tenable.ot™

DATA SHEET

ADHERING TO THE NIST FRAMEWORK WITH TENABLE.OT

United States' national security depends on the reliability and continuous operations of the nation's critical infrastructure. The increasing complexity and connectivity of critical infrastructure systems are exposing them to cybersecurity threats which put their safety and reliability at risk.

The NIST Framework was created through collaboration between government and the private sector, in response to the Executive Order (EO) 13636: Improving Critical Infrastructure Cybersecurity, which calls for the development of a risk-based Cybersecurity Framework. It provides a set of industry standards and best practices to help organizations manage and reduce cybersecurity risk to critical infrastructure. NIST is considered to be the authoritative standard to which organizations both in the US and overseas map their cyber security strategies.

Tenable.ot supports the implementation of the NIST 1,1 Cybersecurity Framework.

Tenable.ot aligns with the CSF primary directive of identifying, managing and reducing the cyber risk of critical infrastructures and the Industrial Control Systems (ICS) on which they rely, by providing comprehensive visibility into critical control assets and activities associated with them.

Managing and Reducing Risk to Critical Infrastructure with Tenable.ot

Tenable.ot protects industrial networks from cyber threats, malicious insiders and human error. With threat detection and mitigation, asset inventory, vulnerability management and configuration control, Tenable's OT security capabilities identify and predictively prioritize threats and vulnerabilities to maximize the safety and reliability of your operational technology environment.

Tenable.ot empowers security and operations teams in industrial organizations with:

- Complete Visibility into your converged attack surface while measuring and controlling cyber risk across your OT and IT systems.
- Advanced Threat Detection to proactively identify weak points in the OT environment before an attack ever occurs. Tenable.ot's multi-detection engine, identifies policy violations, detects anomalous behaviors and tracks signatures for potential high-risk events.
- Asset Inventory gives you deep insights and unparalleled situational awareness into your infrastructure without impacting operations.
- Risk-Based Vulnerability Management leverages domain expertise in industrial security for OT assets, and Nessus for IT assets. Tenable's VPR scoring generates vulnerability and risk levels using each asset in your ICS network.
- Configuration Control track malware and user-executed changes made over your network or directly on a device. Tenable.ot provides a full history of device configuration changes over time.

Tenable.ot's Alignment to the NIST Framework Core Functions*

The table below maps the functionality of Tenable.ot's to the five pillars of the CSF and relevant categories:

IDENTIFY (ID)

CATEGORY	SUBCATEGORY	TENABLE.OT
Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	ID.AM-1: Physical devices and systems within the organization are inventoried	Tenable.ot automatically discovers and maps all OT devices and keeps an up-to-date inventory of these assets. This includes the operator and engineering workstations and controllers (PLCs, RTUs and DCS controllers), and I/Os. Tenable.ot's patented active querying technology enables the discovery of devices even if they aren't actively communicating over the network. Tenable.ot collects highly granular information on each device, including the firmware versions, PLC backplane configurations and serial numbers of the devices. The asset inventory is continuously updated with any changes made to OT devices, as well as when devices are added/removed.
	ID.AM-2: Software platforms and applications within the organization are inventoried	Tenable.ot automatically identifies the configuration settings and the control code on the industrial controllers, facilitating configuration management of these devices. It also classifies IT devices that are used in an OT environment, such as HMIs and engineering stations.
	D.AM-3: Organizational communication and data flows are mapped	Tenable.ot automatically maps communication links and data flows between all of the assets in the organization's network. Tenable.ot's baseline deviation capabilities will also alert on changes in these data flows.

*The following does not represent the NIST Framework guidelines in its entirety. For the full NIST Framework Guidelines, visit: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

IDENTIFY (ID) Continued

CATEGORY	SUBCATEGORY	TENABLE.OT
Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	Tenable.ot supports the implementation of out-of-the-box and custom security policies, providing real-time alerts on every cyber event that takes place within the OT network. Alerts can be exported to a variety of systems including SIEM, SOAR, NGFWs and SOCs. Alerts can also be sent to a ticketing system or sent via email to any internal or external stakeholder.
	ID.GV-4: Governance and risk management processes address cybersecurity risks	Tenable.ot supports the governance and risk management processes by providing full and detailed analysis on the industrial environment, network behavior, asset inventory and risk posture.
Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	ID.RA-1: Asset vulnerabilities are identified and documented	Tenable.ot's Risk Assessment report includes a vulnerability drill down tab that dives into vulnerabilities that exist in the environment. Full details are provided for each vulnerability, including description, affected assets, severity and mitigation steps. A clear view of the most common and severe vulnerabilities helps prioritize patching and software updates for purposes of reducing the environment's overall risk.
	D.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	Tenable's Risk Assessment report takes into account alerts in the environment, existing known vulnerabilities and specific aspects in the configuration of controllers that may expose them to potentially malicious threats. A vulnerability priority rating (VPR) score goes beyond a CVSS score and quantifies the risk relative to your specific environment.

