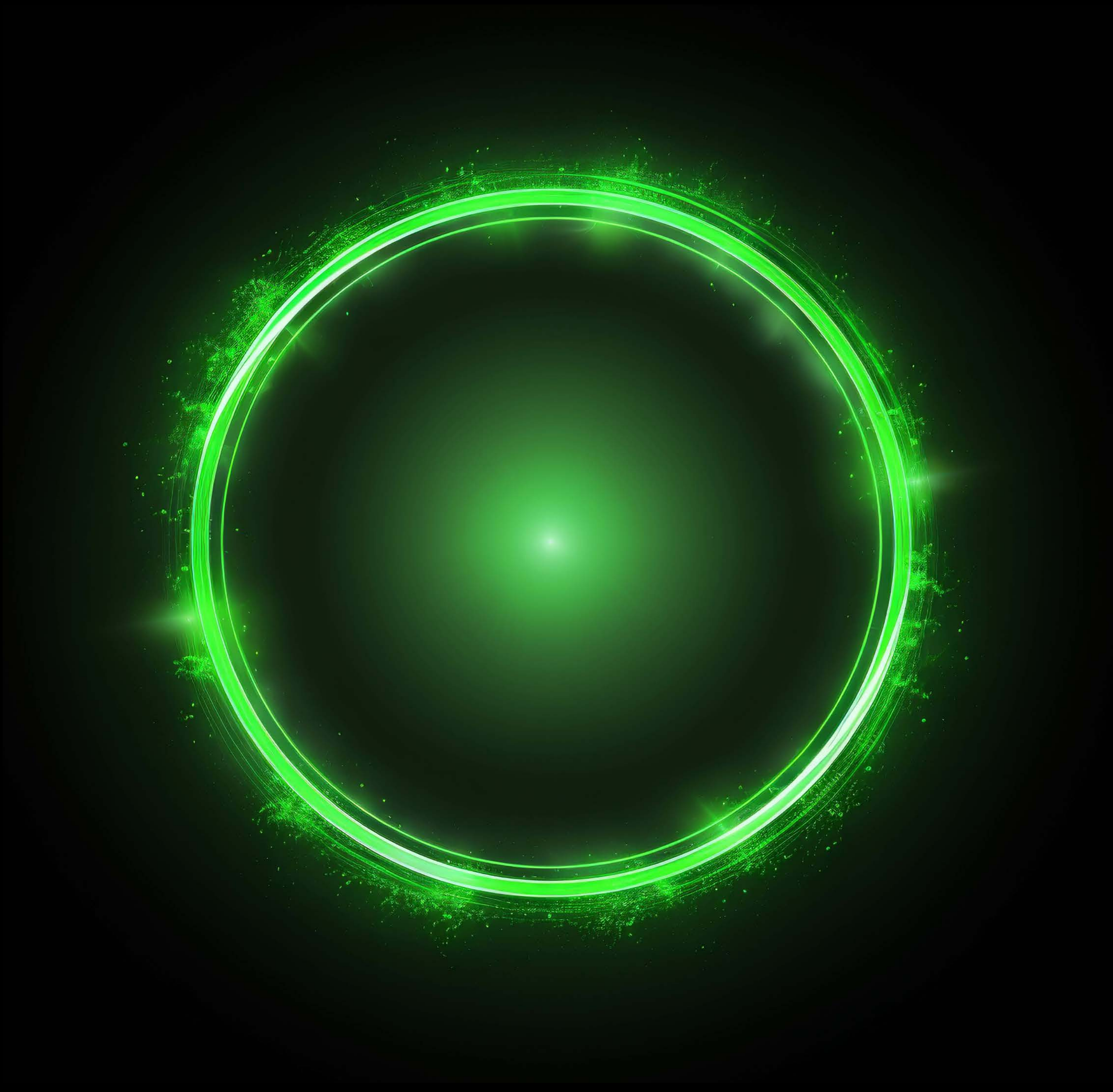


360º OT Security – Second Part (2/3)

Transforming Strategy into Action with Deloitte's Expertise

October 2024

MAKING AN IMPACT THAT MATTERS since 1845

Introduction

As digital technologies reshape the manufacturing industry, they escalate cybersecurity challenges. Therefore, the implementation and operation of resilient OT systems is essential.

With rising cyber threats, Operational Technology (OT) security is more critical than ever, making implementing effective security strategies essential. Deloitte's 360° OT Security Framework provides a comprehensive and customizable solution to meet these needs.

Current Challenges in OT environments

As industrial environments evolve, OT security is facing growing challenges, particularly due to the increasing adoption of digital technologies. Integrating OT and IT systems has extended the potential attack surface, making infrastructures more vulnerable to cyber threats.

However, industry evidence suggests that in real-world applications, OT security concerns are not always prioritized in alignment with their business criticality. Figure 1 shows some key figures about the potential impact of OT security breaches.

Securing OT environments demands more than technical fixes. It requires an organizational cultural shift, where cybersecurity awareness is embedded into all levels of operation and at all times. This transition becomes increasingly complex with legacy systems that lack modern security features. Moreover, resource constraints and a shortage of skilled personnel often delay the implementation of essential security measures.

