

The background of the slide features a faint, light-colored line drawing of several oil pumpjacks (jack-o'-lanterns) in an industrial setting. The pumpjacks are shown in various stages of their pumping cycle, with their long walking beams and counterweights visible. The drawing is detailed, showing the mechanical components like the crankshafts, connecting rods, and the wellhead structures. The overall style is technical and industrial, typical of engineering or petroleum industry documentation.

Enhancing Operational Technology (OT) Cybersecurity in the Petrochemical Industry

*Using Common Approach of
American Petroleum Institute (API) 1164 & IEC62443*



INDUSTRY OVERVIEW

The petrochemical industry is a segment of the chemical industry that produces chemicals using petroleum and natural gas as raw materials. These chemicals, known as petrochemicals, are essential for manufacturing a wide range of products that are used in everyday life and various industrial applications. The industry encompasses a variety of processes, from the extraction of raw materials to the production and distribution of finished products.

Key Aspects of the Petrochemical Industry

1. Raw Materials



- **Crude Oil:** A primary raw material, refined to produce various products including gasoline, diesel, and other fuels.
- **Natural Gas:** Another essential raw material used to produce a range of chemicals.

2. Primary Petrochemicals



These are the basic building blocks produced from petroleum and natural gas. The three primary categories are:

- **Olefins:** Includes ethylene, propylene, and butadiene. These are used in the production of plastics, synthetic rubber, and other chemicals.
- **Aromatics:** Includes benzene, toluene, and xylene isomers. These are used in the production of dyes, synthetic detergents, and synthetic fibers.
- **Synthesis Gas (Syngas):** A mixture of hydrogen and carbon monoxide used to produce ammonia, methanol, and other chemicals.

3. Production Processes



- **Cracking:** The process of breaking down large hydrocarbon molecules into smaller ones, typically using heat (thermal cracking) or catalysts (catalytic cracking).
- **Reforming:** A process that converts alkanes to aromatics.
- **Polymerization:** A process where small molecules called monomers combine to form large chain-like molecules called polymers, used in making plastics and synthetic fibers.

