CYBERBIT
PROTECTING A NEW DIMENSION

Aligning with Tier 4 NIST Framework for Critical Infrastructure Cybersecurity

with Cyberbit SCADAShield ICS/SCADA Security Solution

White Paper

www.cyberbit.com | sales@cyberbit.com

Table Of Contents

Cybersecurity Technology for ICS

ICS networks used to be isolated systems that ran on specialized, proprietary hardware and software. They were not connected to the internet and therefore the only way malicious actors could damage them would be a physical attack from the outside or internal sabotage by authorized personnel. Today, most ICS networks have evolved to use IP devices that can connect to the internet to allow connectivity and remote access management. IP devices have brought with them great operational advantages, but at the cost of opening previously "air gapped" ICS networks to the danger of cyber-attack.

The NIST Framework for Improving Critical Infrastructure Cybersecurity has laid forth a comprehensive industry standard for cybersecurity of ICS networks. This guideline addresses every aspect of cybersecurity protection for critical infrastructure, transportation, chemical and pharmaceutical, pulp and paper, food and beverage and discrete manufacturing. Modern, connected ICS networks have much in common with internet technology (IT) networks, but they also have unique characteristics and requirements that make securing them a special case;

> Many of these differences stem from the fact that logic executing in ICS has a direct effect on the physical world. Some of these characteristics include significant risk to the quotations health and safety of human lives and serious damage to the environment, as well as serious financial issues such as production losses, negative impact to a nation's economy, and compromise of proprietary information.
>
> - Guide to Industrial Control system (ICS) Security, NIST

Cyberbit SCADAShield

Cyberbit SCADAShield is a detection system for ICS networks that helps organizations implement the NIST framework at the highest level of adaptive security - Tier 4.

Cyberbit SCADAShield is aligned with NIST guidelines to help industrial organizations reduce their cybersecurity risk. According to NIST, "behavioral anomaly detection technology can provide a key security component in sustaining business operations, particularly those based on ICS[1]." Cyberbit developed SCADAShield to meet the special security needs of modern ICS systems by providing; OT asset discovery and visibility, detection of known OT threats, unknown OT threats and anomalies, as well as deviations from operational restrictions, by using 7-layer deep packet Granular Deep Packet Inspection (GDPI).

Achieve Tier 4 NIST Framework Implementation

The NIST Framework defines an organization's cybersecurity maturity and level of practice with the follow four tiers:

- Tier 1: Partial
- Tier 2: Risk Informed
- Tier 3: Repeatable
- Tier 4: Adaptive

This whitepaper will describe how Cyberbit SCADAShield helps ICS organizations that seek the highest level of cybersecurity achieve Tier 4 adaptive risk management. The SCADAShield platform enables organizations to move from simple ICS perimeter security to continuous ICS threat monitoring, asset discovery, and threat intelligence. In particular, ICS-specific behavioral analytics and machine learning rapidly detect anomalous behavior.

[1] https://csrc.nist.gov/publications/detail/white-paper/2016/11/07/[project-description]-securing-manufacturing-ics/draft

NIST Tier 4 - Adaptive Cybersecurity Implementation

The NIST Cybersecurity Framework document defines the highest level of implementation, Tier 4, as follows:

Risk Management Process

The organization adapts its cybersecurity practices based on lessons learned and predictive indicators derived from previous and current cybersecurity activities. Through a process of continuous improvement incorporating advanced cybersecurity technologies and practices, the organization actively adapts to a changing cybersecurity landscape and responds to evolving and sophisticated threats in a timely manner.

