MOXA

Cybersecurity 101 - the Industrial Cybersecurity Terms You Should Know

Common Terminology

Common Cybersecurity Terms You Should Know

Understanding common cybersecurity terminology can help you discuss important matters with IT professionals.

Concept	Defense Mechanism	Threats
Defense in Depth	Firewall	Malware
	IDS (Intrusion Detection System)	Ransomware
	IPS (Intrusion Prevention System)	DoS/DDoS
	DPI (Deep Packet Inspection)	

Defense in Depth

Defense-in-depth Security Architecture

The concept is based on multiple layers of security mechanisms that increase security of the system as a whole. If one of the security mechanisms fails, other mechanisms function as a backup to help keep the network secure.

Industrial Firewall

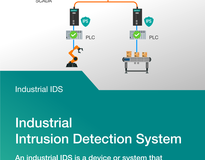
Industrial Firewalls Monitor Traffic to and From Networks

A resilient control network relies on a network that can effectively detect and filter unwanted traffic. Industrial firewalls restrict traffic based on a defined set of security rules.

Industrial IPS

Industrial Intrusion Prevention System

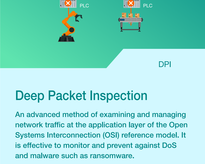
An industrial IPS is a device or system that identifies malicious activity, logs information about this activity, reports it, and then attempts to block or stop it. An industrial IPS takes advantage of Deep Packet Inspection (DPI) technology to get information of the payload of data.



Industrial IDS

Industrial Intrusion Detection System

An industrial IDS is a device or system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered.



DPI

Deep Packet Inspection

An advanced method of examining and managing network traffic at the application layer of the Open Systems Interconnection (OSI) reference model. It is effective to monitor and prevent against DoS and malware such as ransomware.

Malware

Malware

A general term referring to any software intentionally designed to cause damage to a computer, server, client, or computer network.

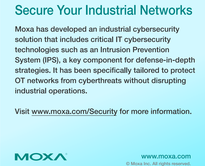
DoS/DDoS

Cyberincidents

- Ransomware hit a leading chipset manufacturer, causing losses of US$ 170 million
- LockerGoga ransomware attack in 2019, which caused losses in excess of US$ 40 million

Denial of Service (DoS) / Distributed Denial of Service (DDoS)

DoS is an attack meant to shut down a machine or network, making it inaccessible to its intended users. It can be accomplished by flooding the target with traffic, or sending information that triggers a crash. DDoS can be conducted by flooding the target with traffic from different hosts to avoid the target getting or sending any information out.



OT-IT Integrated Security

Secure Your Industrial Networks

Moxa has developed an industrial cybersecurity solution that includes critical IT cybersecurity technologies such as an Intrusion Prevention System (IPS), a key component for defense-in-depth strategies. It has been specifically tailored to protect OT networks from cyberthreats without disrupting industrial operations.

Visit www.moxa.com/Security for more information.

MOXA

www.moxa.com

© Moxa Inc. All rights reserved.