These issues, compounded by the challenge of integrating new digital technologies with legacy infrastructures, underscore the need for a structured and scalable OT security implementation approach.

61%
of intrusions reported in industrial companies' IT networks **impacted their OT systems** [1]

93%
of industrial organizations have reported a **breach on their OT networks** [1]

$50 billion
of estimated costs as a result of **unplanned downtime** at manufacturers [2]

Figure 1: Key Figures[1]

Purpose and Focus

In the first part of this whitepaper series, the Deloitte 360° OT Security Framework was introduced, with a focus on the strategy to empower clients to achieve a zero-incident security culture.

The purpose of this second part is to detail the implementation phase, guiding organizations on how to put these strategies into practice and effectively strengthen their operational technology security .

The Deloitte 360° OT Security Framework offers a structured methodology to guide organizations through securing OT systems. The objective of the second part is to guide organizations through the implementation phase, focusing on how to turn strategic security insights based on the assessment and gap analysis covered in the first whitepaper episode into practical and actionable solutions, reinforcing resilience against cyber threats.

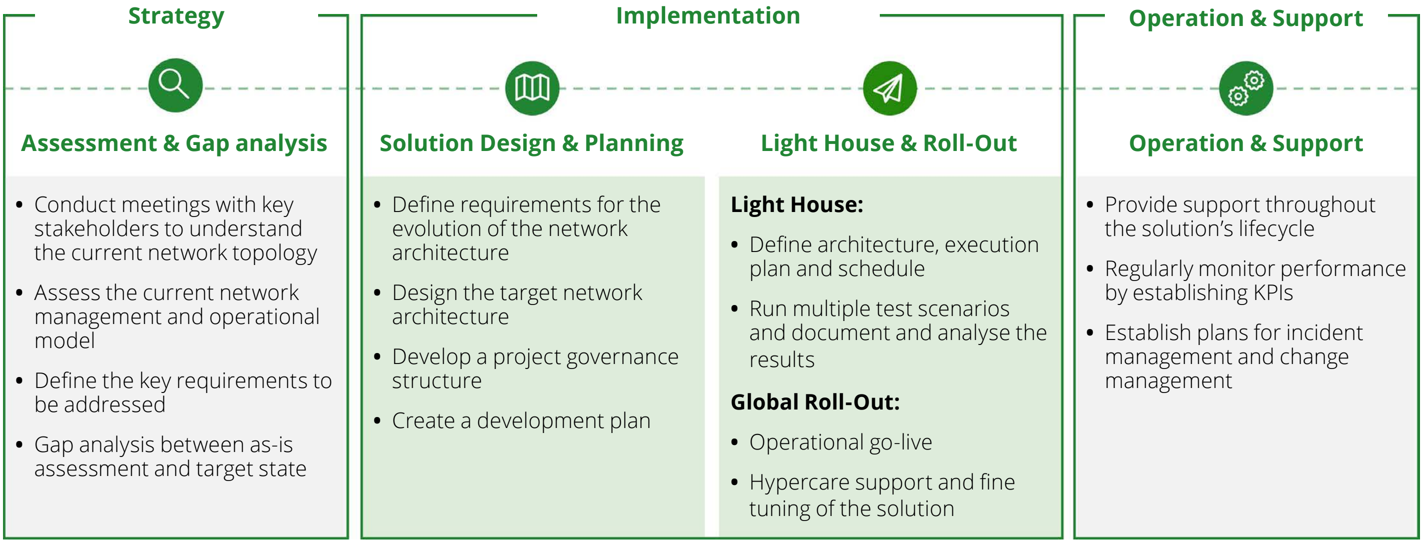
Implementation requires more than just technical solutions; it involves aligning security measures with operational goals, ensuring compliance with industry regulations such as NIS2 and NERC CIP, which strengthens cybersecurity requirements for critical infrastructure and essential services, and managing challenges posed by legacy systems and limited resources. Deloitte's structured approach follows the stages of Solution Design, Light House Testing, and Roll-Out, ensuring that the OT systems are protected against both current and emerging threats.

The final part of this whitepaper series will cover Operations and Support, outlining how organizations can sustain and optimize OT security post-implementation for long-term resilience.

[1] References: [1] Fortinet (2022), [2] Forbes (2021)

Deloitte 360° OT Security Framework

The OT Security Framework, built on years of expertise, is designed to navigate security complexities while seamlessly integrating into daily shop floor routines, avoiding disruption to operations.



