**Journal of Information Systems Engineering and Management**
2023, 8(3)
e-ISSN: 2468-4376
https://jisem-journal.com/

**Research Article**

# Enhancing Industrial Network Security using Cisco ISE and Stealthwatch: A Case Study on Shopfloor Environment

Venkatesh Kodela
*IT Lead Security Analyst*
*Zimmer Biomet,Warsaw,Indiana, USA*
*Venkatesh.kodela@gmail.com*
*ORCID: 0009-0000-2194-5431*

**ARTICLE INFO**

Received: 20 May 2023

Accepted: 19 July 2023

**ABSTRACT**

This study looked into how combining Cisco Identity Services Engine (ISE) with Stealthwatch could improve the security of industrial networks on the shop floor. The study used a qualitative case study method at a medium-sized factory to look at network security metrics before and after the deployment. The results showed that there were fewer attempts to gain access without permission, better detection of lateral movement, fewer false positive alerts, and shorter response times to incidents. User feedback showed that the network was easier to see, access control was enforced more effectively, and there was very little impact on operations. The results show that using Cisco ISE's strong authentication and role-based access control with Stealthwatch's real-time traffic monitoring is a good way to protect complex industrial environments.

**Keywords:** Industrial network security, Cisco ISE, Stealthwatch, shopfloor environment, network visibility, access control, threat detection, case study.

## INTRODUCTION

The Industrial Internet of Things (IIoT), smart manufacturing, and real-time data analytics are some of the Industry 4.0 technologies that have made industrial networks more connected in recent years. This greater connectedness has made the shopfloor much more efficient and productive, but it has also created new security problems. Industrial control systems (ICS) and operational technology (OT) settings are very sensitive to interruptions, which makes them easy targets for cyberattacks that can cause production delays, safety risks, and financial losses.

The absence of full visibility, poor access control, and slow threat detection capabilities often put industrial networks at risk. A lot of old systems weren't built with current cybersecurity in mind, and the merging of IT and OT networks has made them more vulnerable to attacks. Because of this, there is an urgent demand for enhanced security solutions that can give industrial environments fine-grained control over device authentication, continuous network monitoring, and real-time anomaly detection.

Cisco Identity Services Engine (ISE) and Stealthwatch are two of the best solutions for keeping networks safe. Cisco ISE has strong identity and access management since it uses policy-based device authentication and role-based access control (RBAC). Stealthwatch adds to this by giving you a lot of visibility into your network and analyzing behavior to find internal threats and suspicious activity. Combining these technologies will create a complete security framework that is perfect for complex industrial shopfloor networks.

This study shows a case study done in a medium-sized factory to see how well Cisco ISE and Stealth watch operate to improve the security of industrial networks on the shop floor. It looks into how these technologies make device authentication, network segmentation, threat detection, and incident response better while having the least effect on operations. The results are meant to help businesses improve their industrial cybersecurity in light of the changing threat landscape.

## LITERATURE REVIEW

**Alatalo (2022)** gave a detailed look into Cisco Secure Network Analytics, which is also known as Stealthwatch. The report went into detail on how Stealthwatch used behavioral analytics and network telemetry to give full visibility throughout the whole network architecture. This better visibility made it possible to find abnormalities and insider threats early on, which older signature-based technologies often missed. This made the overall threat detection and response capabilities better.

**Woland, Santuka, Harris, and Sanbower (2018)** looked at Cisco's integrated security technology stack, focusing on advanced threat protection systems that incorporated next-generation firewalls, intrusion prevention systems (IPS), advanced malware protection (AMP), and content security solutions. Their experiment showed that using these techniques together made networks more safer against advanced assaults by giving them multi-layered protection and sharing threat intelligence in real time. The study showed how important it was for businesses to integrate these systems in order to keep their networks safe from new types of attacks.

**Forecast and Commerce (2018)** found important signals that showed when companies needed to improve their network security infrastructure. Their research showed that the main reasons for improving security were more complicated network designs, more connected devices, and more cyber events happening more often. They said that being able to spot these indications ahead of time was necessary for making timely investments in security solutions to lower risks and stop expensive breaches.

