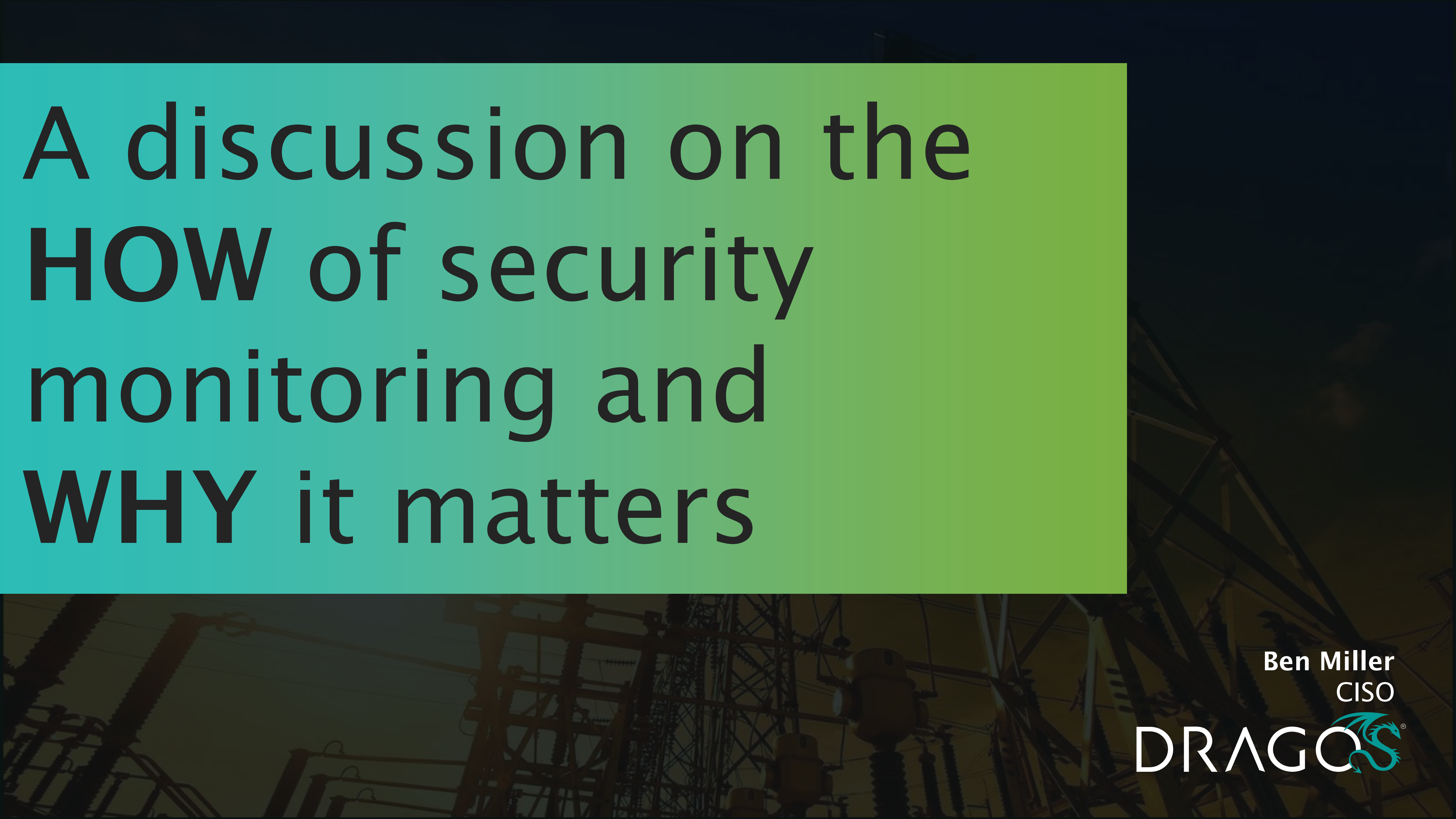
A discussion on the **HOW** of security monitoring and **WHY** it matters



Ben Miller
CISO
DRAGOS

2021

“incentives do not adequately exist to detect, log, or gain visibility needed”

2009

DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
FIDELITY
BRAVERY
INTEGRITY

2009

Downloader.generic.dx detected

DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
FIDELITY
BRAVERY
INTEGRITY

