DRAGOS

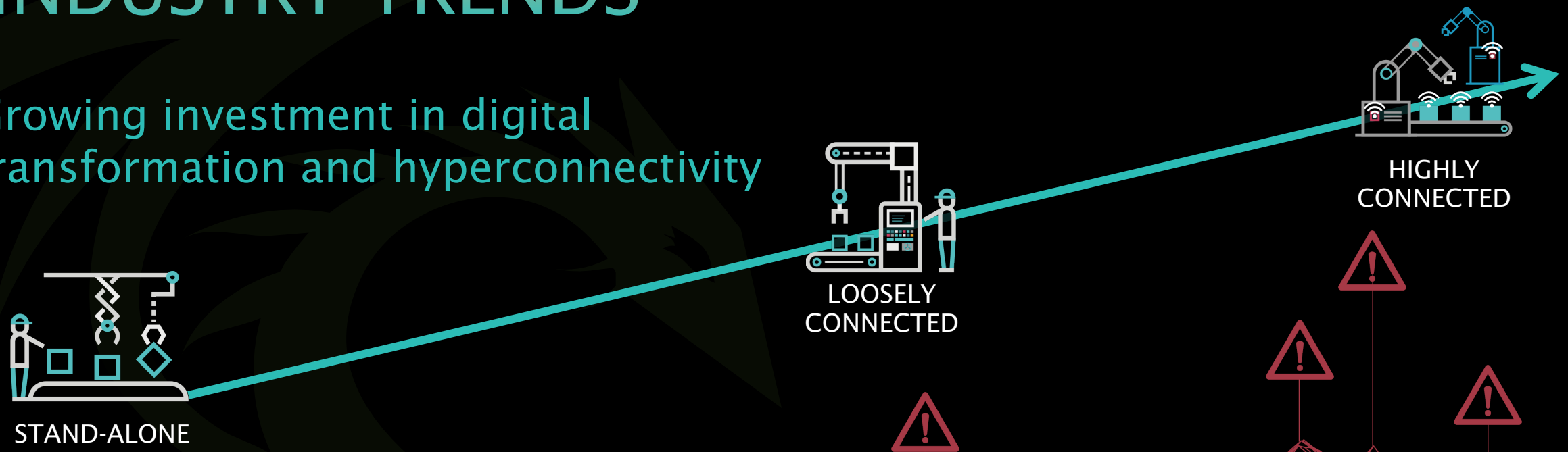
Gulf Cooperation Council – ICS Threat Perspective

Agenda

- Sector Overview
  - Electric
  - Oil & Gas
  - Water
- Trends and their impact on ICS
  - Supply Chain
  - Ransomware
- Recommendations