4. End Products



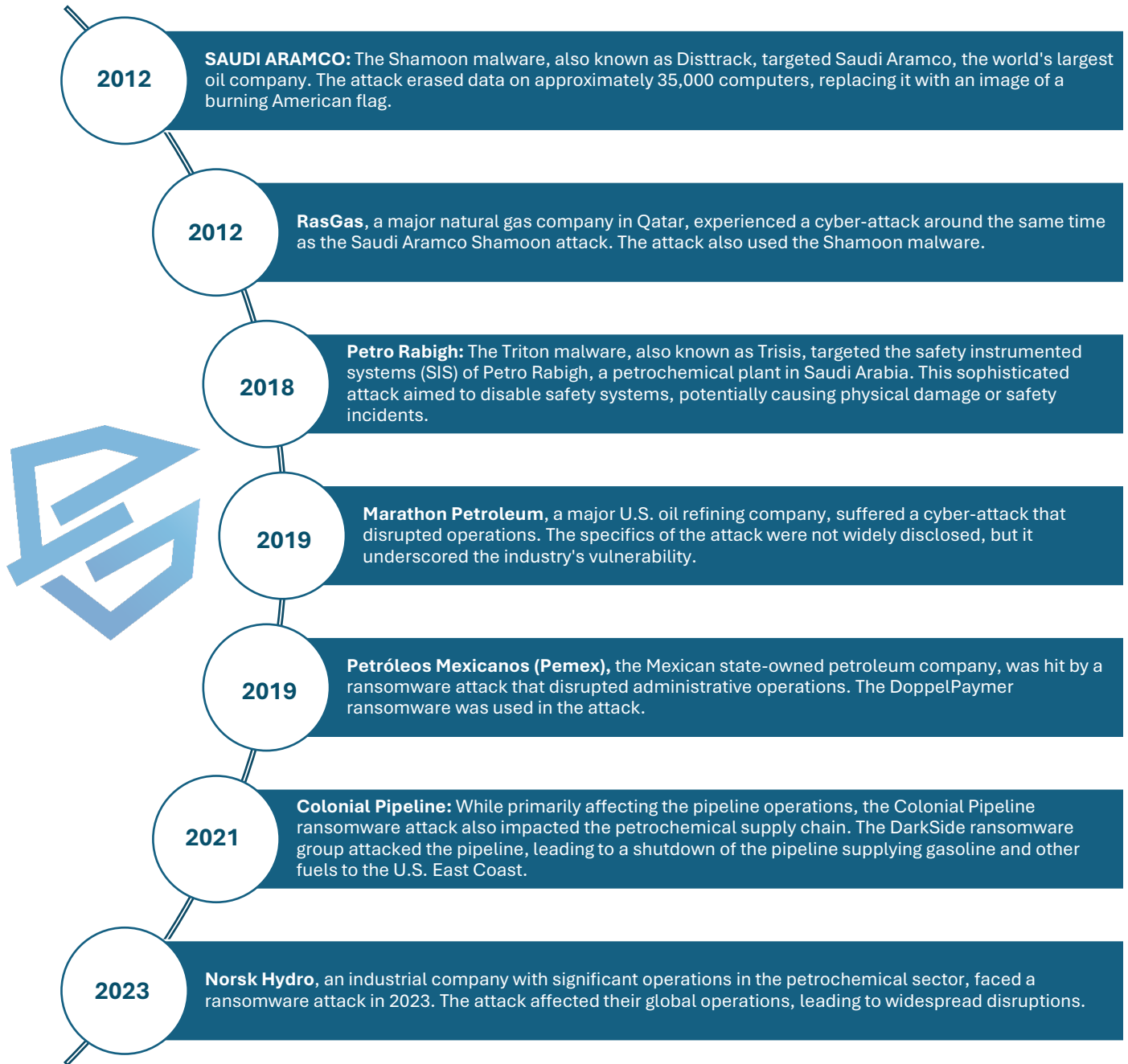
Petrochemicals are used to manufacture a wide range of products, including:

- **Plastics:** Used in packaging, containers, household goods, automotive parts, etc.
- **Synthetic Rubber:** Used in tires, footwear, and industrial applications.
- **Fibers:** Includes nylon, polyester, and acrylic, used in textiles and apparel.
- **Solvents, Fertilizers & Detergents etc.**





Cyber Attacks Timeline





STANDARDS APPLICABLE TO PETROCHEMICAL

The petrochemical industry must adhere to a variety of cybersecurity standards to protect its critical infrastructure from cyber threats. Here are some of the key cybersecurity standards and frameworks applicable to the petrochemical sector:

1. AMERICAN PETROLEUM INSTITUTE (API) Standard 1164

Developed by the American Petroleum Institute (API), Standard 1164 provides cybersecurity guidance for pipeline SCADA (Supervisory Control and Data Acquisition) systems.

Key Features:

- Focuses on protecting pipeline control systems from cyber threats.
- Includes recommendations for securing communication networks and control systems.
- Provides guidance on incident response and recovery.
-

Risk Management Framework	<p>API 1164 emphasizes a risk management approach, which includes:</p> <ul style="list-style-type: none">• Risk Assessment: Identifying and evaluating potential cybersecurity risks to SCADA systems.• Risk Mitigation: Implementing appropriate security controls and measures to mitigate identified risks.• Continuous Monitoring: Regularly monitoring and reassessing risks to adapt to evolving threats.
Security Controls and Measures	<ul style="list-style-type: none">• Access Control:<ul style="list-style-type: none">○ Implement access control measures to ensure that only authorized individuals can access IACS components and data.○ Use role-based access control (RBAC) to assign access based on job functions.• User Authentication and Authorization:<ul style="list-style-type: none">○ Require strong authentication mechanisms for users and devices.○ Use multi-factor authentication (MFA) where appropriate.• System Integrity:<ul style="list-style-type: none">○ Ensure the integrity of systems and data through measures like cryptographic checksums and digital signatures.• Data Confidentiality:<ul style="list-style-type: none">○ Protect sensitive data at rest and in transit using encryption and other confidentiality measures.• Restricted Data Flow:<ul style="list-style-type: none">○ Limit and control the flow of data between different segments of the IACS network.• Timely Response to Events:



