	Baseline Security Measures	Enhanced Security Measures	CYE / OTORIO Solution
Identify	**Asset Management**		
	Establish and document policies and procedures for assessing and maintaining configuration information, tracking changes made to pipeline cyber assets, and patching/upgrading operating systems and applications. Ensure that the changes do not adversely impact existing cybersecurity controls.	Employ mechanisms to maintain accurate inventory and detect unauthorized components.	OTORIO's continuous risk assessment platform RAM^2 provides complete asset inventory, including third-party technologies.
	Develop and maintain a comprehensive set of network/system architecture diagrams or other documentation, including nodes, interfaces, remote and third-party connections, and information flows.	Review network connections periodically, including remote and third-party connections. Develop a detailed inventory for every endpoint.	CYE's asset discovery capabilities combined with OTORIO's OT asset inventory capabilities. CYE reviews the real-time architecture and checks communication matrixes in the network using a hands-on assessment, as well as multiple scans.
	Review and assess the classification of pipeline cyber assets as critical or non-critical at least every 12 months.		
	Business Environment		
	Ensure that any and all changes that add control operations to a non-critical pipeline cyber asset result in the system being recognized as a critical pipeline cyber asset with enhanced security measures being applied.		OTORIO's continuous risk assessment platform RAM^2
	Governance		
	Establish and distribute cybersecurity policies, plans, processes and supporting procedures commensurate with the current regulatory, risk,legal and operational environment.		CYE's cyber risk management platform CYE assists in creating the policy, plans and processes and translating the regulations into tangible work plans for the technical teams. OTORIO's continuous risk assessment platform RAM^2 connects to every asset within the OT/IoT environment, enriching data and distributing it across the network.

	Review and assess all cybersecurity policies, plans, processes, and supporting procedures regularly - at least every 36 months, or when there is a significant organizational or technological change. Update as necessary.	Review and assess all cybersecurity policies, plans, processes, and supporting procedures regularly - at least every 36 months, or when there is a significant organizational or technological change. Update as necessary.	CYE's cyber risk management platform CYE reviews the policies from the perspective of a hacker in order to identify gaps in platforms and technologies. This data is further enriched by OTORIO RAM^{2,} which continuously checks the environment against a dynamically updated compliance database. It then assigns a compliance score to every machine, sector and site, allowing operational teams to understand their compliance standing, while helping them fulfill regulatory requirements.
Identify	Risk Management Strategy		
	Develop an operational framework to ensure coordination, communication and accountability for information security on and between the control systems and enterprise networks.		CYE's cyber risk management platform Our risk dashboard in our cybersecurity platform, Hyver, helps organizations and security teams effectively manage their security risks, while providing full visibility into their attack surface.
	Risk Assessment		
	Establish a process to identify and evaluatevulnerabilities and corresponding security controls.	Ensure that threat and vulnerability information received from data sharing forums and sources is made available to those responsible for assessing and determining the appropriate course of action.	CYE's security assessment helps organizations identify and evaluate vulnerabilities and determine which attack routes are most critical to block in order to secure their business critical assets.

	Baseline Security Measures	Enhanced Security Measures	CYE / OTORIO Solution
Protect	Access Control		
	Establish and enforce unique accounts for eachindividual user and administrator, as well as security requirements for privileged accounts, while prohibiting the sharing of these accounts. In instances where systems do not support unique user accounts, implement appropriate compensating security controls(e.g., physical controls).	Restrict user physical access to control systems and control networks through the use of appropriate controls. Employ more stringent identity and access managementpractices (e.g., authenticators, password- construct, access control).	Can be validated by CYE CYE assists in creating policies of "zero trust," as well as the validation of implementation. OTORIO offers advanced, secure, remote and privileged access management capabilities to the OT environment, promoting zero trust implementations in the digitized industrial sector.
	Ensure that user accounts are modified, deleted,or de-activated expeditiously for personnel who no longer require access or are no longer employed by the company.		Can be validated by CYE CYE assists in creating policies of "zero trust," as well as the validation of implementation. OTORIO offers advanced, secure, remote and privileged access management capabilities to the OT environment, promoting zero trust implementations in the digitized industrial sector.
	Establish and enforce access control policies for local and remote users. Procedures and controls should be in place for approving and enforcing policies for remote and third-party connections.	Monitor physical and remote user access to critical pipeline cyber assets.	Can be validated by CYE CYE assists in creating policies of "zero trust," as well as the validation of implementation OTORIO offers advanced, secure, remote and privileged access management capabilities to the OT environment, promoting zero trust implementations in the digitized industrial sector.
	Ensure appropriate segregation of duties is inplace. When this is not feasible, apply appropriate compensating security controls.		Can be validated by CYE CYE assists in creating policies of "zero trust," as well as the validation of implementation.

