Meeting the TSA Cybersecurity Requirements for Airports and Aircraft with SentinelOne Singularity XDR

March 28, 2022
by Neil Torpey

The New TSA Cybersecurity Requirements

The new cybersecurity amendment requires that impacted TSA-regulated entities develop an approved implementation plan that describes measures to improve their cybersecurity resilience and prevent disruption and degradation to their infrastructure.

> The amendment emphasizes performance-based measures, requiring impacted entities to assess the effectiveness of these measures proactively.

The TSA cybersecurity requirements aim to strengthen the security of aviation systems and protect against cyber threats. The requirements include:

- Stronger access controls
- Regular vulnerability assessments
- Incident response plans
- Adoption of cybersecurity best practices, such as encryption and multi-factor authentication
- Micro-segmentation to reduce the attack surface

The emergency amendment mandates the following actions for impacted TSA-regulated entities:

- Develop network segmentation policies and controls to ensure that operational technology systems can continue to operate safely in the event that an information technology system has been compromised, and vice versa
- Create access control measures to secure and prevent unauthorized access to critical cyber systems
- Implement continuous monitoring and detection policies and procedures to defend against, detect, and respond to cybersecurity threats and anomalies that affect critical cyber system operations
- Reduce the 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 in a timely manner using a risk-based methodology

The new requirements highlight the need for a comprehensive and proactive cybersecurity approach. By leveraging solutions such as SentinelOne Singularity XDR, enterprises in the aviation industry can improve their security posture, meet the new TSA cybersecurity requirements, and ensure compliance.

SentinelOne Singularity XDR for Meeting the TSA Cybersecurity Requirements

SentinelOne Singularity XDR is a comprehensive solution that can help enterprises in the aviation industry improve their security posture, meet the new TSA cybersecurity requirements, and ensure compliance.

The following are the key functionalities of SentinelOne Singularity XDR and their business outcomes that can help enterprises meet these requirements:

Scalability and Manageability

SentinelOne's firewall control solution is highly scalable and easy to manage. It has a central management architecture that simplifies policy management and ensures consistency, making it easier to meet the TSA's requirements. Unlike Microsoft solutions, which can be difficult to manage, SentinelOne supports cross-OS management, enabling enterprises to manage micro-segmentation policies dynamically across multiple operating systems, including Windows, macOS, and Linux.

Business Outcomes:

- Reduced operational overheads
- Improved security posture
- Simplified policy management

Easy-to-Implement Micro-Segmentation

Micro-segmentation is critical to reducing the attack surface in enterprise environments.

SentinelOne Singularity XDR provides easy-to-implement micro-segmentation, which improves visibility and strengthens overall security posture.

Business Outcomes:

- Reduced attack surface
- Improved visibility
- Strengthened overall security posture

Dynamic Policy Assignment Based on Endpoint Tags and Location Awareness

Dynamic policy assignment based on endpoint tags and location awareness is essential to managing micro-segmentation effectively. SentinelOne Singularity XDR enables enterprises to dynamically and automatically determine what firewall policies to assign to specific machines based on location, simplifying policy management and enhancing security.

The tagging of policy assignments across different scopes and the ability to assign policies per application instead of per machine makes SentinelOne Singularity XDR a highly scalable solution.

Business Outcomes:

- Improved efficacy of security policies
- Reduced time spent managing endpoint policies
- Enhanced security posture

Advanced Multi-Tenancy and Inherited Policies

SentinelOne Singularity XDR's advanced multi-tenancy provides a centralized console for managing security policies, alerts, and incidents for multiple customers, making it ideal for enterprises with multiple sub-agencies, such as federal agencies. Additionally, SentinelOne Singularity XDR supports inherited policies, which are dynamically assigned per application, making it easier to manage policies across large-scale environments.

Business Outcomes:

- Streamlined security operations
- Simplified policy management
- Reduced operational overheads

Conclusion

The TSA cybersecurity requirements mandate robust cybersecurity measures to protect against cyber threats in the aviation industry. SentinelOne Singularity XDR can help enterprises meet these requirements by providing advanced multi-tenancy, dynamic policy assignments based on endpoint tags, and easy-to-implement micro-segmentation.

By leveraging these functionalities, enterprises can improve their security posture, reduce the risk of cyber attacks, and ensure compliance with the new TSA cybersecurity requirements.

To learn more about how SentinelOne https://www.sentinelone.com/platform/singularity-xdr/Singularity XDR can help your enterprise meet compliance, contact us or request a demo.

Read more about Cyber Security

- SentinelOne's Cybersecurity Predictions 2023 | What's Next?
- Avoid's macOS Ventura 13 New Security Changes to Be Aware Of
- SentinelOne Debuts at the Top of MITRE Engenuity ATT&CK® Operations Evaluation, Sets Why…
- Best-of-Breed Identity Threat Detection and Response Meets Best-of-Breed XDR
- Cyber Risks in the Education Sector | Why Cybersecurity Needs to Be Top of the Class
- Cybersecurity Glossary: An Infosec User's Guide to Getting Started on Thursday