INDUSTRY TRENDS

Growing investment in digital transformation and hyperconnectivity



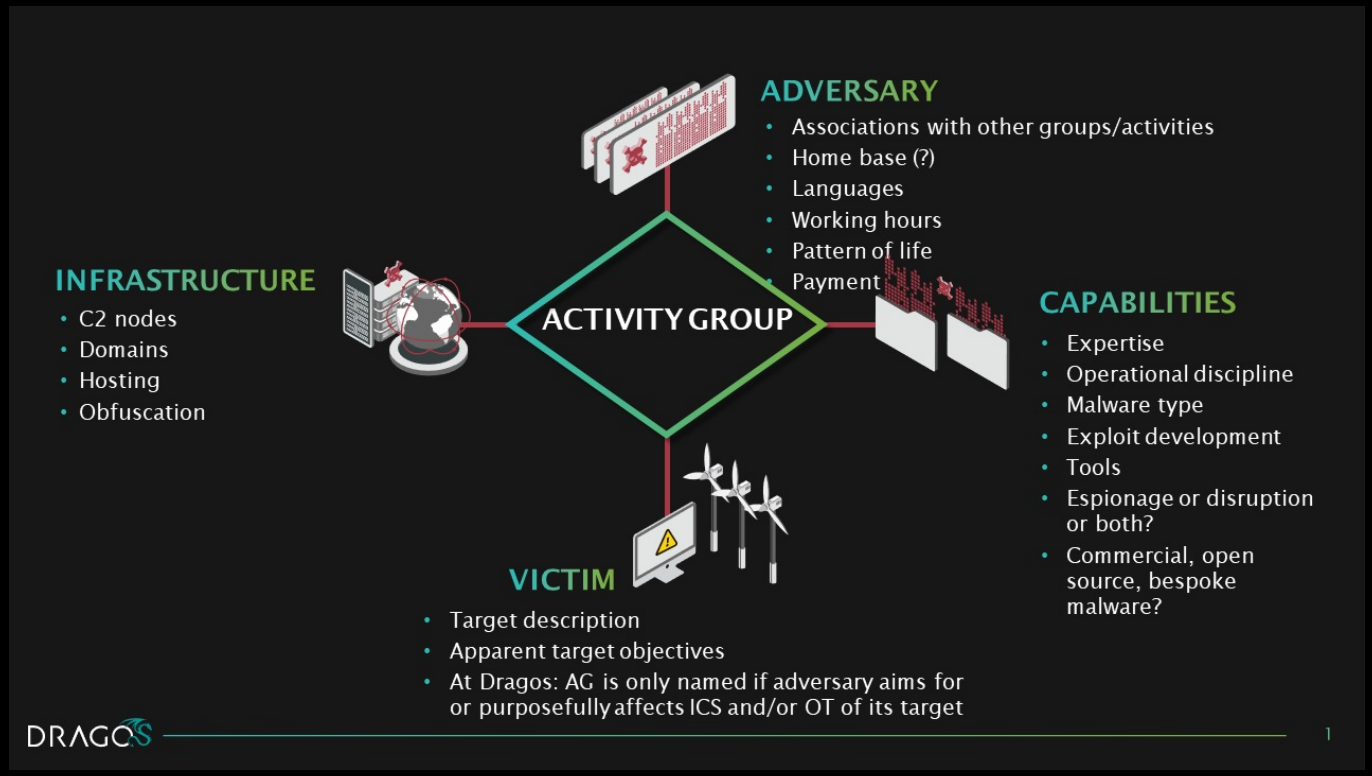
Greater exposure to malicious cyberthreats

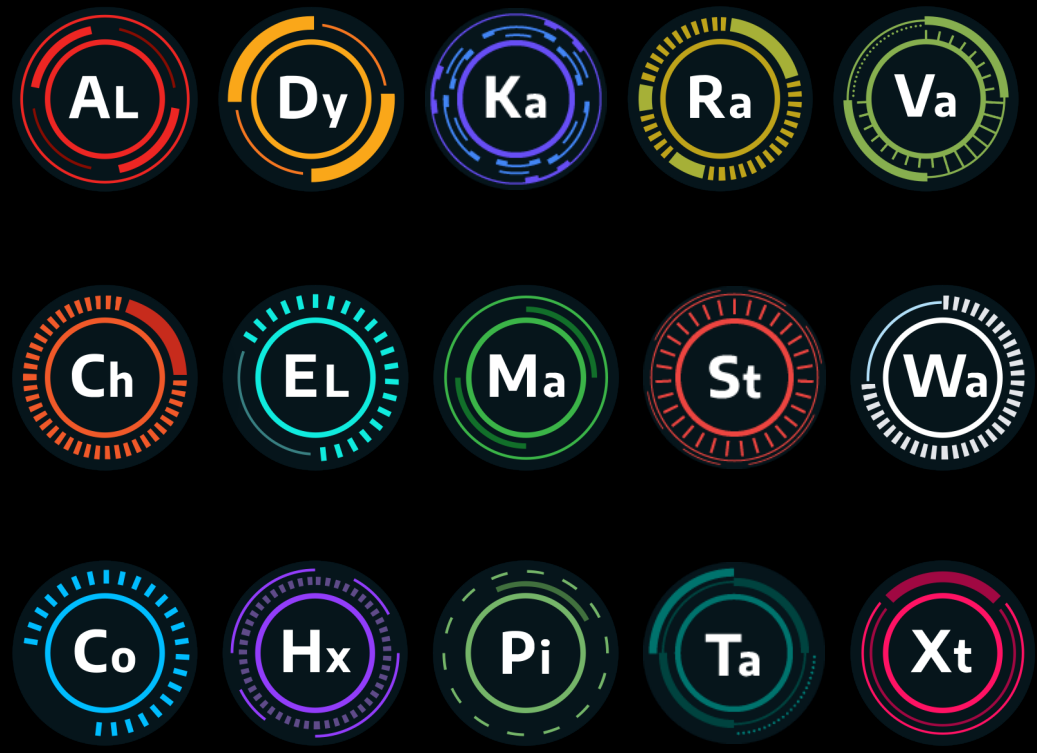
“Threat groups are rising 3X faster than they’re declining…”

Source: Dragos 2020 YiR

What is an Activity Group (AG?)

