |

% of OT Techniques

# WHO USES ATT&CK FOR ICS?

## ANALYSTS

- Standardize Language
- Training
- OT SOC

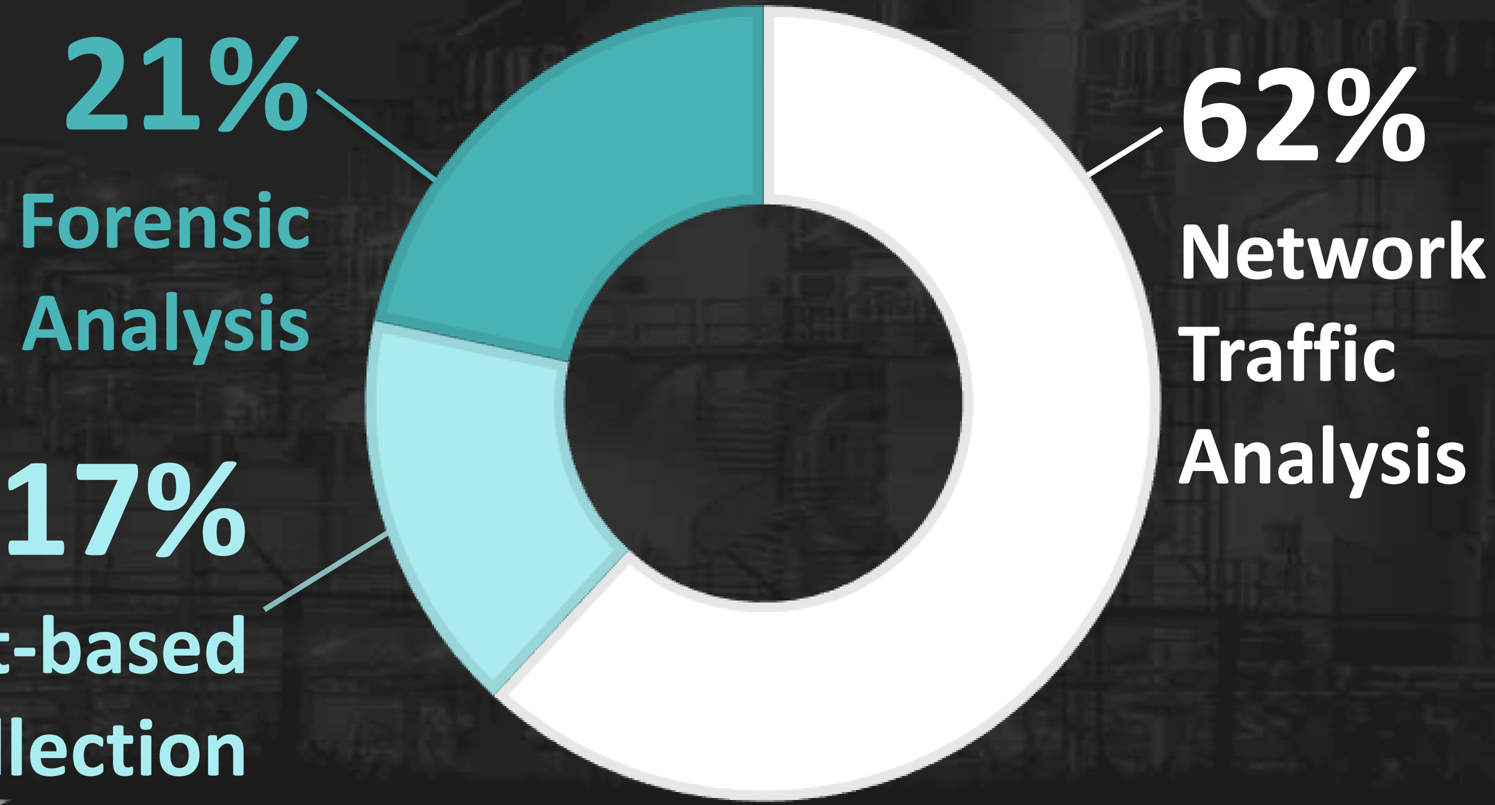
## IR/THREAT HUNTERS

- ICS Specific Tradecraft
- ICS Specific IR Playbooks

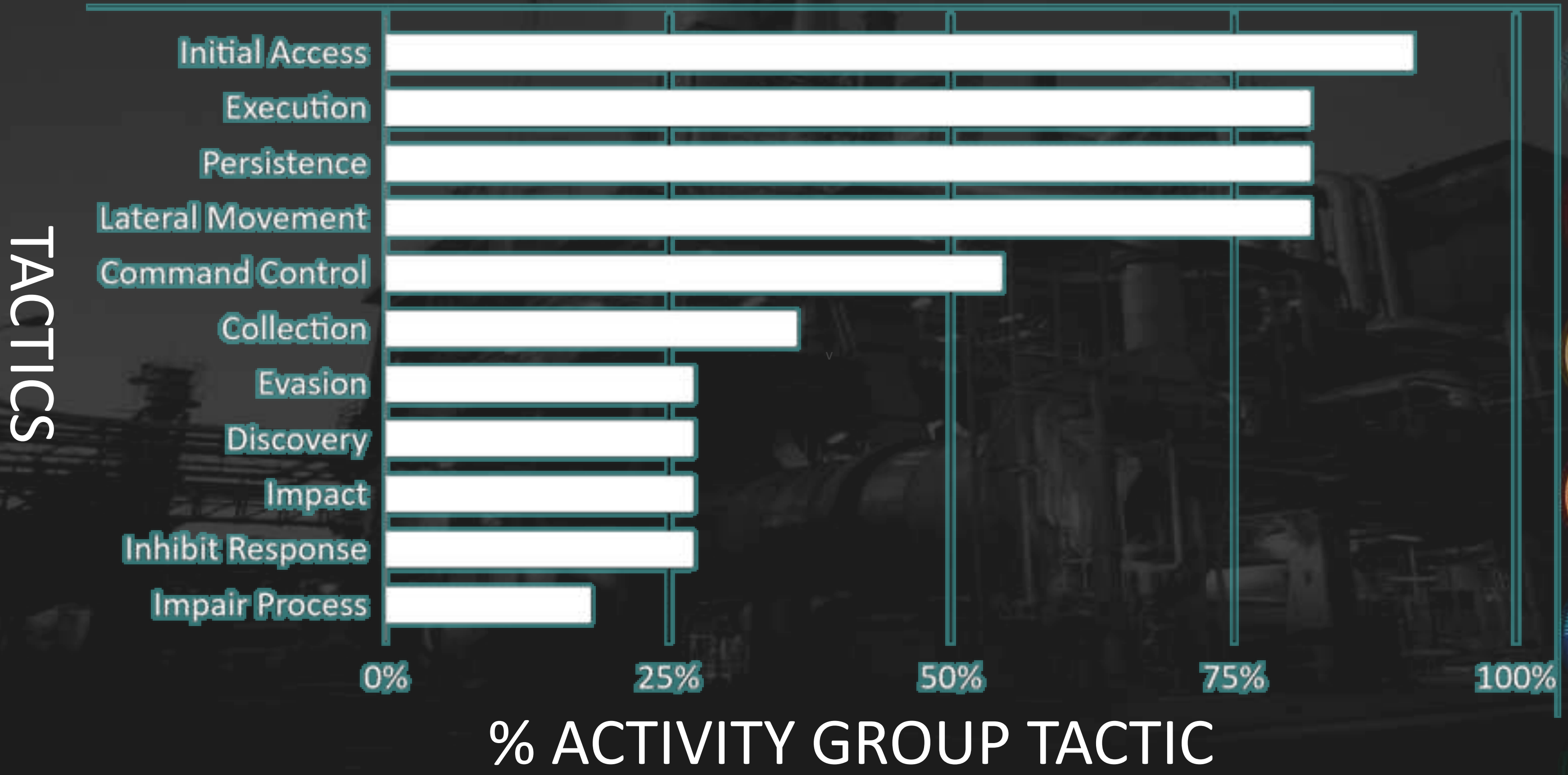
## PEN TESTERS

- Adversary Emulation
