Safeguarding Predictive Maintenance

A guide to securing your business from cyber threats.
siemens.com

SIEMENS

Introduction

Predictive Maintenance and other connected technologies associated with the smart factory revolution offer huge opportunities for production efficiency and visibility, but they also bring an additional operational risk – security.

Cyber-attacks are increasing, and the manufacturing sector is being hit with data theft, ransoms for access to locked data, machinery downtime, site safety, and build quality threats.

In this whitepaper we look at the security considerations organizations should be taking note of when implementing a scalable Predictive Maintenance program.

SENSEYE PREDICTIVE MAINTENANCE SECURITY

The importance **of security**

What can be done to minimize the risks of cyber attacks.

One of the world's largest producers of automation tools, suffered a ransomware infection which impacted all its locations across 76 countries for more than a week.[1]

A hacker put an airport's security system access onto the dark web for sale for just $10.[2]

The city of Atlanta was hit by a ransomware attack, holding its online services to ransom for $55,000 in bitcoin. It is reported that the city spent over $2.5 million recovering from the attack.[3]

Ransomware hit a large FMCG producer in Australia, after disrupting leading steel and oil firms in Russia.[4]

The same month, a leader in the Automotive sector was forced to halt production in one of its factories in Japan after finding WannaCry malware across its international networks, including Japan, North America, Europe, and China.[5]

The NHS in the UK was crippled by the WannaCry ransomware, which locked access to files until a ransom was paid.

'Security cannot be ignored, but it should also not be the reason to halt innovation'

The same ransomware quickly went on to attack several more factories around the world.[6]

Clearly, security cannot be ignored, but it should also not be the reason to halt innovation. Within the manufacturing sector, there is a huge opportunity in the use of technology to streamline production for cost savings, increased quality, and visibility from start to finish.

Security considerations

Supply Chain:

- Security extends further than just your organization. It is important to ensure any components you acquire are themselves secure
- Organisations must enforce strict requirements upon its suppliers to ensure that security standards are met throughout the supply chain
- Checks for certifications must be conducted, particularly ISO27001

Continuous improvement:

- Organizations must continuously review the security of their products and processes
- Monitor industry sources for cybersecurity
- Track new vulnerabilities and developments in the community
- Automatically test all changes for common vulnerabilities.
- Automatically test the correct behavior of authorization logic.
- Third-Party penetration tests from accredited expert testers.Security isn't a one-shot process. Vulnerabilities and exploits are continually developing, and your security processes must do so as well.

New vulnerabilities are being discovered constantly, and hackers often use automated tools to scan cloud-facing networks for known vulnerabilities.

Frequently they will be looking for issues that are known by the community, and for which security patches are available but have not yet been applied by administrators.

Consequently, it is important to monitor the latest information on vulnerabilities and breaches relevant to your organization, its tools, and infrastructure, and to ensure that your systems are kept up to date.

No matter how vigilant the organization, there is an ever-present risk of a security incident, and the organization must be prepared to handle such a situation.

An in-house security team should be in place to ensure that security is regularly assessed, and they should have in place policies and playbooks for how to handle various incidents that may occur.

These should include steps to contain the issue, gather any relevant evidence, resolve, recover and of course review the company’s response paying attention to lessons learned.

Depending on the nature of the incident and the data that was exposed (if any), third parties such as the information commissioner may need to be notified.

Regular exercises should be performed in which an incident is simulated, and response teams run through the playbooks to assess their suitability.

Further exercises should be performed to ensure adequate coverage of risks by the playbooks.

Training

Security is something that requires buy-in from the entire organization. While there may be a team dedicated to it, security practices must be followed by every employee in the organization.

Employees should be regularly trained on the security policies in place within the company, which should be designed to minimize risk, and employees should be able to identify common threats.

Can your employees identify:

- Attempts at social engineering?
- Phishing / Smishing and similar attacks?
- Do they know what to do in the event of suspicious activity?

Zero Trust

Don't trust – verify.
Is a user who they say they are? How confident are we? Did they sign in using multiple factors? Are they signing in from an unusual location? Is their activity different from usual?

These are all essential factors that must be considered.

Continuous monitoring

The monitoring tools on an organization's systems are its eyes and ears. It is important to pay close attention to activity to establish a baseline against which suspicious behavior can be detected.

Inbound and outbound network activity, service requests, user activity, and server load may all be useful sources of data in this regard. Furthermore, in the event of an incident, logs will form a crucial part of the investigation performed by the organization's security response team.

