New Approaches to Detecting Threats in OT Environments

CSX

2024

CSX OPERATIONS

CSX Network Reaches Nearly Two-thirds of the U.S. Population

- Approximately **20,000 route miles** across 26 states, including the District of Columbia
- **Most advanced** intermodal terminals in North America
- **Connection to 240+** short line partners and **70+** port terminals
- **Reliable service with transparency** through Trip Plans
- Compliant, resilient and secure **Data Center Colocation Management** services

# OF EMPLOYEES	CARLOADS	CAPITAL INVESTMENT
23,000	3.4M	~$2.3B

Figures from December 2023

CHALLENGES IN SECURING TRAIN CONTROL SYSTEMS

Gaining Cyber Visibility is Difficult

- Comms networks are large and complex
- 3500+ mobile assets
- Operating over a large geographic area
- High cost of monitoring technologies
- False positive rate can be high
- Requires lots of expertise to operate
- Difficult to scale
- Complex threat landscape

NETWORK DETECTION AND RESPONSE

Threat Detection

- Continuous monitoring of networks
- Detects threats as they happen
- Advanced analytics and machine learning used to identify unusual patterns in network traffic

Automated Response

- Works with SIEM/SOAR to enable a faster response to threat actors in the network
- Reduces time to respond to threats
- Reduces risk
- Minimizes potential damage caused by attacks

Visibility

- Comprehensive view of network activities
- Helps CSX to understand and monitor all network traffic
- Can inspect encrypted traffic depending on configuration

