Thought leadership
Cisco public

The bridge to possible

Cisco Transportation Thought Leadership

Secure transportation operations

Highlights

- An incomplete view of the asset security posture can provide significant attack opportunities to bad actors without being detected. Asset inventory and visibility is foundational to a strong security practice.

Secure transportation operations

Trend overview

In the past two years, the increase in ransomware incidents across the transportation industry has changed every security conversation. These incidents have prompted detailed NIST frameworks for agencies to follow as the occurrence of cyberattacks intensifies. The very public attack on a subway in April 2021 created an environment of immediate action. Although no one was injured in the attack, it did cause a great deal of disruption and created industrywide awareness. Security is now a formal requirement. So, what does compliance mean, and what does “being secure” look like? The primary principles of secure operations remain the same, whether they are regulated or not. Three requirements that keep coming up in conversations about secure operations are as follows.

- Visibility of assets
- Posture
- Activity

In the transportation industry, projects are typically delivered on an individual basis. Thus, networks and other control assets often vary. As a result, the inventory of control system assets, instrumentation, and communication assets is also very diverse. Keeping an updated inventory of all assets and their security vulnerabilities is nearly impossible. However, an incomplete view of the asset security posture can provide significant attack opportunities to bad actors without being detected. Asset inventory and visibility is foundational to a strong security practice.

Strong risk mitigation

Cybersecurity risk mitigation, including firewalls, endpoint security, malware detection, behavioral analytics, and more, is where the bulk of money is spent. Because there are so many mitigation tools to choose from, a systematic approach is helpful in ensuring maximum risk mitigation.

A response plan

With stronger regulation around the reporting of incidents, we are all more aware of how common security breaches are. This makes a response plan essential. The plan articulates which experts get called in to assess damage and restore operations. It also identifies a methodology for communication, reporting, and other post-incident action items. Security has become a necessary companion to the benefits of digital operations. They exist in lockstep on the journey to safe, agile, and responsive operations.

Industry point of view

In the last decade, Cisco has established itself as a leader in IT security, integrating at least 10 major acquisitions into a single solution suite with comprehensive capabilities. In the past few years, Cisco has leveraged this integrated capability into the operations side of industry. Cisco also leverages tools that address OT (operational technology) visibility, risk mitigation, and incident response.

Asset visibility

The most significant challenge to implementing great asset visibility solutions has been the cost of deploying software at the edge to analyze local behavior. Cisco has integrated this capability into its network infrastructure, so that one device can provide data switching and routing as well as an agent to report on asset conditions and behavior. This simplifies deployment and reduces the cost of a parallel infrastructure.

Risk mitigation

Systematic risk mitigation is an involved process that includes a careful assessment of the communication flows most critical to the operation. In each flow, every device and operator introduces possible risk. There are a lot of tools that help assess and mitigate risk. The design of an optimal security framework and operation is the key. Cisco has service teams, partners, and security tools that make this mitigation process very effective.

Incident response

A good response plan ensures that teams and tools are at the ready for quick action. Cisco has service teams, partners, and security tools on standby for quick action. The response tools are integrated into the visibility and mitigation tools, so that security operations personnel are not learning new systems in a time of crisis.

Conclusion

As a leader in security, Cisco is ready to work with you to assess, mitigate, and respond to your security requirements. Across IT and OT, Cisco uses a world-class, integrated approach to securely protect your assets. For more information on how Cisco can help your organization, reach out to your Cisco account team or connect with the transportation team directly through the following links.

More information

- Cisco.com/go/transportation
- Cisco portfolio for transportation
- Security resilience for the unpredictable
- 10 ways Cisco delivers XDR capabilities today
- Realize SASE your way with Cisco
- Zero Trust Security for a Modern Workforce

CXX-XXXXXX-00 03/22