As well as network activity, other internal sources such as configuration changes should be monitored. Often a breach occurs due to nothing more than accidental misconfiguration of a service.

Sometimes the issue is that the default configuration from a vendor is weak and has not been changed (the classic example being the use of default passwords). Having a robust change-management process will help in this regard, as well as performing regular internal audits, but it is also important to have specialist third parties perform regular audits of your systems to find any issues that may have been missed internally.

In addition, there are several automated tools that can directly scan your configurations, to ensure they're secure. With the increased move towards cloud environments, such tools are invaluable to ensure all cloud assets are protected.

Third-party auditing

Best practice dictates that independent third parties are used for regular external security audits, at least annually or upon any significant change to your infrastructure.

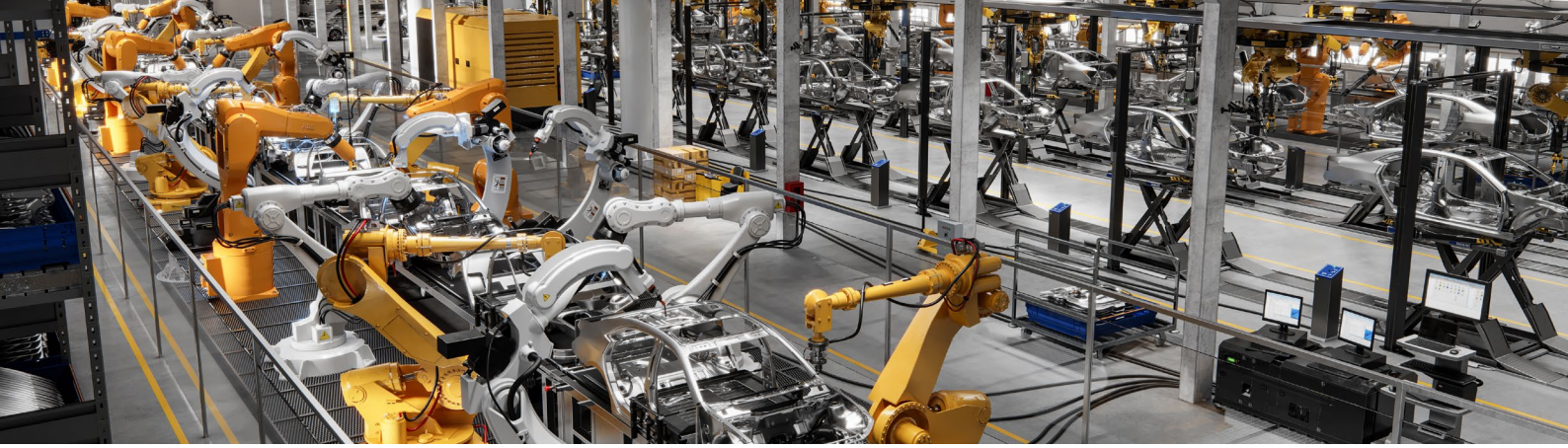
Using independent security experts enables solution providers to proactively identify any potential vulnerabilities so they can quickly mitigate any potential risks or concerns and keep in pace with the ever-changing cybersecurity environment.

These activities should include security audits and rigorous vulnerability scans and penetration testing to ensure the protection being offered by the solution meets industry expectations.

All Predictive Maintenance vendors should be able to supply security documentation, answer any questions and provide IT teams with the information they need. Industrial and office computers are internal.

Ensuring staff is mindful of security, updating passwords, ensuring antivirus software is up to date, encrypting data, keeping on top of permissions, maintaining a firewall; these are some of the areas that are critical in maintaining a secure network.

However, any addition to a network carries additional risk and needs to be properly assessed.



Benefits of Cloud Predictive Maintenance vs On-Premise Solutions

Predictive maintenance is reshaping asset management, with cloud-based solutions emerging as a superior alternative to traditional on-premise systems.

Cloud predictive maintenance offers a transformative approach to asset management, delivering unmatched scalability, flexibility, cost-effectiveness, collaboration, and analytics capabilities.

Embracing cloud-based solutions empowers organizations to drive efficiency, agility, and innovation in asset management, unlocking sustainable growth and competitive advantage.

Scalability:

Cloud solutions offer unparalleled scalability, eliminating the need for costly hardware upgrades. Businesses can effortlessly adjust to changing demands without constraints, ensuring seamless operations regardless of scale.

On-premise solutions often require significant investments in hardware infrastructure, limiting scalability. Expansion may necessitate costly upgrades and complex integrations, hindering agility and responsiveness.