2009

Email with malicious attachment delivered

Downloader.generic.dx detected

DNS Lookup <maliciousdomain>

http request <maliciousdomain>

http connection / transfer <maliciousdomain>

SMB NetShareEnum / Query Info commands issued <domain controller>

FTP Connect <ipaddress>

FTP put

2010

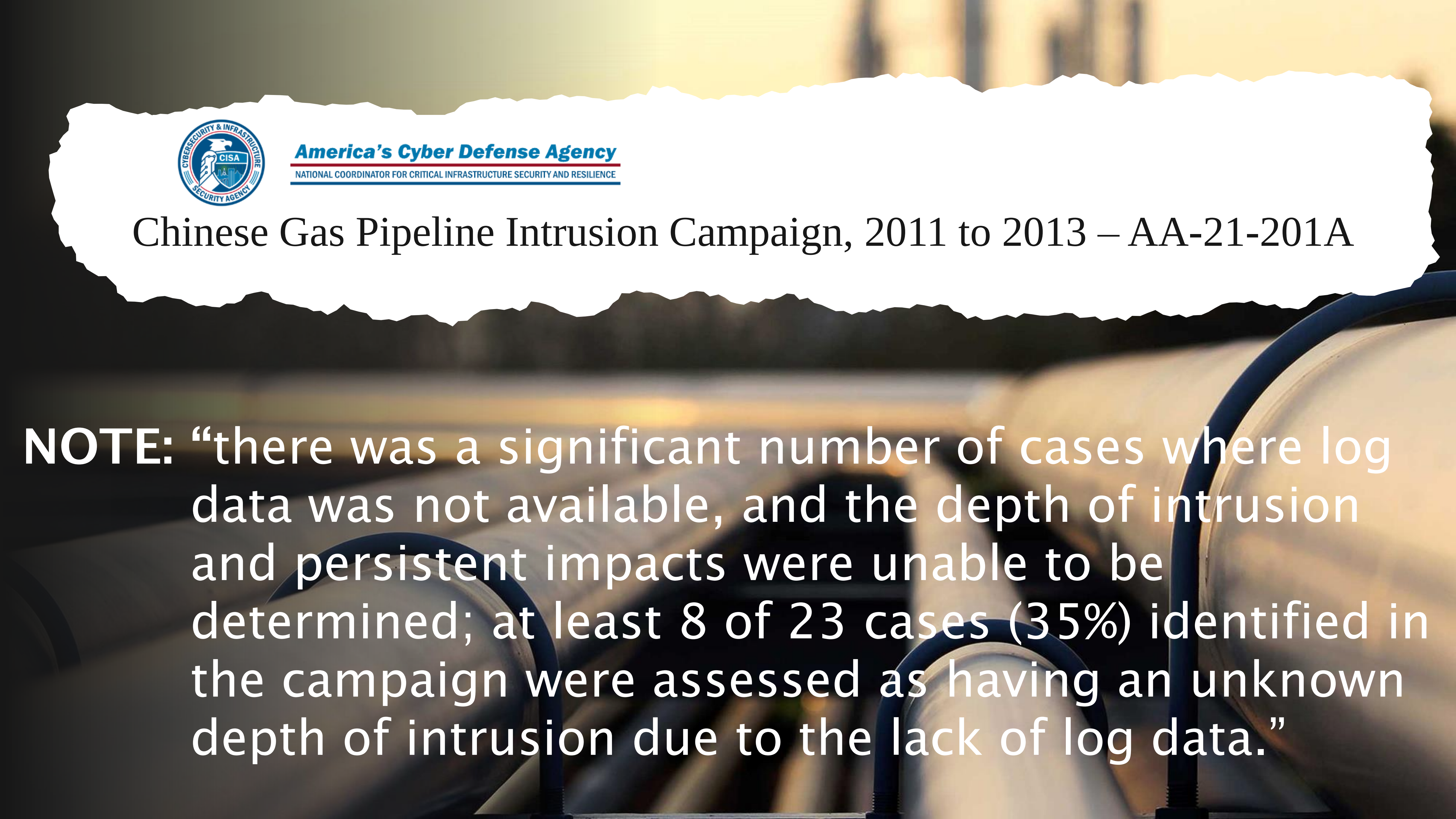
"SO CORPORATE IS MORE DEFENDED THAN OUR REGULATED ENVIRONMENT?"