Strategy

Assessment & Gap analysis

- Conduct meetings with key stakeholders to understand the current network topology
- Assess the current network management and operational model
- Define the key requirements to be addressed
- Gap analysis between as-is assessment and target state

Implementation

Solution Design & Planning

- Define requirements for the evolution of the network architecture
- Design the target network architecture
- Develop a project governance structure
- Create a development plan

Light House & Roll-Out

Light House:

- Define architecture, execution plan and schedule
- Run multiple test scenarios and document and analyse the results

Global Roll-Out:

- Operational go-live
- Hypercare support and fine tuning of the solution

Operation & Support

Operation & Support

- Provide support throughout the solution's lifecycle
- Regularly monitor performance by establishing KPIs
- Establish plans for incident management and change management

Figure 2: Deloitte 360° OT Security Framework

Navigating the Deloitte 360° OT Security Framework

Through collaboration with partners and clients, Deloitte has developed a comprehensive OT security model utilizing trusted components, established processes, reliable vendors, and a detailed implementation roadmap. Its primary objective is to enable clients to identify potential risks and effectively detect, assess, and mitigate threats. The **Deloitte 360° OT Security Framework** prioritizes cybersecurity capabilities that enhance an organization's resilience to cyber threats. By ensuring compliance with critical regulations like **NIS2 (Network and Information Security Directive 2)**, the framework helps organizations meet legal requirements, avoid penalties, and strengthen their security posture through adherence to high cybersecurity standards. Compliance with NIS2 safeguards against regulatory risks and promotes best practices in cybersecurity. Implementing standardized and robust security measures significantly reduces the risk of downtimes, protecting against costly operational disruptions and maintaining productivity. Preventing downtime is crucial for avoiding financial losses and ensuring continuous operation.

Built on years of best-practice experience, the framework employs a proven methodology to evaluate an organization's current and target maturity levels of cyber capabilities. This methodology forms the foundation for a tailored roadmap to strengthen security posture and operational resilience. The Deloitte 360° OT Security Framework offers a strategic approach to safeguarding your organization against evolving cyber threats while ensuring compliance with key regulations such as the NIS2 directive, as illustrated in Figure 3. This directive emphasizes four essential phases of security — **Protect, Detect, Respond, and Recover** — which align closely with the framework's structure. By focusing on strategy, implementation, operations, and support, Deloitte minimizes operational losses due to downtime and strengthens overall security, delivering a holistic solution for enhancing OT security.

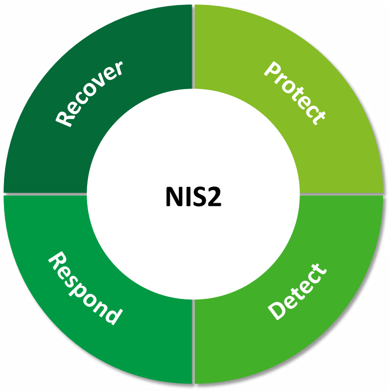


Figure 3: NIS2 Compliance

1. Strategy

As detailed in the previous part, the strategy phase establishes the foundation for a secure OT environment by conducting a comprehensive network assessment and gap analysis. This phase is critical in defining the current security posture and identifying areas for improvement. In collaboration with key partners, a tailored assessment methodology is provided to clients, culminating in a detailed network assessment report.

The process begins by defining the scope of the IT/OT environment, analyzing the network topology, identifying deployed technologies, and engaging key stakeholders from both IT and OT teams. Data is gathered through various customized methods to ensure a thorough understanding of the environment. Once collected, the data is systematically analyzed to generate a comprehensive report.

From this analysis, key security objectives for the desired future state are established. By comparing the current state with the target security posture, the gap analysis provides a clear pathway for developing a strategy that will enhance OT security and address identified vulnerabilities.

2. Implementation

The Deloitte 360° OT Security Framework identifies the Implementation Phase as a critical point where strategic insights are transformed into actionable security solutions. This phase builds on the findings from the Assessment and Gap Analysis, turning them into concrete steps to establish a robust, secure, and resilient OT environment capable of addressing complex cybersecurity challenges.

Solution Design & Planning

This phase begins with designing a secure OT architecture based on identified gaps, focusing on scalability, performance, and resilience. A project governance structure ensures alignment with business goals and proactive risk management.

A detailed development plan guides the project through key milestones, ensuring smooth execution while minimizing disruptions.

Light House Phase & Roll-Out

The Light House Phase tests the OT security architecture in a controlled environment, validating its effectiveness before full deployment. A phased Roll-Out follows, gradually deploying security measures across the organization. Continuous feedback and monitoring help address any issues early on. Once validated, the solution moves into the Global Roll-Out.

3. Operation & Support

The final phase is where the longevity of the OT security solution is ensured. Once the system is live, continuous real-time monitoring and performance tracking are implemented to maintain security and operational integrity. Through the establishment of Key Performance Indicators (KPIs), the effectiveness of the security framework is measured.

This involves continuous improvement cycles that allow for the solution to evolve in tandem with new threats and operational needs. Incident management and change management frameworks are embedded within daily operations, ensuring that any disruptions are swiftly managed, and that the system remains agile in the face of unforeseen challenges.

By fostering a culture of resilience and proactive defense, the Deloitte 360° OT Security Framework ensures that the security solution is not a static deployment but a dynamic system, continuously adapting to safeguard critical as well as non-critical infrastructure and maintain operational excellence. A holistic approach is provided to maintain the deployed OT solution, combining proactive risk management with ongoing support and monitoring. By leveraging technologies like predictive analytics , organizations can detect potential vulnerabilities before they turn into incidents. The framework's focus on long-term operational resilience guarantees that security measures evolve as the business grows, ensuring sustained protection against both current and future threats.

