IBM Consulting
Cybersecurity Services

Keep your business more secure with OT security solutions

Operational technology (OT) security solutions from IBM Consulting help protect your business

Highlights

Establishes effective OT cybersecurity governance and risk management

Improves OT infrastructure visibility

Protects OT networks from unauthorized access and threats

Monitors the OT environment for threats

Responds effectively to cyberincidents

The importance of operational technology (OT) security in today's Fourth Industrial Revolution (Industry 4.0) cannot be overstated. As companies embark on their digital transformation journey, industrial control systems (ICS) and other OT systems become more intertwined with corporate networks and the internet. As a result, their connectivity exposes vulnerabilities that can be exploited by cyberthreats. The potential consequences of such a cyberattack are not just financial; it can also disrupt critical infrastructure and even result in injury or death. Owner operators and engineers must remember that their systems aren't safe and reliable if they're not secured.

IBM Consulting® Cybersecurity Services provides OT security solutions that are suitable for your specific needs. We can help you develop a comprehensive OT security program based on your specific risk profile. Our services include:

- OT security governance solutions
- Risk assessments
- Asset identification and management
- Network visualization and segmentation solutions
- Vulnerability management
- Identity management
- Threat detection and intelligence
- 24x7 monitoring and incident response solutions

IBM can help you establish an OT security operations center (SOC) or monitor your OT environment through our global OT SOC infrastructure.

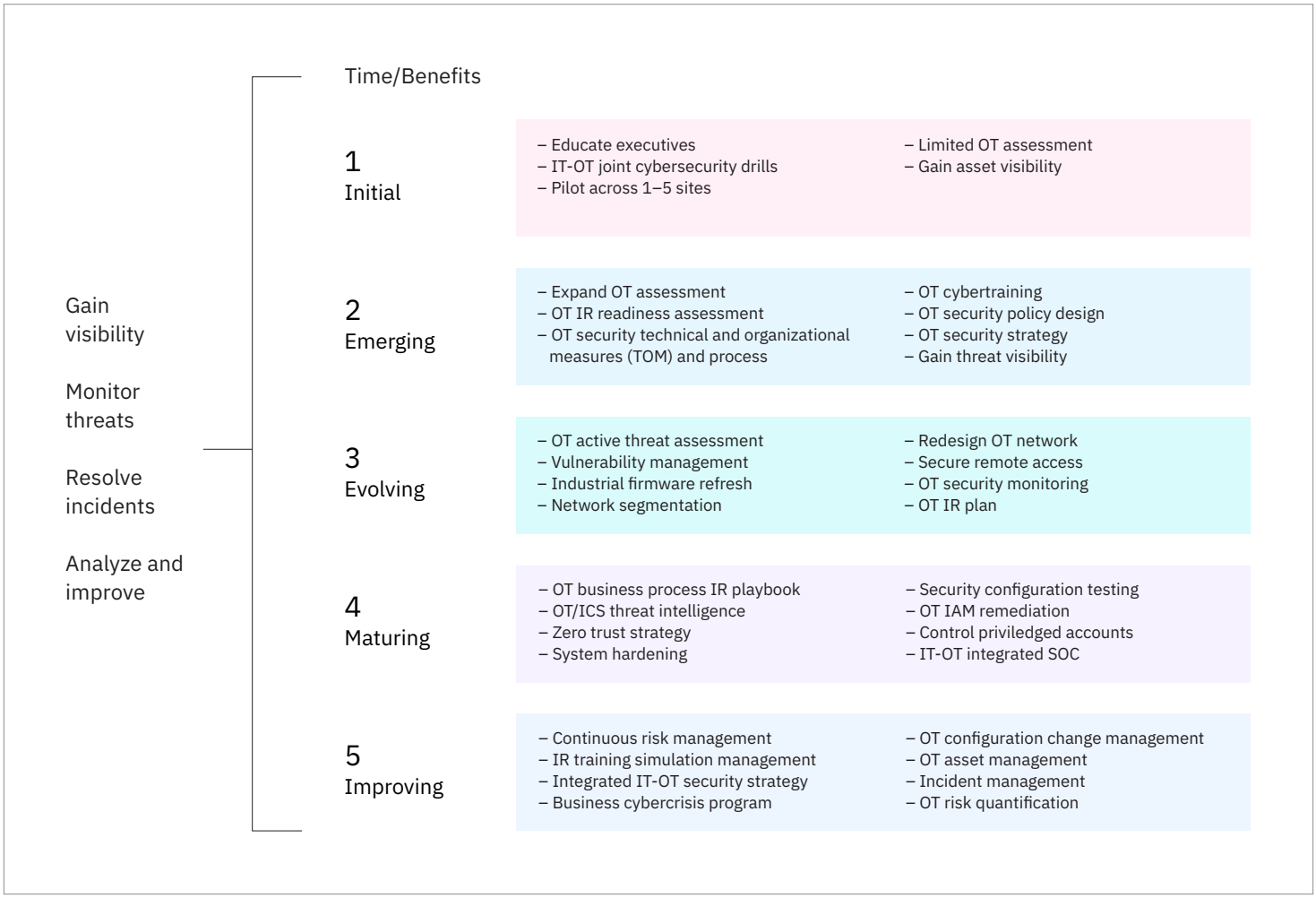


Figure 1. Five stages of the OT and IoT security journey

Developing an OT security program is a journey, and we understand that every organization is on its own unique path to securing the business. Some have established a mature security program and are looking to upgrade, whereas others are just getting started. However, they all share a common goal: to strengthen their OT security programs and reduce the risk of increased threats.

