DRAGOS

KNOW YOUR ADVERSARIES

A Fireside Chat on The European ICS/OT Threat Landscape

Magpie Graham, Principal Adversary Technical Director
Kyle O'Meara, Principal Adversary Hunter II
Faye Greenslade, Principal Adversary Hunter
Casey Brooks, Principal Adversary Hunter

AGENDA

1 Implications of RU-UA Conflict

2 Threat Group Activity

3 Ransomware Trends & Events

4 Industry Sector Threats

5 Takeaways & Recommendations

6 Questions

Implications of the RU-UA Conflict

Electric

Natural Gas

Telecoms

Threat Group Activity in Europe

KAMACITE

Ka

ELECTRUM

EL

PETROVITE

Pv

XENOTIME

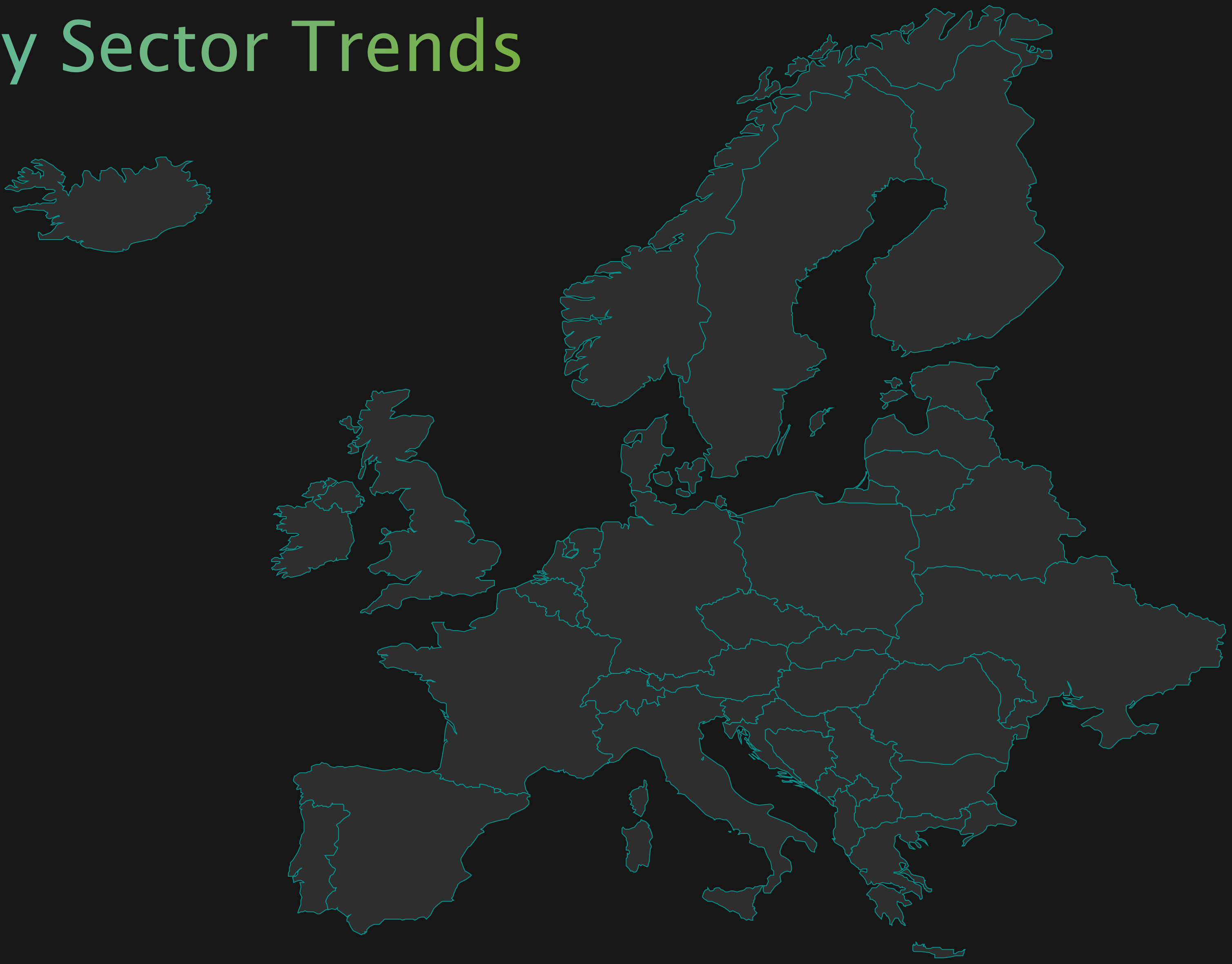
Xt

European Industry Sector Trends

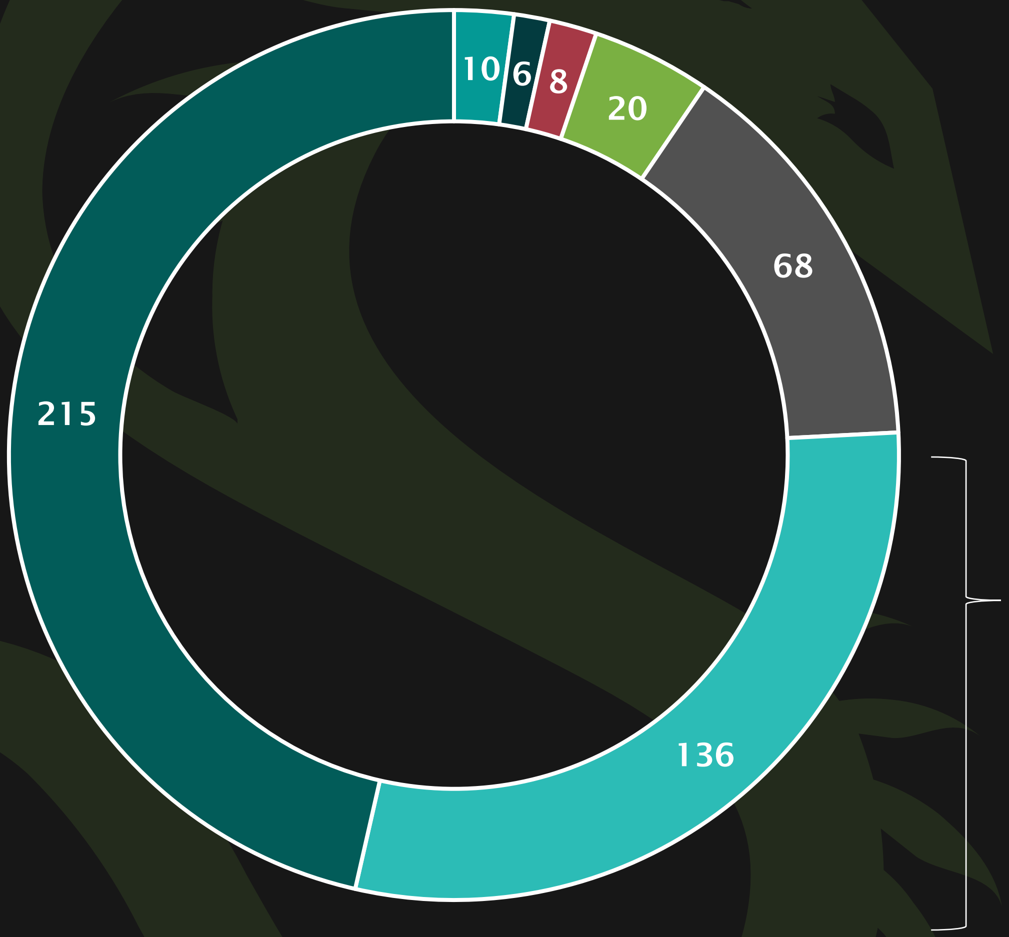
Oil & Gas

Electric

Renewable Energy



RANSOMWARE ATTACKS IN EUROPE



29% of ransomware attacks targeting industrial organizations in Q1/Q2 2023 occurred in Europe

Takeaways & Recommendations

The conflict between Russia & Ukraine has driven an increase in geopolitically motivated cyber activity in Ukraine, & across Europe.

OT Threat Groups continue to evolve their capabilities European energy sectors.

Ransomware & supply chain compromises present significant risks, especially for manufacturers.

FIVE CRITICAL CONTROLS

5 CRITICAL CONTROLS FOR EFFECTIVE OT CYBERSECURITY

01
ICS Incident Response Plan

02
Defensible Architecture

03
ICS Network Monitoring Visibility

04
Secure Remote Access

05
Risk-based Vulnerability Management

Q&A

QUESTIONS AND ANSWERS

Thank you!