CHECKLIST

Checklist: Critical Information Infrastructure

ICS Cyber Security Considerations

Indegy
Activate All Your Senses

CRITERIA	COMMENTS
1 Automated Asset Discovery and Management	
Discovers level 2 control devices: operator stations, engineering workstations, and servers (Windows/Linux-based)	
Discovers level 1 control devices: PLCs, RTUs, DCS controllers	
Discovers level 0 devices (I/Os)	
Discovers non-communicating assets	
Provides detailed information onasset type, specific models, OS and firmware versions, and more (for level 1 & level 2)	
Provides interactive asset map displaying assets, communication patterns, protocols used, and conversations	
2 Continuous Network Activity Monitoring, Anomaly, and Threat Detection	
Detects threats and anomalies by monitoring device communications and protocols (both external and internal)	
Out of the box security policies for threat and anomaly detection	
User-friendly granular policy customization engine for threat and anomaly detection	
OT data-plane protocols coverage	
OT control-plane engineering protocols coverage	
3 Controller Integrity Validation	
Identifies changes to controllers made over the network, including configuration changes, code changes, and firmware downloads	
Identifies changes made to controllers by physically connecting to the devices (via serial cable or USB device)	
4 Vulnerability Assessment and Risk Management	
Risk score by device	
Vulnerability assessment for all control devices	
5 Incident Detection and Response	
Real-time alerts on suspicious activities and threats detected in ICS networks	
Full audit trail of ICS activities	
Historical controller information to support backup and recovery	
6 Architecture and Enterprise Readiness	
Both HW and SW-only implementations are available	
Quick deployment, no training required	
Centralized solution management, data aggregation, alerts, and reporting	
Out of the box integration: Active Directory, SIEM, Syslog, REST API, data exports	

You should consider Indegy if....

Your ICS needs protection from cyber attacks, malicious insiders, and human error

You are looking to reduce costs associated with operational disruptions

You need a solution that has zero impact on operations

You are looking to secure a regional, national, or distributed organization

You want a solution that is easy to deploy and manage