ARMIS®

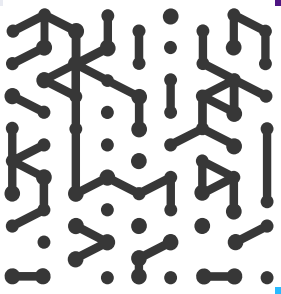
WHITE PAPER

Recognizing the Different Security Needs of IT and OT Systems:

A Case for the Armis Centrix™ Platform

© Copyright Armis 2023

Table of Contents



© Copyright Armis 2023

Introduction

At Armis, we regularly speak about the benefits of a holistic, multi-faceted approach in Cybersecurity. No example highlights this more than the disparate needs of IT and OT systems. As organizations continue to digitize and increasingly rely on both environments, understanding their distinct security needs is essential for ensuring operational integrity, data protection and production uptime (to name a few) . While IT systems are primarily focused on data processing and management, OT systems monitor and control cyber physical processes. This paper explores the differences between IT and OT security requirements and illustrates how Armis Centrix™ is specifically designed to cater to the unique needs of both environments.

Defining IT and OT Systems

IT Systems encompass technologies used for processing, storing, and managing data. They typically operate in office settings, data centers, or cloud environments. The primary focus of IT is on data confidentiality, integrity, and availability, adhering to the CIA triad.

Conversely, OT systems are used to operate and control physical processes in industrial settings such as factories, power plants, and utilities. The primary focus here is on real-time control and automation, prioritizing safety, uptime, reliability, and operational resilience.

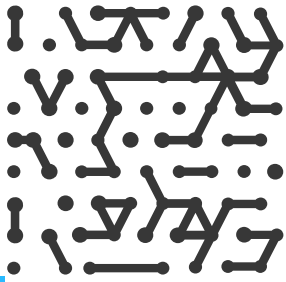
Asset Types Referred to in this Paper

IT (Information Technology):

This refers to the use of computers, networks, and software to manage and process information. IT encompasses a range of technologies used for data storage, retrieval, transmission, and manipulation, primarily in business and organizational contexts.

IoT (Internet of Things):

IoT describes a network of physical devices embedded with sensors, software, and other technologies that connect and exchange data over the internet. These devices can include everyday objects like home appliances, vehicles, and industrial equipment, enabling remote monitoring and automation.



© Copyright Armis 2023

BMS (Building Management System):

A BMS is a computer-based control system that manages a building's mechanical and electrical equipment, such as HVAC (heating, ventilation, and air conditioning), lighting, security, and fire systems. It helps optimize energy usage, enhance occupant comfort, and ensure operational efficiency.

ICS/OT (Industrial Control Systems / Operational Technology):

ICS refers to the hardware and software systems used to control and monitor physical processes in industrial environments. OT involves the technologies used in industrial operations, including manufacturing, power generation, and water treatment, focusing on the real-time control and monitoring of machinery and processes.

CPS (Cyber-Physical Systems):

CPS are integrations of computational algorithms and physical processes. These systems involve a tight coupling between the cyber (software) and physical (hardware) components, allowing for real-time monitoring and control. (Some put supervisory control and data acquisition (SCADA) in this category while others break it out separately.) Examples include smart grids, autonomous vehicles, and advanced manufacturing systems, where sensors and actuators work together with software to optimize performance and enable advanced functionalities.

Understanding the Security Landscape

IT Landscape Requirements

- **Data Protection:** IT systems prioritize confidentiality, integrity, and availability of data.
- **Compliance:** Regulatory frameworks require organizations to safeguard sensitive information.
- **Incident Response:** Rapid detection and response to data breaches and cyberattacks are essential.

OT Landscape Requirements

- **Operational Continuity:** OT systems focus on maintaining uptime and safe operations, often in real-time.
- **Safety:** The risks associated with operational failures can have dire consequences, including physical harm to personnel.
- **Legacy Systems:** Many OT systems run on outdated technology, complicating security efforts.

© Copyright Armis 2023

Key Differences in Security Needs

Definition

- An **IT system** (Information Technology) consists of computers, networks, and software that manage and process data for business, administrative, and communication purposes.
- An **OT system** (Operational Technology) includes hardware and software that monitor and control physical devices and processes in industrial environments, such as manufacturing plants, utilities, and critical infrastructure.

Category	IT (Information Technology)	OT (Operational Technology)
Definition	Systems used for processing, storing, and managing data	Systems used for monitoring and controlling physical processes
Primary Focus	Data processing, communication, and security	Real-time control and automation of physical systems
Environment	Office, data centers, cloud environments	Industrial environments (factories, power plants, utilities)
Priority	Data confidentiality, integrity, and availability (CIA triad)	Safety, uptime, reliability, and operational continuity
Latency Requirements	Higher tolerance for delays (milliseconds to seconds)	Requires low latency for real-time control (microseconds to milliseconds)
Device Types	Computers, servers, routers, switches, storage devices	PLCs (Programmable Logic Controllers), sensors, SCADA systems, HMIs
Communication Protocols	TCP/IP, HTTP, HTTPS, FTP, DNS	Proprietary and specialized protocols (Modbus, DNP3, OPC, Profibus)
Security Approach	Focus on protecting data from unauthorized access or attacks	Focus on protecting physical processes and preventing safety incidents

