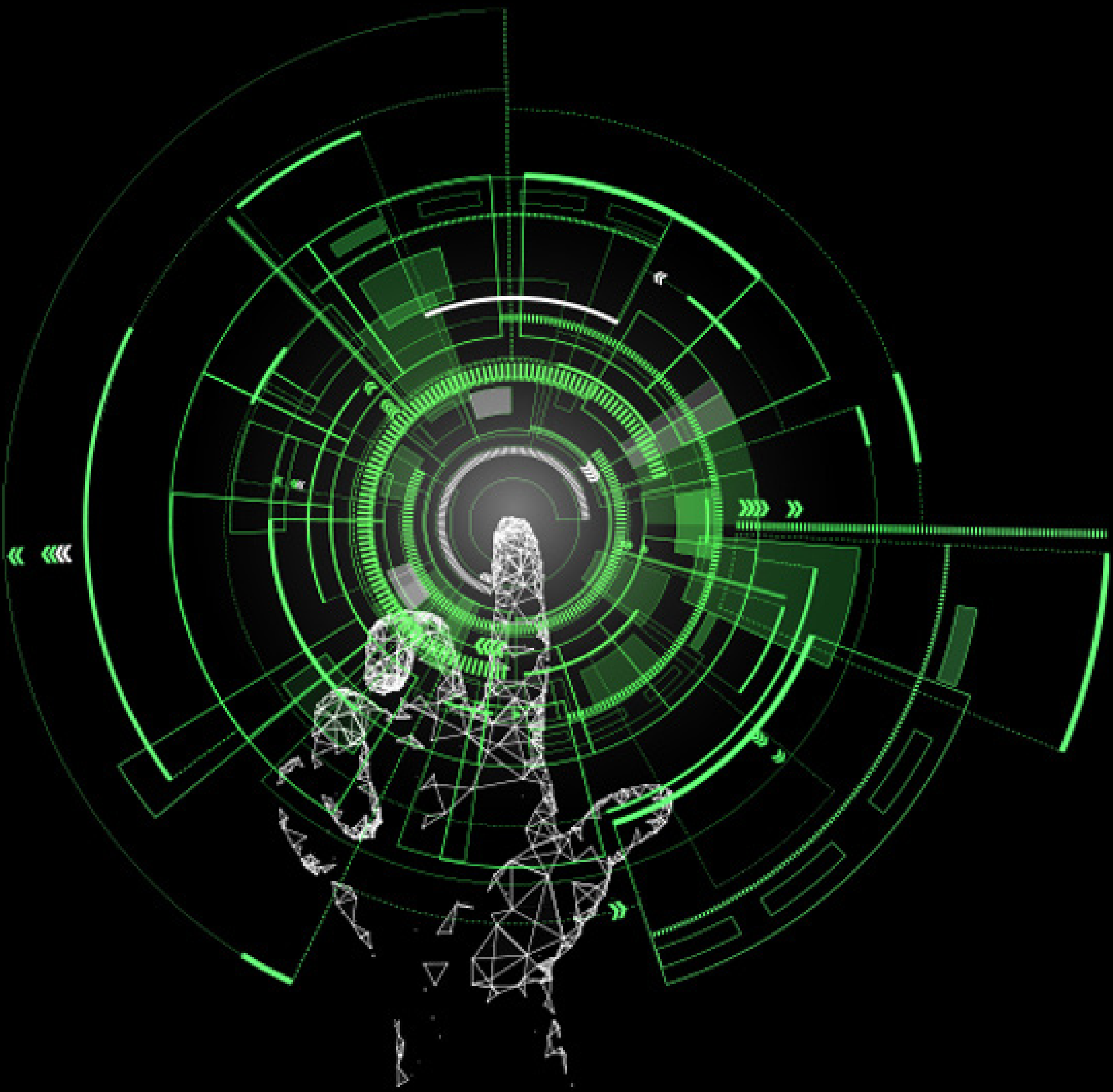
Deloitte.