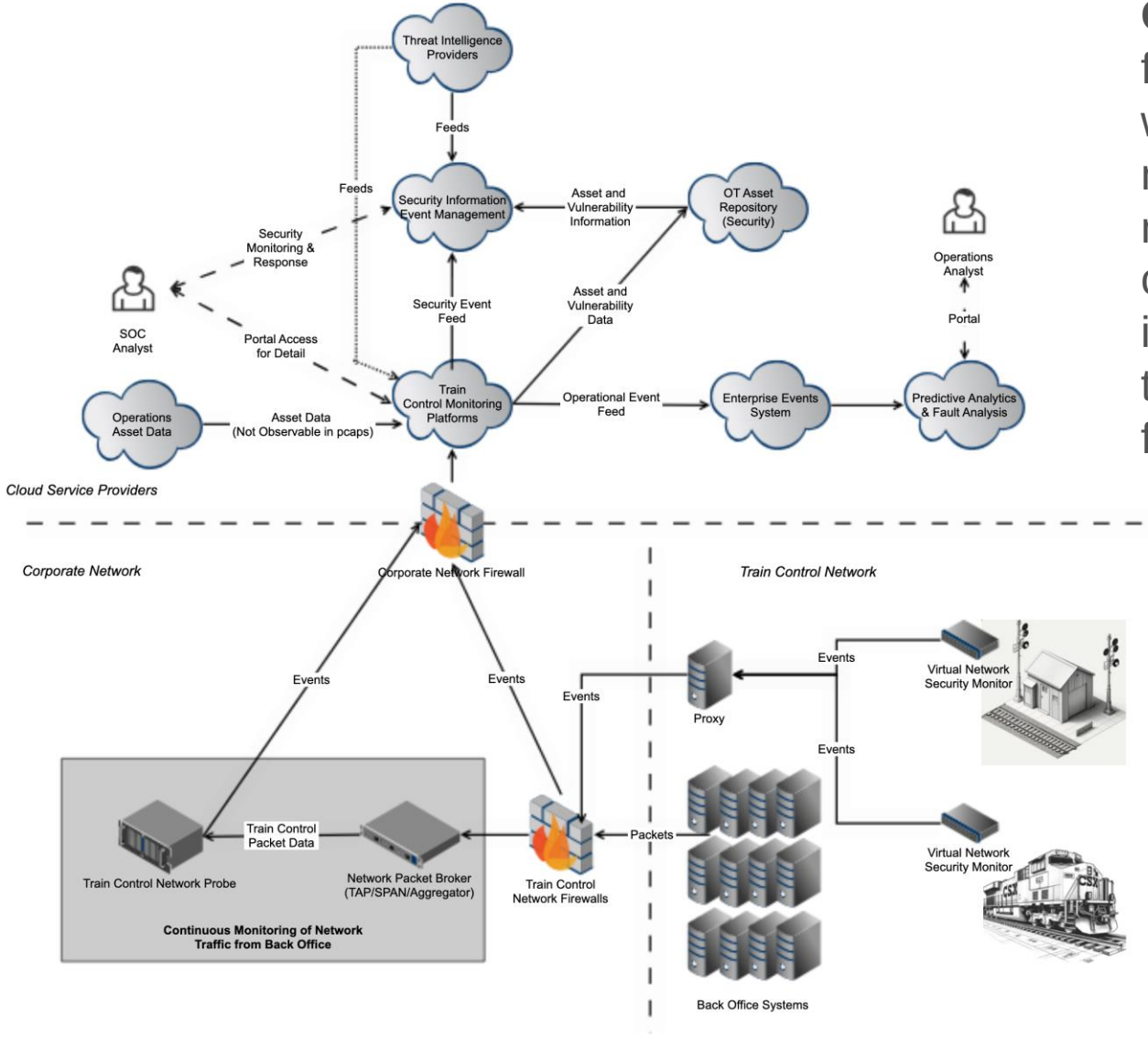
Improved Threat Intelligence

- Incorporates threat feeds allowing CSX to benefit from the latest information on emerging threats
- Reduces dwell time by aiding in early ID of attackers

TRAIN CONTROL NETWORK MONITORING CONCEPT AT CSX

SOC Analyst has access to high quality events in SIEM enriched by threat intelligence feeds, asset information, and vulnerability data. Portal can be used to gain added detail and context if needed.

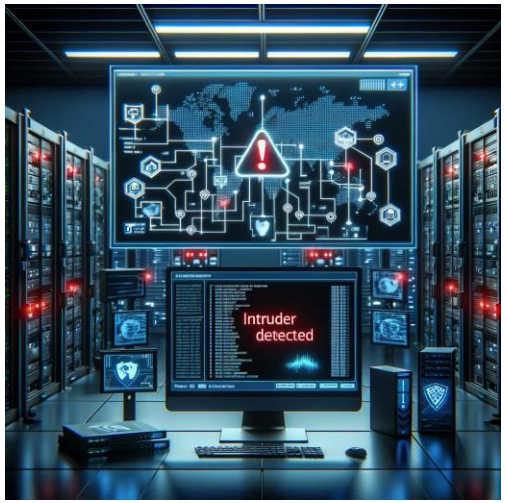
Packet data and other network-based events are aggregated in network probes, packet aggregators, and other collection points prior to transmission to Train Control Monitoring Platforms.



Operations Analyst benefits from same network analysis with real-time indications of miscommunicating, misconfigured, and network congestion telemetry. Data is presented to this user in the systems already in use for predictive analytics.

Capture architecture leverages edge processing to maximal effect to reduce potential congestion introduced by monitoring processes. Monitoring processes are virtualized to minimize footprint on field assets.