- Crown Jewels

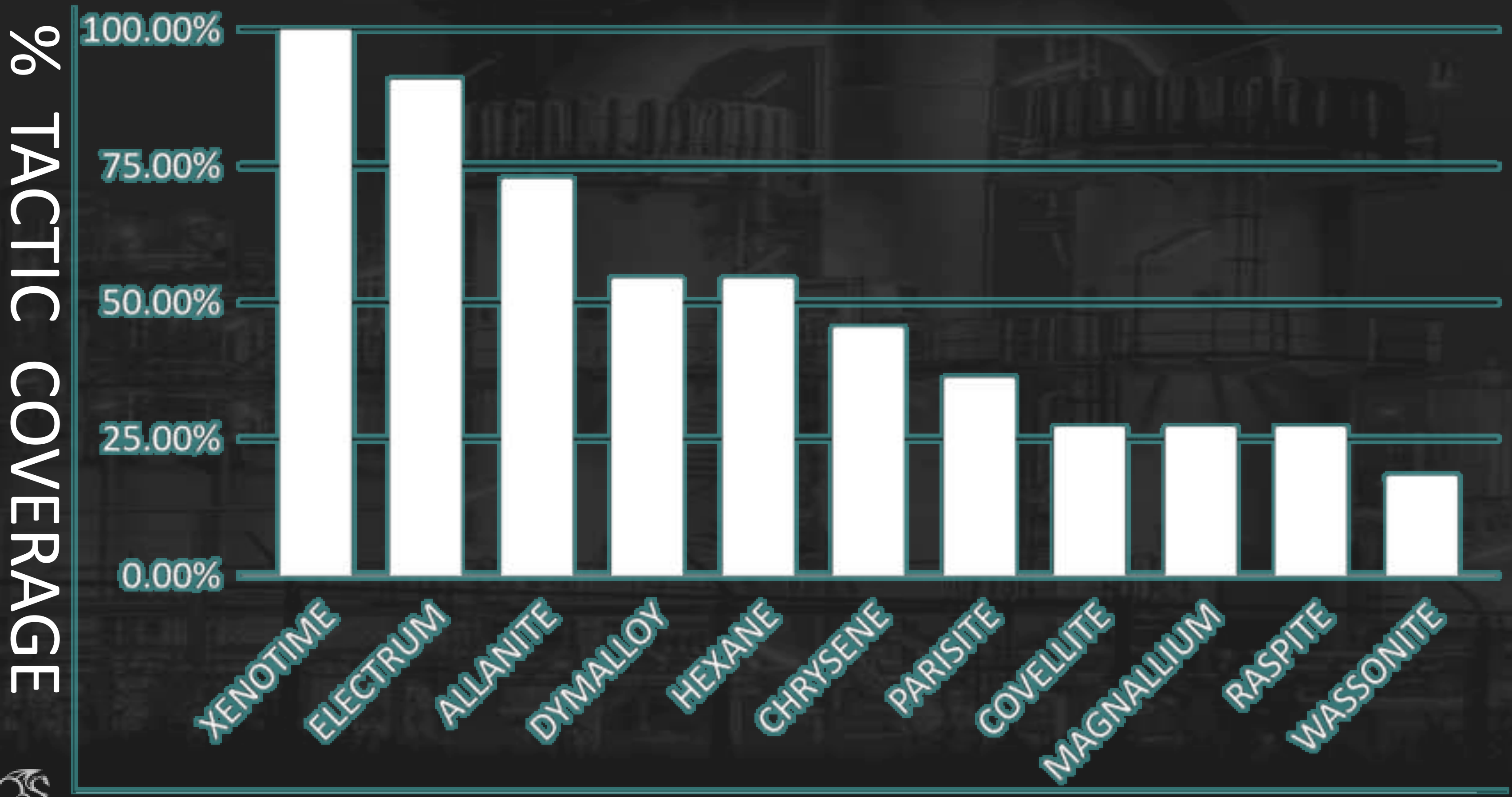
# TECHNIQUE DETECTION REQUIREMENTS



# ATT&CK FOR ICS TACTICS



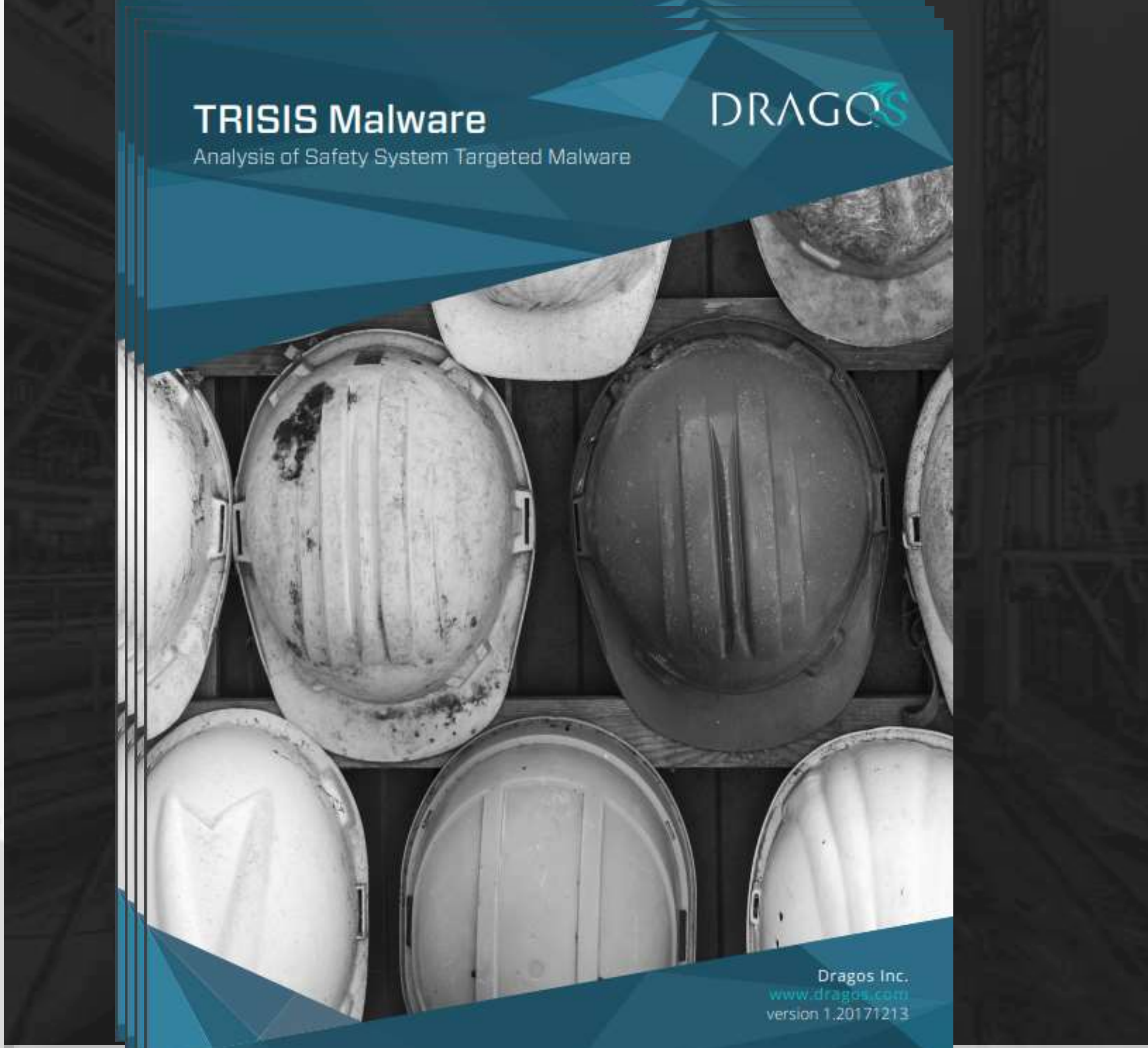
# ACTIVITY GROUP GAPS



# ACTIVITY GROUP ICS CAPABILITES

| ACTIVITY GROUPS | | | | | |
|---|---|---|---|---|---|
| XENOTIME | 🟥 | 🟥 | 🟥 | 🟥 | ICS DISRUPTION |
| ELECTRUM | 🟥 | 🟥 | 🟥 | 🟥 | |
| ALLANITE | 🟥 | 🟥 | 🟥 | | ICS ACCESS |
| DYMALLOY | 🟥 | 🟥 | 🟥 | | |
| WASSONITE | 🟧 | 🟧 | | | ICS RECON |
| CHRYSENE | 🟨 | | | | IT NETWORK |
| COVELLITE | 🟨 | | | | |
| HEXANE | 🟨 | | | | |
| MAGNALLIUM | 🟨 | | | | |
| PARISITE | 🟨 | | | | |
| RASPITE | 🟨 | | | | |