By integrating real-time monitoring, dynamic testing, and hyper care support, the Deloitte 360° OT Security Framework ensures that security is not only deployed but actively maintained and enhanced, providing organizations with the resilience needed to thrive in today's interconnected world. Deloitte´s 360° OT Security Framework offers a structured approach to securing operational technology environments through its Strategy, Implementation, and Operation and support phases.

By systematically determining vulnerabilities and deploying robust security measures, organizations can enhance the resilience of their OT systems against evolving cyber threats. In the next chapter, we will detail the next phase—Implementation Preparation: Solution Design & Planning—which focuses on establishing a solid foundation through detailed design and planning processes.

Implementation Preparation: Solution Design & Planning

Empowering Your Team for OT Security Success: Tailored Preparation for Seamless Implementation.

Introduction

The Implementation Phase directly follows the Strategic Phase and builds on its results. The knowledge gained during the plant assessment is used to specify the OT environment and formulate concrete requirements for target solutions. Consequently, the formalization in the form of the Fit-Gap Analysis serves as the initial basis for the Implementation Phase. The implementation phase is divided in two sub-phases, solution-design & planning and Light House implementation & Roll-Out.

Design Target Network Architecture

Designing a robust network architecture within the Deloitte 360° OT Security Framework starts with identifying key requirements obtained within the assessment phase, focusing on business objectives, critical OT processes, and the need for scalability, reliability, and performance. These are balanced with budget constraints while ensuring technical needs such as critical OT applications, performance metrics, and security measures are addressed. The network must support future OT growth and incorporate layered security architectures with encryption, firewalls, and Zero Trust models. Ensuring high availability and optimizing performance for real-time applications are crucial, alongside integrating compliance with standards, such as ISA-95 and ISA-99. Both logical and physical aspects are considered in the design. A detailed network diagram defines segments and security zones, including those recommended by the ISA models. ISA-95 provides guidance on integrating enterprise and control systems, ensuring seamless operations. Meanwhile, ISA-99 focuses on creating secure industrial automation networks. Security zones are defined to include an Industrial Demilitarized Zone (iDMZ), which acts as a buffer layer between OT and IT environments, providing an additional security barrier against potential threats.

Incorporating a multi-layered security strategy ensures comprehensive protection against evolving threats. The strategic placement of firewalls, switches, and careful planning for connectivity ensures smooth integration and operations. Selection of appropriate hardware and software guarantees performance, while designing for redundancy and high availability prevents system failures. Security features protect OT assets, and SIEM (Security Information and Event Management) tools provide centralized monitoring and management.

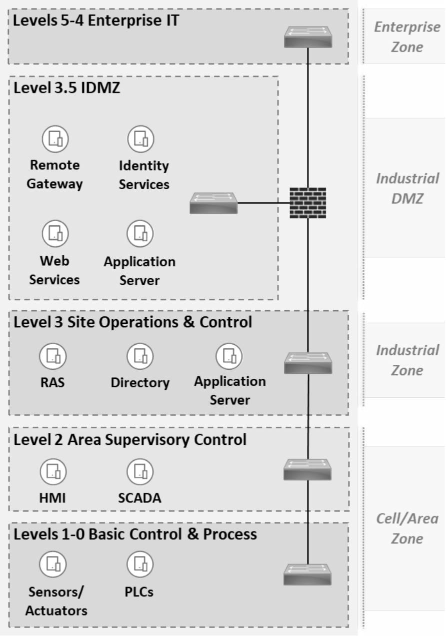


Figure 4: Network Reference Architecture

Develop a Project Governance

While a well-designed network architecture forms the foundation for secure and efficient OT operations, long-term success and resilience demand a robust governance structure. Governance is essential for managing roles, responsibilities, and decision-making processes, ensuring that the network and its security measures align with organizational objectives and regulatory standards.

As shown in Figure 4, the project governance framework is divided into several components. A RACI matrix defines roles and responsibilities, establishing clear accountability. Key roles include project sponsors, who set the strategic direction; project managers, who oversee operations; OT security architects, who design and implement security solutions; and stakeholder representatives, who facilitate collaboration. Effective stakeholder management is crucial for success, particularly on the shop floor. A Cybersecurity Program that outlines essential policies, procedures, and controls is a central element of the governance framework. This program is regularly updated to address emerging threats and technological advancements.