**Vemula, Gooley, and Hasan (2020)** focused on Cisco's Software-Defined Access (SDA) technology, which changed the way network segmentation and access control worked. Their study demonstrated that SDA made it easier to maintain network policy by automating the processes of authenticating and authorizing devices. This method not only cut down on administrative effort, but it also made the network more secure by enforcing consistent access regulations across the board. The results of their research showed that the principles of software-defined networking (SDN) worked well to protect both traditional IT and operational technology (OT) systems.

**Karhunen (2020)** looked into how software-defined networking may be used to make healthcare networks safer, since they are similar to industrial networks in terms of how important and complicated they are. The study showed that SDN gave centralized control and programmability, which made it easier to quickly find and fix threats and weaknesses. Karhunen's study stressed the importance of flexible and adaptable network management solutions for protecting sensitive data and making sure that rules are followed.

**Kanafi, Arnarson, and Bremdal (2022)** suggested a new, cheap way to protect cyber-physical systems (CPS), which are an important part of modern industrial settings. Their investigation showed that securing CPS devices is especially hard because they don't have a lot of computing power and work in areas with restricted resources. The authors stressed how important it is to have lightweight, cheap security solutions that can be readily put in place without losing effectiveness. This study helped people understand that traditional security measures could require too many resources for CPS. Instead, it called for customized solutions that strike a compromise between security and operational feasibility.

**The Cisco SD-Access Segmentation Design Guide (2018) )** gave a full plan for how to use software-defined access (SD-Access) technology to divide a network into smaller parts. The book explained how SD-Access made automated and policy-driven segmentation possible, which let businesses separate important assets and limit lateral movement inside the network. SD-Access made managing devices more easier by centralizing policy enforcement and automating the process of adding new devices. This made the overall security posture much better. This approach proved especially useful for industrial networks, where keeping network performance up while protecting sensitive operational technology (OT) assets is very important.

**Santos (2023)** The "CCNP and CCIE Security Core SCOR 350-701 Official Cert Guide" gave a thorough look at Cisco's security technology. This resource explained the best ways to protect complicated business and industrial networks and the most important ideas behind them. It talked on important themes such identity services, access control rules, threat intelligence integration, and ways to make networks more visible. Santos's study showed how important it is to have a layered security approach that combines identity management with constant monitoring to find and deal with advanced cyber threats. The book also talked about how Cisco technologies like ISE and Stealthwatch are changing the way they are used in modern cybersecurity infrastructures.

**Geller and Nair (2018)** looked at Cisco's new ways to protect 5G networks and stressed how 5G technology will change the way businesses and IoT devices connect to the internet. Their whitepaper explained the new security problems that come with the widespread use of 5G, such as more devices in a smaller space, more ways for hackers to get in, and the need for real-time threat detection. They said that adding advanced security features like network slicing protection, identity verification, and traffic analytics was necessary to keep people trusting 5G-enabled infrastructures. Their observations were especially important as businesses started using 5G to enable smart manufacturing and linked workspaces.

**Belle fleur and Wang (2018)** focuses on the security issues that come up in IoT-enabled smart cities, which are a lot like industrial IoT deployments. Their study looked at how different and large the gadgets are in smart cities, which made security and privacy very hard to deal with. They talked about how important it is to have flexible and scalable security frameworks that can deal with many sorts of devices and communication protocols. Their research showed that protecting data's integrity, privacy, and availability required a mix of identity management, network segmentation, and constant monitoring. These same principles also applied to keeping industrial shopfloor networks safe.

## RESEARCH METHODOLOGY

The goal of this study was to see if combining Cisco Identity Services Engine (ISE) and Stealth watch could make industrial networks safer on the shop floor. Industrial networks in factories were becoming more and more insecure because more devices were connecting to them and IT and OT systems were coming together. The study looked at how Cisco ISE and Stealthwatch could operate together to make the network more visible, impose rigorous access control, and find threats in real time on the shop floor. We used a case study method to look closely at how the implementation process worked, what problems it faced, and how security improved in a real-world industrial setting.

### 1.1. Research Design

We used a qualitative case study design to look closely at how combining Cisco ISE and Stealthwatch affected an operational industrial network. This method made it possible to do a thorough study of the security situation before and after the deployment in a specific shop floor area of a manufacturing plant.