According to ABI Research, in 2023 a staggering 70% of industrial organizations experienced a cyberattack,[1] underscoring the urgent need for robust security solutions. Organizations must evolve from running a manual, reactive security program to following a more effective automated, proactive approach. As depicted in figure 1, there are five stages to an OT security journey. For most of our clients, the first goal is to achieve *Stage 3 – Evolving*, where processes are documented, standardized and integrated across the organization. The OT and IoT security journey is a multiyear program.

To move up the maturity ladder, you need to focus on five key areas.

Establish effective OT cybersecurity governance and risk management
We can help your organization establish the required OT cybersecurity governance framework that supports your risk management strategies and objectives through these services:

- **OT cybersecurity operating model:** All OT cybersecurity programs must include a documented and approved operational model. However, many businesses struggle with it, because their enterprise security operating model doesn't cover OT. This leaves each of their industrial operations or business units to fend for themselves, which usually means that OT security isn't performed at all or is executed poorly. IBM Consulting has assisted many clients in developing an OT cybersecurity operating model tailored to their specific needs.

- **OT cybersecurity policy development:** You must develop comprehensive OT cybersecurity policies that outline the rules, expectations and overall approach your organization uses to maintain the reliability and continuity, safety, efficiency, security and compliance of the industrial OT environment.

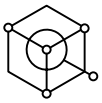
- **Risk assessment:** All organizations must conduct a thorough risk assessment on a regular basis to identify OT cybersecurity issues. This is best done by an unbiased third-party assessor. An OT risk assessment involves examining the client's OT security architecture, systems and programs to identify vulnerabilities and potential gaps that could result in a cyberphysical incident and disrupt business operations.

- **Quantitative risk assessment:** Many businesses use this strategy to assess risks. They assign numerical values to the likelihood and impact of potential cybersecurity events. This technique allows for a more objective and measurable analysis of risks, which helps organizations set priorities based on informed decisions and potential business impact. Conducting a qualitative risk assessment helps business stakeholders better understand OT security risks.

- **OT cybersecurity compliance monitoring:** Your security operations center (SOC) must be able to monitor your OT environment to ensure OT security regulatory compliance. Your SOC team is in charge of ensuring that your business meets its regulatory obligations by constantly monitoring and assessing security threats. They contribute to compliance with requirements such as the North American Electric Reliability Corporation (NERC), Critical Infrastructure Protection (CIP), Environmental Protection Agency (EPA) and Transportation Security Administration (TSA), which help you avoid penalties imposed by the government and other authorized bodies. With our OT security service, you can help ensure compliance with these regulatory standards and more.

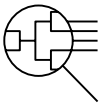
Improve OT infrastructure visibility
Many businesses don't have a comprehensive grasp of their assets, systems and network topology in industrial environments. Asset inventories are frequently recorded manually, networks are not effectively segmented and cybersecurity vulnerabilities are often unknown. This is a high-priority issue. You can't secure what you don't know you have. Without a thorough understanding of your assets, you can't put effective security measures in place to secure them. We can help you eliminate this roadblock to OT security.

Our services include:



Asset discovery and inventory tools, and integration with configuration management database (CMDB)

Vulnerability assessment, ranking and remediation management



Network topology analysis and segmentation solutions

Protect OT networks from unauthorized access and threats
Securing OT systems requires a comprehensive approach that prioritizes access controls as a critical step. By implementing robust OT access controls, your organization can help ensure the reliability, security and safety of its OT systems, which is essential for maintaining business operations and protecting people, assets and the environment. We can help you develop and implement a context-sensitive OT identity access management (IAM) strategy, enabling the right user to access the right data under the right conditions.

In addition, we provide a privileged-access management solution using products specifically designed for your OT environment, so you can track user activity to support incident triage. See figure 2 to understand how IBM implements an effective OT IAM strategy.

We've helped numerous clients select the right OT IAM security product for their environment. Also, we have the required skills to deploy, configure, monitor and manage these products to meet your unique requirements.