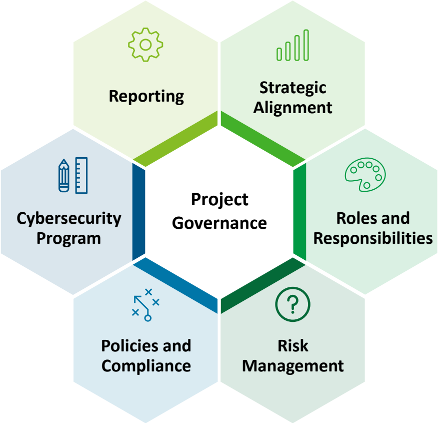


Figure 5: Project Security Governance

The Cybersecurity Steering Group Committee, comprising C-level executives and key stakeholders, drives strategic decisions to align OT security efforts with broader organizational cybersecurity goals. Risk management involves continuous monitoring and assessments to identify and mitigate potential threats. Regular reviews of the cybersecurity strategy ensure its effectiveness against evolving threats. Performance metrics and KPIs assess the impact of cybersecurity initiatives, providing transparency and enabling informed decision-making. The Technical Advisory Board offers expert insights and recommendations, supported by operational committees focused on compliance, technical solutions, and change management.

Effective communication is integral to governance, supported by a targeted communication strategy designed to meet diverse stakeholder needs. Detailed analysis and segmentation of stakeholders ensure that communication delivery is effective and engaging.

Create Development Plan

In order operationalize the deployment of the designed OT security solution a roadmap is developed. Outlining critical milestones, timelines, and resources to align security initiatives with business and operational goals.

The plan details key phases, from the procurement of essential hardware and software to the integration of security controls such as firewalls, network segmentation, and Intrusion Detection Systems/Intrusion Prevention Systems (IDS/IPS). Each phase adheres to leading cybersecurity standards.

Resource allocation assigns specific responsibilities to OT security teams, network engineers, and project managers, ensuring full accountability. The plan also details the necessary tools and technologies for monitoring, threat detection, and risk mitigation within OT environments.

As previously mentioned, a risk management framework is embedded, addressing potential challenges such as hardware failures, security breaches, and configuration errors. The plan includes incident response protocols and mitigation strategies to minimize operational disruption and maintain system integrity. The plan follows a phased deployment approach, starting with a Light House deployment for validation, followed by extensive testing and full Roll-Out. Timelines and critical path activities are carefully structured to maintain project momentum and include contingency measures for unforeseen delays. Documentation is maintained throughout, covering architectural diagrams, configurations, and security protocols, ensuring transparency and alignment with stakeholder expectations.

The Deloitte 360° OT Security Framework ensures the development plan is both secure and adaptable, supporting the continuous evolution of operational resilience.

Target Operating Model

A key component in implementing and operating OT security services is the Target Operating Model (TOM). TOM defines the desired future state of how organization’s people, processes, and technologies interact to ensure resilient OT security. A strong TOM is crucial in manufacturing digitalization, where OT converges with IT. This model supports the security of critical manufacturing processes while maintaining stable operations and enabling fast incident resolution.

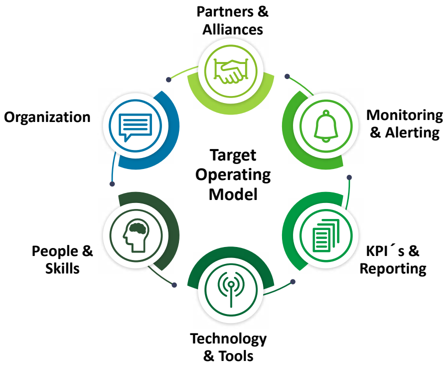


Figure 6: Dimensions of a Target Operating Model

Figure 6 illustrates the six dimensions of a Target Operating Model that form the foundation for establishing OT services.

From an organizational perspective, the OT security team structure and service processes—such as incident management, change management, and configuration management—are aligned with the plant organization. Roles like OT Vulnerability Manager, OT Incident Manager, and OT Change Manager are established. To effectively fill these roles, required skills are specified to ensure a good fit. Continuous training is necessary to strengthen OT engineers and IT personnel to manage complex security challenges. Cybersecurity and industrial systems certifications are vital to bridge the knowledge gap between OT and IT.

To support service operators from a technology and tool perspective, the TOM promotes the seamless integration of service management tools on the shop floor. Monitoring and alerting are critical aspects of this integration. Continuous monitoring tools such as IDS/IPS and Security Information and Event Management (SIEM) platforms are critical for detecting suspicious activity in real-time. KPIs and reporting are indispensable for tracking the effectiveness of the TOM in OT security. Organizations can evaluate security performance by establishing specific, measurable KPIs—such as the number of incidents detected, response times, system uptime, or Overall Equipment Effectiveness (OEE)—and identify areas for improvement. Regular reporting ensures transparency, enabling leadership to make informed decisions and adjust strategies to maintain alignment with security goals and regulatory requirements.

Implementation Execution: Light House & Roll-Out

Transition from Pilot Success to Full-Scale Deployment, Enhancing OT Security at Every Stage While Preserving Operational Stability

Introduction

After completing the solution design and planning phases within the Deloitte Framework, the focus shifts to the Light House Deployment. The OT security solution is tested in a controlled environment before implementing it on a larger scale. The phased approach supports a structured transition from design to live deployment.

The high-level network architecture is tailored to the specific operational environment of the Light House Plant, using OT security best practices to derive a detailed, low-level network design, setting the groundwork for subsequent implementation steps. Through systematic testing, the architecture can be validated, ensuring it meets the required standards and performance criteria. After successful validation and handover to operations, the solution is ready for the operational go-live and subsequent broader Roll-Outs.