Flexibility:

Cloud platforms provide unrestricted access from any location, enabling real-time monitoring and analysis. Unlike on-premise systems, maintenance teams are not tethered to specific locations, fostering agility and responsiveness.

On-premise systems tie maintenance teams to specific locations, impeding flexibility, knowledge capture and collaboration. Accessing real-time data and insights becomes challenging, especially for organizations with distributed operations.

Cost-Effectiveness:

Cloud-based models reduce upfront investments and ongoing maintenance costs associated with on-premise solutions. With a pay-as-you-go pricing model, organizations only pay for resources utilized, optimizing budgets and maximizing ROI.

Maintaining on-premise hardware incurs substantial costs, including maintenance, upgrades, and replacements. These expenses can strain budgets and divert resources from core business objectives.

Robust Security Measures:

Cloud service providers invest heavily in security infrastructure, employing advanced encryption, authentication, and access control mechanisms. Compared to on-premise solutions, which may lack comprehensive security protocols, cloud-based platforms offer enhanced protection against cyber threats and data breaches.

Senseye Predictive Maintenance Security Facts

At a Glance

ISO27001 Certified

ISO9001 Certified

CSA STAR Level 1

Senseye Predictive Maintenance is certified against ISO27001:2013. Transition to the ISO27001:2022 specification is set for late 2024. Senseye is also covered by CSA STAR Level 1.