360° OT Security

Towards a Zero-incident Culture

April 2024

MAKING AN IMPACT THAT MATTERS since 1845

Introduction to the current state of OT Security

With the rising acceptance of Industry 4.0, the landscape of the manufacturing industry has been shifting to accommodate emerging digital technologies

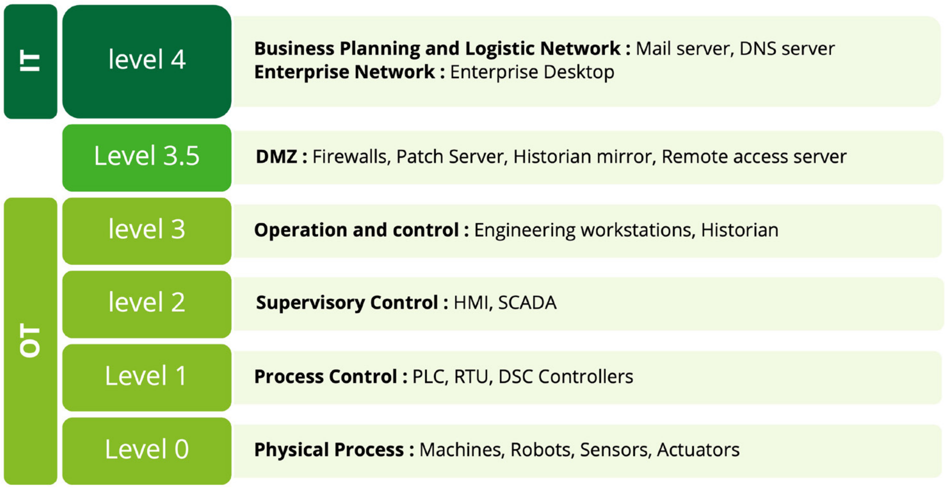
While Industry 4.0 promises a smarter, more automated future for manufacturing, it also presents a challenge for Operational Technology (OT) security, which is struggling to keep pace with the evolving threat landscape. Furthermore, manufacturers encounter the challenge of increasing costs of material and energy, demographic shifts, limited skilled workers, and stringent legal and regulatory requirements.

These challenges are further on amplified with frequent cyber-attacks in industrial OT environments, posing a delicate balance for companies: integrating digital technologies while ensuring cyber resilience. Many businesses often fail to prioritize security measures due to insufficient regulations and a reluctance to dedicate necessary resources towards OT security. This lack of security consideration during technological transitions increases the vulnerability to potential security threats. This paper aims to cast a lens on the critical need for OT security in an era of interconnectedness and increasing cyber threats.

OT Security and its importance in todays interconnected world

OT has become the foundation of many critical sectors in the interconnected industrial world, including manufacturing, healthcare, energy, and transportation. OT systems are becoming increasingly integrated with the IT infrastructure. While it unlocks significant value by enhancing efficiency and data analysis, it also exposes organizations to a complex and ever-evolving cybersecurity landscape. Regardless of progress with IoT in manufacturing areas, cybersecurity threats persist and are intensifying, with a significant number of organizations reporting breaches within the past years. This increasing vulnerability reinforces the importance of enhancing security measures across global OT infrastructures.

Furthermore, the rise in various malicious activities such as ransomware attacks, malware intrusions, and phishing incidents adds to this issue. The situation further darkens with predictions from Gartner, which highlight the potential hazards to humans in manufacturing environment resulting from increased, targeted OT cyberattacks by 2025 (Gartner, 2023). These threats require the development of robust strategies, focusing not just on protecting information, but on safeguarding human life and the environment. The cybersecurity threats pose serious financial implications extending to billions, making it an issue of concern not just for the CTOs, but for the CEOs as well. This escalating commitment shows the significance of OT Security in organizational strategies and highlight the importance of continuous advancements in practices to counter growing risk.