	<ul style="list-style-type: none">○ Implement monitoring and logging mechanisms to detect and respond to security incidents promptly.● Patch Management:<ul style="list-style-type: none">○ Establish a patch management process to ensure that security updates are applied promptly.● Vulnerability Management:<ul style="list-style-type: none">○ Regularly identify, assess, and mitigate vulnerabilities in IACS components and systems. <hr/> <p><i>[REPLIL INDUSTRIAL PATCH MANAGER] provides centralized visibility of OEM patches and tools to manage, deploy and report the missing, installed and vulnerable systems.</i></p> <hr/>
Physical Security	<ul style="list-style-type: none">● Ensuring that physical access to SCADA system components is restricted to authorized personnel only.● Implementing measures such as surveillance, access controls, and physical barriers to protect critical infrastructure.
Employee Training and Awareness	<ul style="list-style-type: none">● Conducting regular cybersecurity training and awareness programs for employees.● Ensuring that personnel are aware of their roles and responsibilities in maintaining SCADA system security.● Promoting a culture of cybersecurity awareness throughout the organization.
Vendor & Third-Party Management	<ul style="list-style-type: none">● Assessing the cybersecurity posture of vendors and third-party service providers.● Ensuring that third-party systems and services comply with the organization's cybersecurity requirements.● Establishing contractual obligations for cybersecurity standards and practices with vendors.
Compliance and Auditing	<ul style="list-style-type: none">● Regularly auditing SCADA systems to ensure compliance with API 1164 and other relevant cybersecurity standards.● Conducting periodic reviews and assessments to identify and address gaps in security controls.● Documenting and reporting compliance status to relevant stakeholders.





2. IEC 62443

ISA/IEC 62443 is a series of standards developed by the International Society of Automation (ISA) and the International Electrotechnical Commission (IEC) specifically for industrial automation and control systems (IACS).

Key Features:

- Provides a comprehensive framework for securing IACS.
- Addresses security vulnerabilities throughout the lifecycle of IACS.
- Includes requirements for both technical and management processes.
-

General Security Program	<ul style="list-style-type: none">• Security Policy and Procedures:<ul style="list-style-type: none">○ Establish and maintain security policies, procedures, and practices.• Risk Assessment and Management:<ul style="list-style-type: none">○ Conduct regular risk assessments to identify and mitigate risks to IACS.• Personnel Security:<ul style="list-style-type: none">○ Ensure that personnel are screened, trained, and aware of cybersecurity policies and procedures.
Technical Security Controls	<ul style="list-style-type: none">• Access Control:<ul style="list-style-type: none">○ Implement access control measures to ensure that only authorized individuals can access IACS components and data.○ Use role-based access control (RBAC) to assign access based on job functions.• User Authentication and Authorization:<ul style="list-style-type: none">○ Require strong authentication mechanisms for users and devices.○ Use multi-factor authentication (MFA) where appropriate.• System Integrity:<ul style="list-style-type: none">○ Ensure the integrity of systems and data through measures like cryptographic checksums and digital signatures.• Data Confidentiality:<ul style="list-style-type: none">○ Protect sensitive data at rest and in transit using encryption and other confidentiality measures.• Restricted Data Flow:<ul style="list-style-type: none">○ Limit and control the flow of data between different segments of the IACS network.• Timely Response to Events:<ul style="list-style-type: none">○ Implement monitoring and logging mechanisms to detect and respond to security incidents promptly.
Network Security Controls	<ul style="list-style-type: none">• Network Segmentation:<ul style="list-style-type: none">○ Use network segmentation to isolate critical systems and limit the impact of potential security breaches.• Firewalls and Intrusion Detection/Prevention Systems:<ul style="list-style-type: none">○ Deploy firewalls and intrusion detection/prevention systems to protect IACS networks.• Secure Remote Access:<ul style="list-style-type: none">○ Ensure that remote access to IACS networks is secure and monitored.