# MAPPING XENOTIME ACTIVITY TO ATT&CK FOR ICS



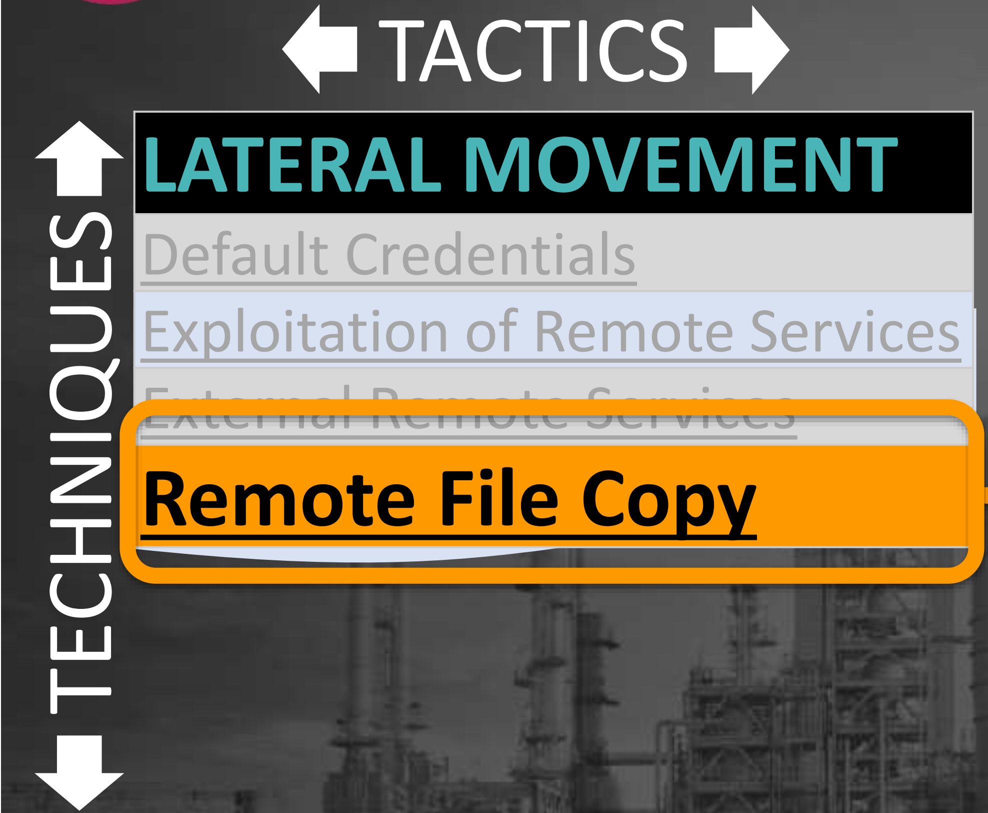
TRISIS Malware

Analysis of Safety System Targeted Malware

DRAGOS

Dragos Inc.
www.dragos.com
version 1.20171213

# XENOTIME REMOTE FILE COPY



TACTICS

TECHNIQUES

LATERAL MOVEMENT

