Catalogue v. 1.0

Advisory Services from Omny

Bringing your industrial cybersecurity plan to life

PUBLIC

omnysecurity.com

Solution

Brief

Table of Contents

Overview of Omny Advisory Services

Enhance your security posture and protect your physical and digital assets by leveraging the strategic advantage provided by Omny Advisory Services. Feel supported by top industrial, security, and threat intelligence professionals back by advanced assessment technology. With limited disruption to your existing systems, the Omny team can help assess and design unique plans for your physical and operational security needs.

Supported by technology

Omny Risk, our advanced software solution, plays a crucial role in enhancing the capabilities of our Advisory Services team. By leveraging the power of technology, Omny Risk enables us to effectively quantify risk by analyzing both public and company-related knowledge. Acting as a strategic partner, Omny Risk provides valuable insights and a comprehensive overview of potential threats to your sites and assets. With this intuitive interface, our Advisory Services team can quickly assess the effectiveness of various mitigations and determine the most suitable course of action. By utilizing Omny Risk, we empower our team to deliver efficient and informed risk management strategies, enhancing the protection and resilience of your organization.

Advisory services at a glance

Cyber Threat Assessments

Tailored cyber threat intelligence modeling based on knowledge of at-risk assets, exploited vulnerabilities, and the impact on operational technology (OT), as well as planning readiness exercises for your own OT infrastructure.

Security Risk Assessments

A comprehensive evaluation that aims to continuously identify risks within your company, technology, and processes, ensuring the presence of adequate controls to mitigate security threats.

Asset & Control Assessments

By comprehending the value and significance of each asset within your organization, the Omny team can assist you in effectively prioritizing the implementation of controls in your security process.

Business Continuity Assessments

Utilizing your company's strengths to address potential weaknesses in cybersecurity practices, Omny's objective is to promote business continuity and avoid a potential attack with the inevitable damage and downtime that results.

Business Impact Analysis

Omny helps you understand the potential impact of an attack and the resulting downtime. We can then design the foundation for making informed investments in prevention and mitigation strategies.

OT Architecture Security

Let us review and restructure your IT and OT security architecture. We take your unique business context into account in order to maintain the integrity of your security posture.

Advisory to the IEC 62443 Series of Standards

Allow Omny to assist with the digitalization of your organization and the alignment of your organization with the IEC 62443 international cybersecurity standards for industrial businesses. Including both technical and process-related cybersecurity practices, your business can improve internal standards and guide the implementation of these standards across your entire organization.

IEC 62443 Security Level GAP Analysis

Identify the gaps or discrepancies between where your organization's cybersecurity practices currently stand and where you would like for them to be in accordance with the IEC 62443 standards.

IEC 62443 Risk Assessment

We define the scope, establish security level targets, and identify high-risk areas for a full cyber analysis; allowing for the quick determination of high risk areas and facilitating the creation of an effective risk strategy throughout your organization.

IEC 62443 CSMS Security Advisory

Providing guidance for a Cyber Security Management System, or CSMS. Omny provides an all-encompassing range of practices and actions designed to address cyber risks and establish appropriate countermeasures.

IEC 62443 CSMS Maturity Assessment

Let Omny assist in prioritizing your security enhancements based on your specific requirements. We help to find a proper fit, suggest financial investments, and promote the collaboration between business and technical stakeholders.

Our Expertise

Karl Bernhoff Binde

Director, Advisory

Binde is a security specialist and former Head of Security Architecture at Ernst & Young (EY). With a masters in Communication Technology from NTNU, his career as a security analyst spans from OT Security Architect to Risk Manager.

Certifications:

SABSA Chartered Security Architect (SCF), ISO27001 & ISO27701 Lead Implementer, ITIL 4 Foundation, Prince2.

Rajesh Kenge

OT Specialist

Kenge is an OT specialist with broad experience in cybersecurity and network infrastructure for OT networks. With more than 25 years experience, he comes to Omny as a former Cybersecurity Manager at Honeywell.