System Development and Maintenance	<ul style="list-style-type: none">• Security by Design:<ul style="list-style-type: none">○ Incorporate security considerations into the design and development of IACS components and systems.• Patch Management:<ul style="list-style-type: none">○ Establish a patch management process to ensure that security updates are applied promptly.• Vulnerability Management:<ul style="list-style-type: none">○ Regularly identify, assess, and mitigate vulnerabilities in IACS components and systems. <hr/> <p><i>[REPLIL INDUSTRIAL PATCH MANAGER] provides centralized visibility of OEM patches and tools to manage, deploy and report the missing, installed and vulnerable systems.</i></p> <hr/>
Physical Security Controls	<ul style="list-style-type: none">• Physical Access Control:<ul style="list-style-type: none">○ Implement measures to control physical access to IACS components and facilities.• Environmental Controls:<ul style="list-style-type: none">○ Ensure that environmental controls (e.g., temperature, humidity) are in place to protect IACS components.
Security Management and Governance	<ul style="list-style-type: none">• Security Leadership and Governance:<ul style="list-style-type: none">○ Establish leadership and governance structures to oversee the cybersecurity program.• Security Metrics and Reporting:<ul style="list-style-type: none">○ Develop metrics and reporting mechanisms to measure and communicate the effectiveness of the cybersecurity program.• Continuous Improvement:<ul style="list-style-type: none">○ Implement a continuous improvement process to enhance the cybersecurity posture of the IACS over time.

3. NIST SP 800-82

National Institute of Standards and Technology (NIST) Special Publication 800-82 provides guidance on securing Industrial Control Systems (ICS), including those used in railroads. It offers a comprehensive framework for identifying vulnerabilities and implementing protective measures.





4. NIST Cybersecurity Framework (NIST CSF)

Developed by the National Institute of Standards and Technology (NIST), the Cybersecurity Framework provides guidelines for managing and reducing cybersecurity risk.

Key Features:

- Provides a common language for understanding, managing, and expressing cybersecurity risks.
- Based on existing standards, guidelines, and practices.
- Consists of five core functions: Identify, Protect, Detect, Respond, and Recover.

5. CIS Critical Security Controls

The Center for Internet Security (CIS) Critical Security Controls are a set of best practices for cybersecurity.

Key Features:

- Provides a prioritized set of actions to protect against the most pervasive cyber threats.
- Includes controls specifically relevant to industrial environments, such as secure configurations for hardware and software.
- Emphasizes practical and effective security measures.

6. OG86 - Operational Technology (OT) Cybersecurity for the Oil & Gas Industry

OG86, developed by the Oil & Gas Cybersecurity Network (OGCN), is a framework specifically for the oil and gas sector, which includes the petrochemical industry.

Key Features:

- Provides sector-specific guidance on securing OT environments.
- Covers risk assessment, security controls, and incident response.
- Aligns with broader industry standards and frameworks.





7. IEC 61511

IEC 61511 is an international standard for the functional safety of safety instrumented systems (SIS) for the process industry sector.

Key Features:

- Addresses the safety lifecycle and risk assessment for SIS.
- Includes requirements for the security of SIS to protect against cyber threats.
- Complements IEC 62443 for a holistic approach to industrial cybersecurity.

8. EU Directive on Security of Network and Information Systems (NIS Directive)

The NIS Directive is a European Union directive focused on improving the cybersecurity of critical infrastructure, including the petrochemical sector.

Key Features:

- Requires member states to develop national cybersecurity strategies.
- Establishes requirements for the security of network and information systems.
- Mandates incident reporting and cooperation among EU member states.

WHY REPLIL

REPLIL provides comprehensive product lines for industrial assets, using a risk-based approach to cover the entire patch management flow in alignment with DHS and IEC62443 strategies. Our offerings include:

- **IEC62443-4-1 / IEC62443-4-2 Compliant Products**
- **Agentless Patch Management:** Robust tools designed specifically for critical OEM systems.
- **Customized Reporting & Dashboards:** Tailored to meet all compliance requirements.
- **Centralized Management Console (CMC):** Centralized visibility and control across distributed sites.