2010

“WE NEED TO DEFER THAT DISCUSSION”

2011

NERC RULES OF PROCEDURE



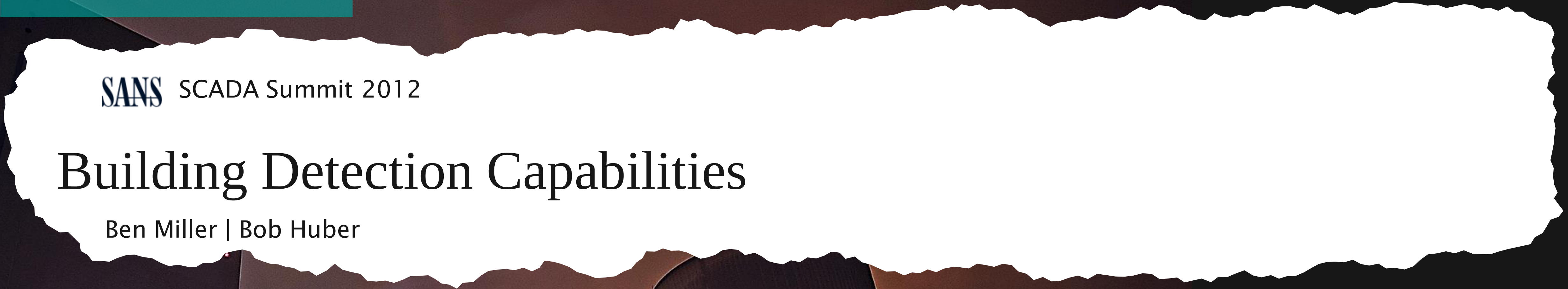
America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

Chinese Gas Pipeline Intrusion Campaign, 2011 to 2013 – AA-21-201A

NOTE: "there was a significant number of cases where log data was not available, and the depth of intrusion and persistent impacts were unable to be determined; at least 8 of 23 cases (35%) identified in the campaign were assessed as having an unknown depth of intrusion due to the lack of log data."

