DARKTRACE
Evolving threats call for evolved thinking™

White Paper

TSA Cyber Security Compliance for Aviation

DARKTRACE

Contents

Introduction

The aviation cyber security policy initiated by the Department of Homeland Security contains vital processes aviation companies must take to secure their digital ecosystems. Among the various policies are vital concepts like managing risk, assets, and detect-ing, responding, and reporting cyber-attacks.

The following sections provides insight on how Darktrace's AI technology can support aviation companies that need to comply to the requirements listed in the Cyber Security Self-Assessment document distributed by the Transportation Security Administration.

Aviation Cyber Security Measures

/ Do your cybersecurity plans incorporate any of the following approaches?

National Institute of Standards and Technology (NIST), Framework for Improving Critical Infrastructure Cybersecurity.

Yes, Darktrace assists with meeting and enforcing NIST requirements across several domains including: Asset Management, BC&DR, Configuration Management, Continuous Monitoring, Data Classification & Handling, Endpoint Security, Identification & Authentication, Incident Response, Network Security, Physical Security, Risk Management, Threat Management and Vulnerability & Patch management.

Asset Management

/ Has your company established and documented policies and procedures for the following?

Assessing and maintaining configuration information.	Darktrace PREVENT can identify vulnerable and misconfigured infrastructure associated with the target company. This can support the effective management of assets and minimize the likelihood of misconfigured, exploitable infrastructure.
	Darktrace can be leveraged to provide a backstop for misconfigurations and take action to disrupt communications traffic on prohibited ports, protocols, or services.
Tracking changes made to cyber assets.	N/A - Darktrace can support an asset management program by dynamically learning about devices in an organization. This information can be queried in the Darktrace UI or can be connected to the system of record via API. Darktrace can support a documentation program through tagging devices and visualizing data flows from those devices.
Ensuring that the changes do not adversely impact existing cybersecurity controls.	N/A - Darktrace detects and responds accordingly to anomalous change activity associated with cyber assets.

/ Has your company evaluated and classified cyber assets using the following criteria?

Critical cyber assets, which are operational technologies (such as ICS or SCADA) systems that can control operations.	N/A - The visibility of Darktrace's Cyber AI platform supports identification of critical functions. Darktrace can help organizations understand data flows between devices and entities on the network (including OT).
Non-critical cyber assets, which are OT systems that monitor operations.	N/A - Darktrace can help organizations understand data flows between devices and entities on the network (including OT).

DARKTRACE

/ Has your company developed and maintained a comprehensive set of:

Network/system architecture diagrams or other documentation, including nodes, interfaces, remote and third-party connections, and information flows.

N/A - Darktrace can be used to detect new assets added to the network, including rogue wireless devices. All WAPs are seen and monitored. Anomalous behavior from the WAP or devices connecting to WAP are investigated and alerted.

Darktrace PREVENT provides an overview of systems associated with the company.

/ For critical cyber assets, does the OT environment have a detailed software and hardware inventory of cyber asset endpoints?

Yes, for operating system and firmware.

Darktrace can support an asset management program by dynamically learning about devices in an organization. This information can be queried in the Darktrace UI or can be connected to the system of record via API. Darktrace can support a documentation program through tagging devices and visualizing data flows from those devices.

Darktrace can be used to detect new assets added to the network.

/ For critical cyber assets, has an inventory of the components of the operating system been developed, documented, and maintained that accurately reflects the current OT (such as ICS or SCADA)

Yes, for operating system and firmware.

Darktrace can support an asset management program by dynamically learning about devices in an organization. This information can be queried in the Darktrace UI or can be connected to the system of record via API. Darktrace can support a documentation program through tagging devices and visualizing data flows from those devices.