COMPREHENSIVE APPROACH INLINE TO MAJOR CYBERSECURITY STANDARDS

All major cybersecurity standards refer to a common approach of comprehensive OT Cybersecurity



Risk Assessment and Management

Conducting thorough risk assessments to identify vulnerabilities and potential threats is the first step in enhancing OT cybersecurity. This involves:

- **Asset Inventory:** Maintaining an up-to-date inventory of all OT assets, including hardware, software, and network components.
- **Threat Modeling:** Understanding potential threat vectors and their implications.
- **Vulnerability Management:** Regularly scanning for and addressing vulnerabilities in OT systems.



Segmentation and Network Security

Implementing robust network segmentation can limit the impact of a cyber-attack by containing it within a specific segment. Key practices include:

- **Demilitarized Zones (DMZs):** Creating DMZs between IT and OT networks to control data flow.
- **Firewalls and Intrusion Detection Systems (IDS):** Deploying firewalls and IDS to monitor and protect network traffic.
- **Internal Logical / Physical Segmentation:** Implement VLANs to limit the exposure of various zones and limit communication. VLANs alone is not enough and must supplement with IDS and Router on a Stick Concept.








Identity & Access Control:

Implementing robust identity and authentication mechanisms is crucial to ensure the security of the industrial control systems and the safety of critical infrastructure.

- **Centralized Authentication**
 - **Active Directory (AD):** Active Directory (AD) is a widely used centralized authentication service developed by Microsoft. It enables administrators to manage permissions and access network resources efficiently. AD integrates well with Windows environments and can be extended to support various other applications and services.
- **AAA (Authentication, Authorization, Accounting) Servers**
 - AAA servers are critical in managing access control within OT environments. They provide a framework for ensuring that only authorized users can access specific resources, monitor their activities, and ensure compliance with security policies. Examples include RADIUS (Remote Authentication Dial-In User Service) and TACACS+ (Terminal Access Controller Access-Control System Plus).
- **Multi-Factor Authentication (MFA)**
 - MFA enhances security by requiring users to provide two or more verification factors to gain access to a resource. This can include something they know (password), something they have (security token), and something they are (biometric verification).
- **Role-Based Access Control (RBAC)**
 - RBAC restricts system access to authorized users based on their role within an organization. Roles are defined according to job responsibilities, and permissions are assigned to these roles rather than individual users.





	<ul style="list-style-type: none">• Public Key Infrastructure (PKI)<ul style="list-style-type: none">○ PKI uses pairs of cryptographic keys to verify user identities and secure communications. Digital certificates issued by a trusted Certificate Authority (CA) are used to authenticate users and devices within the network.
	<p>Malware Protection</p> <p>Implementing robust endpoint protection can limit the impact of potential exploits and unauthorized applications. Endpoint protection must provide a methodology (Lock Down) to cover the legacy assets.</p> <ul style="list-style-type: none">• Data Leakage Protection• Device Hardening• Application Whitelisting• Host Based IPS
	<p>Secure Remote Access</p> <p>Remote access to OT systems should be tightly controlled and secured to prevent unauthorized access. Measures include:</p> <ul style="list-style-type: none">• Multi-Factor Authentication (MFA): Implementing MFA for all remote access.• VPNs and Encryption: Using Virtual Private Networks (VPNs) and encryption to secure remote connections.
	<p>Regular Patching and Updates</p> <p>Keeping OT systems up to date with the latest patches and updates is crucial to mitigating vulnerabilities. This requires:</p> <ul style="list-style-type: none">• Patch Management Policies: Establishing policies for timely application of patches and updates.• Testing and Validation: Testing patches in a controlled environment before deployment to ensure compatibility and stability. <p>Learn How REPLIL can support your patch Management Journey</p>
	<p>Incident Response and Recovery</p> <p>Developing and maintaining a robust incident response plan is essential for minimizing the impact of cyber-attacks. This includes:</p> <ul style="list-style-type: none">• Incident Response Teams: Forming dedicated teams trained to respond to OT cybersecurity incidents.• Regular Drills and Simulations: Conducting regular drills and simulations to ensure preparedness.• Backup and Recovery Plans: Implementing comprehensive backup and recovery plans to restore normal operations quickly after an incident.
	<p>Training and Awareness</p> <p>Enhancing cybersecurity awareness and training among employees is critical. Key initiatives include:</p> <ul style="list-style-type: none">• Regular Training Programs: Providing ongoing cybersecurity training tailored to OT environments.• Awareness Campaigns: Running campaigns to raise awareness about the importance of OT cybersecurity and safe practices.