IT

level 4 — **Business Planning and Logistic Network :** Mail server, DNS server
Enterprise Network : Enterprise Desktop

Level 3.5 — **DMZ :** Firewalls, Patch Server, Historian mirror, Remote access server

OT

level 3 — **Operation and control :** Engineering workstations, Historian

level 2 — **Supervisory Control :** HMI, SCADA

Level 1 — **Process Control :** PLC, RTU, DSC Controllers

Level 0 — **Physical Process :** Machines, Robots, Sensors, Actuators

Figure 1: IT / OT Security Purdue Model

Potential impact of successful breaches in OT environment

In Manufacturing Industries, it's crucial for safety and risk management leaders to prioritize the physical dangers to people and the environment than focusing on data theft. Organizations are encouraged to reflect on past experiences involving both cyber and non-cyber incidents which led to loss of control, power, feed supply, or capacity, along with major equipment breakdowns, to better understand the potential impacts of OT breaches.

The consequences extend beyond financial loss, including system damage or unavailability, corrupted data files, data leaks, or notified malicious intrusions. This can lead to a production stop or even create faulty parts without detecting those.

Economic impacts potentially affect financial losses, while social consequences can vary, starting from impacting the public on a smaller scale up to causing major disturbances or changes in the society. Reputational impact could lead to potential negative publicity. Physical impacts are also a significant concern since it involves potential harm to employees, patients, or customers. Psychological impacts might cause confusion, discomfort, frustration, worry, or anxiety among the group of people affected by these breaches (e.g., company employees, customers, etc.) Furthermore, the environment is not exempted from the potential impact of these breaches, necessitating careful considerations.

Evolving threat landscape in OT environment

The manual detection, analysis, and mitigation of threats becomes challenging and can also result in unidentifiable devices and unauthorized access. In 2023, approximately 38.6% of ICS computers globally experienced attacks. (Kaspersky, 2024) Ransomware is becoming a major threat to security, causing production downtime and product delivery interruptions in one out of six attacks. Surprisingly, 72% of these attacks targeted the manufacturing sectors which is alarming (Dragos, 2023).

In addition to those recent geopolitical conflicts, such as the Russia-Ukraine and Israel-Gaza conflicts, have led to the prevalence of cyber-attacks. Hacktivism, characterized by politically or ideologically motivated hacking and cybercrime, has increasingly disrupted operations and leaked sensitive data. This trend is anticipated to escalate in 2024. According to Kaspersky's findings, sectors critical to economic security, such as manufacturing, energy, oil, and gas companies, are increasingly becoming targets of cyber-attacks. These industries serve as the foundation for both individual countries and political alliances, making them lucrative targets for malicious actors seeking to disrupt economic stability and strategic interests (Kaspersky, 2024).

Real world OT incidences in past years

To emphasize the relevance of OT Security some OT incidents from the last years will be listed below.

In 2021, the Colonial Pipeline cyberattack resulted in a five-day shutdown of gas and oil transmission and sales. In 2022, a cyberattack against Deutsche Wind Technik, a leading German wind energy company, caused that company to shut down the remote systems controlling 2000 wind turbines for nearly 24 hours. Nordex SE, a turbine producer, announced a ransomware attack in March that caused an IT shutdown. Another turbine maker, Enercon GmbH, was also impacted in 2022 by an attack that took nearly 6000 turbines offline.

In February 2022, an attack on Toyota Motor parts and components supplier Kojima Industries forced the automaker to suspend operations in 28 production lines across 14 plants in Japan for at least a day. The impact from the attack – which also affected Hino and Daihatsu Motors - was massive, with Toyota announcing that it had to temporarily reduce production by 5% or 13,000 units - a third of its global output. This clearly demonstrates the importance of automotive cybersecurity to ensure operational continuity.