PROTECT (RR)

CATEGORY	SUBCATEGORY	TENABLE.OT
Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	ID.AM-1: Physical devices and systems within the organization are inventoried	Industrial controllers usually don't support authentication. To compensate for that, Tenable.ot serves as a control through auditing successful and unsuccessful access attempts made by users and alerting in real-time on unauthorized access and anomalies. Furthermore, Tenable.ot partners with many of the top PAM vendors to add robust and seamless access control features to the OT environment.
	PR.AC-2: Physical access to assets is managed and protected	In most cases, industrial controllers can be easily accessed (i.e. physically). Such access cannot be monitored over the network. Tenable.ot's patented active technology is used to monitor all physical access and assures no unauthorized changes were made to controller configurations, code, firmware and/or settings.
	PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	Given industrial controllers don't typically support authentication, Tenable.ot serves as a compensating control by auditing successful and unsuccessful access attempts made by users and alerting in real-time on unauthorized access and anomalies. Furthermore, Tenable.ot partners with many of the top PAM vendors to add robust and seamless access control features to the OT environment.
Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	PR.DS-1: Data-at-rest is protected	Since data-at-rest and data-in-transit on industrial controllers are not protected, Tenable.ot is used as a compensating control to monitor all access and changes to this data. It also alerts in real-time on suspicious and unauthorized access and changes.
	PR.DS-2: Data-in-transit is protected	
	PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	All assets within the OT networks are automatically mapped and inventoried. The user is alerted in real-time on all changes made to the inventory, including devices that are being connected or disconnected from the network. Formal asset removal procedure is facilitated by the system as well.
	PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	Tenable.ot's patented active technology verifies that industrial PLCs' code, firmware and setting integrity are secured.

PROTECT (RR) Continued

CATEGORY	SUBCATEGORY	TENABLE.OT
Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained	Tenable.ot's Configuration Control is used to automatically build a baseline of the industrial controllers' firmware, code and hardware configurations. This information is backed up per asset, and is used to perform periodic controller integrity checks. Users can set the identified configuration as the baseline. Tenable.ot extracts the names and module numbers of all the modules on the controller's backplane. The user can be alerted on changes identified in either of the modules on the backplane.
	PR.IP-3: Configuration change control processes are in place	Every configuration change is automatically identified and flagged, regardless of whether it's done over the network or via physical access to the device. User-defined policies are used to distinguish authorized changes from unauthorized/malicious ones. Users can resolve alerts through the system and set new configuration baselines as needed.
	PR.IP-12: A vulnerability management plan is developed and implemented	Tenable.ot recognizes and alerts on vulnerabilities to both IT and OT assets based on known vulnerabilities issued in the CVE list as well as newly discovered vulnerabilities identified by the Tenable zero day research team.
Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.	R.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	Any remote access to the network, whether authorized or not, is automatically identified, flagged and logged. The system alerts on unauthorized/malicious access.
Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	Tenable.ot produces and stores a very comprehensive system log, facilitating the consumption of this information by Tenable.sc, NGFW, and SOAR systems.
	PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality	Given industrial controllers usually do not support authentication, Tenable.ot serves as a compensating control, by auditing successful and unsuccessful access attempts made by users, and providing real-time alerts on suspicious and unauthorized access. Tenable.ot partners with many of the top PAM vendors to add robust and seamless access control features to the OT environment.