At Dragos, an AG is *different* than just another name for an adversary





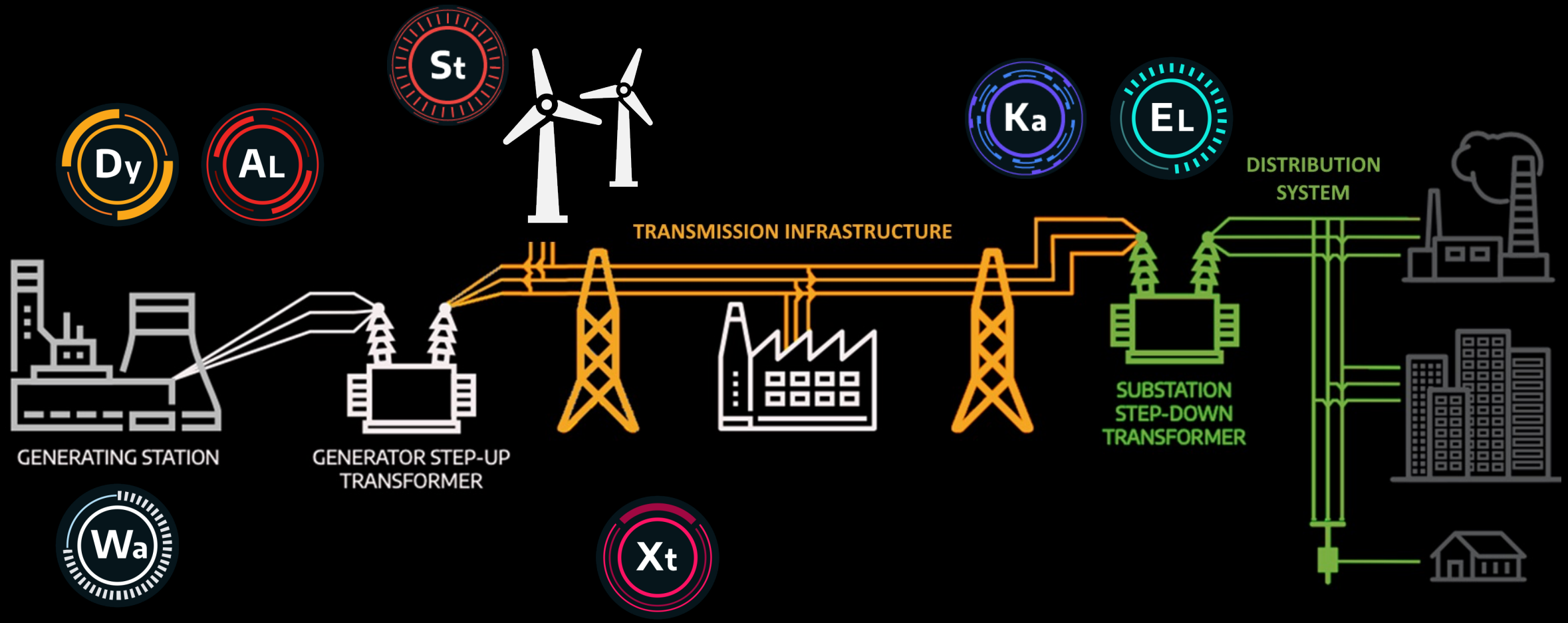
Known Activity Groups Targeting Electric

11 groups targeting Electric:

- ALLANITE
- CHRYSENE
- DYMALLOY
- ELECTRUM
- KAMACITE
- MAGNALIUM
- PARISITE
- STIBNITE
- TALONITE
- WASSONITE
- XENOTIME

