Volume 10, Issue 7, July– 2025 International Journal of Innovative Science and Research Technology
ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25jul1859

Smart HVAC Manufacturing: Enhancing Operations Through IT/OT Unity

Aakarsh Mavi[1]

Publication Date: 2025/08/14

Abstract:- The convergence of Information Technology (IT) and Operational Technology (OT) in HVAC manufacturing is unlocking new levels of operational efficiency, automation, and data-driven decision-making. However, this digital unification also introduces significant cybersecurity challenges. Historically isolated, IT and OT systems were built with distinct goals and security models, making their integration a prime target for vulnerabilities and exploitation. This research explores a proactive approach to securing smart HVAC manufacturing by automating security audits across these blended environments.

The core objective is to design intelligent systems that continuously and autonomously assess the security posture of both IT and OT domains, especially at their intersection where traditional security frameworks often fall short. By automating vulnerability identification and assessment, the proposed framework aims to bridge critical gaps in visibility, communication, and threat response between IT and OT layers.

The methodology emphasizes real-time monitoring, AI-driven anomaly detection, and automated patch management to ensure swift remediation of emerging threats. Leveraging advanced security automation tools including machine learning-based analytics, this approach reduces reliance on manual processes, minimizes human error, and provides scalable, adaptive defense mechanisms. Ultimately, the research contributes to building resilient, future-ready HVAC manufacturing systems that not only optimize performance through IT/OT unity but also stand strong against an evolving cyber threat landscape.

Keywords:- *Metadata Management, AI-Based File Management, Machine Learning, Natural Language Processing (NLP), Cloud Integration, Document Security, Role-Based Access Control (RBAC), Anomaly Detection, Encryption, Duplicate Detection, Intelligent Search, Regulatory Compliance, IoT Integration, Predictive Analytics, Blockchain for Document Authentication, Automated Workflow, Secure Data Storage, Audit Logs, Smart File Categorization, DNS.*

How to Cite: Aakarsh Mavi (2025), Smart HVAC Manufacturing: Enhancing Operations Through IT/OT Unity. *International Journal of Innovative Science and Research Technology*, 10(7), 3576-3582. https://doi.org/10.38124/ijisrt/25jul1859

I. INTRODUCTION

As technology evolves, we're seeing a huge merging of Information Technology (IT) and Operational Technology (OT) in today's manufacturing settings. This has really boosted efficiency, productivity, and sparked a wave of innovation. But with this integration comes a new set of security issues. IT and OT were originally built to operate independently, each with their own security needs and ways of working. IT focuses on data processing, communication, and business operations, while OT is all about controlling physical machines and industrial processes. The difference in how they were designed, along with their growing interconnections, opens the door to possible vulnerabilities, making manufacturing sites prime targets for cyber threats.[1]

Identify applicable funding agency here. If none, delete this.

In the past, security strategies for IT and OT were developed separately, and there wasn't much focus on the risks that come from blending the two. As businesses increasingly link IT with OT for real-time monitoring, data sharing, and automation, the lines between these traditionally separate areas are starting to blur. This merging creates new chances for attack and increases security risks, like unauthorized access and data breaches that can throw a wrench into manufacturing processes. For example, a cyberattack on OT can halt production, damage machinery, and even put workers' safety on the line. Meanwhile, a breach in IT can expose sensitive business information and customer data!

With the swift merging of IT and OT, old-school manual security audits just can't keep pace. They fall short in handling the size, complexity, and speed of these integrated environments. There's a pressing need for automated security audit frameworks that can continuously analyze the security status of both IT and OT systems. Automation can quickly spot weaknesses and security gaps in these interconnected systems,

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25jul1859

helping to catch potential threats before they grow into major security breaches.

This paper dives into automating security audits within IT/OT converged manufacturing environments. The main aim is to create and implement systems that continuously evaluate the security status of both IT and OT infrastructures, focusing on detecting vulnerabilities stemming from their interactions. It also looks at automating remediation processes to ensure any security gaps are swiftly addressed. By using modern automation frameworks, this research aims to offer a scalable, proactive strategy for securing IT/OT environments, lowering the risk of cyber threats, and boosting the resilience of manufacturing ecosystems against changing security challenges.

