tenable.ot™

CHECKLIST

OT CYBER SECURITY CONSIDERATIONS

CRITERIA		COMMENTS
VISIBILITY ACROSS THE OT INFRASTRUCTURE		
	Discovers all IT and OT based devices in the OT Environment	
	Provides interactive asset map displaying assets, communication patterns, protocols used, and conversations	
	Role-based access control	
ASSET INVENTORY		
	Deep situational analysis including detailed information on asset type, specific models, firmware version, ladder logic and more	
	Identifies non-communicating or "dormant" assets	
THREAT DETECTION		
	Policy based detection with customization capabilities (network based)	
	Anomaly based detection with customization capabilities (network based)	
	Leveraging of third party/open sourced security database; ie: Suricata (network based)	
	Active querying capabilities with no impact to operations (device based)	
	Proactive weakpoint and risky behaviors and configuration identification with attack vectors	
	OT data-plane protocols & control plane engineering coverage	
	Fine tuning capabilties for each detection method	
	Real-time alerts on suspicious activities and threats detected in OT networks	
VULNERABILITY ASSESSMENT AND RISK MANAGEMENT		
	Identification the IT & OT vulnerabilities that are specific to your OT enviornment	
	Triages the severity of the vulnerability (VPR scoring) based on how it affects your enviornment	
CONFIGURATION CONTROL		
	Identification of network based changes to PLCs, including configuration changes, code changes, and firmware downloads	
	Identification of changes made to PLCs by physically connecting to the devices (via serial cable or USB device)	
	Audit trail of changes made from one "snapshot" version to the next	
	Snapshotting capabilities based on activity, time and/or user invoked	
	Historical controller information to support backup and recovery	
	Full audit trail of ICS activities	
ARCHITECTURE AND ENTERPRISE READINESS		
	Flexible implementation options	
	Centralized solution management, data aggregation, alerts, and reporting	
	Out of the box integration with leading security partners, Active Directory, SIEM, Syslog, REST API, data exports	

You should consider Tenable.ot™ if:

- Your OT environment needs protection from cyber attacks, malicious insiders, and human error
- You are looking to reduce costs associated with operational disruptions
- You need full visibility across converged IT/OT operations
- You want OT security at the device and network level
- You want a solution that easily integrates with into your existing security solutions