Encryption at Rest

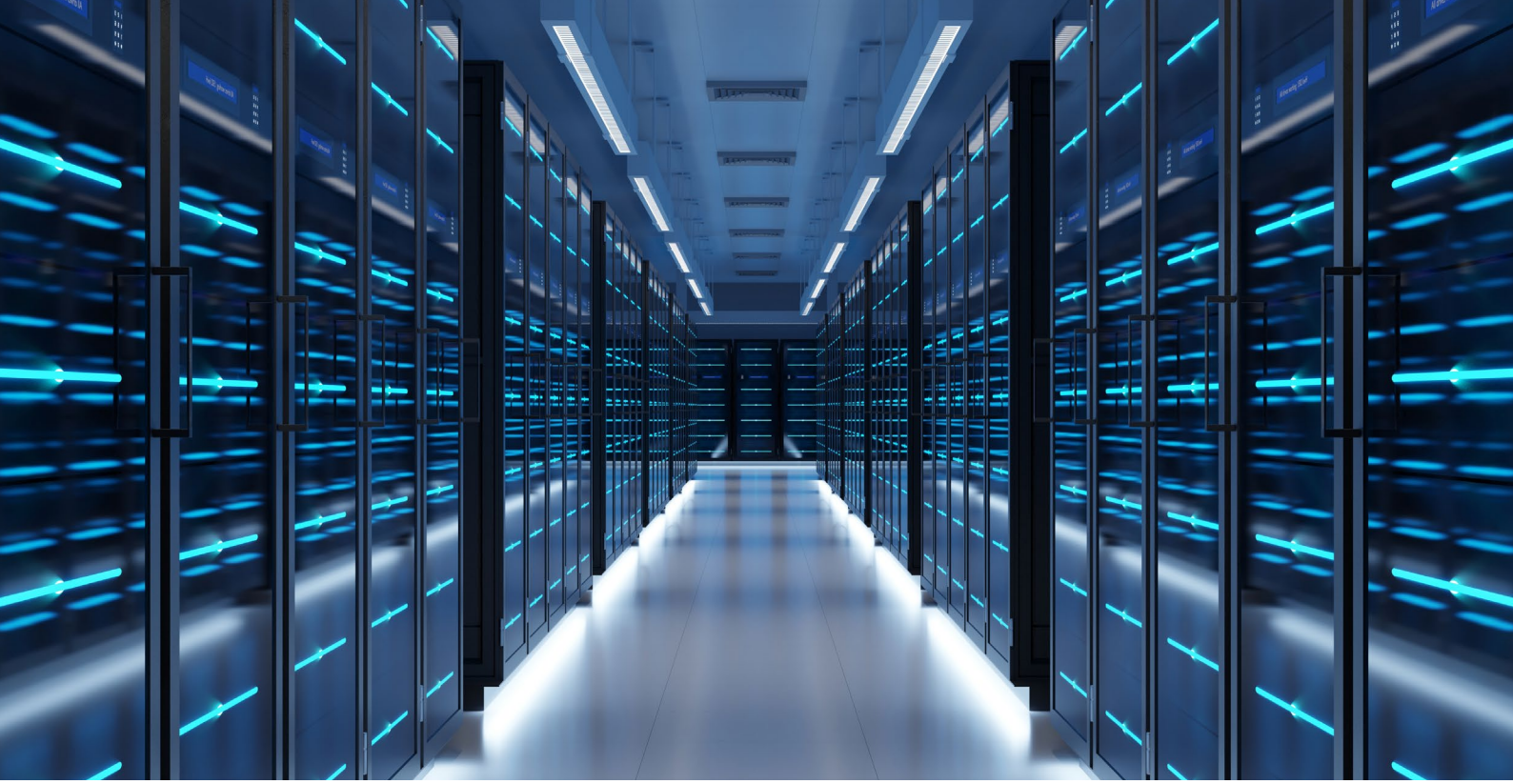
Encryption in Transit

European Data Residency

Data processing and storage occurs in the EU. Data is encrypted at rest using AES-256, and in transit using TLS1.2. Clear text and TLS1.1 or earlier are blocked.

SSO Integration

Senseye integrates with your organization's identity provider for single sign-on. Mechanisms include SAML and OIDC, allowing for easy integration with many platforms, including Microsoft EntraID and Okta.



Senseye Predictive Maintenance Security Facts

ISO27001 - Senseye's ISMS covers all business operations and is certified against ISO27001:2013 by LRQA. Transition to the 2022 specification will be audited in December 2024.

ISO9001 - Senseye's QMS is certified against ISO9001:2015 by LRQA.

CSA STAR - To aid in transparency, Senseye has opted into CSA STAR Level 1.

NIS2 - Senseye is NIS2 compliant.

Deployment Model - Senseye is a cloud-based software-as-a-service product running in Azure and AWS.

Tenancy Model - Senseye predictive maintenance is a multi-tenant application. Tenants data are logically separated from one-another.

Update Model - Senseye operates a continuous integration / continuous deployment pipeline. Fixes and new features are continuously deployed.

Security Testing - All changes undergo manual code reviews and automated static analysis before being published to production. These check for common issues based on the OWASP Top 10. Automated unit and integration tests also test API functionality and authorization logic to ensure tenant separation, and access control behavior.

Encryption at Rest - Data is encrypted at rest using AES-256. This is achieved via the volume encryption methods available in AWS and Azure.

Encryption in Transit - Data is encrypted in transit using TLS1.2. Senseye's APIs are configured to reject TLS1.1 or earlier connections.

Data Residency / GDPR - All data storage and processing is in the EU. Supplier agreements include EU SCCs to ensure GDPR compatibility.

Penetration Tests - Senseye's application and infrastructure is tested annually by expert CREST -acreddited penetration testers.

Single Sign-On - Senseye supports integration with SSO Identity Providers via SAML or OIDC.

Vulnerability Management - CVEs of all dependencies are monitored and patched in line with their severity.

Incident Response - Senseye has a comprehensive incident response plan, which includes explicit steps to communicate with the customer within 24 hours of detection.

Supply Chain - Senseye follows Siemens' comprehensive supply chain management processes to ensure cybersecurity standards are maintained throughout the supply chain.

More Information - Please see siemens.com/senseye

Conclusion

Security is a major concern for any business, and it is crucial to put in place a thorough and robust security strategy to minimize the risk of a cyber-attack.

However, when a cloud-based Predictive Maintenance solution is designed with security in mind it can be safer than having some third-party software installed inside the network.

Getting full commitment from all stakeholders, internal and external, to ensure continuous improvement, ongoing network monitoring, transparency regarding solution providers' security arrangements and protecting network access means that risk can be balanced with innovation and opportunity.

To learn more about Sensye Predictive Maintenance. Visit **here.**

References:

1. www.zdnet.com/article/major-german-manufacturer-still-down-a-week-after-getting-hit-by-ransomware
2. www.mcafee.com/blogs/consumer/consumer-threat-notices/airport-security-system-dark-web-rdp-shop
3. www.wired.com/story/atlanta-spent-26m-recover-from-ransomware-scare
4. www.theguardian.com/technology/2017/jun/28/petya-cyber-attack-cadbury-chocolate-factory-in-hobart-hit-by-ransomware
5. www.forbes.com/sites/peterlyon/2017/06/22/cyber-attack-at-honda-stops-production-after-wannacry-worm-strikes
6. www.theguardian.com/technology/2017/may/12/global-cyber-attack-ransomware-nsa-uk-nhs