Enhancing Business Security through Asset Management

A whitepaper

Sekurinova

A W-INDUSTRIES Company

Introduction

In an era where cyber threats are constantly evolving, asset management has emerged as a cornerstone for safeguarding organizational assets and data. Maintaining an up-to-date inventory of assets has become the cybersecurity cornerstone to ensure that security measures are appropriately applied, vulnerabilities are promptly identified and mitigated, compliance with legal and regulatory requirements is maintained, and resources are efficiently allocated.

This proactive approach allows for better planning, response strategies, and resilience against cyber threats, minimizing potential damages from breaches or attacks. This whitepaper synthesizes insights from the National Institute of Standards and Technology's Internal Report (NISTIR) 8183. By adopting a comprehensive asset management strategy, businesses can significantly enhance their cybersecurity posture, mitigate risks, and ensure operational resilience.

Did you know majority of organizations do not recognize half of the assets after the initial asset discovery? Effective asset management is critical for identifying, managing, and securing these assets against cyber threats. It encompasses not only the physical and digital assets but also the processes and people interacting with these assets.

1. The Cybersecurity Imperative

Cybersecurity is no longer an IT concern but a strategic business imperative. The proliferation of connected devices, the expansion of IoT, and the advent of sophisticated cyber threats have made asset visibility and security management critical for maintaining business continuity and compliance.

2. Asset Management and Cybersecurity

Asset management plays a pivotal role in cybersecurity by ensuring that all assets are accurately inventoried, assessed for vulnerabilities, and monitored for threats. It provides the foundation for a robust security posture by enabling organizations to:

- Accurately identify and categorize assets across the IT and OT landscapes.
- Assess and prioritize vulnerabilities and risks associated with each asset.
- Implement proactive security measures and controls to mitigate identified risks.

3. NISTIR 8183 and Cybersecurity Frameworks

NISTIR 8183 outlines a comprehensive approach to managing cybersecurity risks associated with information systems and assets. It advocates for integrating asset management into the broader organizational risk management processes, aligning with frameworks like the NIST Cybersecurity Framework. This integration enables businesses to better anticipate, respond to, and recover from cyber incidents.

4. Industry Solutions

Work smarter and not harder. Automate the discovery and continuous monitoring of assets on your network.

- Real-time visibility into asset inventories, including OT and IoT devices.
- Advanced threat detection and response capabilities.
- Integration with existing IT and security infrastructures for streamlined operations.

5. Best Practices for Asset Management

To effectively leverage asset management for cybersecurity, organizations should:

- Conduct regular asset inventories and classifications.
- Implement continuous monitoring and vulnerability assessment tools.
- Foster cross-functional collaboration between IT, OT, and security teams.
- Adopt a layered security approach that includes both preventive and detective controls.

Conclusion

In today's digital age, effective asset management is a critical component of a comprehensive cybersecurity strategy. By leveraging insights from frameworks like NISTIR 8183 and adopting advanced asset management solutions, businesses can enhance their security posture, protect against cyber threats, and ensure long-term resilience.