II. LITERATURE REVIEW

We've been hearing a lot about how Information Technology (IT) and Operational Technology (OT) are coming together. This shift is grabbing attention in both schools and workplaces because there's a growing need for efficiency, automation, and insights based on data in manufacturing.[2] However, this blending raises some real concerns about cybersecurity. IT and OT systems have different focuses when it comes to security—IT is all about keeping data safe, while OT emphasizes availability and safety. So, it's essential to get a grip on the challenges we face in securing IT/OT convergence and to understand why automating security audits is so important to tackle the emerging vulnerabilities and threats.[6]

Understanding IT/OT Convergence and Its Security Challenges The merging of IT and OT systems, often called the Industrial Internet of Things (IIoT) or Industry 4.0, is changing the game for manufacturing plants. By bringing digital tech into the mix, manufacturers can make their operations smoother, cut down on costs, and make better decisions through real-time data analysis. But while this connectivity is great, it also opens the door to new security risks. Traditionally, OT systems were pretty isolated from typical company networks, which often meant they didn't have the advanced security features that IT systems usually do.

A report from the European Union Agency for Cybersecurity (ENISA) points out that merging IT and OT greatly expands the possible attack surface in manufacturing settings. Vulnerabilities that used to be an issue only for IT systems are now a major concern for OT systems. The Stuxnet attack in 2010 showed just how damaging compromising OT environments can be (ENISA, 2018). Plus, as OT systems become more connected to the internet and integrated with enterprise IT networks, their risk of cyberattacks grows, making traditional security measures just not enough anymore.

Frameworks for Securing IT/OT Integration Frameworks have been developed to tackle the security challenges of combined IT/OT environments. The NIST Cybersecurity Framework (NIST, 2018) is one of the most recognized ones out there. It offers guidance on how to identify, protect, detect, respond to, and recover from cybersecurity incidents. However, it was mainly built with IT systems in mind, so it needs some tweaks to fit the strict uptime, safety, and real-time performance requirements of OT environments.

Another important framework is the ISA/IEC 62443 standard, created by the International Society of Automation (ISA). This standard is all about the secure design and operation of control systems and includes guidance on risk assessment, access control, and system hardening. But as Turner et al. (2019) noted, it doesn't fully integrate IT security, leaving some gaps in merged environments. Research by Liu et al. (2019) indicates that bringing these two worlds together requires a well-rounded approach to cybersecurity, one that keeps in mind the unique traits of both IT and OT systems. This means acknowledging that OT systems are safety-critical and that IT systems need to deliver speedy, real-time data processing. An integrated approach is key to ensuring smooth operations while still paying attention to security.

Making Security Audits Easier Through Automation The idea of automating security audits in IT/OT environments is gaining traction, with several studies emphasizing the benefits of automating vulnerability management and continuous monitoring. Traditional security audits often rely on manual or semi-automated processes, which can be slow and prone to mistakes, especially in the fastpaced IT/OT world. That's why automated solutions are so essential for keeping security audits synchronized with the swift changes and interactions between IT and OT systems.

One way to automate these audits is by using vulnerability management tools that automatically check both IT and OT systems for known vulnerabilities. Tools like Nessus and OpenVAS are popular in IT circles for performing these scans, but they often struggle with OT systems because of the specialized protocols and devices involved. Some recent work by Zhang et al. (2020) has been all about adapting these tools for OT systems by incorporating OT-specific vulnerability databases and creating hybrid systems that can evaluate vulnerabilities across both domains.

Alongside vulnerability scanning, automated threat intelligence platforms are making their way into security audit processes, providing real-time insights into emerging threats. Platforms like IBM QRadar and Splunk have been used to automate the collection, analysis, and reporting of security incidents in both IT and OT settings. By connecting data from IT and OT, these platforms help identify potential security risks that might slip through the cracks in traditional manual audits.