Electric Threat Perspective

Operational Segments



Generation

Threat Landscape and Assessment

Intrusions are increasing; non-destructive in nature

Activity

- AGs with demonstrated intent or capabilities against Electric Power Generation
  - XENOTIME – High capability, electric activity observed in NA/APAC
  - DYMALLOY – Accessed generation, including HMI screenshots
  - ALLANITE – Accessed generation, related to DYMALLOY
  - WASSONITE – Attacked nuclear generation admin networks in APAC
  - STIBNITE – Targeted wind generation in Azerbaijan

- Disruptions: None publicly known in Electric Generation to date
- Impact: Reconnaissance, espionage, and sensitive access

Transmission

Threat Landscape and Assessment

Activity

- AGs which are a threat to transmission operations:
  - ELECTRUM – Transmission substation attack, CRASHOVERRIDE
  - KAMACITE – Facilitates stage 1 access for ELECTRUM

- CRASHOVERRIDE
  - Targeted transmission substation relays
  - Power outage in Kiev and surrounding area
  - ICS Capabilities: ABB devices, IEC 61850, Manufacturing Message Specification (MMS), OPC DA, and common C2 features

Dragos assesses with moderate confidence the attack can be adapted to other equipment and situations

Distribution

Threat Landscape and Assessment

Activity

- KAMACITE – Facilitator for BLACKENERGY2 in 2015
- ELECTRUM – 2015 Ukraine power attack

- No ICS-specific malware used. Operations controlled remotely via existing tools in the OT environment.
- Attack fundamentals could be replicated elsewhere
- Disrupting electric power requires understanding of specialized operational environments

Oil & Gas

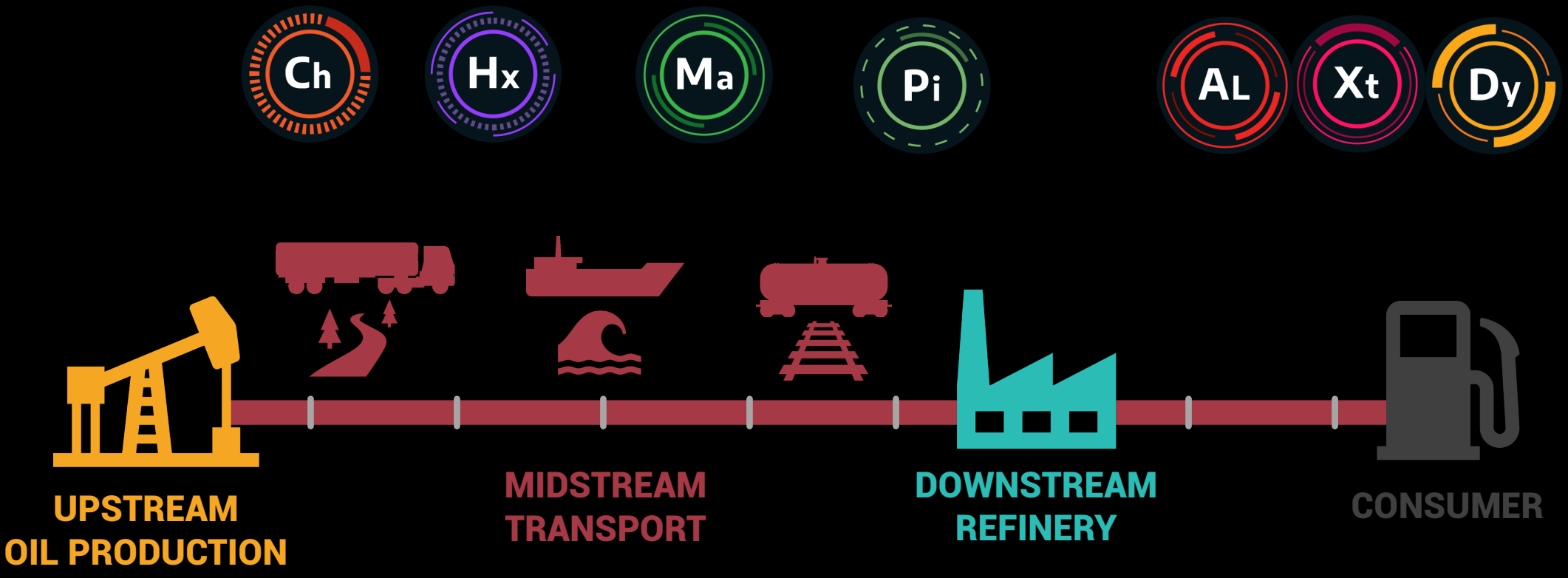
THREAT PROLIFERATION

KNOWN ACTIVITY GROUPS TARGETING O&G

Six activity groups targeting O&G:

- XENOTIME
- CHRYSENE
- MAGNALLIUM
- HEXANE
- PARISITE
- DYMALLOY

Operational Segments



Upstream

Threat Landscape and Assessment

Landscape

- Dragos has not observed recent upstream infrastructure cyber targeting
- Production Operations and Exploration
- XENOTIME is the most likely known adversary to watch for in the GCC, based on plausible motive and capability.

Watch For:

- Remote accessibility, including cellular and 3rd party
- Limited logging and ICS monitoring

Midstream

Threat Landscape and Assessment

Landscape

- Midstream cyber attacks have not been observed in the GCC, but have been observed elsewhere
- Expect emerging threats in this segment

Example:

- Colonial Pipeline: This ransomware attack did not manipulate the pipeline but did affect the billing systems and a voluntary shutdown resulted due to safety concerns.
- Societal effects were observed through temporary gas shortages, and regulatory response demonstrating this as a significant geopolitical target.

Downstream

Threat Landscape and Assessment

In the current threat landscape, there are several adversaries that demonstrate the intent and motivation to target downstream environments, specifically in refinement.

- XENOTIME
- DYMALLOY
- ALLANITE

Assessment: O&G downstream segment threat environment is the largest target currently for O&G.

Major Areas of Concern for Downstream:

- SCADA-Assets with direct access to the internet
- Dual-homed assets between SCADA and IT network
- Limited ICS/OT network visibility

Water Sector

Water Infrastructure

GCC countries rely heavily on desalination plants

- GCC accounts for >50% of global desalination plants
- Power generation and water production are often co-located

Recent Attack on Water

- April 2020: Multiple water facilities targeted which fed residential areas
- Reported intent was to increase chlorine level
- Remote attack, PLC exposed without authentication mechanisms, valve logic changed

Supply Chain

The ICS OEM Nexus

- OEMs often have remote access to critical parts of customer networks
  - This means that hackers who breached an OEM could potentially use their credentials to control critical customer processes
- Compromising an OEM magnifies the potential risks to infrastructure
  - Infections in the critical infrastructure sector occurred on IT networks as well as on industrial control system networks that manage critical functions