Project Management

Ensuring a seamless transition to enhance OT security necessitates strong project management, which includes consistent time planning, effective stakeholder coordination, efficient resource management, thorough risk management, and procurement processes. To achieve the successful implementation of the target OT security solution, it is crucial to engage stakeholders from both, business and IT domains.

The initial steps include procuring necessary hardware and software, followed by on-site installation and configuration. This setup defines network segmentation as outlined in the logical architecture and integrates security appliances such as firewalls and IDS/IPS systems to activate all security measures. Efficient resource allocation is a critical part of the execution plan. Clearly defining the tasks for network engineers, IT staff, and project managers, along with securing the necessary tools, is essential.

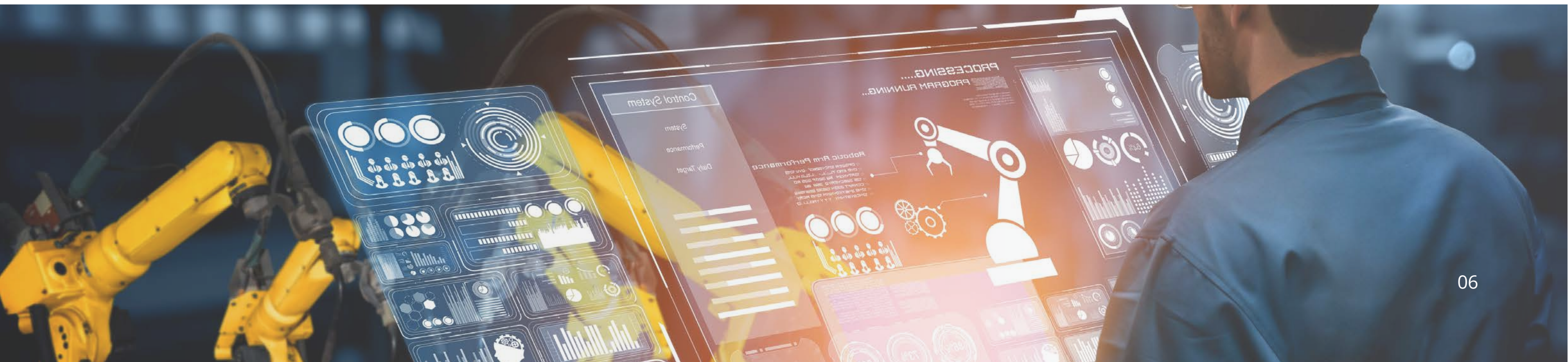
Concurrently, risk management addresses potential issues like hardware failures or security breaches. Mitigation strategies include backup and recovery plans, spare hardware availability, and incident response protocols to minimize disruption during implementation within the Light House Plant. Moreover, comprehensive documentation and securing necessary approvals are imperative steps in the process. Key documents, including architectural diagrams, configuration details, procedural guides, and risk management plans, must be compiled and regularly updated to reflect any changes. The approval process ensures that all necessary endorsements from stakeholders and project sponsors are secured before advancing further. A final sign-off from relevant parties confirms acceptance of the architecture and the detailed execution plan.

Low-level Design (Light House Plant)

The Low-Level Design translates the high-level architecture into a plant-specific framework. This involves a detailed analysis of the plant infrastructure, focusing on network segmentation, data flows, security zones, and device placements. The objective is to support operational processes while enforcing stringent security controls. Continuous stakeholder feedback is integrated to ensure that the final design is optimized for both functionality and security. This tailored design serves as the foundation for a secure and scalable deployment, addressing all necessary protections to mitigate potential risks.

Light House Implementation

Following the detailed network design, the Implementation phase ensures a strategic deployment of the OT security solution. The Implementation Phase is structured and begins with deploying the solution in a Development (DEV) environment to isolate and test configurations. This step identifies and resolves issues early, without impacting live operations. Upon successful testing in the DEV environment, the solution transitions to the Quality Assurance (QA) environment, where it faces extensive testing using simulated production data and realistic operational scenarios. The goal is to validate that the solution can meet the operational demands and security challenges expected in production.



After successful validation in QA, the solution is deployed to the Production (PROD) environment. This phased deployment includes the gradual integration of security controls such as network segmentation, firewalls, and IDS. This method ensures that the security framework is embedded seamlessly within the operational infrastructure. By following a phased approach, risks are minimized, security measures are validated, and operations remain stable throughout the deployment process.

Testing of Light House Plant

The testing phase ensures that the OT security solution is robust, resilient, and ready for live deployment within the Light House Plant. The primary focus is identifying and eliminating network vulnerabilities that could be exploited in real-world scenarios. Segmentation testing guarantees that the network is effectively partitioned, restricting unauthorized access to critical systems and reducing the risk of widespread breaches. Passive monitoring provides real-time visibility into network traffic, enabling the detection of threats without interfering with ongoing operations.