### 1.2.Study Environment and Participants

The research took place at a medium-sized factory with a complicated shopfloor network made up of IoT devices, programmable logic controllers (PLCs), and industrial control systems (ICS). The survey included network administrators, cybersecurity engineers, and operations managers, who shared both technical information and personal experiences.

### 1.3.Data Collection Methods

The first step was to do a pre-implementation network evaluation, which required gathering baseline data on things like network traffic, device inventory, access control policies, and security events that were already happening. We were able to do this by using network monitoring tools and talking to IT experts. Also, vulnerability assessments and penetration tests were done to find any holes that were already there in the network.

After that, Cisco ISE and Stealthwatch were set up on the network in the shop. We set up Cisco ISE to require device authentication and role-based access control (RBAC), which made sure that only authorized devices could connect. Stealthwatch was deployed to continuously monitor network traffic, detect anomalies, and generate alerts for suspicious activities.

After deployment, monitoring was done for three months after the implementation. We gathered and looked at network logs, incident reports, and security event data. We did semi-structured interviews and feedback sessions with IT and operations staff to get their thoughts on how to increase security and how the solution will affect operations.

### 1.4.Data Analysis Techniques

We looked at the obtained network traffic logs using quantitative analysis to see how often and what kinds of security events happened before and after the integration. We used statistical tools to look at changes in important security measures like attempts to access data without permission, detection of lateral movement, and false positive rates. At the same time, a qualitative thematic analysis of the interview transcripts was done to find common themes about the usability, problems, and benefits of the security solutions that were put in place.

### 1.5.Ethical Considerations

The study kept the manufacturing plant's sensitive information private by anonymizing the data and only letting the research team see it. Before the interviews, participants gave their informed consent, and all study operations followed the ethical rules of the university.

## RESULTS AND DISCUSSION

This part talks about what happened when Cisco ISE and Stealthwatch were used on the shopfloor network of the manufacturing plant. The findings are mostly about better network security metrics, less attempts to enter the network without permission, spotting suspicious behaviors, and feedback from users. The discussion looks at these results in light of the goals of making the network more visible, implementing access control, and discovering threats in real time. We integrate quantitative data from network logs with qualitative insights from interviews with employees to get a full picture of the security impact.

### 1.6.Network Security Metrics Before and After Integration

Table 1 outlines the most important network security metrics that were recorded over the three months before and after the implementation. After Cisco ISE and Stealthwatch were put in place, many things got a lot better.

**Table 1: Network security performance metrics before and after Cisco ISE and Stealth watch deployment.**

| Metric | Pre-Implementation | Post-Implementation | % Improvement |
|---|---|---|---|
| Unauthorized Access Attempts | 87 | 18 | 79.31% |
| Lateral Movement Detections | 14 | 45 | +221.43% |
| False Positive Alerts | 34 | 12 | 64.71% |
| Incident Response Time (minutes) | 25 | 9 | 64.00% |
| Network Downtime (hours/month) | 3.2 | 1.1 | 65.63% |