Default Credentials

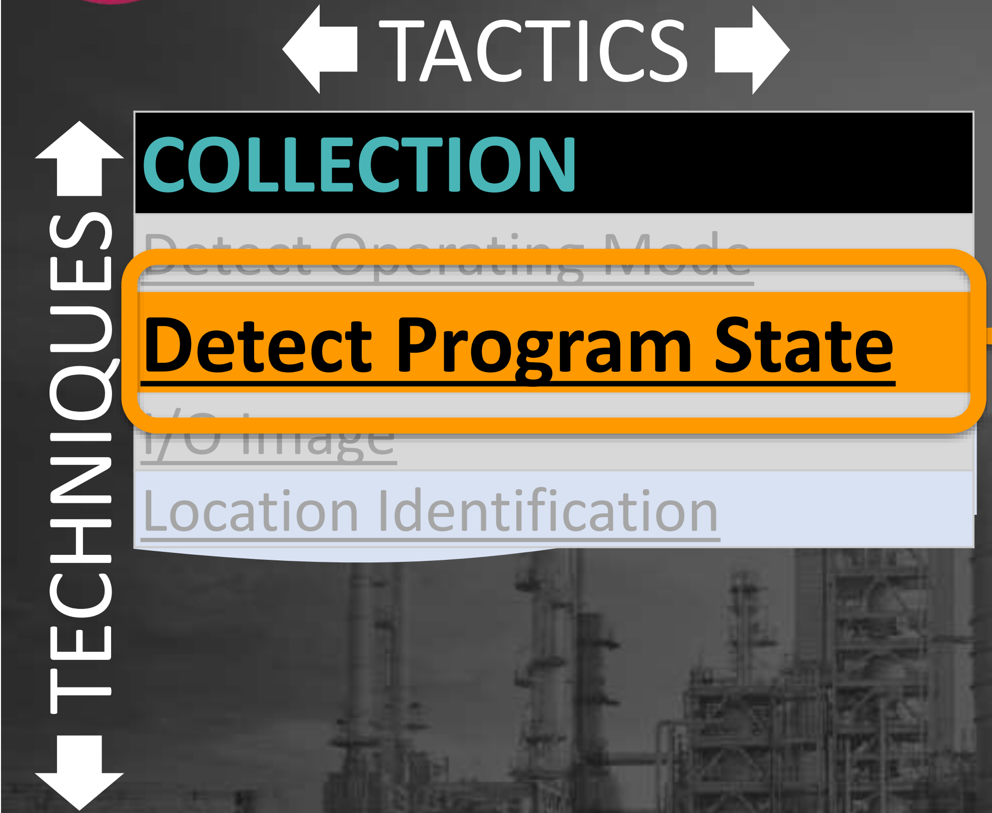
Exploitation of Remote Services

External Remote Services

**Remote File Copy**

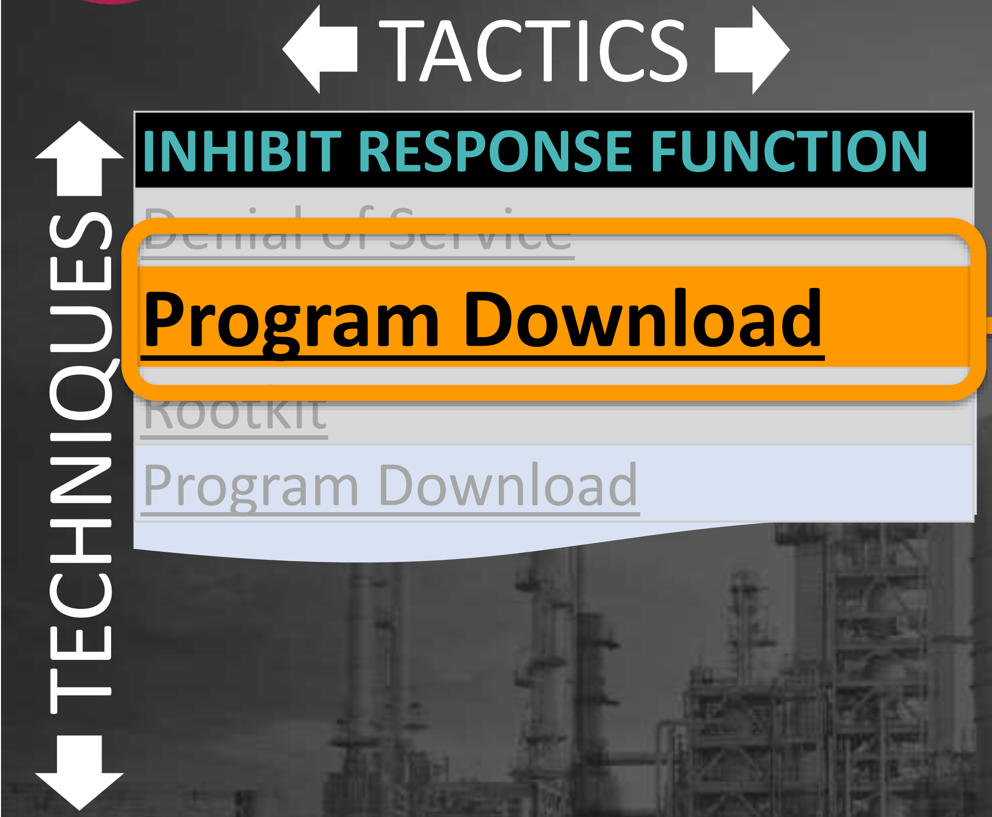
"TRISIS is a compiled Python script using the publicly-available 'py2exe' compiler. "