This proactive monitoring allows immediate threat identification and rapid response, ensuring issues are contained before they escalate. Equally important is validating ITSM/OTSM processes, such as Incident Management, Change Management, and Problem Management. These tests ensure the team is fully prepared to manage security incidents, with streamlined processes in place for quick resolution. Every team member must be knowledgeable and capable of handling incidents efficiently, ensuring that disruptions are minimized, and operations continue smoothly. Through risk and threat modeling, various attack scenarios are simulated to assess the system's ability to withstand cyber threats. This continuous testing and feedback loop further refines the security solution, ensuring it meets the demands of the real-world environment.

The OT security solution is thoroughly validated by addressing vulnerabilities, ensuring segmentation integrity, implementing passive monitoring, and testing incident response processes. This comprehensive approach establishes a strong foundation for the global Roll-Out, ensuring the solution is optimized for performance and security.

Operational Go-Live & Hypercare Support (Light House Plant)

After successfully validating the OT security solution with the Light House deployment, the focus shifts to the Global Roll-Out, which includes the operational Go-Live, Hypercare support, and solution optimization. The objective is to preserve the integrity of the original deployment while adapting to each site's specific conditions, ensuring seamless integration of security measures with minimal operational disruption.

The Go-Live phase starts after thorough testing and completion of all preparatory steps. A key prerequisite is the development of an Operational readiness checklist, which verifies that the operations team is fully equipped for deployment. This checklist confirms team training, monitoring solutions' readiness, and that all critical systems are primed for production. Once operational readiness is confirmed, the PROD deployment initiates the Go-Live phase. This phase relies on real-time monitoring to ensure system stability and security. Advanced algorithms continuously monitor performance metrics, identify anomalies, and detect potential security threats.

Throughout this phase, immediate support is available to address any incidents that arise, ensuring minimal disruption and maintaining operational continuity. The primary focus during this phase is incident management. A structured incident response framework, aligned with industry standards such as NERC CIP for critical infrastructure protection, allows for the efficient resolution of security events.

Additionally, a feedback loop is implemented to continuously evaluate both user experience and system performance, enabling data-driven improvements in security measures and operational efficiency.

Knowledge transfer is a critical component, ensuring the OPS (Operations) team can fully manage and maintain the solution post-Hypercare. Upon completing this phase, the system is formally handed over to the OPS team, marking its full integration into daily operations and establishing a resilient defense against evolving threats.

Global Roll-out

Following the successful deployment and stabilization of the OT security solution at the Light House Plant, the Global Roll-Out phase is initiated. This phase is pivotal in scaling the validated solution to all relevant sites across the organization. The objective is to ensure a standardized deployment process, while addressing the distinct operational environments of each site.

Through a structured, phased approach, the organization can implement localized adaptations that meet site-specific requirements without compromising the overall integrity of the solution. The Global Roll-Out builds upon the insights gained during the Light House deployment and Go-Live phases. A comprehensive analysis is conducted for each site to adapt the solution according to its unique conditions, ensuring strict adherence to the 360° OT Security Framework. This method guarantees a consistent level of security and operational resilience across all sites.

By the end of the Global Roll-Out, the OT security solution is fully embedded throughout the entire organization, providing a scalable and resilient defense against security threats. This comprehensive implementation strengthens operational continuity at all sites and enhances the organization's overall security posture, positioning it effectively to address both current and future cyber threats.

Conclusion

Elevate Your OT Security to the Next Level: Partner with Deloitte to Implement Advanced Solutions and Foster a Zero-Incident Security Culture for Lasting Protection

Recap of key aspects

This whitepaper has journeyed through Deloitte's 360° OT Security Framework, to manage the complexities of OT security. The process begins with the Planning Phase, establishing a solid foundation through in-depth network assessments and gap analyses. These assessments identify critical vulnerabilities and set the stage for enhancing the OT security posture. Building on these insights, the Build Phase focuses on Solution Design and Planning. This phase includes crafting a robust network architecture and a detailed project governance structure to ensure a comprehensive approach.

Moreover, an overall strategy, a strong security architecture and a secure network topology are planned to ensure alignment with NIS2 compliance and a holistic security solution, encapsulating Detection of IT/OT Convergence, Remote Access, Information and Event Management, and Vulnerability Response mechanisms. The Light House Phase then follows, allowing for controlled testing and validation of the security solutions in a real-world environment before broader deployment. This phase is crucial for fine-tuning the solution and meeting all operational requirements.

Finally, as discussed in the preceding sections, the Global Rollout extends the validated solutions across all relevant sites. This phase ensures consistency in deployment while accommodating each location's unique requirements. The framework ensures that security measures are integrated into OT environments by combining real-time monitoring, hypercare support, and continuous feedback mechanisms.

Final Thoughts & Outlook

OT security requires more than technical fixes; it demands changes in organizational behavior and governance. Deloitte's framework embeds security practices into daily operations, reducing risks, protecting critical infrastructure, and ensuring continuous operation amid growing cyber threats. The framework evolves to address new threats while aligning with organizational goals. It promotes a zero-incident culture by increasing security awareness at all levels. Adopting the Deloitte 360° OT Security Framework helps companies significantly reduce risk and protect OT assets long-term. As OT environments integrate advanced technologies, security challenges will increase. The final phase of this series will focus on Operation and Support, covering monitoring, performance evaluations, and incident management. This phase is crucial for maintaining resilient OT systems and aligning with industry standards.