Integrated Risk Management Program

There is an organization-wide approach to managing cybersecurity risk that uses risk-informed policies, processes, and procedures to address potential cybersecurity events. The relationship between cybersecurity risk and mission/business objectives is clearly understood and considered when making decisions. Senior executives monitor cybersecurity risk in the same context as financial risk and other organizational risks. The organizational budget is based on understanding of current and predicted risk environment and future risk appetites. Business units implement executive vision and analyze system level risks in the context of the organizational risk appetite and tolerances. Cybersecurity risk management is part of the organizational culture and evolves from an awareness of previous activities, information shared by other sources, and continuous awareness of activities on their systems and networks. Cybersecurity risk is clearly articulated and understood across all strata of the enterprise. The organization can quickly and efficiently account for changes to business/mission objectives and threat and technology landscapes in how risk is communicated and approached.

External Participation

The organization manages risk and actively shares information with partners to ensure that accurate, current information is being distributed and consumed to improve cybersecurity before a cybersecurity event occurs.

- "Framework for Improving Critical Infrastructure Cybersecurity"
Version 1.1 National Institute of Standards and Technology April 16, 2018

Identify, Detect and Respond

The NIST cybersecurity framework core describes requirements for five high-level functional areas; Identify, Protect, Detect, Respond and Recover. Each section below will enumerate how deploying Cyberbit SCADAShield helps an organization achieve Tier 4 implementation in the **Identify**, **Detect** and **Respond** functions.

Identify (ID)

The ID requirements include risk assessment and risk management strategy as defined below:

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 Subcategory	SCADAShield Tier 4 Compliance
ID.AM-1: Physical devices and systems within the organization are inventoried **NIST SP 800-53 Rev. 4 CM-8**	Asset Management: Ability to identify device types over the OT network: engineering station, HMI, PLC/RTU, SCADA server, asset types, identify OT controllers firmware / OS type, firmware version, controller type, serial number, IP, MAC, last seen, last firmware update.
ID.AM-3: Organizational communication and data flows are mapped **NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8**	Network map that displays all discovered assets, protocols and communication between all entities in the OT network.

Risk management strategy (ID.RM)

The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.

ID.RA Subcategory	SCADAShield Tier 4 Capabilities
ID.RA-1: Asset vulnerabilities are identified and documented **NIST SP 800-53 Rev. 4 CA-2, CA-7, CA-8, RA-3, RA-5, SA-5**	Detection of asset vulnerabilities, based on research and known CVE's including explanation and references to CVE database.
ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources **NIST SP 800-53 Rev. 4 PM-15, PM-16, SI-5**	CVE's - known vulnerabilities that have been received from information sharing forums.
ID.RA-3: Threats, both internal and external, are identified and documented **NIST SP 800-53 Rev. 4 RA-3, SI-5, PM-12, PM-16**	SCADAShield detects threats originated from: CVE's, policy violations, anomalies, human errors and system malfunctions. All include full description and documentation of the vulnerability. Full audit of all network communication.
ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk **NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-16**	Threats, vulnerabilities, blacklist policy violations and whitelist policy violations are used to calculate the risk score of each asset.

Risk management strategy (ID.RM)

The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.

ID.RM Subcategory	SCADAShield Tier 4 Compliance
IID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders **NIST SP 800-53 Rev. 4 PM-9**	Risk assessment is defined by an algorithm that calculates asset vulnerabilities, blacklisting policies related to the asset, whitelisting policy violations and the industrial process that the asset is part of. Together all these factors determine the risk assessment.
ID.RM-2: Organizational risk tolerance is determined and clearly expressed **NIST SP 800-53 Rev. 4 PM-9**	SCADAShield comes with default risk tolerance settings that can be customized to reflect the organization's risk management strategy.

Detect (DE)

The DE requirements involve developing and implementing the appropriate activities to identify the occurrence of a cybersecurity event. The Detect Function enables timely discovery of cybersecurity events. Examples of outcome categories within this Function include: Anomalies and Events; Security Continuous Monitoring; and Detection Processes.

Anomalies and events (DE.AE)

Anomalous activity is detected in a timely manner and the potential impact of events is understood.