# XENOTIME DETECT PROGRAM STATE



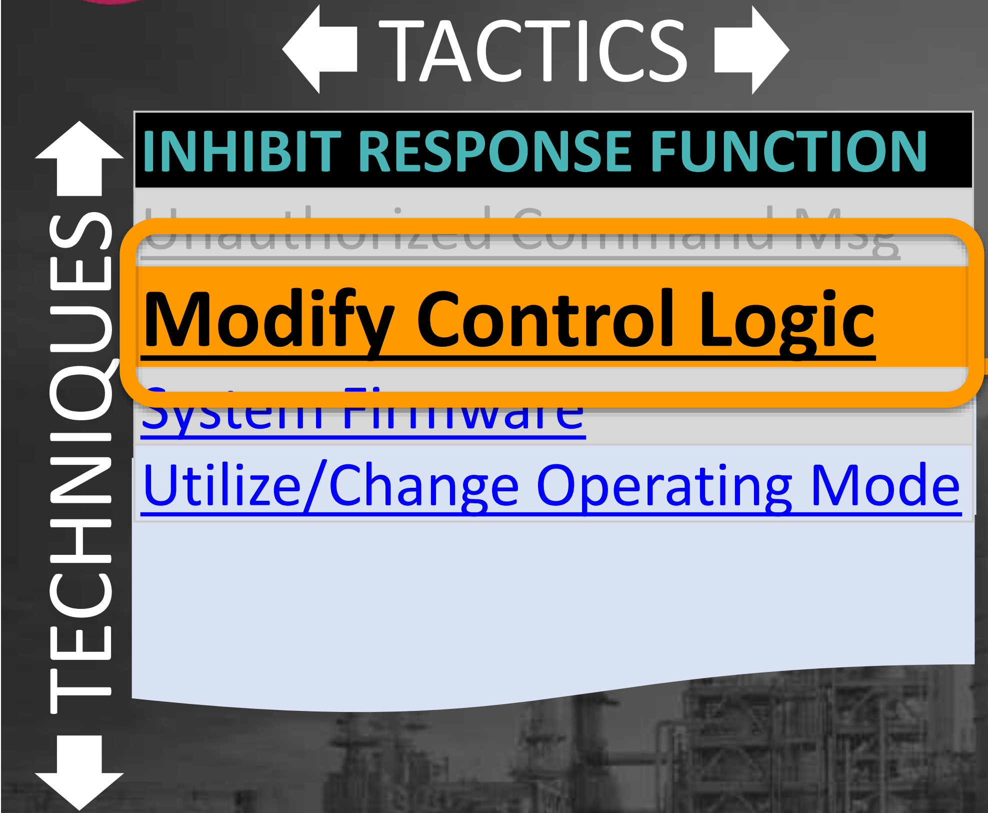
"**XENOTIME** detects TriStation key state (TS_keystate) - STOP, PROG, RUN, REMOTE"

# XENOTIME PROGRAM DOWNLOAD



"**XENOTIME** detects Copy 'Start Code' for Logic Replacement and Verifies Offsets"