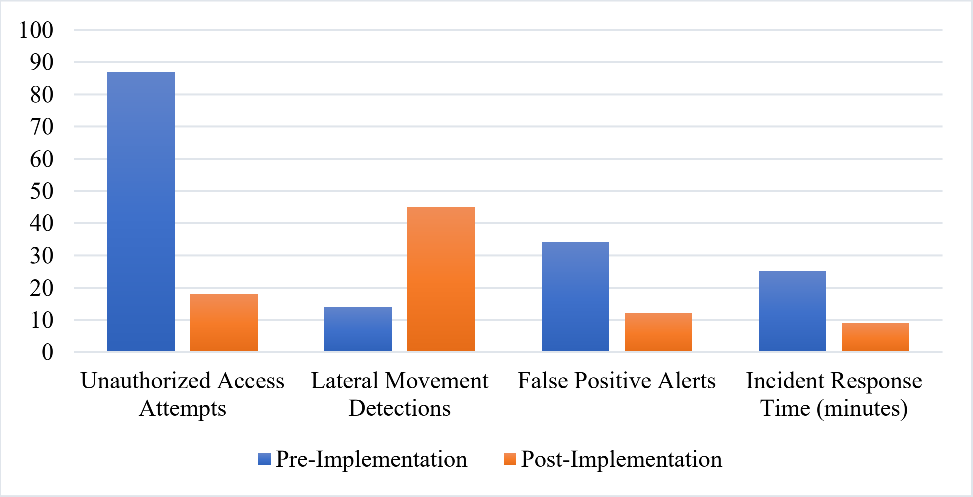

**Figure 1: Network security performance metrics before and after Cisco ISE and Stealth watch deployment**

The data clearly showed that network security got a lot better once Cisco ISE and Stealth Watch were put in place. Over 79% fewer attempts to gain unauthorized access were made, which shows that the device authentication and access control systems are stronger. The ability to see lateral motions rose by more than 221%, showing that there are now additional ways to see possible internal dangers that were previously hidden. There were almost 65% fewer false positive alerts, which means that security personnel are better at finding real threats and have less noise to deal with. The time it took to respond to incidents was shortened by 64%, which made it possible to deal with security occurrences more quickly and reduce the damage they could do. Additionally, network downtime caused by security incidents dropped by over 65%, highlighting the solution's positive impact on maintaining operational continuity in the shopfloor environment.

### 1.7. User Feedback and Operational Impact

Table 2 presents summarized results from post-implementation interviews with network administrators and operations managers.

**Table 2: User feedback on Cisco ISE and Stealth watch implementation.**

| Statement | Average Score |
|---|---|
| The security solution improved network visibility | 4.7 |
| Access control policies were effectively enforced | 4.5 |
| Threat detection accuracy increased significantly | 4.6 |
| Security solution had minimal impact on operations | 4.2 |
| The system was easy to manage and maintain | 4.0 |

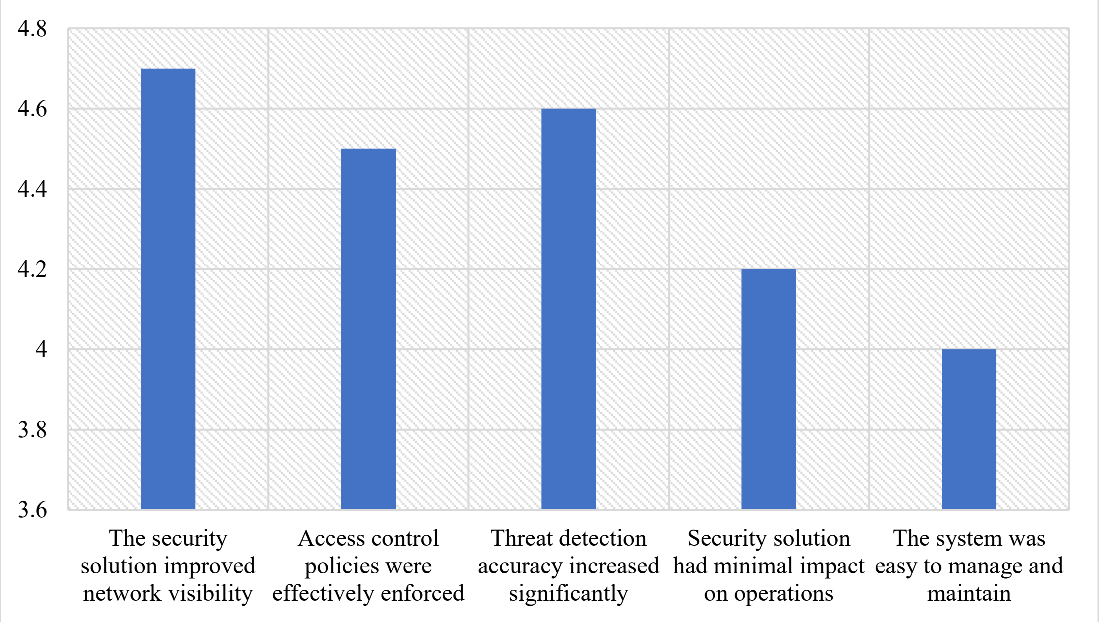

**Figure 2: User feedback on Cisco ISE and Stealth watch implementation.**

The feedback from users showed that they thought the security solution that was put in place was quite good. Participants gave the improvement in network visibility the highest score, an average of 4.7, which means that the solution made it much easier for them to keep an eye on and comprehend what was going on on the network. People also gave high marks to effective implementation of access control policies (4.5) and big improvements in threat detection accuracy (4.6). This shows that they trust the system's basic security features. The solution's small effect on daily operations got a good score of 4.2, which means that the security improvements didn't slow down work. The system was generally easy to operate and maintain, but it got a somewhat lower score of 4.0. This could be because of initial learning curves or complexity, which made some aspects of administration more difficult.