2012



SANS SCADA Summit 2012

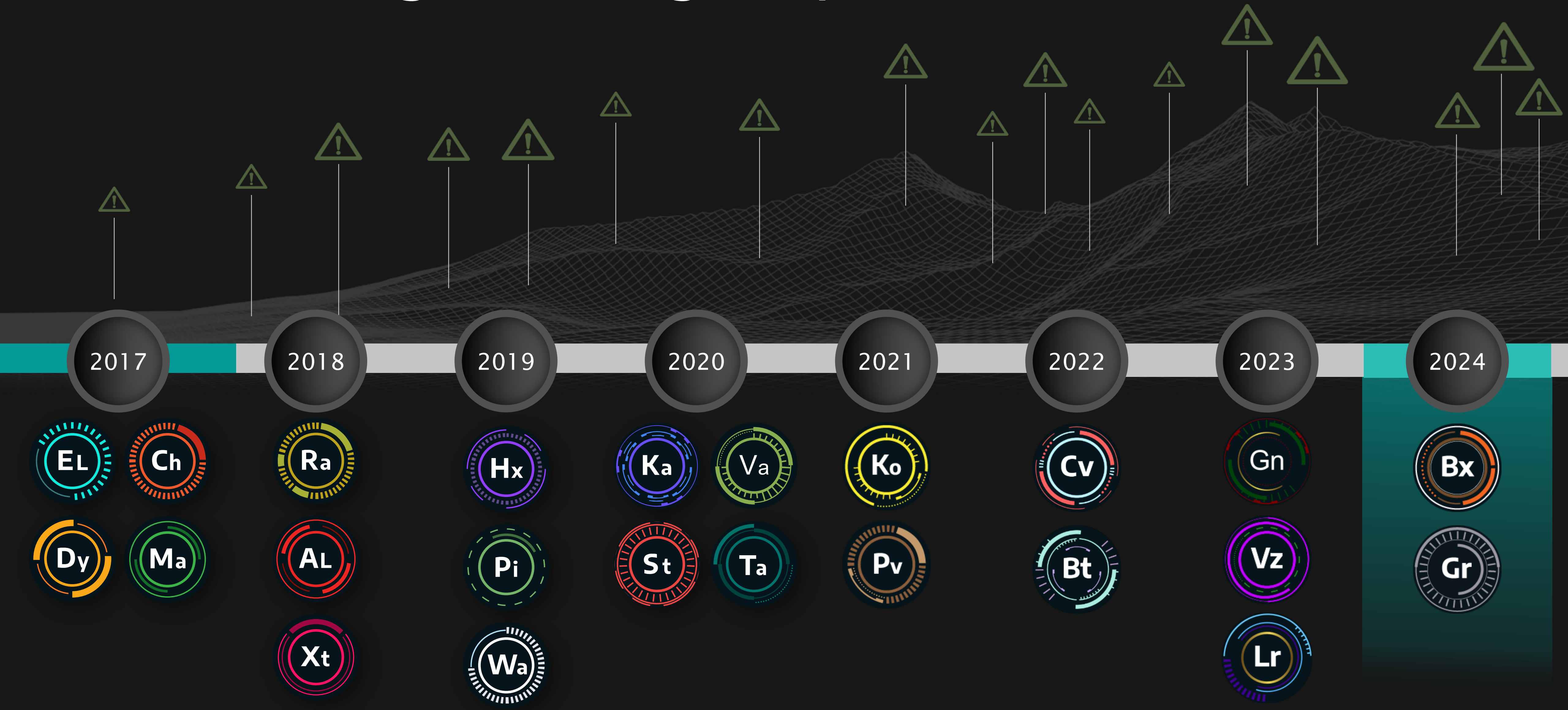
Building Detection Capabilities

Ben Miller | Bob Huber

“IS NERC SAYING WE NEED TO RETAIN LOGS FOR 1 YEAR?!@”