- *Fixing Security Gaps Between IT and OT*

Finding vulnerabilities in IT and OT environments is super important, but being able to fix those gaps automatically is just as critical. A study by Brindescu et al. (2020) shows that using automated remediation solutions can really speed up our response to incidents and keep vulnerabilities from being exploited. These solutions follow set policies and playbooks to handle things like automatic patching, updating system configurations, and making adjustments to access controls, making sure we close security gaps before they can be taken advantage of.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25jul1859

In OT systems, where even a little downtime can be a big deal, it's essential to design automated remediation carefully so it doesn't disrupt operations. That's why remediation solutions for IT and OT convergence often include validation steps to check that changes won't mess with critical operations or safety protocols. Take a manufacturing plant, for example—automated patch management needs to consider operational dependencies and make sure that patches don't interfere with how production equipment works.

III. FRAMEWORK DESIGN

This framework is all about automating security audits for those environments where IT and OT converge. It focuses on providing ongoing, real-time security monitoring, spotting vulnerabilities, and optimizing the process of fixing security issues that pop up between IT and OT systems. By integrating security measures from both areas, it uses automation to make security audits more efficient and effective. Here's a quick rundown of how the framework is set up:

A. Framework Overview

The framework has three key goals:

- *Ongoing Security Evaluation:*

Automatically check the security status of both IT and OT systems in real-time, paying special attention to vulnerabilities that pop up when these systems interact.

- *Spotting Security Weaknesses:*

Find gaps in security controls between IT and OT systems, ensuring a cohesive security strategy that covers both areas.

- *Quick Fixes for Vulnerabilities:*

Optimize the process of resolving identified vulnerabilities and security issues, so they can be addressed quickly and effectively.

The framework includes these essential parts:

- Security Monitoring Layer
- Vulnerability Assessment Layer
- Threat Intelligence Integration
- Remediation and Response Layer
- Auditing and Reporting Layer

B. Security Monitoring Layer

The security monitoring layer keeps an eye on both IT and OT systems 24/7, making sure any changes or unusual activity are spotted right away. It uses various tools and sensors specifically personalized for both IT and OT environments:

- *Monitoring IT Systems:*

We employ standard IT tools like Splunk, Prometheus, and SolarWinds to monitor IT infrastructure, including networks, servers, and user devices. These tools gather data on network traffic, system logs, and performance metrics.

- *Monitoring OT Systems:*

We use specialized tools like Claroty and Nozomi Networks to monitor industrial control systems (ICS) and SCADA systems. These tools pay attention to specific protocols, such as Modbus, DNP3, and OPC, to catch anomalies within OT networks.

All the data collected from IT and OT systems is stored in a central location, enabling this monitoring layer to identify potential security events that could affect the interaction between IT and OT systems.

C. Vulnerability Assessment Layer

This layer takes on the task of scanning both IT and OT systems to discover known vulnerabilities and potential security lapses.Additionally, modern frameworks are evolving to include software supply chain transparency using SBOMs, which are essential for identifying vulnerabilities in third-party components that span across IT and OT environments.[4] It incorporates:

- *Automated Vulnerability Scanning:*

Tools like Nessus [nessus2021], OpenVAS, and Tenable.sc are used to scan IT systems for known vulnerabilities. For OT systems, we use specialized tools like Industrial Defender and SCADAsafe to evaluate potential threats to ICS and SCADA devices.

- *Correlation of Cross-domain Vulnerabilities:*

We gather the vulnerability data from both IT and OT systems in a central database, which helps us identify any overlapping vulnerabilities that may affect both areas, like shared network interfaces. Contextual Vulnerability Scoring: Using the SCSS (Subdomain Vulnerability Scoring System) framework, we prioritize vulnerabilities based on their exposure, criticality, and impact. This makes it easier to focus remediation efforts where they're needed most.