Certifications:

CCIE, Nozomi, CCNA R&S, CCNA Security, Certified Ethical Hacker v8, Docker Certified Associate.

Tommy Evensen

Director, Customer Success

Evensen is a cybersecurity evangelist with over twenty years of experience working in the IT/OT domain. He has held a breadth of strategic positions across the Oil & Gas industry and is an active member of the Norwegian Electrotechnical Committee (NEK).

Certifications:

ISA/IEC 62443, CCNP, GSTRT, GICSP

Audun Scheide

Delivery Manager and OT specialist

Scheide is a cybersecurity risk professional with expertise in both cybersecurity and business acumen. Specializing in the development of cutting-edge technology to promote business continuity and compliance in regulations like NIS2.

Certifications:

Prince2, Microsoft: Security, Compliance and Identity Fundamentals, ITIL, Scrum Master.

Expertise continued

Joachim Haugberg

Delivery Manager & OT Specialist

Haugberg is our delivery lead with extensive operational technology experience in the energy sector. He's held various roles in ABB delivering OT infrastructure throughout Norway and Europe.

Erik Haugvaldstad

Customer Success & Solutions Architect

Coming from a background in the energy industry, Haugvaldstad is currently interested in the inner workings of Data & AI, security, and DevSecML ops. As a Solution Architect for Omny, he is well-positioned to help companies understand their specific needs from a high level down to the technical expertise.

Srivathsan Desikan

Senior ICS Engineer

Desikan is a subject matter expert with almost two decades of experience working as an engineer in industrial organizations. He has an international perspective having worked with top companies around the world. He also has additional expertise in PLC, DCS, and SCADA packages.

Siri Johnsen

Senior Advisor & Threat Analyst

Johnsen's career spans over a decade between both private and public organizations. Her valuable breadth of experience in threat analysis, intelligence and societal security gives her a unique understanding of the dynamics of threats and risks into the operational technology (OT) domain.

Professional services in detail

Cyber Threat Assessments

A cyber threat assessment is a methodical examination of possible threats to your organization's OT and IT infrastructure. It entails the identification and analysis of potential risks with your own business context, including malware, hacking attempts, or data breaches, which may jeopardize the security and reliability of the organization's systems.

Omny provides tailored cyber threat intelligence modeling based on knowledge of at-risk assets, exploited vulnerabilities, and the impact on your operational technology (OT). We can also help in the planning of readiness exercises for your team in their own OT environment.

Why do this?

A cyber threat assessment helps a business understand their current security posture to then develop strategies for mitigation and prevention against cyber threats. An assessment is a fundamental component to understanding your risk and will enable the organization to build a robust cybersecurity risk management plan.

Professional services in detail

Security Risk Assessments

A security risk assessment involves identifying vulnerabilities within the IT ecosystem and assessing the financial risks they pose to the organization. These risks can range from potential downtime and associated profit-loss to legal expenses, compliance penalties, as well as customer churn and lost business. Conducting a thorough and comprehensive risk assessment enables you to effectively prioritize your security initiatives within your overarching cybersecurity program. With Omny, this assessment is a smooth process that takes a fraction of the usual time to complete. This is made possible through our technology, Omny Risk, which quickly helps to identify potential risks within your organization, technologies, and processes.