© Copyright Armis 2023

Category	IT (Information Technology)	OT (Operational Technology)
Network Types	Enterprise networks (LAN, WAN)	Industrial control networks (ICS, SCADA, DCS)
Patch Management	Regular patching and updates; downtime can be scheduled	Infrequent patching; minimal downtime tolerated due to 24/7 operations
Life Cycle	3 - 5 years (hardware/software updates)	10 - 20 years or longer (due to high cost of replacement and downtime)
Risk Factors	Data breaches, malware, insider threats	Safety risks, physical damage, catastrophic failures (power grids, factories)
Governance	Managed by CIO and IT teams	Managed by operations/engineering teams (Plant Managers, OT Engineers)
Regulations/ Compliance	Driven by data protection regulations (GDPR, HIPAA, CCPA)	Driven by safety and industry-specific regulations (NERC CIP, IEC 62443)
Physical Environment	Climate-controlled environments (data centers, offices)	Harsh environments (temperatures, vibration, humidity in industrial settings)

Armis Uniquely Addresses the Different Needs of IT and OT

It isn't an overstatement to say that the interconnectedness of IT and OT systems is prolific, whether intentional or as a natural evolution of technological integration. These systems often share data across domains to maximize operational efficiency, creating environments where rapid information exchange is the norm. As organizations strive for greater efficiency, data-driven decision-making, and streamlined operations, the lines between IT and OT are blurring. As a result, the traditional silos between these systems are being dismantled, allowing for a more seamless exchange of information and resources. With this in mind, organizations should strive to find a security solution that recognizes and caters to this blending of systems.

© Copyright Armis 2023

Enhanced Data Utilization

The rise of IoT devices and advanced analytics has revolutionized how businesses harness and interpret vast amounts of data from both IT and OT systems. By leveraging data flows from interconnected networks, organizations can monitor and optimize processes, predict maintenance needs, and ultimately boost operational efficiency. This transformation empowers companies to detect anomalies in real-time, enabling preventive measures that prevent costly disruptions.

Advanced Analytics in SaaS Solutions

Organizations are increasingly adopting sophisticated platforms from OT equipment manufacturers like Rockwell Automation and cloud providers like Google Cloud and AWS Industrial Data Fabric to leverage their analytics capabilities. Armis Centrix™ enhances these solutions by delivering advanced analytics specifically tailored for the critical infrastructure and manufacturing sector.

Real-Time Data Processing: Armis Centrix™ enables instant insights that facilitate quick decision-making and issue resolution, empowering teams to act swiftly when challenges arise. This capability is crucial in environments where every second counts and downtime can significantly affect production.

Predictive Analytics: Utilizing cutting-edge artificial intelligence and machine learning algorithms, Armis Centrix™ helps forecast trends, pinpoint risks, and advise on maintenance needs, thus significantly reducing downtime and optimizing operational efficiency. These analytics offer a forward-looking perspective that mitigates potential issues before they escalate.

Improved Decision-Making

Plant Managers operating in the world of interconnected IT and OT systems require a holistic view of operations. Such a viewpoint integrates real-time and historical data from both environments, enabling decision-makers to anticipate changes and make informed choices that enhance productivity and reduce downtime. The ability to have a comprehensive operational view allows for nuanced strategy development and implementation, supporting better resource allocation and process optimization.

Shared Security Challenges

With increased interconnectedness, the security landscape becomes more complex. Cyberattacks exploiting vulnerabilities in IT systems can have catastrophic consequences for OT environments, potentially disrupting physical processes. This reality underscores the need for a unified security strategy that is robust and adaptable enough to address both domains, integrating threat intelligence, risk management, and incident response seamlessly across both IT and OT systems.

© Copyright Armis 2023

Regulatory Compliance

Organizations face increasing scrutiny from regulatory bodies regarding cybersecurity practices. The convergence of IT and OT systems facilitates a more comprehensive approach to compliance, ensuring both domains adhere to necessary regulations and standards. Such alignment not only improves security posture but also enhances corporate reputation and trust among stakeholders.

Streamlined Operations

The integration of IT and OT systems allows organizations to automate processes that span both domains, leading to streamlined operations. Automation in these hybrid environments can result in more reliable performance, faster response times, cost savings, and enhanced service delivery. The amalgamation of automated protocols and manual oversight creates a robust operational framework, ensuring maximum efficiency and productivity.

Call to Action

Organizations must prioritize the integration of IT and OT security strategies. We encourage decision-makers to explore the capabilities of Armis Centrix™ and consider how it can be tailored to their unique operational needs. By investing in a comprehensive security solution, organizations can safeguard their assets, ensure compliance, and maintain operational integrity in the face of evolving cyber threats.

Final Thoughts

As IT and OT systems continue to converge, understanding their distinct security needs is paramount. Armis Centrix™ is uniquely positioned to address these differences, providing organizations with a robust security solution that safeguards both data and physical processes. By leveraging this platform, businesses can achieve a cohesive security strategy that enhances operational integrity and protects against evolving threats in both IT and OT environments.

© Copyright Armis 2023

Armis, the asset intelligence cybersecurity company, protects the entire attack surface and manages the organization's cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world Armis ensures that organizations continuously see, secure, protect and manage all critical assets.

Armis secures Fortune 100, 200 and 500 companies as well as national governments, state and local entities to help keep critical infrastructure, economies and society safe and secure 24/7.

Armis is a privately held company headquartered in California.

1.888.452.4011

Website

Platform
Industries
Solutions
Resources
Blog

Try Armis

Demo
Free Trial