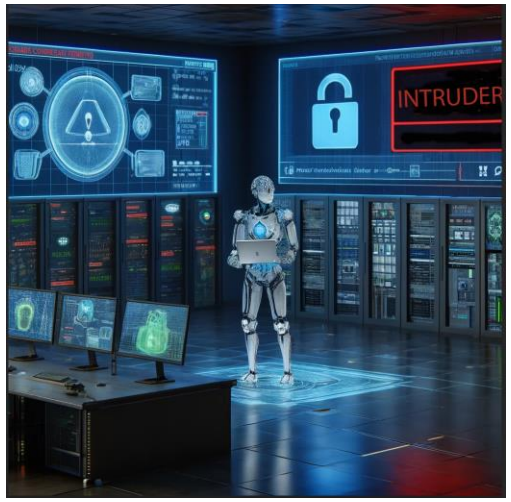
USE CASES FOR NETWORK DETECTION AND RESPONSE AT CSX TO DETECT



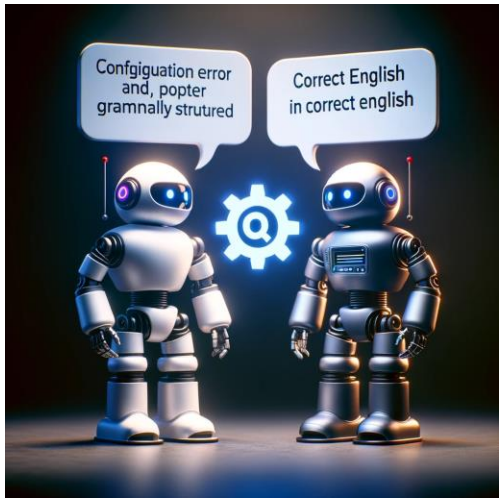
Network intrusion OR…

Message tampering OR…

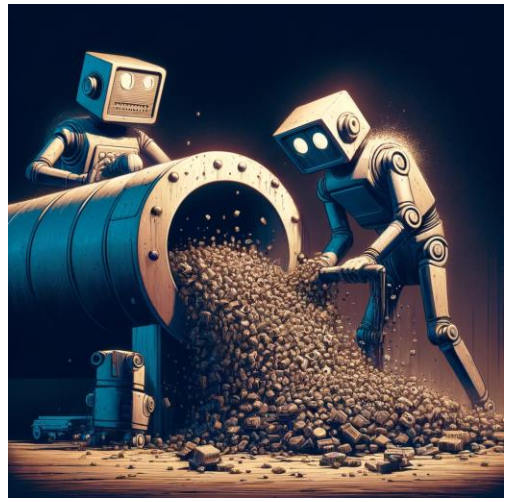
Denial of service OR…



Inadvertent enforcement on authorized actor



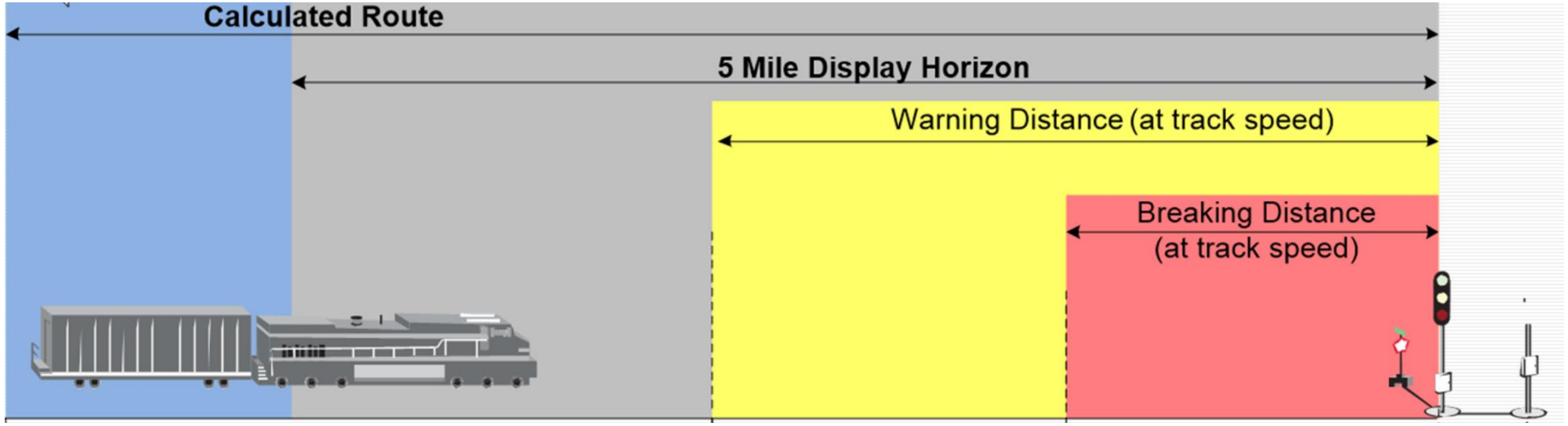
Inadvertently mangled messaging



Self-inflicted resource exhaustion

PTC ENFORCEMENT RESEARCH

Goal: Automate data collection and event synthesis from network packet captures from locomotives involved in a false enforcement. This approach benefits from the fact that information passed “over the wire” is the ground truth regarding what transpired from the perspective of communications and messaging. Packet captures are often a pulled in the partially manual process. Our aim is to automate as much of the evidence collection and analysis as possible given constraints in the coverage we have with our sensors today.



Current Lines of Effort for I-ETMS equipped locomotives:

- ELM Connectivity Not Sufficient (< 2 connections OR < 2 data centers for each WIU)
- TMC 5201 Message Flood
- Wayside Status Message Gaps


CSX