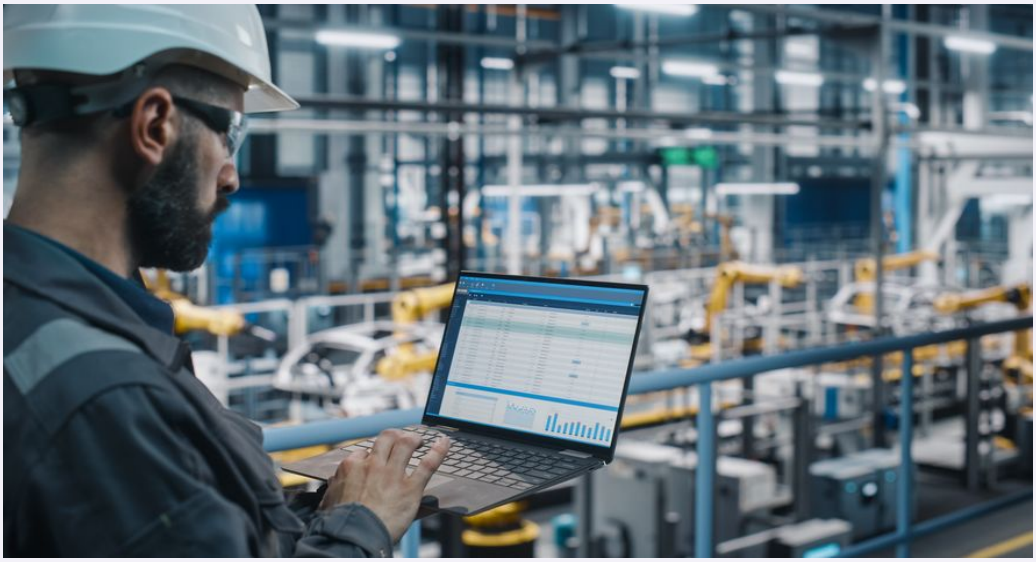
Why do this?

Security risk assessments are crucial for developing a comprehensive security management strategy. These assessments provide valuable insights into potential security threats and vulnerabilities, allowing businesses to mitigate risks and safeguard critical assets. Our assessments thoroughly evaluate all aspects of security systems, identifying and prioritizing vulnerabilities in order to implement effective security countermeasures.

Professional services in detail

Asset & Control Assessments

An asset and control assessment is a fundamental activity for reviewing company cybersecurity practices. It is crucial to understand and get an overview of the assets of the organization in order to be able to protect them. This involves identification, classification and evaluation of both assets and controls of your cybersecurity infrastructure. By leveraging our industry expertise, Omny's team will review and evaluate the state of your company's assets and controls. By comprehending the value and significance of each asset within your organization, the Omny team can assist you in effectively prioritizing the implementation of controls in your current and future security processes. The assessment will provide a strong foundation for further enhancing the security posture of your organization.



Why do this?

Modern organizations need insight into the values belonging to their assets and how those assets might be affected in the event of a cybersecurity incident. Without specific controls in place, that company could be vulnerable to an attack. This assessment is critical in the development of protective measures, ensuring the security and integrity of these assets and protecting your business

Professional services in detail

Cyber Maturity Assessments

A cyber maturity assessment evaluates an organization's level of readiness and effectiveness in managing cyber risks. It helps measure the organization's ability to prevent, detect, and respond to cyber threats. By assessing your cyber maturity, your business can better identify areas for improvement and develop strategies to enhance your overall cyber resilience.

Omny aligns with the Norwegian National Security Authority's (NSM) basic principles for information security. With these principles and our team competencies in the field, Omny can help evaluate your company’s own cybersecurity maturity.

Why do this?

A cyber maturity assessment from Omny offers valuable insights into your company’s cyber vulnerabilities. It can also help you to identify and prioritize areas for improvement, and demonstrates compliance with corporate and operational standards for now and in the future. Create strategic plans for your cybersecurity practices and create a plan for compliance.