D. Threat Intelligence Integration

Integrating real-time threat intelligencex is key to keeping our framework up-to-date with any new threats and attack methods.Integrating real-time data into threat intelligence systems significantly enhances detection and response accuracy, as shown in recent studies emphasizing data fusion and live analytics for cyber defense.[3] Here's how our threat intelligence module works:

- *Threat Data Sources:*

We gather threat intelligence feeds from various sources like MITRE ATTCK, ThreatConnect, and open-source platforms such as OpenDXL. This helps us stay in the loop about the latest vulnerabilities, malware, and attack techniques.

- *AI and ML Integration:*

We use machine learning algorithms to sift through the threat data, spotting patterns and trends that might point to new threats targeting both IT and OT systems.[5]

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25jul1859

➢ *Risk Assessment and Alerting:*

The framework evaluates the risk associated with each vulnerability or anomaly based on the threat intelligence data. It sends out automated alerts whenever it spots high-risk threats.

E. Remediation and Response Layer

This layer is all about automating the process to fix any vulnerabilities and security gaps we find. Our goal is to guarantee that remediation happens quickly and efficiently:

➢ *Automated Patching and Configuration Management:*

We use tools like Ansible, Puppet, or Chef to automatically apply patches to affected systems. The automation kicks in to run playbooks for both IT and OT systems, making sure updates roll out smoothly with minimal disruption. As mentioned in paper by Sanat and Aakarsh [talwar2023˙secauto] Ansible can be leveraged to automatically patch and monitor.

➢ *Access Control Management:*

We set up automated access control policies to limit unauthorized access to critical OT devices and IT networks. This includes dynamically adjusting firewall rules, network segmentation policies, and enforcing role-based access controls (RBAC).

➢ *Safety Validation for OT Systems:*

Since OT environments are safety-critical, we've built-in validation steps to make sure our automated fixes don't disrupt operational processes or safety protocols. For instance, patching a device in OT may need checks to ensure machine calibration and safety features remain intact.

F. Auditing and Reporting Layer

This layer aims to give a clear view of the entire security auditing and remediation process. It makes sure all actions are logged for transparency, compliance, and ongoing improvements:

➢ *Audit Logging:*

All security events—like finding vulnerabilities, remediation actions, and configuration changes—are logged into a central SIEM (Security Information and Event Management) system for traceability and compliance auditing.

➢ *Compliance Reporting:*

Our framework generates compliance reports based on industry standards like NIST, ISO/IEC 27001, and ISA/IEC 62443. These reports display the security status of both IT and OT systems, pointing out any gaps and documenting our remediation efforts.

➢ *Continuous Improvement:*

We analyze the data from auditing and reporting to spot trends, recurring vulnerabilities, and areas where we can improve. Over time, the framework evolves to enhance its vulnerability [scarfone2007] identification and remediation processes based on feedback and new threat intelligence.

G. Integration with Existing IT/OT Security Systems

Our proposed framework is built to blend smoothly with current IT and OT security setups. Its modular design allows it to work alongside traditional IT security tools (like SIEM systems and vulnerability scanners) and OT-specific solutions (such as ICS firewalls and OT intrusion detection systems). The framework prioritizes interoperability, helping organizations strengthen their security posture at the growing intersection of IT and OT systems.

IV. IMPLEMENTATION

This framework is all about making security audits, vulnerability checks, and fixing issues way easier for both IT and OT systems. In this section, we'll break down how each part of the framework works, using various automation tools and techniques, along with some simple code snippets and explanations that are easy to follow.

A. Security Monitoring Layer Implementation

➢ *Tools:*

- IT System Monitoring: Splunk, Prometheus, SolarWinds
- OT System Monitoring: Claroty, Nozomi Networks, or custom-built OT monitoring tools *2) Steps:*
- Set up monitoring for IT systems using Splunk or
- Prometheus.
- Set up OT system monitoring using OT-specific monitoring tools such as Nozomi Networks or Claroty.
- Aggregate the data into a central monitoring dashboard (using Splunk or Grafana).