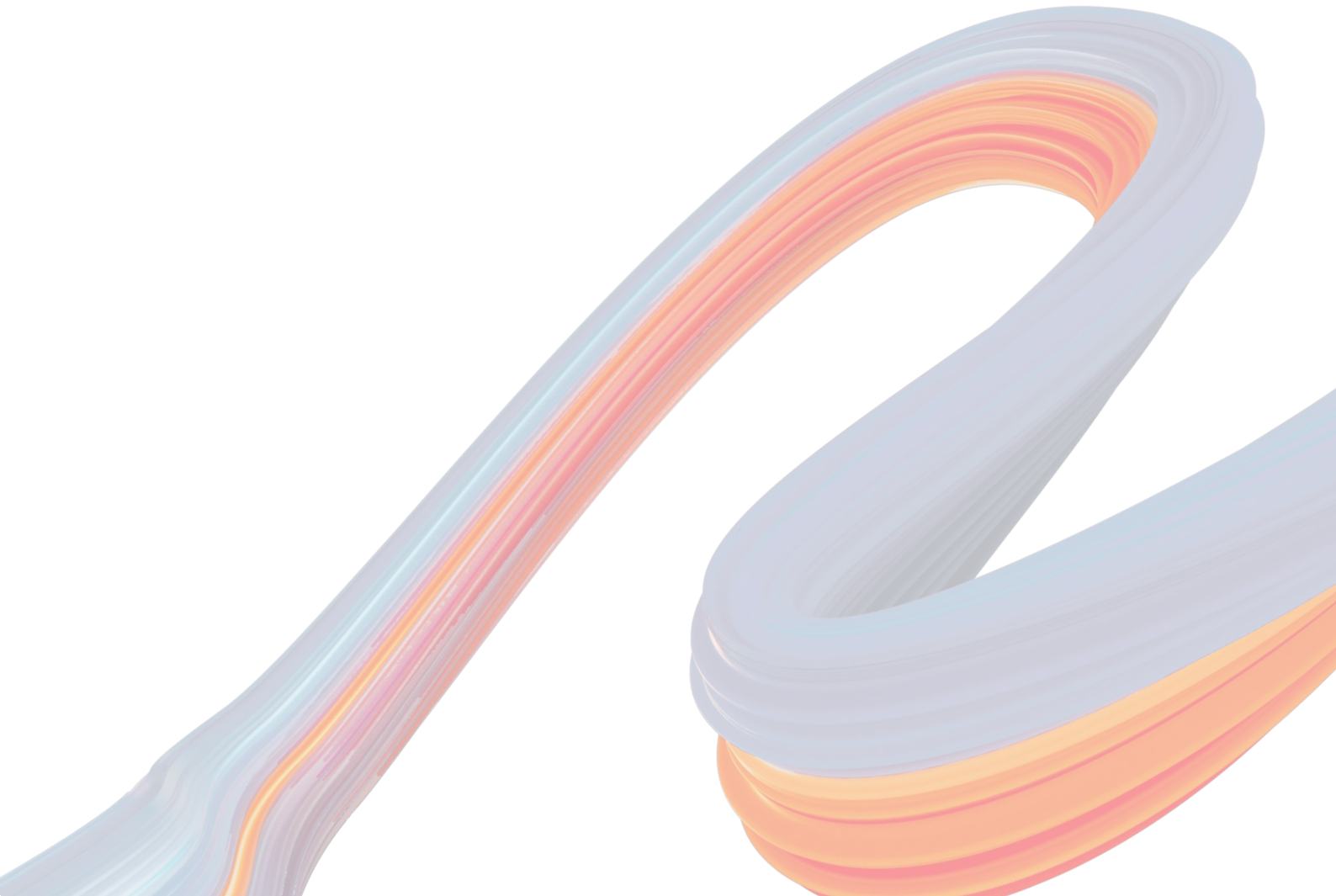
For networked systems, this can be set up as part of Darktrace's wider visibility of the network. Tags can be used to mark storage and processing devices, while the platform will automatically monitor transmissions relating to them. Models can abe created for any special requirements around the sensitive data systems.

/ For critical cyber assets, does your company:

Review network connections periodically, including remote access and third-party connections.	N/A - Darktrace monitors all network connections for all assets.

/ For critical cyber assets, has your company implemented the following measures?

Employ more stringent identity and access management practices (e.g., authenticators, password-construct, access control).	Darktrace integrates with third part zero-trust and monitors user behavior. Darktrace works closely with identity providers to action risky sign-ins and malicious attempts to access internal systems.



DARKTRACE

Business Environment

/ Does your company have:

A designated individual solely responsible for cyber of IT and OT systems.	N/A - Darktrace covers IT and OT security under one UI that your security professional can use to monitor IT and OT systems.

/ Does your company:

Ensure that any change that add control operations to a non-critical cyber asset result in the system being recognized as a critical cyber asset and enhanced security measures being applied?	Within the Darktrace tool it is possible to add high risk tag or other pertinent tag to devices.

