Compliance: Security Directive Pipeline-2021-02c SDO2C

DARKTRACE

For economic and national security, the Transportation Security Agency (TSA) has issued a security directive for the nation's pipelines. The directive applies to Owners/Operators of hazardous liquid and natural gas pipelines or liquified natural gas facilities that are deemed critical.

GOALS

- Implement network segmentation policies and controls to ensure that the OT system can continue to safely operate in the event of an IT compromise.
- Implement Access Control measures to secure and prevent unauthorized access to Critical Infrastructure.

/ Darktrace products meeting the standards:

On page 1 you will find descriptions of Darktrace products, including their potential added value to your team and security systems.
On page 2 you will find the Darktrace product name that covers the according regulatory requirement.

/ Darktrace DETECT:

DETECT learns what makes an organization unique, from the ground up. Powered by Darktrace Self-Learning AI, DETECT continuously learns about your organization's digital activity. It can detect known and unknown threats by identifying subtle deviations from normal cyber activity, making it possible for the security team to identify attacks in real time, not after the damage has been done. Additionally, this understanding is continuous, meaning, that it does not take a static baseline over a single period in time. Instead, it constantly updates its understanding of normal as the organization changes.

DETECT analyzes millions of data points for every digital asset to ask: Is this device behaving normally? It then generates simple outputs that human security teams can quickly and easily understand to get to the bottom of an incident. Typically, a physical appliance will sit off the core switch, running a port mirroring session. However, Darktrace provides complete coverage across OT, cloud, SaaS, email, and endpoints environments with lightweight agents.

/ Darktrace RESPOND:

Darktrace RESPOND delivers autonomous, always-on action to contain and disarm attacks within seconds. When a threat is detected, RESPOND leverages Darktrace's understanding of your organization to pinpoint signs of an emerging attack, interrupting malicious or dangerous activity while allowing normal business to continue. Darktrace has manual and autonomous capabilities that allow it to be set to human confirmation mode, requiring the security team to confirm its response before any action is taken. When set to fully autonomous, RESPOND will take action anytime, day or night, providing value for smaller teams that do not have around the clock monitoring.

Because Darktrace RESPOND doesn't rely on pre-programming, threat characteristics are not defined in advance. This enables it to neutralize unknown and unpredictable cyber-attacks that have never been seen before on the first encounter, before damage spreads. The AI technology runs autonomously, at all times, elevating humans from making micro-decisions about individual. RESPOND acts within guidelines and boundaries set by the security team.

/ Cyber AI Analyst:

AI Analyst is included in both the DETECT and RESPOND functionalities. It will create readable, executive-level reports for each incident that will state what happened, how Darktrace detected the anomalous activity, the response Darktrace took or would suggest taking, and recommendations moving forward, keeping the human in the loop. AI Analyst is designed to save time as they can triage multiple incidents into one easy to read report. The result is that time-to-meaning and time-to-response are dramatically reduced – allowing security team members time to use their expertise where it really matters.

Further, the AI Analyst reports can give as much granular information as needed. This can range from IP strings, ports or files accessed, time of the anomalous activity, and how rare accessing the information is for the individual user. Additionally, Darktrace can store event logs for up to a year for each device, and AI Analyst reports can get as granular as packet capture data.

/ Cyber AI Loop

Darktrace DETECT and RESPOND form part of Darktrace's technology vision of a Cyber AI Loop, which empowers defenders to reduce cyber risk and disruption at every stage of the attack life cycle – from proactive measures taken to harden security before an attack gets in, to detecting and responding to an attack. The Cyber AI Loop makes it possible for business to prevent, detect, respond, and heal, from a cyber-attack all at once.

Streamlining detection and response systems, Darktrace is specifically designed to cut across multiple facets of your organization and enable unified detection and response, spanning across email, cloud, SaaS applications, industrial systems, endpoints, and the corporate network. Darktrace DETECT and RESPOND is available across all of these coverage areas.

SECURITY DIRECTIVE PIPELINE-2021-02C SDO2C

/ Regulations for cyber systems:

- Implement continuous monitoring and detection and procedures to detect cyber threats and correct anomalies that affect cyber critical systems
- Reduce risk of exploitation of unpatched systems through the application of security patches and updates to systems using a risk-based methodology
- Establish a cyber security program and submit it to TSA annually, specifically launch it 90 days after July 21, 2022

/ Owner/operator requirements:

Provide information on segmentation and how they will create zone boundaries. This will have multiple logical zones including critical, consequential, and operational necessity zones.

- Prevent unauthorized communication between zones, prohibit OT systems from traversing the IT system and vice versa unless encrypted content or its not feasible
  - Darktrace DETECT and Darktrace RESPOND
- Implement access control measures to prevent unauthorized use, ie identification and authentication policies and procedures
  - Darktrace DETECT and Darktrace RESPOND
- List and description of IT/OT system interdependencies all external connections to operational technology systems zone boundaries including descriptions of logical zones based on critical consequence and operational necessity
  - Darktrace DETECT
- Multi-Factored Authentication
  - Not part of Darktrace's capabilities
- Policies and procedures to manage access rights based on principals of least privilege and separation of duty
  - Darktrace DETECT, Darktrace/OT, Darktrace/Apps, Darktrace/Email
- Limit use of shared accounts to those that are critical for operations
  - (Darktrace DETECT, Darktrace/OT, Darktrace/Apps, Darktrace/Email)
- Implement continuous monitoring and detection policies and procedures designed to prevent, detect, and respond to cyber security threats and correct anomalies affecting critical cyber systems. 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
  - Darktrace DETECT, Darktrace RESPOND, Darktrace/OT, Darktrace/Apps, Darktrace/Email
- Logging requirements for continuous collection of data to analyze intrusions and anomalous activity
  - Darktrace DETECT, Darktrace RESPOND

/ Mitigation measures to manage IT from spreading to OT:

Patch management strategy: patch management ensures all critical security patches, updates, and critical cyber systems are current.

- Must determine criticality of patches and updates current implementations timeline
  - Darktrace DETECT, Darktrace/OT
- Prioritize security patches and updates of cissus known exploited vulnerabilities catalog
  - Darktrace DETECT, Darktrace/OT

Darktrace's NIST Integration satisfies this requirement and will give all this information outside of patching the vulnerability itself.

/ Cyber security incident response plan:

- Prompt containment of an infected server or device
  - Darktrace RESPOND
- Segregation of infected network to ensure malicious code does not spread
  - Darktrace RESPOND
- Security and integrity of backup data including measures to secure backups separate from the system
  - Darktrace protects backup servers and the data as it is being transferred
- Isolating OT information
  - Darktrace/OT