DE.AE Subcategory	SCADAShield Tier 4 Capabilities
DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed **NIST SP 800-53 Rev. 4 AC-4, CA-3, CM-2, SI-4**	SCADAShield continuous scanning and monitoring creates a baseline which is the OT network policy. Each policy contains the expected data flow and system behavior.
DE.AE-2: Detected events are analyzed to understand attack targets and methods **NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, SI-4**	All detected policy deviations trigger an alert which includes reasoning. SCADAShield Insights component stores all OT network communication data and uses it for root cause analysis and forensic investigation.
DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors **NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, IR-8, SI-4**	All event data and alerts are aggregated and correlated and are clearly explained with response recommendations provided.

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 Subcategory	SCADAShield Tier 4 Capabilities
DE.CM-1: The network is monitored to detect potential cybersecurity events **NIST SP 800-53 Rev. 4 AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4**	SCADAShield continuously monitors the OT network and alerts whenever there is a potential threat, policy deviation, anomaly, human error or system malfunction.
DE.CM-2: The physical environment is monitored to detect potential cybersecurity events **NIST SP 800-53 Rev. 4 CA-7, PE-3, PE-6, PE-20**	SCADAShield continuously scans and monitors the physical environment in order to detect potential threats.
DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed **NIST SP 800-53 Rev. 4 AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4**	SCADAShield continuously scans and monitors to ensure that every policy deviation; including, human error, unauthorized connections, devices or software, will be detected, generate an alert and suggest the right remediation action.
DE.CM-8: Vulnerability scans are performed **NIST SP 800-53 Rev. 4 RA-5**	SCADAShield continuously monitors the OT network to detect vulnerabilities.

Detection processes (DE.DP)

Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.

IDE.DP Subcategory	SCADAShield Tier 4 Capabilities
DE.DP-2: Detection activities comply with all applicable requirements **NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14, SI-4**	SCADAShield scanning and detection automatically creates a baseline for all policies, enforces policies and detects deviation.
DE.DP-4: Event detection information is communicated to appropriate parties **NIST SP 800-53 Rev. 4 CA-2, CA-7, PE-3, PM-14, SI-3, SI-4**	In case of a policy deviation, SCADAShield triggers the corresponding alert including a detailed explanation of the threat and communication templates for sharing information with all the appropriate entities.

Response (RS)

Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.

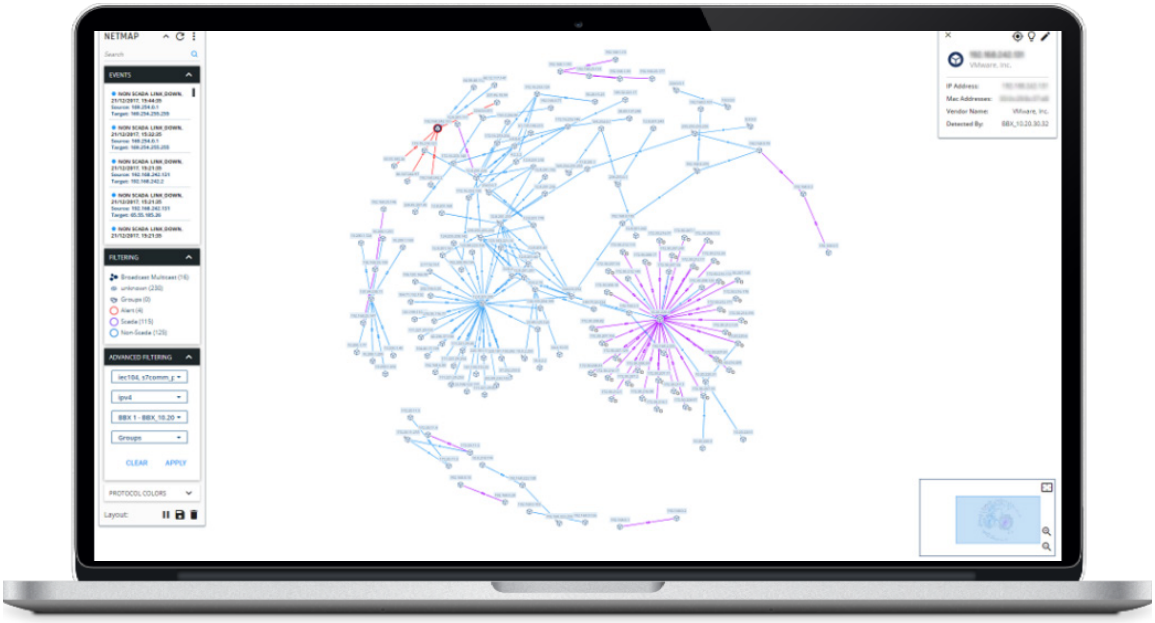
Analysis (RS.AN)