# XENOTIME MODIFY CONTROL LOGIC



TACTICS

TECHNIQUES

INHIBIT RESPONSE FUNCTION

Unauthorized Command Msg

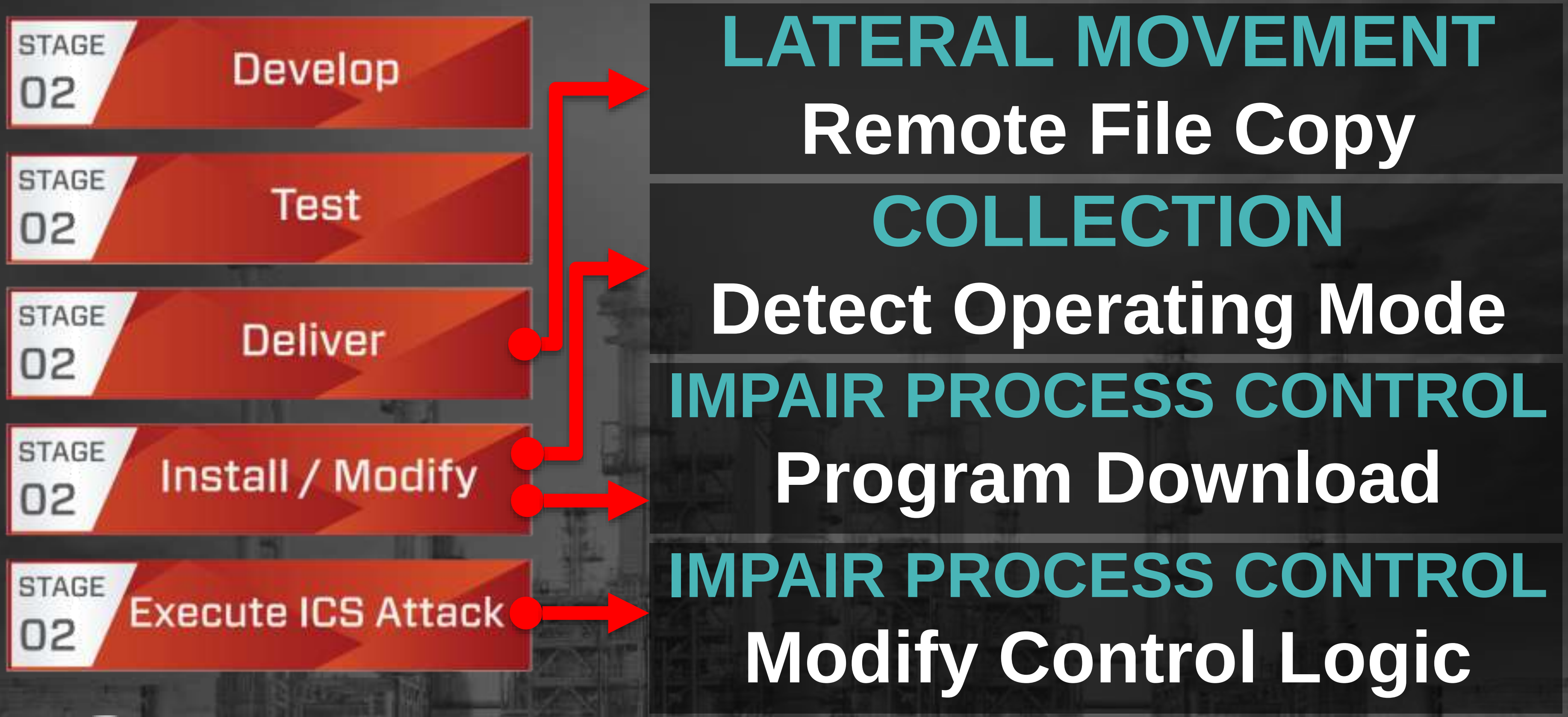
**Modify Control Logic**

System Firmware

Utilize/Change Operating Mode

“**XENOTIME** uploads new logic to disable normal safety system response”