Example of IT Monitoring (Splunk):

```
# Install the Splunk Forwarder on IT systems wget -O splunk-
8.2.0-a7fbbf7f7ab5-Linux-x86_64.tgz "
https://www.splunk.com/page/download"
tar -xvf splunk-8.2.0-a7fbbf7f7ab5-Linux-x86_64.tgz
./splunk start --accept-license
# Forward logs to the Splunk server
./splunk add forward-server <central_splunk_server
>:9997
./splunk add monitor /var/log/syslog
```

Example of OT Monitoring (Nozomi Networks):

- Install and configure Nozomi Networks for real-time monitoring of industrial control systems (ICS).
- Data is aggregated and viewed via Nozomi's dashboard, focusing on ICS protocols like Modbus or DNP3.

B. Vulnerability Assessment Layer Implementation

➢ *Tools:*

- Nessus (for IT systems)
- Industrial Defender (for OT systems)
- Custom integration for cross-domain vulnerability correlation *2) Steps:*

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25jul1859

- Run vulnerability scans on both your IT and OT systems. Use Nessus for IT and Industrial Defender for the OT side.
- Store vulnerability results in one central database, like MySQL or PostgreSQL.
- Correlate vulnerabilities from both domains (IT and OT) to identify overlapping risks.

Example of Vulnerability Scanning (Nessus for IT):

```
# Run a vulnerability scan on a target IT server nessus -q -x -i
target_ip --policy="Full Audit" -output="scan_results.xml"
```

Example of Vulnerability Scanning (Industrial Defender for OT): Use Industrial Defender's API to automatically scan industrial devices (ICS) for known vulnerabilities:

```
# Send a vulnerability scan request to Industrial
    Defender API url =
'https://api.industrialdefender.com/v1/scans/ start'
headers = {'Authorization': 'Bearer <API_KEY>'} response
= requests.post(url, headers=headers)
# Capture and log the response if response.status_code ==
200:
print("Scan started successfully.")
else: print("Error starting scan:", response.text)
```

Correlating Vulnerabilities (Cross-domain) with SCSS Framework: import json

```
# Example of correlating IT and OT vulnerabilities and scoring
using SCSS
def correlate_vulnerabilities(it_vulns, ot_vulns):
merged_vulns = [] for vuln in it_vulns:
for ot_vuln in ot_vulns: if vuln['affected_system'] == ot_vuln['
affected_system']:
score = calculate_scss_score(vuln, ot_vuln)
                                merged_vulns.append({'vulnerability
': vuln['id'], 'score': score}) return
merged_vulns
def calculate_scss_score(it_vuln, ot_vuln):
# Calculate SCSS score based on risk exposure, age, etc.
return (it_vuln['risk_level'] + ot_vuln[' risk_level']) / 2
# Example of IT and OT vulnerabilities data it_vulns = [{'id':
'CVE-2021-1234', 'affected_system
': 'Server-1', 'risk_level': 8}] ot_vulns = [{'id': 'OT-
CVE-2021-5678', '
affected_system': 'Server-1', 'risk_level': 7}]
merged_vulns = correlate_vulnerabilities(it_vulns,
ot_vulns)
print(json.dumps(merged_vulns, indent=4))
```

C. Threat Intelligence Integration

➢ *Tools:*

- MITRE ATTCK framework • IBM QRadar or custom threat intelligence feeds *2) Steps:*
- Bring in threat intelligence from places like MITRE ATTCK, OpenDXL, or commercial threat feeds.
- Look at real-time threat data and check it against vulnerabilities found in both IT and OT systems.

Example of Threat Intelligence Feed (Python Integration with OpenDXL): from opentdxl import OpenDXLClient

```
# Connect to OpenDXL client =
OpenDXLClient('<client_ip>', '<client_port >')
# Get threat intelligence data from OpenDXL threat_data =
client.get_threat_data()
# Analyze and correlate threat data with vulnerability scan
 results
def analyze_threats(vulnerability_data, threat_data) : for vuln
    in vulnerability_data: for threat in threat_data:
if vuln['id'] in threat['vulnerabilities ']:
                                print(f"Threat detected: {threat['
 name']} for vulnerability {vuln
                            ['id']}")
```

D. Remediation and Response Layer Implementation

➢ *Tools:*

- Ansible for automation of remediation tasks • Puppet or Chef (optional) for configuration management *2) Steps:*
- Automate patch management with Ansible to roll out security updates for both IT and OT systems.
- Verify remediation in OT systems to confirm that the patches won't disrupt critical operations.