DETECT (DE)

CATEGORY	SUBCATEGORY	TENABLE.OT
Anomalies and Events (DE.AE): Anomalous activity is detected in a timely manner and the potential impact of events is understood.	DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	Tenable.ot enables the user to define a baseline based on existing network traffic and behaviors. Tenable.ot receive alerts in the event of any deviations. The Tenable.ot baseline can be updated at any time.
	DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	Tenable.ot's integrates with the larger Tenable portfolio such as Tenable.io and Tenable.sc as well as leading SIEM, SOAR, NGFW solutions where they are utilized for data correlation between multiple sources.
	DE.AE-5: Incident alert thresholds are established	Tenable.ot offers very granular and customizable policies, allowing administrators to set custom thresholds and customize incident alerts. Using Tenable.ot's policy system, administrators can configure alerts based on specific parameters. It is also possible to define the allowed ranges for them. Users are alerted in the event of deviations.
Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	DE.CM-1: The network is monitored to detect potential cybersecurity events	Tenable.ot continuously monitors all OT activities, including activities taking place over proprietary control-plane protocols. Tenable.ot identifies real-time anomalies, suspicious and unauthorized activities, enabling it to detect and alert on cybersecurity events.
	DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	Since industrial controllers can be easily accessed physically, The Tenable.ot's patented active technology is used to monitor physical access and ensure such access wasn't used for unauthorized or malicious changes of controller configurations, code, firmware and settings. Tenable.ot also monitors abnormal changes of set-points. Using the policies system, the user can configure to alert on changes made to specific parameters, as well as defining the allowed ranges and deviations for alerts. This can be used to alert on changes resulting from physical access/manipulation of sensor information.
	DE.CM-4: Malicious code is detected	Malicious code is detected in three different ways: 1. by monitoring engineering activities which are used for updating control code. 2. by periodically verifying controllers' code and validating its integrity. 3. by flagging anomalous net-flows that may be caused by the existence of malicious code.

DETECT (DE) Continued

CATEGORY	SUBCATEGORY	TENABLE.OT
Security Continuous Monitoring (DE.CM)(continued)	DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	Any access by an external service provider to the network, whether authorized or not, is automatically identified, flagged and logged. A comprehensive audit trail tracks all service provider activities and ensures services were delivered as planned. Real-time alerts are sent on any unauthorized/ suspicious activity.
	DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	Tenable.ot detects and alerts on all ICS access and activities including unauthorized network connections, new devices that are being connected, deviations from the network traffic baseline, and all changes made to the industrial controllers' software.
	DE.CM-8: Vulnerability scans are performed	Tenable.ot's vulnerability assessment functionality provides detailed information on the vulnerabilities that exist in the environment. Full details are provided for each vulnerability (whether IT or OT based), including description, affected assets, severity and mitigation steps. A clear view of the most common and severe vulnerabilities helps prioritize patching and software updates for purposes of reducing the environment's overall risk.
Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.	DE.DP-4: Event detection information is communicated	Tenable.ot provides users with various methods to receive event information: 1. User Interface 2. Other Tenable portfolio products such as Tenable.sc and Tenable.io as well as leading security product such as NGFWs, SIEM and SOAR. 3. Popular ticketing systems and Email Each alert contains detailed information relevant to that specific event i.e. who, what, when, where, etc. Tenable.ot also supports retaining of full packet captures for forensic analysis. This allows the user to download a copy of the traffic in PCAP format to further investigate alerts and network events.

Respond (RS)

CATEGORY	SUBCATEGORY	TENABLE.OT
Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.	RS.CO-2: Events are reported consistent with established criteria	Tenable.ot offers very granular, customizable policies to alert on specific events based on predefined criteria. This includes source device, user, destination device, protocols used and time of the event.
Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.	RS.AN-3: Forensics are performed	Tenable.ot is a key source of forensics information: raw network traffic, audit trail of configuration and code changes, as well as comprehensive details about the assets inventory. This information provides unparalleled forensic support. Tenable.ot also retains full packet captures for forensic analysis, allowing users to download a copy of the traffic in PCAP format to further investigate alerts and network events.
	RS.AN-5: Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)	Tenable.ot recognizes and alerts on vulnerabilities to industrial controllers, based on known vulnerabilities listed in the CVE list as well as newly discovered vulnerabilities by Tenable research. Exact matching of vulnerabilities to controllers is performed based on Tenable.ot's detailed knowledge of controller models and firmware versions. There is also the option of raising an alert whenever a new vulnerability is identified.
Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.	RC.RP-1: Recovery plan is executed during or after an event	Tenable.ot helps simplify and accelerate recovery processes, as it stores historical information about controller configurations and settings. This directly supports asset backup and recovery.

ABOUT TENABLE

Tenable, Inc. is the Cyber Exposure company. Over 30,000 organizations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus, Tenable extended its expertise in vulnerabilities to deliver the world's first platform to see and secure any digital asset on any computing platform. Tenable customers include more than 50 percent of the Fortune 500, more than 30 percent of the Global 2000 and large government agencies. Learn more at www.tenable.com.