CYBERSECURITY ROADSHOW

The ABCs of Cybersecurity for Manufacturing

TERM	CATEGORY	DEFINITION
Antivirus	Terminology	Programs that are designed to prevent, search for, detect, and remove software viruses, and other malicious software like worms, trojans, adware, and more.
Asset Management	Terminology	Asset management tool is a dedicated application/software which is used to record and track an asset throughout its life cycle.
Automated Detection	Terminology	Network and Host based Intrusion Detection Systems and Antivirus Software
Black listing	Terminology	Application blacklisting, sometimes just referred to as blacklisting, is a network administration practice used to prevent the execution of undesirable programs. Such programs include not only those known to contain security threats or vulnerabilities but also those that are deemed inappropriate within a given organization.
CIS CSC 20	Standards/ Compliance	A framework managed by the Center for Internet Security (CIS) that includes 20 critical security controls (CSC). This framework is common in the private sector and was developed with government and private sector groups.
CMMC	Standards/ Compliance	Cybersecurity Maturity Model Certification. CMMC builds on DFARS by adding a new verification component to the cybersecurity requirements. Third-party assessors soon will need to certify that contractors are in compliance. This is most common for DOD suppliers.
Control level	Terminology	A general term that indicates the safeguarding and disseminating requirements associated with CUI Basic and CUI Specified.
Controlled Environment	Terminology	Any area or space an authorized holder deems to have adequate physical or procedural controls (e.g., barriers or managed access controls) to protect CUI from unauthorized access or disclosure.
Controlled Unclassified Information	Terminology	Information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls.
Covered Defense Information (CDI)	Terminology	CDI means unclassified controlled technical information or other information (as described in the Controlled Unclassified Information (CUI) Registry) that requires safeguarding or dissemination controls pursuant to and consistent with laws, regulations, and Government wide policies, and is— (1) Marked or otherwise identified in the contract, task order, or delivery order and provided to the contractor by or on behalf of DoD in support of the performance of the contract; or (2) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract.

TERM	CATEGORY	DEFINITION
Denial of Service (DoS)	Terminology	Denial of Service attack or Distributed Denial of Service attacks. Each involves flooding a computer or network with online traffic until it slows or crashes. In a DDoS attack, multiple computers carry out a coordinated attack, often using a botnet or group of hijacked connected devices to multiply traffic exponentially.
DFARS or NIST 800-171	Standards/ Compliance	Defense Federal Acquisition Regulation. It seeks to ensure cybersecurity in the nation's supply chain and specifies the contracting rules that companies doing business with DoD, military departments, and defense agencies must follow. It governs things like contract administration, contract pricing, contracting officers' responsibilities, purchasing thresholds, research and development, and who can conduct procurement for the military.
DoD	Terminology	U.S. Department of Defense
Encrypted Protocol	Terminology	A formula used to turn ordinary data, or "plaintext," into a secret coded message known as "ciphertext." The ciphertext can reside in storage or travel over unsecure networks without its contents being divulged to unauthorized people.
Hardware	Terminology	Hardware is best described as a device, such as a hard drive, that is physically connected to the computer or something that can be physically touched.
ICS	Terminology	Industrial Control Systems (ICS) are computer-controlled systems that automate or remotely monitor or control production, handling or distribution in manufacturing and other industries. Many of these systems connect directly or indirectly to the internet, making them vulnerable to cyber-attacks.
Incident Analysis	Terminology	Understand Normal Behaviors, Create a Log Retention Policy, Perform Event Correlation.
Information Technology (IT)	Terminology	The use of systems (especially computers and telecommunications) for storing, retrieving, and sending information.
ISO 27002	Standards/ Compliance	Code of practice for information security controls - essentially a detailed catalog of information security controls that might be managed through the Information Security Management System (ISMS)
Manual Detection	Terminology	Problems reported by users
MEP	Terminology	Manufacturing Extension Partnership, run out of the NIST office. MEP is a public-private partnership with Centers in all 50 states and Puerto Rico dedicated to serving small and medium-sized manufacturers.
Multi-Factor Authentication (MFA)	Terminology	Multi-factor authentication is an electronic authentication method in which a computer user is granted access to a website or application only after successfully presenting two or more pieces of evidence to an authentication mechanism: knowledge, possession, and inherence.

TERM	CATEGORY	DEFINITION
NERC CIP	Standards/ Compliance	North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) is a set of requirements designed to secure the assets required for operating North America's bulk electric system.
Network Intrusion Detection System (NIDS)	Terminology	Continuous monitoring network traffic and systems to detect cybersecurity events.
Network Security	Terminology	Network security consists of the policies and practices adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources.
Network Segmentation	Terminology	Network segmentation in computer networking is the act or practice of splitting a computer network into subnetworks, each being a network segment. Advantages of such splitting are primarily for boosting performance and improving security.
NICE	Terminology	National Initiative for Cybersecurity Education. Hosted by NIST, this collection of resources aims to close hiring gaps in the cybersecurity workforce.
NIST	Terminology	National Institute of Standards and Technology. NIST is a U.S. Department of Commerce agency whose mission is to promote innovation and competitiveness in manufacturing. Its robust cybersecurity programs offer many resources for industry. Resources like the Cybersecurity Framework, voluntary guidance that organizations can use to manage and reduce their cybersecurity risk.
NIST Cyber Security Framework (CSF, NIST Wheel)	Standards/ Compliance	The NIST Cybersecurity Framework provides a policy framework of computer security guidance for how private sector organizations in the United States can assess and improve their ability to prevent, detect, and respond to cyber attacks.
Operational Technology (OT)	Terminology	Operational technology, monitors and manages industrial process assets and manufacturing/industrial equipment.
Password Management	Terminology	A password manager is a computer program that allows users to store, generate, and manage their personal passwords for online services. A password manager assists in generating and retrieving complex passwords, potentially storing such passwords in an encrypted database or calculating them on demand.
Patch	Terminology	A patch updates one component of a system's software, perhaps to fix a bug or error discovered after product release.
Software	Terminology	Software is a general term used to describe a collection of computer programs, procedures, and documentation that perform some task on a computer system.
Unclassified Controlled Technical Information (UCTI)	Terminology	Technical data or computer software with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination.

TERM	CATEGORY	DEFINITION
Web Application Security	Terminology	Web application security is a branch of information security that deals specifically with security of websites, web applications and web services. At a high level, web application security draws on the principles of application security but applies them specifically to internet and web systems.
White listing	Terminology	Application whitelisting is the practice of specifying an index of approved software applications or executable files that are permitted to be active on a computer system. The goal of whitelisting is to protect computers and networks from potentially harmful applications.