Analysis is conducted to ensure adequate response and support recovery activities.

RS.AN Subcategory	SCADAShield Tier 4 Capabilities
RS.AN-1: Notifications from detection systems are investigated **NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, PE-6, SI-4**	SCADAShield uses forensic capabilities that allow users to investigate all alert oriented communications.
RS.AN-2: The impact of the incident is understood **NIST SP 800-53 Rev. 4 CP-2, IR-4**	
RS.AN-3: Forensics are performed **NIST SP 800-53 Rev. 4 AU-7, IR-4**	SCADAShield stores all OT network communication in the Insight component which includes analytical abilities, filtering and value search.

About Cyberbit SCADAShield

Cyberbit SCADAShield is a non-intrusive solution for OT network monitoring, detection, forensics and response. It discovers and visualizes all OT network components and communications, monitors both OT and IT protocols, and enables OT and IT managers to detect, analyze and respond to network anomalies, vulnerabilities and threats. By using Granular Deep Packet Inspection (GDPI), SCADAShield identifies the specific fields which should be analyzed in each layer of the inspected protocol. SCADAShield analyzes both IP and serial protocols, taps all network activities and maps all assets. As a result, it provides IT and OT managers with unmatched visibility and security of their OT network and facilitates advanced detection, easy analysis, and faster response.



About Cyberbit

Cyberbit provides a consolidated detection and response platform that protects an organization's entire attack surface across IT, OT and IoT networks. Cyberbit products have been forged in the toughest environments on the globe and include: behavioral threat detection, incident response automation and orchestration, ICS/SCADA security, and the world's leading cyber range. Since founded in mid-2015 Cyberbit's products were rapidly adopted by enterprises, governments, academic institutions and MSSPs around the world. Cyberbit is a subsidiary of Elbit Systems (NASDAQ: ESLT) and has offices in Israel, the US, Europe, and Asia.

sales@cyberbit.com | www.cyberbit.com

US Office:
3800 N. Lamar Blvd. Suite 200
Austin, TX 78756
Tel: +1-737-717-0385

Israel Office:
22 Zarchin St. Ra'anana
Israel 4310602
Tel: +972-9-7799800

CYBERBIT
PROTECTING A NEW DIMENSION

Identify (ID)