Global Ransomeware Incident 2023

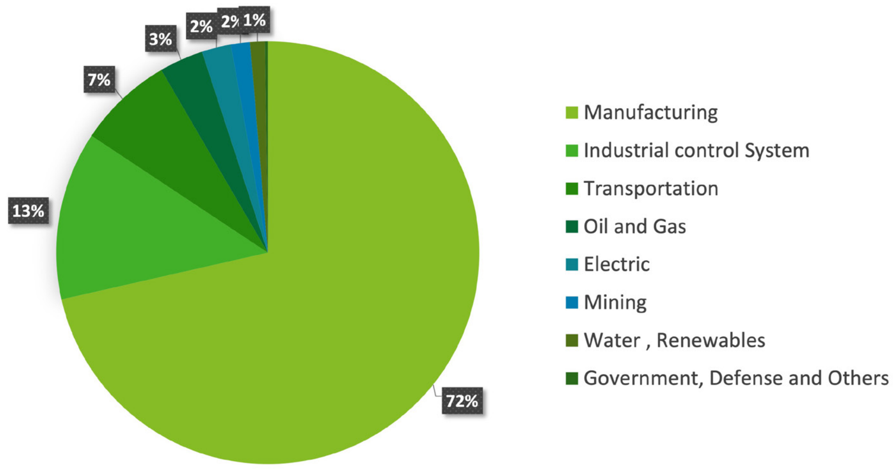


Figure 2: Ransomware incidents by sectors, 2023 as per the Dragos OT Cybersecurity, year in review 2023 report. (Dragos, 2023)

In summer 2022 global building supply manufacturer Knauf was battling the fallout from a cyberattack it suffered. To isolate the attack, Knauf's IT team had to shut down all operations across its businesses globally. (Top Cyber Attacks of 2022 by Sector, 2022)

In 2023, Cloros, an American goods manufacturer, faced a breach that impacted automated systems. Additionally, Brunswick was targeted by a cyber-attack that disrupted its operations for nine days and cost $85 million. Moreover, a supply chain ransomware attack was launched on Applied Materials, a semiconductor technology provider, in February. These incidents underscore the wide-ranging and lasting impact of such cyber-attacks. (Artic Wolf, 2024)