	Change all default passwords for new software, hardware, etc., upon installation. When changing default passwords is not technically feasible (e.g., a control system with ahard-coded password), implement appropriate compensating security controls (e.g., administrative controls).	Employ mechanisms to support the management of accounts.	Can be validated by CYE CYE assists in creating policies of “zero trust,” as well as the validation of implementation. CYE also checks all of the internet perimeters of the organization to locate the types of applications that are Internet-facing. OTORIO offers advanced, secure, remote and privileged access management capabilities to the OT environment, promoting zero trust implementations in the digitized industrial sector.
Protect	Awareness and Training		
	Ensure that all persons requiring access to theorganization’s pipeline cyber assets receive cybersecurity awareness training.	Provide role-based security training on recognizing and reporting potential indicatorsof system compromise prior to obtaining access to the critical pipeline cyber assets.	CYE security training CYE provides a security training to technical personals, management, and employees
	Establish and execute a cyber-threat awarenessprogram for employees. This program should include practical exercises/testing.		CYE security training CYE provides a security training to technical personals, management, and employees.
	Data security and Information Protection		

	Establish and implement policies and proceduresto ensure data protection measures are in place,including identifying critical data and establishingclassification of different types of data, while maintaining specific handling procedures, protections and disposals.		Can be validated by CYE CYE provides a comprehensive assessment of the organization to identify and reach organizational critical assets through real attack vectors. This assessment includes policy reviews and recommendations.
	Protective Technology		
	Segregate and protect pipeline cyber assets from the internet and enterprise networks usingphysical separation, firewalls and other protections.		Use OTORIO RAM^2 to enforce firewall rules and company security policies across the entire OT environment
	Regularly validate that technical controls complywith the organization's cybersecurity policies, plans and procedures, and report results to senior management.		OTRIO's RAM^2 continuously monitors the environment to assess its security posture, ensuring that it is adhering to company policies and industrial standards. The system produces periodic reports – both automatically and on-demand. Can be validated by CYE by providing a comprehensive assessment of the organization.
	Implement technical or procedural controls to restrict the use of pipeline cyber assets for only approved activities.		Can be validated by CYE by providing a comprehensive assessment of the organization OTORIO RAM^2 is utilized to enforce zero trust security policies across the entire OT environment to mandate that devices, services and individuals are continuously authenticated, authorized and validated before given access to assets, applications or data.

	Baseline SecurityMeasures	Enhanced Security Measures	CYE / OTORIO Solution
Detect	Anomalies and Events		
	Implement processes to generate alerts and logcybersecurity events in response to anomalousactivity. Review the logs and respond to alerts in a timely manner.		OTORIO RAM^{2} collects thousands of security events from a variety of data sources and correlates and contextualizes the alerts based on the operational and business process. It then aggregates them into a manageable number of insights in order to significantly reduce "noise" and alert fatigue, enabling organizations to focus only on the most critical data.
	Security Continuous Monitoring		
	Monitor for unauthorized access, introduction of malicious code or communications.		OTORIO offers advanced, secure, remote and privileged access management capabilities to the OT environment, promoting zero trust implementations in the digitized industrial sector.
	Conduct cyber vulnerability assessments asdescribed in your risk assessment process	Utilize independent assessors to conductpipeline cyber security assessments.	CYE's continuous risk assessment to identify and reach the organizational critical assets through real attack vectors. This capability is now combined with OTORIO's cyber-digital-twin, which conducts non-intrusive breach and attack simulations based on multiple attack scenarios for continuous and automated security and risk assessment.

	Baseline SecurityMeasures	Enhanced Security Measures	CYE / OTORIO Solution
Detect	Detection Processes		
	Establish technical or procedural controls for cyber monitoring, intrusion and detection.		OTORIO's RAM^2 provides a platform for continuous (automated) OT security monitoring. By aggregating multiple data sources and correlating and prioritizing them, RAM^2 enhances the performance of other cyber tools, including intrusion detection, ensuring that only the most relevant data is presented to cyber analysts.
	Perform regular testing of intrusion and malwaredetection processes and procedures.		CYE's continuous risk assessment CYE provides a comprehensive organizational assessment.in order to identify critical organizational assets through real attack vectors OTORIO Digital Twin performs continuous breach-and-attack simulations to detect vulnerabilities and security gaps
Respond	Response Planning		
	Establish policies and procedures for cybersecurity incident handling, analysis and reporting, including assignment of specificroles/tasks to individuals and teams.	Conduct cybersecurity incident response exercises periodically.	CYE's cyber risk management platform and incident response readiness program CYE offers an incident response readiness program, as well as a purple team engagement, to test various security policies and procedures
	Establish and maintain a cyber-incident response capability.	Establish and maintain a process that supports 24 hour cyber incident response.	OTORIO's Incident Response (IR) team includes industry veterans with years of proven experience in protecting mission-critical infrastructure.
	Communications		

	Report significant cyber incidents to seniormanagement; appropriate federal, state, local, tribal, and territorial (SLTT) entities and applicable ISAC(s).	Pipeline operators should follow the notification criteria in Appendix B	OTORIO’s continuous risk assessment platform RAM^{2}’s automated reports
	Mitigation		
	Ensure the organization’s response plans and procedures include mitigation measures to helpprevent further impacts.		CYE’s continuous risk assessment CYE offers an incident response readiness program, as well as a purple team engagement, to test various security policies and procedures. These best practices are also embedded into OTORIO’s RAM^{2}, providing teams with a simplified, step-by-step mitigation playbook for future events.
Recover	Recovery Planning		
	Establish a plan for the recovery and reconstitution of pipeline cyber assets within a timeframe that aligns with the organization’s safetyand business continuity objectives.		CYE’s cyber risk management platform CYE offers an incident response readiness program, as well as a management training program, to react to various cyber attack scenarios.
	Improvements		
	Review the organization's cyber recovery planannually. Update as necessary.		CYE’s cyber risk management platform CYE offers an incident response readiness program, as well as a management training program, to react to various cyber attack scenarios.