# XENOTIME ATT&CK FOR ICS DETECTION



STAGE 02 Develop

STAGE 02 Test

STAGE 02 Deliver

STAGE 02 Install / Modify

STAGE 02 Execute ICS Attack

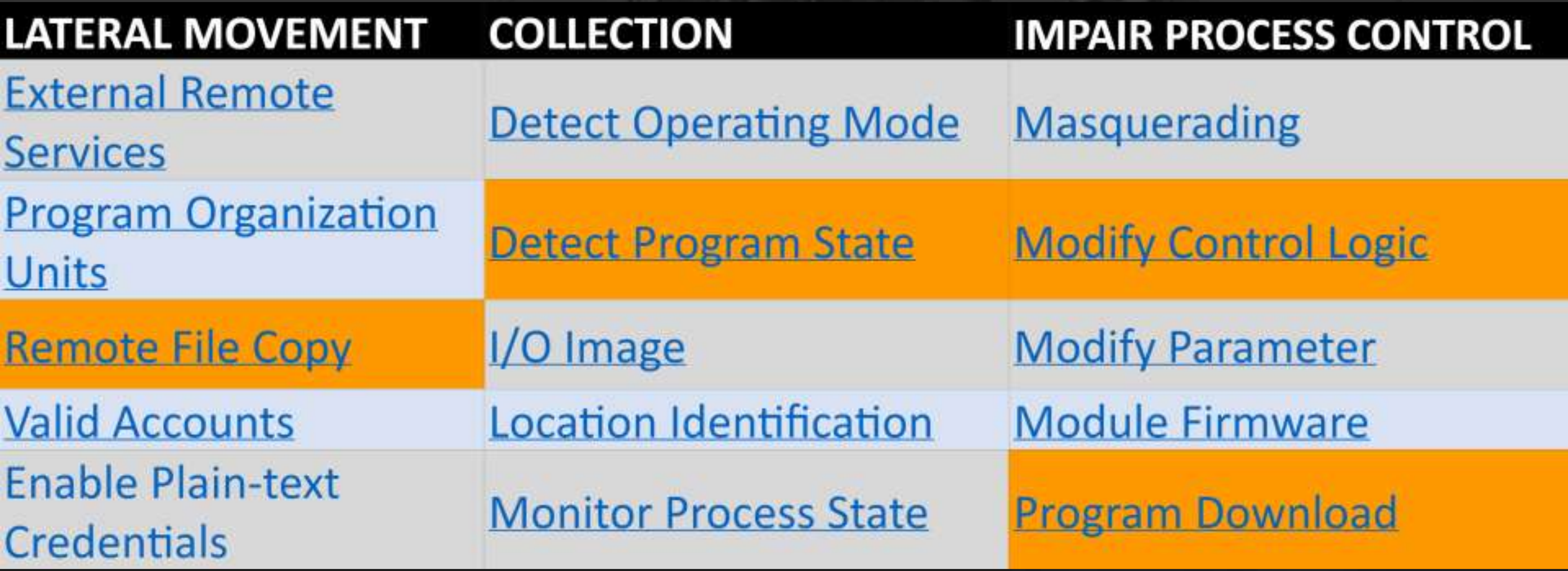
LATERAL MOVEMENT
Remote File Copy

COLLECTION
Detect Operating Mode

IMPAIR PROCESS CONTROL
Program Download

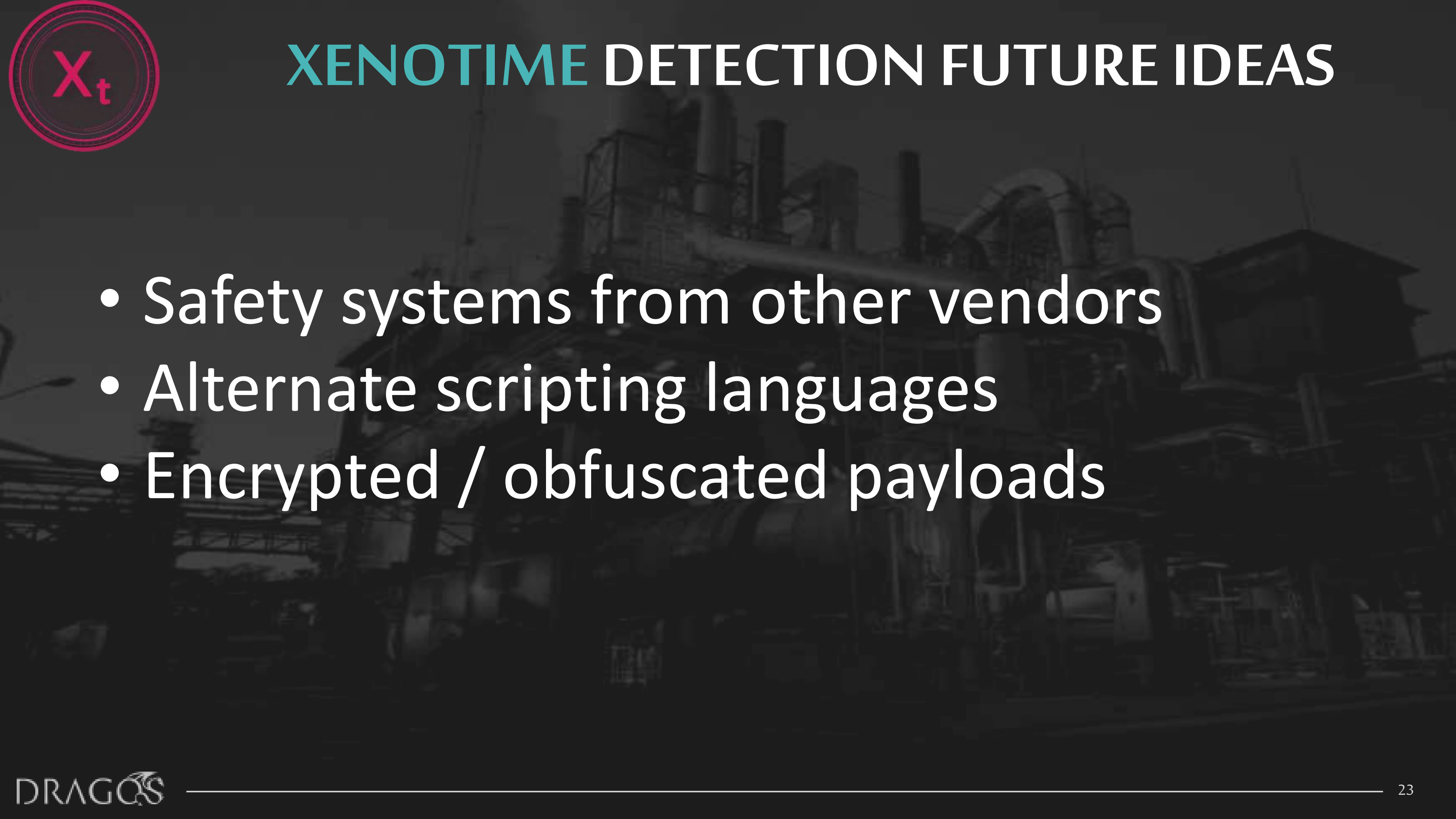
IMPAIR PROCESS CONTROL
Modify Control Logic

# XENOTIME DETECTION COVERAGE



| LATERAL MOVEMENT | COLLECTION | IMPAIR PROCESS CONTROL |
|---|---|---|
| External Remote Services | Detect Operating Mode | Masquerading |
| Program Organization Units | Detect Program State | Modify Control Logic |
| Remote File Copy | I/O Image | Modify Parameter |
| Valid Accounts | Location Identification | Module Firmware |
| Enable Plain-text Credentials | Monitor Process State | Program Download |

# XENOTIME DETECTION FUTURE IDEAS



- Safety systems from other vendors
- Alternate scripting languages
- Encrypted / obfuscated payloads

# ATT&CK FOR ICS CHALLENGES

- SMALL DATASET
- ENTERPRISE VS ICS
- VENDOR / PROCESS / VERTICAL SPECIFIC

# CONCLUSION

1. THREAT BEHAVIOR BASED DETECTIONS ARE RESILIENT
2. THREAT BEHAVIOR DETECTIONS ARE COMPLEX TO OPERATONALIZE
3. ATT&CK FOR ICS IS AN ENCYCLOPEDIA OF INDUSTRIAL THREAT BEHAVIOR

# THANK YOU

DRAGOS