Professional services in detail

Business Continuity Plan

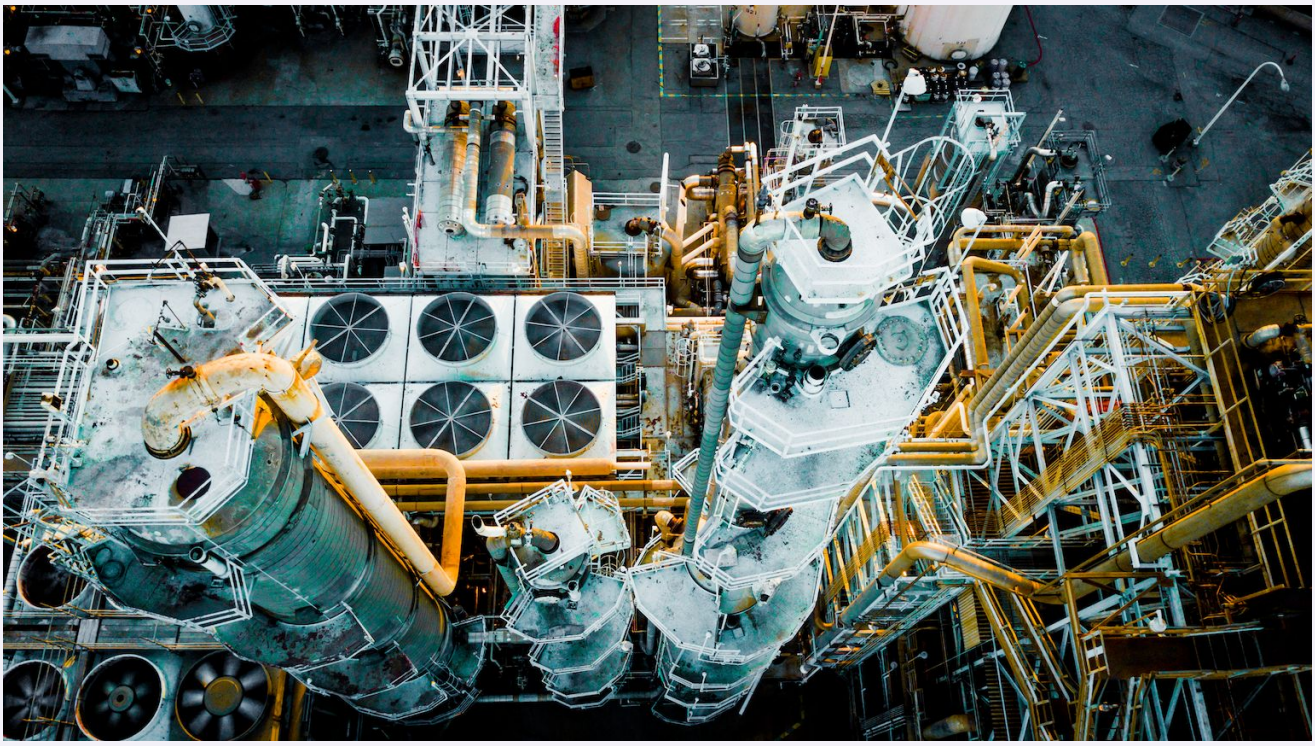
A business continuity plan involves a comprehensive evaluation of an organization's ability to continue its critical operations and services in the event of a disruption or major incident. It involves assessing various vulnerable aspects of the organization, including its processes, systems, resources, and dependencies, to identify vulnerabilities and gaps in its business continuity plans.

Why do this?

For those companies with critical infrastructure, it is important to perform a business continuity assessment to evaluate your preparedness and daily business continuation should an incident occur. Omny can help create this assessment to identify key operations and suggest preventive measures in the event of a security breach.

Business Impact Analysis

A business impact analysis (BIA) helps organizations identify and evaluate the potential effects of disruptions on their critical business operations. It involves assessing the impact of various incidents, such as natural disasters, technology failures, or security breaches, on key business functions, processes, and resources.



Why do this?

An analysis from Omny helps organizations prioritize their recovery efforts, develop effective business continuity plans, and allocate resources appropriately to minimize the impact of disruptions and promote the continuity of essential operations.

Security Awareness

From general employee security awareness, to continual security trainings, Omny is here to help your company strengthen its security culture and create leading practices from the executive offices to the factory floor. Security awareness training involves an entire organization to improve the understanding and behaviors of employees to recognize and respond appropriately to potential security threats, such as phishing emails, social engineering attacks, or data breaches.