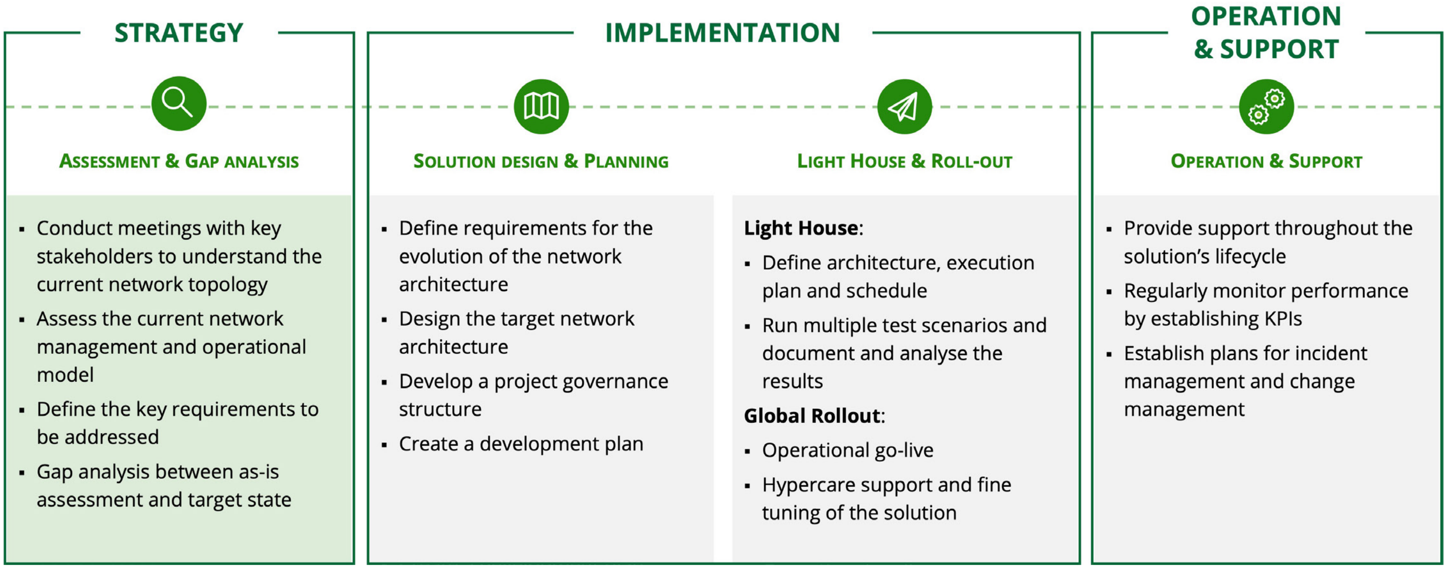
OT Security with NIS2

To cope with this trend of increasing cyber-attacks, political institutions have passed new regulatory directives, such as the NIS2 (Network and Information Security Directive). The NIS 2, a directive of measures for a high common level of cybersecurity, extends the cybersecurity requirements and sanctions to harmonize and improve the level of security in the European member states and includes stricter requirements for different sectors.

Companies falling under the essential company's category of NIS2 then strict security measures before October 2024. NIS2 is set to have a significant impact on OT environments by introducing stringent cybersecurity standards and broadening the scope of affected sectors. To meet these new regulations, companies must implement robust security protocols, establish incident reporting procedures, mitigate supply chain risks, and enhance resilience to cyberattacks. However, most industrial companies are still struggling to keep pace with these security requirements in their digital transformation. (Nomis, 2023)

Deloitte 360° OT Security Framework

A new world full of challenges and opportunities lies ahead of us. Long-year experienced experts have worked together to develop this OT Security Framework to overcome the industry challenges and help clients to take advantage of the industry new opportunities.



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 Rollout:

- 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

Concept of 360° OT Security:

In collaboration with our partners and clients, Deloitte has developed an appropriate end-to-end OT security model using trusted building blocks, suitable processes, reliable vendors, and a thorough implementation roadmap. The primary goal of our approach is empowering our clients to not only identify potential risks but also detect, evaluate and solve threats.

Furthermore, we clutch tightly onto the reassurance of asset operation protection in case of emergencies, fortified with a robust disaster recovery plan. We have crafted an in-depth concept for 360° OT security.

Deloitte recognizes that no organization has unlimited resources to dedicate to cybersecurity. Therefore, it is important that organizations prioritize those cybersecurity capabilities that will contribute most to their overall cyber resilience. The 360° OT Security Framework is the result of multiple years of best practice experience and incorporates a proven methodology to determine current and target maturity of an organization's cyber capabilities and design a roadmap to increase the organization's overall cyber resilience to internal and external threats. The framework also includes content packs, which enable maturity assessments to be conducted against a range of industry standards (as for example the NIS2, ISO/IEC 27001, the NIST Cybersecurity Framework, etc.).

The framework is divided into Strategy, Implementation, and Operation and Support. Within the **strategy** phase the goal is to assess the as-is state in order to build a vision for the future target state which is in line with the overall corporate strategy and provides the most value for the organization. Then, in the **implementation** part the solution will be designed, and the development plan created. Once that is done, it is time for the light house phase and subsequent rollouts of the solution. Finally, once the solution is deployed, **support** throughout the solution´s lifecycle is provided.

1. Strategy

The Strategy phase lays the groundwork for a secure OT future by providing a comprehensive assessment and gap analysis of the OT environment

Network Assessment & Gap Analysis

The Network Assessment & Gap Analysis forms the critical foundation for strengthening the OT security posture. By working with strong partners, we can provide our clients an assessment methodology that ends with the delivery of a network assessment report.

This process starts by clearly defining the IT/OT environment in scope for the assessment. Understanding the current network topology, deployed technologies, and identifying key stakeholders across IT and OT teams is crucial.

Information gathering then takes center stage. This involve sharing assessment questionnaires to IT/OT teams, conducting on-site visits, and holding meetings to delve deeper into network specifics, collect data, and identify potential pain points. Once the data is collected, a thorough analysis is conducted. This analysis culminates in a **comprehensive network assessment report** that details the current state of the OT environment.