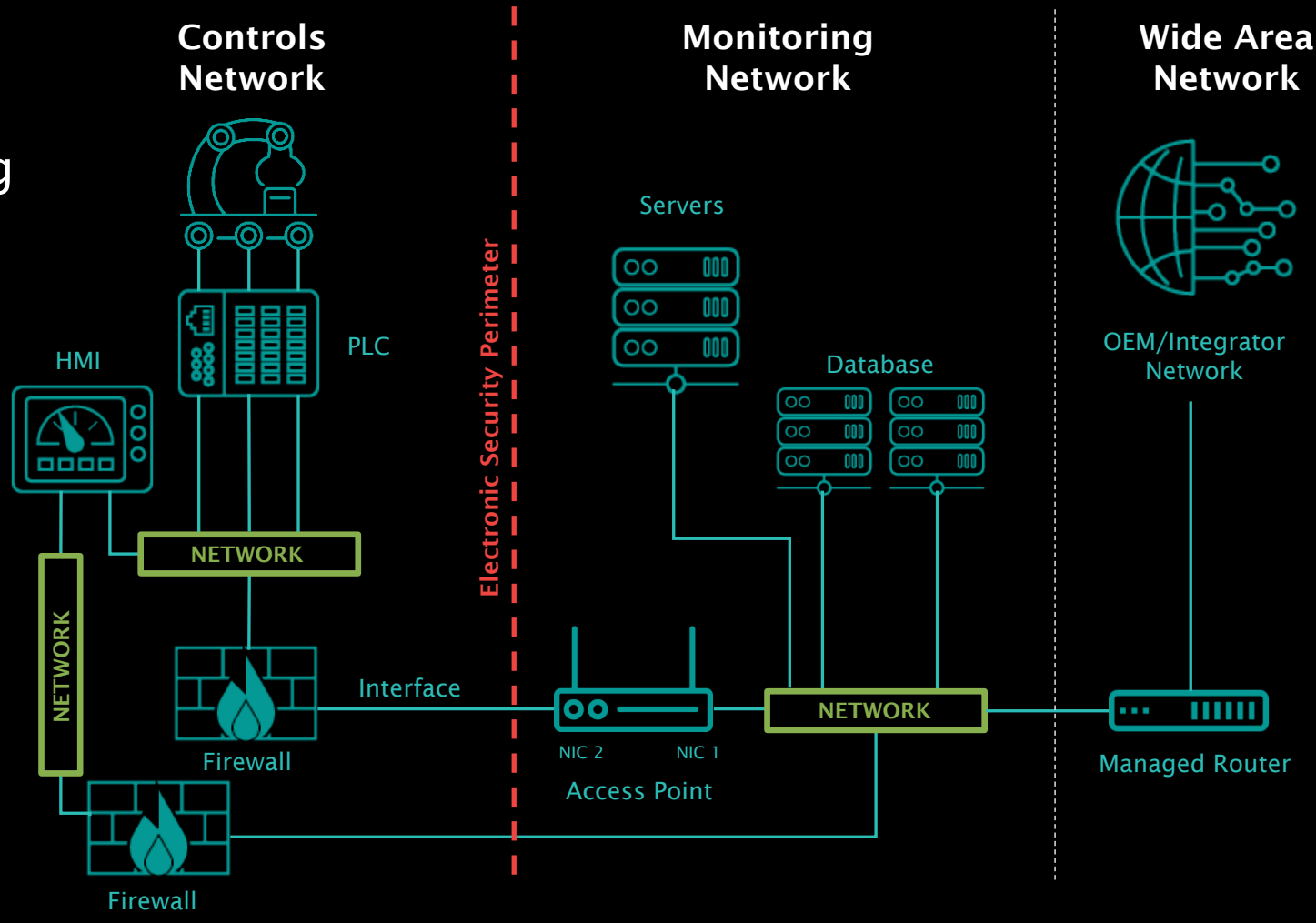
OT Exposure via Remote Access

Use cases:

- Monitoring and troubleshooting
- Patch distribution
- Staff augmentation

Examples:

- SolarWinds
- Numerous OEM compromises direct into DCS/SCADA networks of industrial companies



Ransomware

Ransomware

- REvil ransomware group
- Funding – TTPs - Hide/Re-Emerge
- O&G (All Segments)
- Significant increase in ransomware attacks.

Ransomware Risk Assessments

- Work-From-Home and weak access controls through IT/OT integrated systems
- Proposal to assess risk using an algorithm
  - No Risk Assessment tool is perfect
  - Risk assessment cannot be blind to any system interaction
  - This risk assessment tool considers each of several organizational security functions, and using a qualitative approach calculates estimate of risk per function.
  - Each of the functional risks are then multiplied to get an overall “risk exposure” to malware

Recommendations

Summary Recommendations

DEFENSIBLE ARCHITECTURE

- Perimeter Protection / Firewall / DMZ
- OT Network Segmentation
- Architecture Reviews

MONITORING

- Security Events / Log aggregation / SIEM
- Network Traffic Monitoring i.e., Passive Monitoring

REMOTE ACCESS AUTHENTICATION

- Consolidate Remote Access channels
- Multi-Factor Auth. for ALL remote access
- Constrain exposure, limited users/times/features/file movement

KEY VULNERABILITY MANAGEMENT

- Establish knowledge sources: Vulnerability scans, community/external intelligence
- Apply situational context and remediate

ICS INCIDENT RESPONSE PLAN

- Establish ICS-specific Incident Response Plan
- Practice the plan e.g., Tabletop Exercises

Thank you!

Questions?