Partnering for Success

Deloitte's dedicated OT security specialists collaborate with organizations to enhance security posture. Leveraging the proven methodologies and best practices outlined in this whitepaper, Deloitte offers a suite of end-to-end services tailored to implement the **Deloitte 360° OT Security Framework** and achieve industry-specific security objectives. By adopting a **"Protect - Detect - Respond - Prevent"** approach, the focus shifts from reacting to incidents to proactively preventing them, ensuring maximum factory uptime. By embracing this approach, organizations can significantly reduce the likelihood and impact of incidents. The framework ensures compliance with regulations like **NIS2** and enhances operational resilience by minimizing downtime caused by security breaches. Through collaborative efforts, a resilient security culture empowers organizations to thrive amid ever-evolving cyber threats, maintain uninterrupted operations, and protect revenue streams.

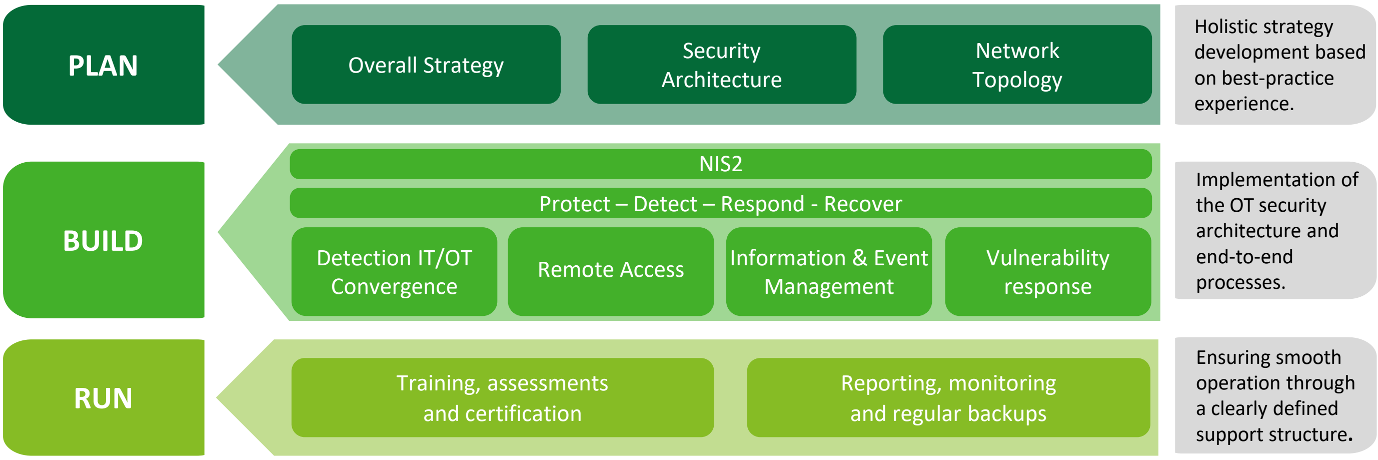

PLAN
Overall Strategy
Security Architecture
Network Topology
Holistic strategy development based on best-practice experience.
BUILD
NIS2
Protect – Detect – Respond - Recover
Detection IT/OT Convergence
Remote Access
Information & Event Management
Vulnerability response
Implementation of the OT security architecture and end-to-end processes.
RUN
Training, assessments and certification
Reporting, monitoring and regular backups
Ensuring smooth operation through a clearly defined support structure.

Figure 7: Deloitte´s 360° Security Framework

Contacts

Kai-Uwe Hess
Partner I Smart Manufacturing
+4915118294406
kahess@deloitte.de

Chris Fangmann
Director I Managed Shop Floor IT/OT
+4915154484240
cfangmann@deloitte.de

Christian Hess
Manager I Managed Shop Floor IT/OT
+4915140678446
chrihess@deloitte.de

Deloitte.

"Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (DTTL), its global network of member firms, and their related entities (collectively, the "Deloitte organization"). DTTL (also referred to as "Deloitte Global") and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/de/UeberUns to learn more.

Deloitte provides industry-leading audit and assurance, tax and legal, consulting, financial advisory, and risk advisory services to nearly 90% of the Fortune Global 500® and thousands of private companies. Legal advisory services in Germany are provided by Deloitte Legal. Our people deliver measurable and lasting results that help reinforce public trust in capital markets, enable clients to transform and thrive, and lead the way toward a stronger economy, a more equitable society and a sustainable world. Building on its 175-plus year history, Deloitte spans more than 150 countries and territories. Learn how Deloitte's approximately 457,000 people worldwide make an impact that matters at www.deloitte.com/de.

This communication contains general information only, and none of Deloitte Consulting GmbH or Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms or their related entities (collectively, the "Deloitte organization") is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities."

Designed by CoReCreative Services. RITM1870277