REPLIL STRATEGY TO SECURE CRITICAL INFRASTRUCTURE USING IEC62443 “SL3” PRODUCTS

To ensure the security and effective management of critical infrastructure, developing a robust strategy for patch management is essential. Below is a comprehensive strategy for using REPLIL Industrial Patch Manager and REPLIL OT Patch Manager for securing critical infrastructure, along with an explanation of the importance of visibility for critical patches.

Importance:

1. Threat Mitigation

- **Timely Response:** Visibility into critical patches enables timely identification and mitigation of vulnerabilities, reducing the risk of exploitation by threat actors.
- **Prioritization:** Clear visibility helps prioritize patches based on the threat landscape and the criticality of vulnerabilities, ensuring that the most severe risks are addressed first.

2. Compliance and Auditing

- **Regulatory Compliance:** Ensuring visibility and proper documentation of critical patches helps meet regulatory and compliance requirements, which often mandate timely vulnerability management.
- **Audit Trails:** Visibility into patching activities provides a clear audit trail, demonstrating due diligence in maintaining a secure infrastructure.

3. Operational Integrity

- **Minimized Downtime:** With visibility into which patches are critical and which systems they affect, organizations can better plan and execute patching activities without causing significant operational downtime.
- **Resource Allocation:** Proper visibility allows for more efficient allocation of resources, ensuring that critical patches receive the attention and urgency they require.

Features:

REPLIL INDUSTRIAL PATCH MANAGER (IPM)	REPLIL OT PATCH SANDBOX (OPS)
Risk-Based Patch Prioritization <ul style="list-style-type: none">• Criticality Assessment: Categorize patches based on the criticality and risk associated with each asset. Patches that address vulnerabilities in high-risk or high-value assets should be prioritized.• Impact Analysis: Evaluate the potential impact of deploying patches on operational continuity. Prioritize patches that fix critical vulnerabilities without significantly disrupting operations. Scheduled Patch Deployment <ul style="list-style-type: none">• Patch Scheduling: Develop a patching schedule that aligns with operational	Testing and Validation <ul style="list-style-type: none">• Pre-Deployment Testing: Test patches in a controlled environment that replicates the production setting to ensure compatibility and effectiveness. This step helps identify potential issues before full deployment.• Post-Deployment Validation: Conduct thorough post-deployment checks to verify that patches have been successfully applied and that they do not negatively impact system functionality.• Advance Test Cases: Automatically execute, test & validate (desktop / web)





<p>downtimes to minimize disruptions. Utilize maintenance windows or planned downtimes for deploying critical patches.</p> <ul style="list-style-type: none">• Phased Rollouts: Implement patches in a phased manner, starting with less critical systems to observe any unforeseen impacts before deploying to critical systems. <p>Automated Patch Management</p> <ul style="list-style-type: none">• Automation Tools: Utilize Replil Industrial Patch Manager and Replil OT Patch Manager to automate the patching process. Automation ensures timely patch application and reduces the risk of human error. <p>Continuous Monitoring:</p> <ul style="list-style-type: none">• Implement continuous monitoring to detect new vulnerabilities and assess the need for patches in real-time. Automated alerts can help promptly address critical vulnerabilities.	<p>based critical applications expected state before & after the installation of a patch.</p>
---	---

Click for more details

[REPLIL Industrial Patch Manager](#)

[REPLIL OT Patch Sandbox](#)

Book a demo to secure critical infrastructure: sales@replil.com