The next step involves defining the key security requirements for the desired target state, which reflects the ideal security posture aimed to achieve. Finally, by comparing the findings from the as-is assessment with the defined target state, a gap analysis is performed. The identified gaps will inform the development of a remediation plan to bridge the gap and achieve the OT security objectives.

Moments that matter

Using our templates and automation tools, we can speed up the process of gathering information and create a report with key findings and recommendations about the network.

2. Implementation

Solution Design & Planning

Following the network assessment and gap analysis, it's time to translate insights into action. Solution Design and Planning bridges the gap between identifying security needs and achieving your desired OT security posture.

> By carefully planning and designing your solution, you lay the groundwork for a **successful OT security implementation.**

This phase starts with defining clear principles and requirements for the evolution of the network architecture that address the identified gaps. With a strong foundation in place, the target network architecture is designed. Then, a robust project governance structure is established to ensure successful implementation. This structure outlines clear decision-making processes and defines roles and responsibilities for all stakeholders.

Finally, a comprehensive development plan that details the timeframe for implementation, identifies the resources required, and outlines the skillsets needed is created.

Light House Phase & Rollout

Before diving into full deployment and rollout, the Light House Phase helps validate the solution. It involves, crafting a execution plan with a clear schedule, and then running multiple test scenarios and document and analyze the results. The Light House validates whether the prototype aligns with the technical guidelines, giving our client confidence before a full-scale implementation.

Following the Light House phase, the **Rollout** involves the operational go-live according to acceptance criteria. It also includes training, providing hyper-care support and fine tuning of the solution.

3. Operation & Support

Deloitte offer operation and support services for the solutions implemented in the network, this way ensuring a stable operation and optimized performance across all sites.

This phase provides comprehensive support throughout the solution's lifecycle, encompassing design, deployment, testing and verification, and even optimization.

Regular performance monitoring is a critical part. By establishing key performance indicators (KPIs), the effectiveness of the security solution can be measured and areas for improvement can be identified. Furthermore, proactive planning is key. Establishing well-defined **incident management** and **change management Plans** plans ensure a coordinated response to incidents and minimizes disruption during planned network changes.

This holistic approach ensures that the OT network remains secure and optimized over the long term.

> A secure OT network doesn't operate in isolation. **Ongoing operation and support** are essential to maintain a strong security posture.

Objectives

OPERATION

- Provide device management services for stable operation
- Monitor and manage systems and devices for uptime
- Update software remotely in regular intervals and conduct health checks

SUPPORT

- Provide support services to ordered products for stable operation
- Categorize service requests and assign it to dedicated level of support within agreed SLA
- Regularly develop status reports

Strategy: Towards a Zero-incident Culture

Throughout the entire journey our framework underscores the significance of cultural factors aiming to emphasize awareness towards OT Security within the organization in order to establish a zero-incident culture.

For years, companies have developed their Information Technology (IT) and Operational Technology (OT) departments as silos, leading to unclear governance and inefficient processes. With the growth of disruptive technologies like the Internet of Things (IoT) an overlap between the two departments is being created. This gap is supported by increased computing power, high speed internet connectivity and the proliferation of "smart" devices. This convergence of IT and OT is often referred to as the fourth industrial revolution.

However, this overlap between IT and OT has also led to new challenges. In this chapter we will focus on the Security Challenges, being more specific, on the key components of a OT Security Strategy.

A robust OT security strategy goes beyond simply deploying security tools. It integrates **people, processes, and technology.** Below are the key components to consider for a 360° OT Security Framework.

Assessment & Fit-Gap Analysis

Gaining a comprehensive understanding of the current state of cybersecurity within the operational technology (OT) environment is crucial before embarking on the journey towards a zero-incident culture.