2024

Tracking threat groups



2017: EL, Ch, Dy, Ma

2018: Ra, AL, Xt

2019: Hx, Pi, Wa

2020: Ka, Va, St, Ta

2021: Ko, Pv

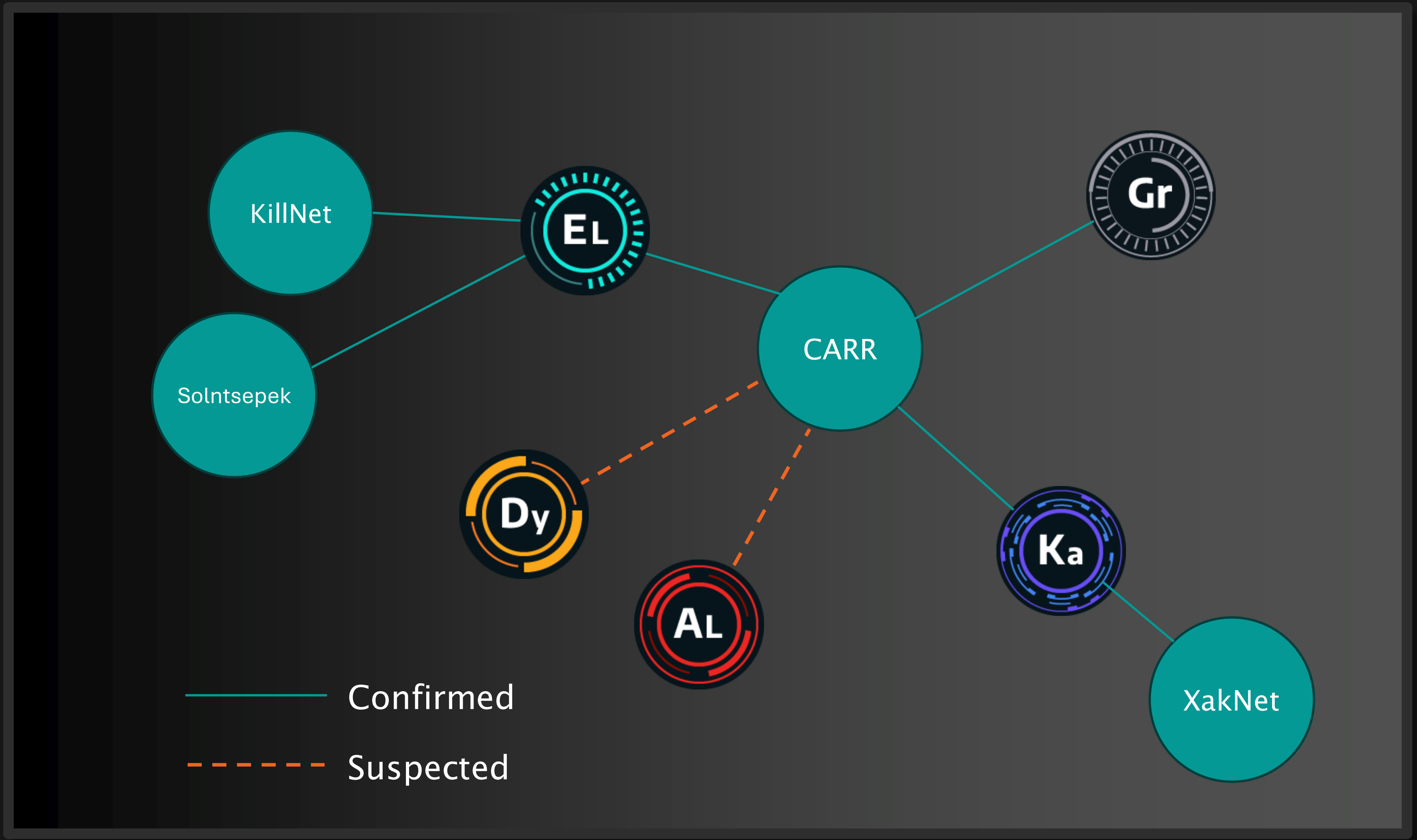
2022: Cv, Bt

2023: Gn, Vz, Lr

2024: Bx, Gr

2024

Convergence of hacktivism and state-sponsored threats



Shared Infrastructure

Intelligence Sharing

Victim Overlaps

2024

Threat group:

VOLTZITE

"Volt Typhoon has successfully gained access to numerous American companies in telecommunications, energy, water and other critical sectors, with 23 pipeline operators targeted…making it the defining threat of our generation"

- US FBI Director Christopher Wray

2024

Tactics, tools, and procedures

FUXNET

8th known ICS malware

Frosty Goop

9th known ICS malware

New ICS- & OT-specific malware

Internet-accessible OT devices

Remote access

Lateral spread after compromise

2024

Ransomware attacks increased by **87%** with **1693** total incidents

1171	Manufacturing
177	Industrial Control Systems
176	Transportation
44	Oil & Gas
41	Communications
30	Electric
20	Government
12	Water
11	Mining
7	Renewables
4	Data Centers

2021

“incentives do not adequately exist to detect, log, or gain visibility needed”

2021

“incentives do not adequately exist to detect, log, or gain visibility needed”

incentives != enforce

- Passive network monitoring
- Flexible, multi-sensor deployment
- Purpose-built for electric environments

***Monitor* … connections, devices, network, communications (R1.1)**

- Traffic modeling baselines
- Configuration baselines

***Detect* anomalous network activity (R1.2)**

- Detection panels
- Active IoC dashboards

***Evaluate* anomalous activity detected to determine action (R1.3)**

Pending CIP-015 Internal Network Security Monitoring

Threat Scenarios: VOLTZITE, ELECTRUM, PIPEDREAM, RANSOMWARE

TTP’s

- Remote Access Exploitation
- Living off the Land (LOTL) techniques
- Sector specific protocols: DNP3, 61850, GE SDI

Needs

- Compound behavioral detections to find threats not identifying as anomalies
- Threat hunting skills to identify advanced tools and adversaries
- Forensic data records with detail to streamline investigation & resolution

▼ ▼ Is this enough? ▼ ▼

- Passive network monitoring
- Flexible, multi-sensor deployment
- Purpose-built for electric environments

***Monitor* … connections, devices, network, communications (R1.1)**

- Traffic modeling baselines
- Configuration baselines

***Detect* anomalous network activity (R1.2)**

- Detection panels
- Active IoC dashboards

***Evaluate* anomalous activity detected to determine action (R1.3)**

Pending CIP-015 Internal Network Security Monitoring

Foundation

Assume you are already compromised

Foundation

Assume the adversary is evading you

Goal

Measurable framework that can allow for creativity and flexibility

Thank you

Ben Miller
CISO

DRAGOS