Rail Cyber Security Mitigation Actions and Testing

DARKTRACE

OVERVIEW

For economic and national security in the United States, the Transportation Security Agency (TSA) has issued a security directive for the nation's railroads. The directive is intended to prevent transportation disruption. Particularly, the directive seeks to implement security in layers to institute a more bountiful protection of systems due to recent intelligence on and growing sophistication of cyber threats.

GOALS:

1. Implement network segmentation policies and controls to ensure that the OT system can continue to safely operate in the event of an IT compromise (Colonial Pipeline).
2. Implement Access Control measures to secure and prevent unauthorized access to Critical Cyber systems (Quasi DT).
3. Implement continuous monitoring and detection procedures to detect cyber threats and correct anomalies that affect cyber critical systems.
4. Reduce risk of exploitation of unpatched systems through the application of security patches and updates to systems using a risk-based methodology (DT OT CVE critical tag).
5. Establish a cyber security program and submit it to TSA annually, specifically launch it 120 days after October 23, 2022.

Who is affected by this?

The affected industry is Freight Railroad Owners and operators. Specifically, each freight railroad carrier that operates rolling equipment on track that is part of the general railroad system of transportation. This includes:

- Each passenger railroad carrier.
- Each public transportation agency.
- Each operator of a rail transit system that is not operating on track that is part of the general railroad system of transportation, including heavy rail transit, light rail transit, automated guideway, cable car, inclined plane, funicular, and monorail systems.
- Each tourist, scenic, historic, and excursion rail owner/operator, whether operating on or off the general railroad system of transportation.

Owner/Operator Requirements

Provide information on segmentation: This includes how operators plan to create zone boundaries. This will have multiple logical zones including critical, consequential, and operational necessity zones.

Implement network segmentation policies

Prevent unauthorized communication between zones and prohibit OT systems from traversing to IT systems and vice versa, unless encrypted content, or its not feasible, otherwise the operator must ensure integrity and prevent corruption or compromise during transit.

Implement access control measures to prevent unauthorized use

For example, identification and authentication policies and procedures. MFA, we cannot do this. Policies and procedures to manage access rights based on principals of least privilege and separation of duty. IE Enterprise immune system.

Implement continuous monitoring and detection policies and procedures

Defend against emails, block ingress and egress communications with known or suspected malicious IP address', control impact of known or suspected malicious web domains or applications. Block and prevent unauthorized code including macro scripts from executing and monitor or block connections from known or suspected malicious command and control servers. Logging requirements for continuous collection of data to analyze intrusions and anomalous activity. Mitigation measures to manage It from spreading to OT.

Patch management strategy

Ensuring that all critical security patches and updates are current. The strategy must include the risk methodology for categorizing and determining criticality of patches and updates and implementation timeline based on criticality and category of assets.

How Can Darktrace Support Railways as a Critical Infrastructure

Darktrace helps clients across the globe comply with their nations cyber-security guidelines. Darktrace delivers AI-powered threat prevention, detection, investigation, and response that can support organizations in their journey towards cyber maturity as defined by the US Security Directive for Railways Cyber Security Mitigation. Through a unified platform approach, Darktrace provides autonomous cyber defense across the entire enterprise, including cloud and SaaS, email environments, corporate networks, remote endpoints, and IT and OT environments.

With Self-Learning AI, Darktrace learns what normal behavior looks like across the business in order to spot the subtle deviations that signal an attack, from novel ransomware to stealthy insiders.

The technology spots emerging threats in real time with Darktrace DETECT, autonomously contains them with Darktrace RESPOND, and takes preemptive action to find vulnerabilities and harden defenses with Darktrace PREVENT – all without relying on any rules, signatures, or prior assumptions. All of these technologies are further supported by the Cyber AI Analyst, which autonomously investigates and triages every potential threat, bringing subtle attacks to light.

To learn more about our products please use the following links:

Darktrace PREVENT >
Darktrace DETECT >
Darktrace RESPOND >
Darktrace/OT >
Darktrace/Network >

Below is a list of railway compliance ordinances directly linked to the Darktrace products that would help railway operators meet these guidelines.

Domain	Number	Description	Darktrace Products
Cyber security implementation plan	2B	No later than 120 days after effective date operators must submit a cyber security plan describing the defense plan including logical and physical security controls.	All Darktrace Products
Identify critical cyber systems	3A	Identify what systems owned by the operator could result in operational disruption.	Darktrace PREVENT, Darktrace DETECT + RESPOND, Darktrace/OT
Implement network segmentation policies	3B	Implement network segmentation policies and controls designed to prevent operational disruption. Provide lists and descriptions of IT and OT system interdependencies, external connections to IT and OT systems, zone boundaries, and more.	Darktrace DETECT + RESPOND, Darktrace/OT
Implement Access Control measures	3C	Implement access control measures, including those for local and remote access, to secure and prevent unauthorized access to critical cyber systems.	Darktrace DETECT + RESPOND/ Network, Darktrace/OT
Implement continuous monitoring and detection policies	3D	Implement monitoring and detection policies and procedures that are designed to prevent, detect, and respond to cyber security threats and correct anomalies affecting critical cyber systems.	Darktrace DETECT + RESPOND, Darktrace/OT, Cyber AI Analyst
Reduce risk of exploitation and unpatched systems	3E	Reduce risk of exploitation of unpatched systems through the application of security patches and updates for operating systems, applications, drivers, and firmware on Critical Cyber Systems.	Darktrace PREVENT, Darktrace DETECT + RESPOND, Darktrace/OT
Develop cyber security assessment program	3F	Develop a cyber security program for proactively assessing and auditing cyber security measures.	Darktrace PREVENT, Darktrace DETECT + RESPOND, Darktrace/OT, AI Analyst

About Darktrace

Darktrace (DARK.L), a global leader in cyber security artificial intelligence, delivers complete AI-powered solutions in its mission to free the world of cyber disruption. Its technology continuously learns and updates its knowledge of 'you' for an organization and applies that understanding to achieve an optimal state of cyber security. It is delivering the first ever Cyber AI Loop, fueling a continuous end-to-end security capability that can autonomously prevent, detect, and respond to novel, in-progress threats in real time. Darktrace employs over 2,200 people around the world and protects over 8,100 organizations globally from advanced cyber-threats.

Scan to LEARN MORE