Example of Remediation (Ansible Playbook):

```
---
- name: Apply patches to IT systems hosts: it_servers tasks:
- name: Update packages on Linux server
  ansible.builtin.yum: name: "*" state: latest
- name: Apply patches to OT systems hosts: ot_devices tasks:
- name: Update firmware on OT device ansible.builtin.shell:
  "fwupdate -i /path/to/ firmware"
```

Safety Validation for OT Systems: Before applying the patch to an OT system, perform a validation to ensure no disruption in critical operations:

```
def validate_ot_remediation(ot_system): # Check system
  status before patching if ot_system['status'] ==
  'operational':
# Proceed with patch if the system is operational
patch_ot_device(ot_system)
else:
                print(f"OT system {ot_system['name']} is in
a non-operational state. Skipping patching.")
def patch_ot_device(ot_system): # Run patch command for
OT system print(f"Patching OT system {ot_system['name
']}...")
```

E. Auditing and Reporting Layer Implementation

➢ *Tools:*

- SIEM Systems (Splunk, QRadar)
- Grafana for visualization *2) Steps:*
- Keep a log of all security events (like vulnerabilities and patching actions) in a centralized system like Splunk or QRadar.
- Create compliance reports (for NIST, ISO/IEC, etc.) to monitor vulnerabilities, remediation efforts, and your overall security stance.

Example of Logging Security Events (SIEM Integration with Python): import logging

```
# Set up logging configuration for SIEM system
logging.basicConfig(filename='security_audit.log',
level=logging.INFO)
```

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25jul1859

```
# Example function to log vulnerability findings def
log_vulnerability(vuln):
logging.info(f"Vulnerability found: {vuln['id']} in
{vuln['system']}")
# Log a sample vulnerability vuln = {'id': 'CVE-2021-1234',
'system': 'Server-1'} log_vulnerability(vuln)
```

Compliance Reporting Example (NIST Report Generation in Python):

```
import logging import json
# Generate compliance report in JSON format def
generate_compliance_report(vulnerabilities):
report = {"compliance": "NIST", "findings": vulnerabilities}
with open('compliance_report.json', 'w') as report_file:
json.dump(report, report_file, indent=4)
# Example report generation
generate_compliance_report([{"id": "CVE-2021-1234",
"risk": "high"}])
```

V. FUTURE WORK

This research lays a strong groundwork for automating security audits in IT/OT converged environments, but there are still plenty of areas we can dive into for improvements. Here are some directions for future work:

- *Broader OT Device Support:*

Right now, the framework supports a limited number of industrial control systems (ICS) and OT devices. Looking ahead, we should aim to expand this support to include a wider range of OT systems, including some older devices and those with unique protocols. This way, we can ensure more thorough coverage of OT assets and boost security in manufacturing settings.

- *Better Integration with Existing IT/OT Tools:*

Currently, the implementation makes use of popular tools like Splunk, Nessus, and Ansible. Future updates could enhance integration with other enterprise IT and OT tools, such as SCADA systems, cybersecurity management platforms, and network monitoring solutions. This would create a smoother experience for users and give them better visibility throughout the entire ecosystem.

- *Real-Time Vulnerability Management:*

The framework already automates vulnerability scanning and remediation, but there's room to improve real-time detection and responses to new vulnerabilities. By incorporating more threat intelligence feeds and enhancing continuous monitoring, the system could automatically adapt to emerging threats, allowing us to tackle vulnerabilities more proactively. we can integrate frameworks like Overview of DNS Domain-Subdomains Vulnerabilities Scoring Framework to tackle DNS related vulnerabilities as well.