Why do this?

By increasing security awareness, organizations can reduce the likelihood of security incidents and enhance overall cybersecurity posture. Employees are not only the first line of defense but they are also the weakest point of an organization. Therefore, take the time to make your greatest weakness, your greatest asset, with Security Awareness from Omny.

Professional services in detail

OT Network Architecture Assessment

OT Security Architecture is a comprehensive framework that provides a blueprint for the design, behavior, and management of secure systems that allows an organization to logically segregate the Process Control Network. This assessment starts with collecting an OT Asset inventory, reviewing the current architecture, and then proposing a segregated network architecture. Omny follows ICS/OT top practices and standards which are designed to be both manageable and scalable. Our proposed network architecture follows the principle of segmenting the OT network into zones based on risk and security requirements.

For example, assets in the same physical location, within the same Purdue Level, with similar security requirements, can be grouped in the same zone.

Why do this?

Combining a top-down and bottom-up approach allows security and compliance-requirements to be implemented and understood across the organization and infrastructure. By segregating your OT network architecture that incorporates OT/ICS leading practices (e.g. Purdue Model), your organization can form a solid base for the Zones and Conduits model. It provides a firm foundation for deploying proactive cybersecurity solutions in different zones based on their security requirements. Omny can help you gain control and manage access to your different network zones while helping to reduce your company’s attack surface.

IEC 62443 Security Level GAP Analysis

A GAP Analysis is elementary for companies who wish to improve their security standing. It is important to first determine your current security posture to better understand how far you will need to go to reach the IEC 62443 Standard. By conducting an IEC 62443 Security Level GAP Analysis with Omny, organizations can identify weaknesses in between their Industrial Control System (ICS) and their operational technology (OT) security systems to then take proactive measures to enhance their cybersecurity defenses, reduce risks, and protect critical industrial processes and assets. Omny advisors will use the specific security requirements outlined in the IEC 62443 standards to determine with are applicable to your organization and determine any gaps or deficiencies in the organization's current security posture and highlights areas that need improvement to align with the desired security levels.

Omny Advisors will assess, compare, prioritize, plan and implement a plan to fill the gap left between IEC 62443 Standards and your company's current security posture.

IEC 62443 Risk Assessment

Different from a regular risk assessment, the IEC 62443 Risk Assessment was specifically designed to adhere to the guidelines created for protection of cybersecurity of industrial automation and control systems. By conducting this assessment, Omny can help organizations gain a comprehensive understanding of the potential vulnerabilities within their own ICS/OT environment under a standardized set of practices. Omny can also help your organization use the information from this assessment to create a formal plan to place new security measures, prioritize resources, and make secure informed decisions to help protect your infrastructure from cyber threats.

IEC 62443 CSMS Security Advisory

A Cybersecurity Management System or, CSMS, refers to a company's environment behind their information and data collection systems. Your CSMS will help govern the individuals responsible, implementation timing, and the necessary actions to encourage consistent security protocols.

When considering the cyber vulnerabilities behind a CSMS, the Omny team would explore your systems and process, become familiar with how they are interconnected with one another and also with existing industrial infrastructure. We would then help to either create secure practices and culture or would adjust existing practices. The specifics of this type of advisory would depend on the organization, industry, and the current threat landscape.

Let Omny take the time to find and understand all potential risks and take steps toward mitigating them. Allow us create actionable information for your organization in order to enhance your cybersecurity posture and continuously protect against potential threats.

IEC 62443 CSMS Maturity Assessment

A maturity assessment is understood as a comparison of your current systems and practices against the IEC 62443 set of standards to use as a guide for improvement. These can be especially helpful when considering your cybersecurity systems and understanding what your company needs to be secure or compliant. This maturity assessment of your cybersecurity management systems would use IEC 62443 as a benchmark to determine where your company is and should aim to be. The Omny team will take the time to evaluate your systems and create a guide for how to improve your systems to enforce cyber resilience.