Governance

/ Has your company established and distributed:

Cybersecurity policies, plans, processes, and supporting procedures commensurate with the current regulatory, risk, legal, and operational environment?	N/A – Darktrace RESPOND can be factored into incident response plans.

Risk Management Strategy

/ Has your company developed:

An operational framework to ensure coordination, communication, and accountability for information security on and between the control systems and enterprise networks?	N/A - The Darktrace platform allows for communication across the user interface for all those accessing and utilizing the tool promoting synergy within the organization when dealing with IT and OT security.

Risk Assessment

/ Has your company developed:

Independent assessors to conduct cybersecurity assessments?	N/A – Darktrace PREVENT can identify and assess cybersecurity risk in line with industry best practice and provide recommendations.
	Darktrace can be used to support the security function on developing new or existing risk mitigation plans, by showing patterns of traffic that might be indicative of a poorly performing control.

/ Has your company established:

A process to identity and evaluate vulnerabilities and compensating security controls.	N/A - Darktrace can help spot misconfigurations or gaps in existing security stacks. It can be used to prohibit vulnerability scanning activities, while permitting authorized users to do so.
	Darktrace can be used to detect and prevent anomalous activity to a device, buying time for a vulnerability to be remediated, even if the vulnerability is not yet known.

Access Control

/ Has your company implemented the following measures?

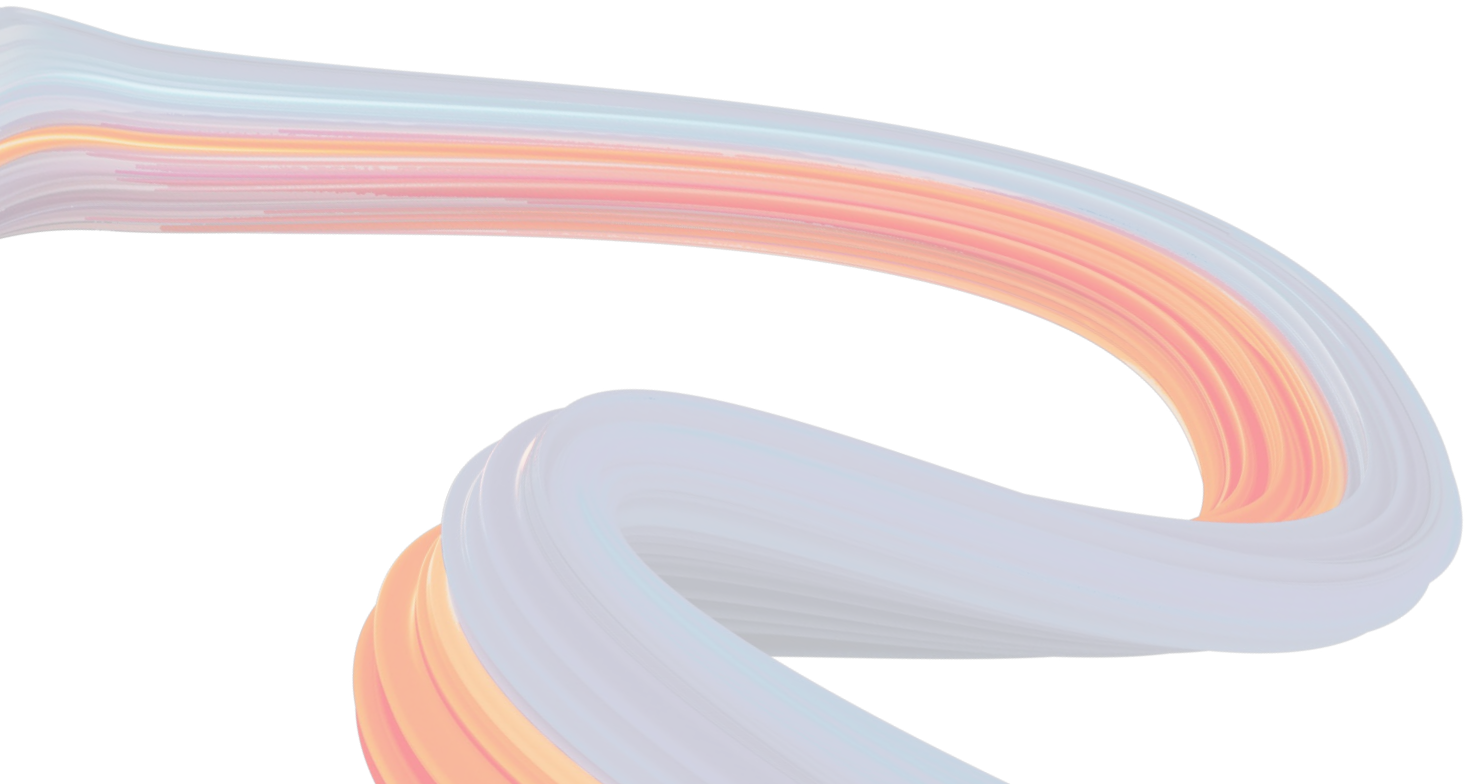
Establish and enforce unique accounts for each individual user and ensure each administrator has an individual account and an administrator account.	N/A - Darktrace can tag and track specifically admin accounts and admin behavior across the network
Establish security requirements for certain types of privileged accounts.	N/A - Darktrace can enforce access restrictions to tagged systems. This would provide a backstop for access controls that are not performing.