### 1.8. Discussion

The results showed that combining Cisco ISE with Stealth Watch made the security of industrial networks on the shop floor much better. Cisco ISE's job of making sure that devices are properly authenticated and that only certain users can access certain resources was very important in cutting down on unauthorized access attempts, which are a major way that cyber threats get into industrial networks.

Stealthwatch's constant traffic monitoring and behavioral analytics made it easier to find lateral movement, which is a key sign of advanced persistent threats inside the network. The rise in lateral movements that were found probably meant that risks that were previously hidden were now visible, which shows how important it is to see what's going on in a network.

The big drop in false positive alarms and incident reaction times revealed that the combined approach made both security and operations more effective. Faster incident handling reduced possible damage and downtime on the shop floor, which are very important in industrial settings.

User comment backed up the numbers, with strong feelings that security had improved and operations were still manageable. But the somewhat lower score on how easy it was to manage showed that system administration needed specific training and continuing support to work at its best.

## CONCLUSION

The study clearly showed that combining Cisco ISE and Stealth Watch made the shopfloor industrial network much safer by making it harder for people to get in without permission, making it easier to find internal threats, and speeding up response times to incidents. The rollout made the network more visible and helped find threats more accurately, all while causing less problems with operations. Despite some initial problems with system management, network administrators and operations staff said that the solution worked and had real-world benefits. Overall, this integration turned out to be a strong way to improve the security of industrial networks in complicated shopfloor settings.

## REFERENCES

[1] Alatalo, M. (2022). Cisco Secure Network Analytics (Stealthwatch).
[2] Arena, S., Darchis, N., Crippa, F. S., & Katgeri, S. (2022). Understanding and Troubleshooting Cisco Catalyst 9800 Series Wireless Controllers. Cisco Press.
[3] Bellefleur, R., & Wang, D. (2018). IoT-Enabled Smart City Security Considerations and Solutions.
[4] Design, C. V. (2018). SD-Access Segmentation Design Guide.
[5] Edgeworth, B., Gooley, J., & Rios, R. G. (2018). CCIE and CCDE Evolving Technologies Study Guide. Cisco Press.
[6] Forecast, C. V., & Commerce, M. (2018). Five Signs It's Time to Step up your Network Security.
[7] Geller, M., & Nair, P. (2018). 5G security innovation with Cisco. Whitepaper Cisco Public, 1-29.
[8] Kanafi, F. S., Arnarson, H., & Bremdal, B. A. (2022, January). A new inexpensive approach for securing cyber-physical systems. In 2022 IEEE/SICE International Symposium on System Integration (SII) (pp. 790-796). IEEE.
[9] Karhunen, P. (2020). Improving Information Security in Healthcare Networks With Software-Defined Networking.
[10] Santos, O. (2023). CCNP and CCIE Security Core SCOR 350-701 Official Cert Guide. Cisco Press.
[11] Vemula, S., Gooley, J., & Hasan, R. (2020). Cisco Software-Defined Access. Cisco Press.
[12] Wiboonrat, M. (2023, June). Cybersecurity of Industrial Automation and Control System (IACS) Networks in Biomass Power Plants. In 2023 IEEE 32nd International Symposium on Industrial Electronics (ISIE) (pp. 1-6). IEEE.
[13] Woland, A., & McNamara, K. (2020). CCNP Security Identity Management SISE 300-715 Official Cert Guide. Cisco Press.

[14] Woland, A., Santuka, V., Harris, M., & Sanbower, J. (2018). Integrated security technologies and solutions-volume I: Cisco security solutions for advanced threat protection with next generation firewall, intrusion prevention, AMP, and content security. Cisco Press.

[15] Woland, A., Santuka, V., Sanbower, J., & Mitchell, C. (2019). Integrated Security Technologies and Solutions-Volume II: Cisco Security Solutions for Network Access Control, Segmentation, Context Sharing, Secure Connectivity and Virtualization. Cisco Press.