High-Level Assessment

Deloitte in collaboration with leading OT cybersecurity solution providers, provides a three-week assessment methodology that results in delivering a high-level network assessment report. Deloitte proposes an assessment methodology made up of 4 phases:

1. **Kick-Off** – Determination of the IT/OT environment in scope for the network assessment and stakeholders identification.
2. **Data gathering** – Sites information is collected through activities and workshops with the IT/OT teams, as well as through the completion of questionnaires.
3. **Automated Network Scan** – An automatic network scan is conducted on strategic network locations, by deployment of state of art data acquisition sensors in collaboration with partner solution providers.
4. **Final Report** – A final report is created based on the data collected from the high-level assessment. This report serves as a baseline to initiate further discussion and activities as part of the subsequent fit-gap analysis stage.

Fit-Gap-Analysis

The fit gap analysis is crucial to bridge the gap between the current state, based on the high-level assessment, and the target state. For doing so, Deloitte conducts workshops, interviews, and advanced network scans to pinpoint gaps between the current and the desired state. This part results in a list of specific needs and recommendations, forming the groundwork for designing a solution that gets the client closer to a zero-incident security culture. The necessary steps that Deloitte proposes to achieve the objective are the following:

1. Kick-Off workshop with stakeholders to clarify schedules, resource needs, and factory-specific requirements; establish ongoing communication with IT/OT teams.
2. Review factory layout, document equipment details, analyze software/network structure, study data flows, review security measures, interview staff, and identify pain points.
3. Install and configure additional network data acquisition sensors to identify OT components via network traffic, passively monitor network activities, log anomalies/incidents, and supplement missing data.

Develop actionable recommendations, gather evaluated network documentation, develop a list of recommendations for action, gather documentation on the evaluated network.

In this context, it is important to consider the Corporate Strategy in order to define an OT Security Strategy that is in line with the overall vision to ensure consistency.

One of the most important aspects of the Cyber Strategy Framework is Change Management. Managing change is challenging due to the heterogenous system landscape, a multitude of stakeholders and a completely different culture compared to IT.

Processes, People and Culture

A thorough understanding of the as-is state is necessary therefore – not only documented processes, but also the day-to-day footprints need to be considered. Next to the processes different hierarchies exist in manufacturing environments. The most obvious one is the organizational hierarchy that is officially documented in an organigram and hence executed in shop floor management. Next to this explicit hierarchy unofficial ones exist, like in technical, but also organizational leadership. People that are widely respected by most colleagues act like ambassadors. Their behavior gets copied by most employees, and once those "hidden champions" of a company are convinced of a new method, process or tool, more and more people start following them.

> "The most important part of a strategy is the fact, that it is being **supported by more than 80%** of the employees of a company. Only then it can lead towards a true zero-incident culture."

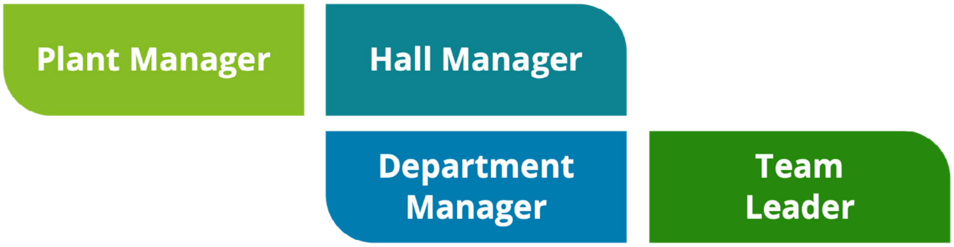


Figure 3: Key Stakeholders

Hence the most efficient way of introducing digital innovation is via convincing ambassadors, besides offering true benefits and additional value to the employees as well as a high usability. An in-depth understanding today's processes and tool surfaces is necessary therefore.

Our approach is to develop a target state together with the most relevant personnel of a factory, at first formulating "if-sentences". One example therefore could be "we are successful if we can solve incidents in less than 30 minutes time". Having a common goal ensures the performance of a project since everybody feels committed and is interested in shaping this future together. Once the technical setup is done, standardized routines like a security feature in the daily shop floor meetings help pushing OT security into the organization.