/ Are authentication methods and specific standards, such as:

Strong credential management or active directory monitoring, employed throughout your company's cyber access control environment and documented in overarching corporate IT/OT security plans?	N/A - Darktrace can be used to detect and interrupt anomalous and unauthorized use.

/ 7.04 - Has your company implemented the following measures?

Establish and enforce access control policies for local and remote users.	No. However, Darktrace can enforce patterns of life or take respond actions on accounts that are being deactivated.
	Darktrace can enforce access restrictions to tagged systems. This would provide a backstop for access controls that are not performing.
Have procedures and controls in place for approving and enforcing remote and third-party connections.	Yes, Darktrace can enforce access restrictions to tagged systems. This would provide a backstop for access controls that are not performing.



Awareness & Training

/ Is there a cyber-threat awareness program for employees that includes:

Practical exercises/testing?	No. However, Darktrace PREVENT can support security teams identify vulnerable assets and accounts and model attack paths to identify which training programs would be essential to implement at their organization.

Protective Technology

/ Do IT/OT systems monitor and manage communications at appropriate IT/OT network boundaries?

	Yes.

Anomalies & Events

/ Has your company implemented processes to respond to anomalous activity through the following?

Generating alerts and responding to them in a timely manner.	Yes. Darktrace provides a centralized, automated method to collect and analyze security-related events in real time.
Logging cybersecurity events and reviewing these logs.	Yes. Darktrace provides a centralized, automated method to collect and analyze security-related events in real time.
	Darktrace provides AI-driven investigation of anomalous events occurring within the organization.

DARKTRACE

Security Continuous Monitoring

/ Does your company monitor for authorized access or the introduction of malicious code or communications?

Yes.

/ Does your company monitor physical and remote user access to critical cyber assets?

Yes.

/ For critical cyber assets, does your company employ mechanisms to detect components that should not be on the network?

Yes.

/ Does your company conduct cyber vulnerability assessments as described in your risk assessment process?

Yes.

Detection Processes

/ Has your company established:

Technical or procedural controls for cyber intrusion monitoring and detection?	Yes.

Response Planning

/ Has your company established:

Policies and procedures for cybersecurity incident handling, analysis, and reporting, including assignments of specific roles/tasks to individuals and teams?	Yes.

/ For critical cyber assets, are cybersecurity incident response exercises conducted periodically?

Yes, Darktrace can be utilized in incident response exercises.

/ For critical cyber assets has your company established and maintained:

A process that supports 24/7 cyber-incident response?	N/A - Darktrace provides real-time, AI-driven investigation of anomalous events occurring within the organization.

/ Has your company established and maintained: a cyber-incident response capability?

A cyber-incident response capability?	Yes, respond can be factored into incident response plan.
	Darktrace conducts an AI-based investigation and triage of all alerts in the platform. This information is set to a timeline and summarized for human consumption.

Mitigation

/ Do your company's response plans and procedures include mitigation measures to help prevent further impacts?

Yes, Darktrace enables us to autonomously detect any sort of "anomaly" within both IT and OT environments. Any malicious threat, misconfiguration, etc., will be detected and investigated (evaluated) by Darktrace.

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

DARKTRACE
Evolving threats call for evolved thinking™

North America: +1 (415) 229 9100
Europe: +44 (0) 1223 394 100
Asia-Pacific: +65 6804 5010
Latin America: +55 11 97242 2011
info@darktrace.com
darktrace.com