Achieve Tier 4 NIST Cyberbsecurity for ICS Networks with Cyberbit SCADAShield

Asset Management (ID.AM)	
ID.AM-1: Physical devices and systems within the organization are inventoried **NIST SP 800-53 Rev. 4 CM-8**	Asset Management: Ability to identify device types over the OT network: engineering station, HMI, PLC/RTU, SCADA Server, asset types, identify OT controllers firmware / OS type, firmware version, controller type, serial number, IP, MAC, last seen, last firmware update
ID.AM-3: Organizational communication and data flows are mapped NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8	Netmap that shows the communication between all entities in the OT network , the communications packets and their values
Risk Assesment (ID.RA)	
ID.RA-1: Asset vulnerabilities are identified and documented **NIST SP 800-53 Rev. 4 CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5**	Detection of asset vulnerabilities, based on research and known CVE's including explanation and references to CVE database
ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources **NIST SP 800-53 Rev. 4 PM-15, PM-16, SI-5**	CVE's - known vulnerabilities that have been received from information sharing forums
ID.RA-3: Threats, both internal and external, are identified and documented **NIST SP 800-53 Rev. 4 RA-3, SI-5, PM-12, PM-16**	"SCADAShield detects threats originated from: CVE's, policy violations, anomalies, human errors and system malfunctions. All include full description and documentation of the vulnerability. Full audit of all network communication"
ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk **NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-16**	Threats, vulnerabilities, black policy violations and white policy violations are used to calculate the risk score of each asset.
RISK MANAGEMENT STRATEGY (ID:RM)	
ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders **NIST SP 800-53 Rev. 4 PM-9**	Risk assessment is defined by an algorithm that calculates asset vulnerabilities, black policies related to the asset, white policy violations and the industrial process that the asset is part of. Together all these factors determine the risk assessment.
ID.RM-2: Organizational risk tolerance is determined and clearly expressed **NIST SP 800-53 Rev. 4 PM-9**	Organizational risk is clearly expressed and visible by determining the risk assessment of every asset

Detect (ID)

Achieve Tier 4 NIST Cyberbsecurity for ICS Networks with Cyberbit SCADAShield

Anomalies and Events (DE.AE)	
DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed **NIST SP 800-53 Rev. 4 AC-4, CA-3, CM-2, SI-4**	SCADAShield continuous scanning and monitoring creates a baseline which is the OT network policy. Each policy contains the expected data flow and system behavior.
DE.AE-2: Detected events are analyzed to understand attack targets and methods **NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, SI-4**	All detected policy deviations trigger an alert which includes reasoning. SCADAShield Insights component stores all OT network communication data and uses it for root cause analysis and forensic investigation.
DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors **NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, IR-8, SI-4**	All event data and alerts are aggregated and corelated and are clearly explained with response recommendations provided
Security Continuous Monitoring (DE.CM)	
DE.CM-1: The network is monitored to detect potential cybersecurity events **NIST SP 800-53 Rev. 4 AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4**	SCADAShield continuously monitors the OT network and alerts whenever there is a potential threat, policy deviation, anomaly, human error or system malfunction.
DE.CM-2: The physical environment is monitored to detect potential cybersecurity events **NIST SP 800-53 Rev. 4 CA-7, PE-3, PE-6, PE-20**	SCADAShield continuously scans and monitors the physical environment in order detect potential threats
DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed **NIST SP 800-53 Rev. 4 AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4**	SCADAShield continuously scans and monitors to ensure that every policy deviation; including, human error, unauthorized connections, devices or software, will be detected, generate an alert and suggest the right remediation action
DE.CM-8: Vulnerability scans are performed **NIST SP 800-53 Rev. 4 RA-5**	SCADAShield continuously monitors the OT network to detect vulnerabilities
Detection Processes (DE.DP)	
DE.DP-2: Detection activities comply with all applicable requirements **NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14, SI-4**	SCADAShield scanning and detection automatically creates a baseline for all policies and enforces policies and detects deviation.
DE.DP-4: Event detection information is communicated to appropriate parties **NIST SP 800-53 Rev. 4 CA-2, CA-7, PE-3, PM-14, SI-3, SI-4**	In case of a policy deviation, SCADAShield triggers relevant alert including and explanation of the threat and the appropriate remediation steps

Response (RS)

Analysis (RS.AN)	
RS.AN-1: Notifications from detection systems are investigated **NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, PE-6, SI-4**	SCADAShield uses forensic capabilities that allow users to investigate all alert oriented communications and root cause analysis
RS.AN-2: The impact of the incident is understood **NIST SP 800-53 Rev. 4 CP-2, IR-4**	
RS.AN-3: Forensics are performed NIST SP 800-53 Rev. 4 AU-7, IR-4	SCADAShield stores all OT network communication in the Insight component which includes analytical abilities, filtering and value search.