When shop floor tools offer exceptional usability, supporting the process becomes more appealing, naturally attracting greater employee participation. A good example is opening the tool in the shop floor meetings through plant leaders or ambassadors using the tool frequently and letting other people watch how to use it on their monitors.

Education & Awareness

Educating and empowering the staff is crucial for a successful OT security strategy. This involves regular security awareness training that equips employees with the knowledge to identify cyber threats and best practices for secure OT operations. Furthermore, establishing security requirements for OT vendors and selecting those with strong security practices ensures a holistic approach to OT security .

> "The most important part of a strategy is the fact, that it is being **supported by more than 80%** of the employees of a company. Only then it can lead towards a true zero-incident culture."

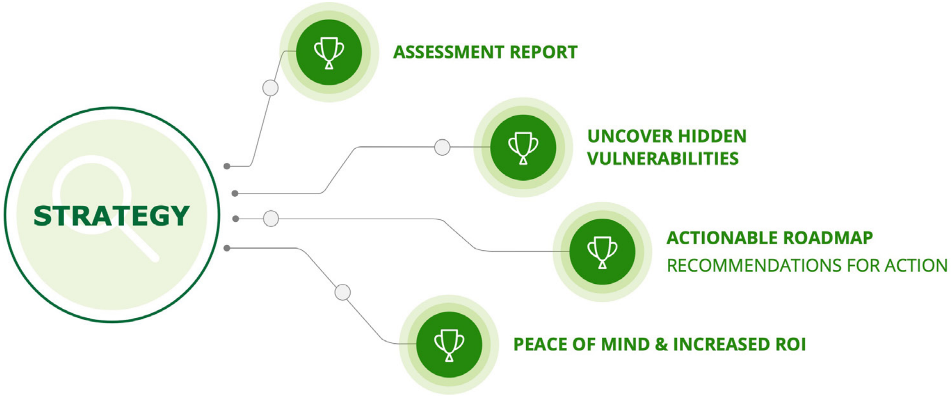

STRATEGY
ASSESSMENT REPORT
UNCOVER HIDDEN VULNERABILITIES
ACTIONABLE ROADMAP
RECOMMENDATIONS FOR ACTION
PEACE OF MIND & INCREASED ROI

Figure 4: Strategy key elements

Conclusion

This whitepaper has introduced the Deloitte 360° OT Security Framework, and the comprehensive strategy that we have designed to empower our clients to achieve a zero-incident security culture

The ever-evolving threat landscape demands a comprehensive and proactive approach to OT security. This whitepaper has introduced the 360° OT Security Framework, a holistic strategy designed to empower Deloitte clients to safeguard their critical infrastructure.

By following and implementing our three-step Security Framework, outlined in Chapter 2, our clients will be able to establish a robust defense against cyber threats. The Strategy phase, explored in Chapter 3, offers a crucial first step, providing a clear understanding of the current security posture and a prioritized roadmap for improvement.

Keep in mind that cultivating a zero-incident culture is an ongoing process, not a final destination. Encouraging cultural shifts means ensuring every individual is conscious and accountable for OT security, integrating this mindset into their daily tasks. Employees should no longer see OT security as an hurdle or obligatory task to perform but something to embody.

By embracing our 360° OT Security Framework and fostering a culture of security awareness within the organization, companies are able significantly reduce risk, ensure operational resilience, and protect the entire OT assets in the long term.

Beyond this whitepaper, our team of OT security specialists is here ready to partner with new clients in their security journey. We offer a range of services to help implement the 360° OT Security Framework and achieve the industry security objectives.

Contacts

Kai-Uwe Hess

Partner I Smart Manufacturing
Tel: +49 15118294406
Mobile: +49 151 1829 4406
kahess@deloitte.de

Chris Fangmann

Director I Managed Shop Floor IT/OT
Tel: +49 6211590161
Mobile: +49 151 5448 4240
cfangmann@deloitte.de

Christian Hess

Manager I Managed Shop Floor IT/OT
Tel: +4969971375279
Mobile: +4915140678446
chrihess@deloitte.de

Deloitte.

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. RITM1728477