With a Maturity Assessment from Omny, prioritize your security investments, develop a roadmap for security improvements, and align your security strategy with your business objectives. Find processes, tools, and machinery to improve your security company-wide. Make your business more resilient and close the security divide between what you have and where you want to be.

Technology to power advisory services

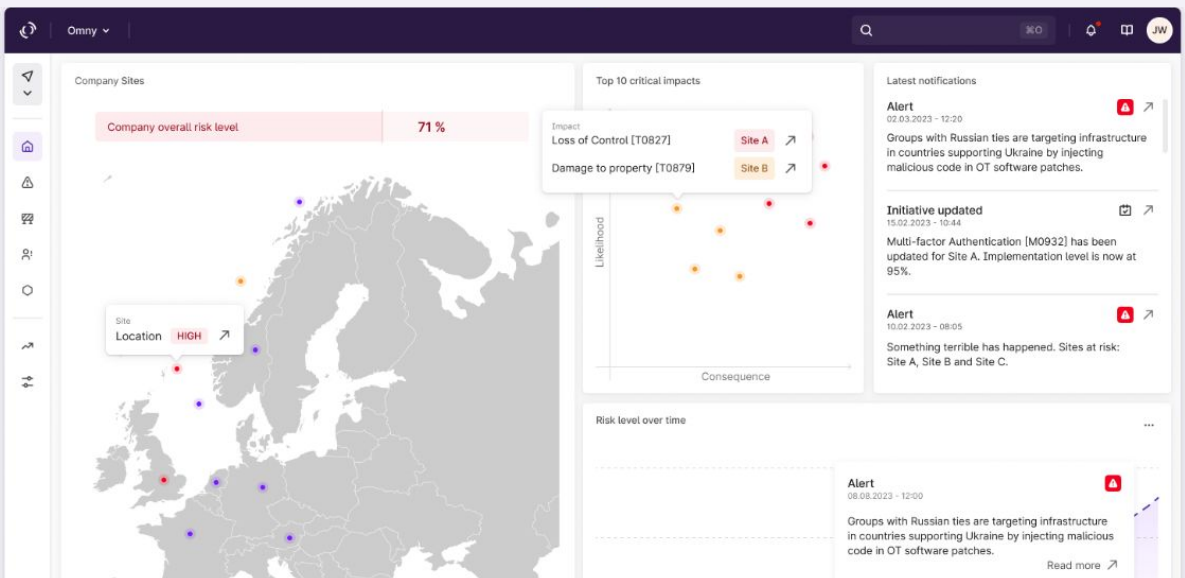
In addition to our team of OT (operational technology) security experts, Omny backs up our assessments with a quantifiable risk picture.

Omny Risk

At Omny, we decided to revisit the separation of product solutions and people solutions. While there is no replacement for the services and knowledge that people can provide, products are there to create efficiency and produce insight. That insight cannot be valuable, however, with action, and action is taken by people.

We like to combine the expertise of people with a product that can provide quantitative values from complex and varied data across several systems in a matter of seconds. Our winning combination allows our advisors to more quickly understand your company's risk position and posture.

Omny Risk, a risk management solution on the Omny Platform provides a more accurate and relevant view of your organization's risk posture, thereby allowing you to quickly and easily identify patterns, relationships, and potential vulnerabilities in your critical systems.



About Omny

Omny is on a mission to make sense of increasingly complex threats to society's most critical infrastructure. Our software leverages the latest advancements in data science and technology to mitigate these threats. Born from the industry and built on domain expertise, Omny is positioned to help companies face their cyber challenges. Omny has an international vision with its headquarters in Oslo, Norway and an additional office in Stavanger, Norway.

To learn more about our products and services, we can be reached at info@omnysecurity.com.

omny