- *Automated Compliance Auditing:*

As regulations like NIST, ISO/IEC, and GDPR keep changing, automating compliance checks may get trickier. Future work might focus on refining how we report compliance, ensuring it adjusts to new requirements as they come up. Plus, the framework could provide ongoing audits to help organizations stay compliant with the latest regulations, eliminating needing those periodic manual checks.

- *Testing for Performance and Scalability:*

We need to dig deeper into how well the framework performs in large-scale manufacturing environments with multiple sites. As IT/OT convergence becomes more complex, making sure the system can handle lots of devices, network traffic, and security data is essential. Future research should look at stress-testing the system in large setups and making optimizations to boost both performance and scalability.

- *User Training and Awareness:*

Another important avenue for future work is developing training resources for IT and OT security teams. The complexities of managing IT/OT convergence require unique skills, so providing ongoing education and awareness programs will be key to ensuring teams are prepared for the changing security challenges.

If we tackle these areas, we can refine the framework to offer a more comprehensive, scalable, and adaptable solution for securing IT/OT converged environments. This will finally help reduce operational risks and improve the overall security posture in manufacturing operations.

VI. CONCLUSION

When it comes to manufacturing, merging Information Technology (IT) and Operational Technology (OT) can be pretty tricky, especially when it comes to keeping everything secure. As these two worlds get more connected, any vulnerabilities in either IT or OT can cause some serious headaches—think outages, data breaches, or even safety issues. This research really emphasizes the need to automate security audits to close those security gaps between IT and OT, guaranteeing that both can operate safely together.

The framework we're suggesting sets up this automation through a layered approach that includes monitoring, vulnerability assessments, threat intelligence, fixing problems, and compliance reporting. By using tools like Splunk, Nessus, Ansible, and OT-specific monitoring systems, we can simplify the way we find and fix vulnerabilities that pop up in both IT and OT. Plus, integrating real-time threat intelligence means we can manage risks proactively, quickly spotting and addressing new threats as they emerge.

By putting this framework into action, organizations can save a ton of time and hassle that comes with manual security audits and fixes, all while boosting their overall security in their IT/OT setups. This way, they can not only spot and tackle security risks faster but also meet industry standards like NIST, which helps lower the chances of cyberattacks and downtime.

In closing, automating security audits for the merging of IT and OT is a critical step in updating and securing today's industrial environments. The framework outlined here offers a solid solution for companies looking to strengthen their security processes while managing risks in an ever-changing digital world. Future work can focus on making the framework even

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25jul1859

better for smooth integration between IT and OT systems, potentially bringing in machine learning and AI for smarter threat detection and response.

REFERENCES

[1]. CISA. *Cross-Sector Cybersecurity Performance Goals (CPGs)*. https://www.cisa.gov/cpg. 2022.

[2]. International Electrotechnical Commission. *IEC 624432-1: Security for Industrial Automation and Control Systems*. IEC, 2010.

[3]. Osha Shukla. "Enhancing Threat Intelligence and Detection with Real-Time Data Integration". In: *International Journal of Engineering Research Technology (IJERT)* 14.04 (2024), pp. 91–96. URL: https://www.ijert.org/ research/enhancing-threat-intelligence-and-detectionwith-real-time-data-integration-IJERTV14IS040201.pdf.

[4]. Osha Shukla. "Software Supply Chain Security: Designing a Secure Solution with SBOM for Modern Software Ecosystems". In: *International Journal of Engineering Research Technology (IJERT)* 13.02 (2024), pp. 1–7.

[5]. URL: https://www.ijert.org/software- supply-chainsecurity-designing-a-secure-solution-with-sbom-formodern-software-ecosystems.

[6]. Robin Sommer and Vern Paxson. "Outside the Closed World: On Using Machine Learning for Network Intrusion Detection". In: *IEEE Symposium on Security and Privacy*. 2010.

[7]. National Institute of Standards and Technology (NIST). *Framework for Improving Critical Infrastructure Cybersecurity*. Tech. rep. U.S. Department of Commerce, 2018. URL: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST. CSWP.04162018.pdf.