OT IAM concepts

OT identity and access management require these components

OT priviledged account management

- OT secure remote session management
- OT secret management and vaulting
- OT critical system password rotation
- Session management and recording

Authentication and authorization

- Static password
- MFA and OTP
- SSO, federation (SAML, OpenID)
- Policy management, least privilege (end users, operators, site administrators)

Auditing and reporting

- Identity and OT remote system access activity reports
- OT remote access session recordings
- SIEM integration
- Metrics
- KPIs

OT identity governance

- Access requests
- Alignment with fundamental business processes (Joiner, Mover, Leaver)
- Access provisioning, just in time provisioning
- Emergency access process
- Centralized and local user management and governance

Figure 2. IBM’s approach to an OT IAM strategy

Monitor the OT environment for threats

Monitoring an OT environment is different from monitoring the traditional corporate IT environment. In fact, many of the traditional SOC procedures won't work for an industrial operation. This is because the stakeholders are different. The SOC analyst can't just raise an incident ticket in the security orchestration, automation and response (SOAR) system and expect it to be handled. The OT SOC process is complex. However, OT security services from IBM Consulting address these differences using a fusion center approach.

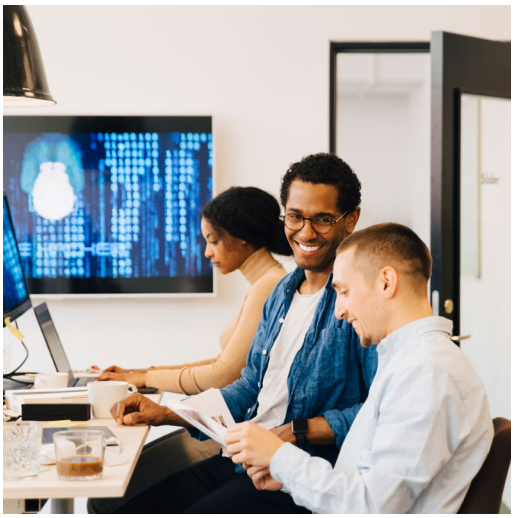
There are four key components to how IBM approaches OT security monitoring:

1. **Holistic SOC approach:** This requires congregated governance with clear roles and responsibilities, an OT-specific incident response plan and processes that include communication and reporting. In addition, aligning language and definitions, including the relationship between security and safety, is crucial for a comprehensive approach.

2. **Threat-driven use cases:** Our use cases incorporate tactics, techniques and procedures (TTPs) used by attackers. This approach, shaped by our global SOC and incident response (IR) experience and ability to leverage threat intelligence, accelerates OT security maturation.

3. **Skilled analysts:** Skilled analysts are critical to OT convergence. They detect, analyze and enrich incidents, which requires a deep understanding of OT systems and technologies. IBM has extensive experience in responding to thousands of OT incidents across various industries. We've developed skilled L1/L2 analysts who possess the necessary expertise to effectively detect and respond to OT threats.

4. **SOC effectiveness:** SOC effectiveness helps your organization detect and respond to threats in a timely and accurate manner. To achieve this, your SOC should incorporate effective IT-OT metrics, analytics and dashboards to provide smart insights and visibility into your OT security system. We perform regular tabletop exercises (TTX) to help ensure preparedness and quick response to potential incidents. SOC effectiveness is also key to reducing false positives, mean time to detect (MTTD) and mean time to respond (MTTR), which helps minimize downtime and maximize efficiency.



Respond effectively to cyberincidents
Everything is connected—including your factories, offices and fleet—so your IR plans must account for OT. IBM provides IR support for OT, partnerships with leading OT vendors, tailored service and certified experts with experience in IT and OT environments. We also provide the ability to assess, plan and respond cohesively across your entire technology landscape.

How does it work? Our portfolio of proactive services is ready to assess and optimize your IR capabilities for your OT environment. Our comprehensive OT IR program is built across four phases comprising:

- **Assess and build:** Assess capabilities and gaps, and develop processes, plans and standard operating procedures.
- **Deploy and enable:** Enable security, management and operations teams on plans and playbooks.
- **Test and validate:** Run technical, functional and crisis simulations.
- **Maintain steady state:** Establish training and assessment schedules and regular updates of plans and playbooks.

Conclusion
More effectively enable OT security with IBM Consulting Cybersecurity Services. Our global consultants, paired with leading technology partners, deliver comprehensive solutions for OT security. Scalable, personalized support can help ensure your business remains protected, efficient and compliant.

Why IBM?
With IBM Consulting Cybersecurity Services, you get comprehensive OT security. We have the industry's most extensive portfolio, backed by global expertise and scalable, personalized support. Our team of OT security and industry specialists, paired with strategic partnerships with leading technology companies, empowers you to achieve your OT security objectives faster, with higher quality and at a lower cost. With IBM, you can trust that your OT security needs are met by a dedicated team that understands the unique challenges of your environment to help ensure your business stays safe, secure—and compliant.

For more information
For more about OT security services from IBM Consulting, contact your IBM representative or IBM Business Partner, or visit ibm.com/services/ot-security.

1. The State of OT Security: A Comprehensive Guide to Trends, Risks, and Cyber Resilience, ABI Research, March 2024 (Link resides outside ibm.com)