Question #1 *Topic 1*

For application-aware firewalls filtering traffic between trust zones, which of the following policies should be applied to a packet that doesn't match an existing rule?

A. Default alert

B. Default deny

C. Application deny list

D. Application allow list

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #2 *Topic 1*

An administrator wants to script the deployment of a security policy, over the network, to a group of workstations not managed by Active Directory. What tool could be used to accomplish this task?

A. secedit.exe

B. secpol.msc

C. gpedit.msc

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #3 *Topic 1*

A brewer uses a local HMI to communicate with a controller that opens a pump to move the wort from the boil kettle to the fermentor. What level of the Purdue model would the controller be considered?

A. Level 2

B. Level 1

C. Level 0

D. Level 3

E. Level 4

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #4 *Topic 1*

How is a WirelessHART enabled device authenticated?

A. Using a WPA2 pre-shared key entered by an administrator

B. Using a join key to send an encrypted request for the shared network key

C. Using the vendor hard-coded master key to obtain a link key

D. Using a PIN combined with the device MAC address

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #5 *Topic 1*

Which type of process is described below?
A fermentor's glycol jacket must maintain a steady temperature during and between batches of beer.

A. Continuous

B. Manual

C. Discrete

D. Batch

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #6 *Topic 1*

What kind of data could be found on a historian?

A. Information needed for billing customers

B. Information for supervising lower-level controllers in real-time

C. Diagrams depicting an overview of the process

D. Runtime libraries that software programs use

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #7 *Topic 1*

Which of the following can an attacker gain by obtaining PLC logic project files for a SCADA system?

A. Data regarding personnel and hiring practices

B. Details about the network architecture

C. Information about operational firewall rulesets

D. Schedule of vendor product releases

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #8 *Topic 1*

Which control helps prevent threats to Integrity?

A. Firewall egress filtering

B. Logging IDS alerts

C. Centralized LDAP authentication

D. Implementing digital signatures

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #9 *Topic 1*

What mechanism could help defeat an attacker's attempt to hide evidence of his/her actions on the target system?

A. Attack surface analysis

B. Application allow lists

C. Sandboxing

D. Centralized logging

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #10 *Topic 1*

An attacker has a goal of obtaining information stored in an ICS. Why might the attacker focus his efforts on the operating system rather than the ICS application?

A. Organizations generally do not define a role or responsibility for dealing with operating systems, leaving them neglected and vulnerable

B. The operating system will have fewer vulnerabilities than the ICS application

C. The ICS is more likely to have vendor-provided security hardening guidance than the operating system will

D. Control of the operating system offers access to applications running on it

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #11 *Topic 1*

An organization has their ICS operations and networking equipment installed in the Purdue model level 3. Where should the SIEM for this equipment be placed in relation to the existing Level 3 devices?

A. On a different subnet in Level 3

B. On a management subnet in Level 4

C. On a management subnet in Level 2

D. On the same subnet in Level 3

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #12 *Topic 1*

Which type of process is described below?
Ten barrels of hot water is moved from the hot liquor tank to the mash tun.
500 kg of milled grist is added to the mash tun.
The mixture is maintained for 60 minutes before being drained to the boil kettle.

A. Batch

B. Discrete

C. Continuous

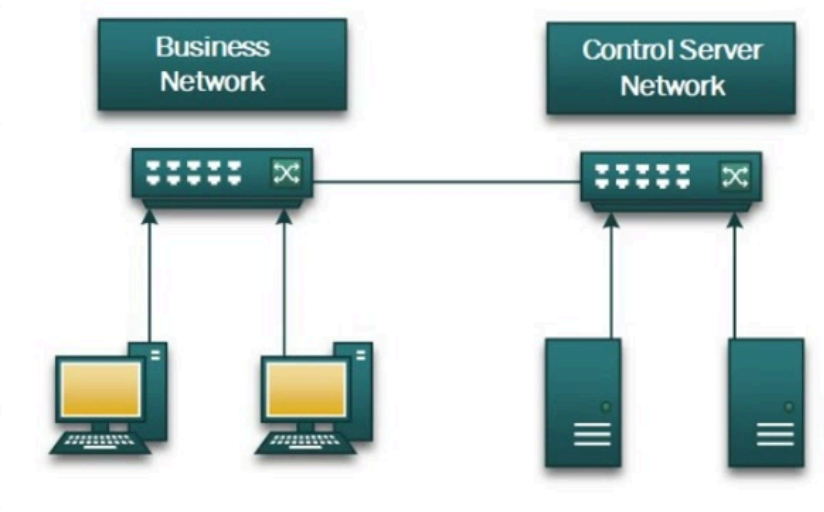
D. Distributed

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #13 *Topic 1*

Based on the following diagram, how many Active Directory domains should be created for this network?



A. One domain with separate groups within

B. Two separate domains within the same tree

C. Two separate domains without a trust relationship

D. One domain with transitive trust

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #14 *Topic 1*

A plant is being retrofitted with new cyber security devices in Purdue Level 3. What should the network security architect suggest for the installation?

A. Add a firewall to segregate the cyber security devices

B. Place the cyber security devices on their own subnet

C. Move the cyber security devices to a DMZ

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #15 *Topic 1*

What do the following protocols have in common?

WirelessHART -

ISA100.11a -
ZigBee

A. Use of IPv6 in the network layer

B. Use in RF mesh networks

C. Ability to use asymmetric join methods

D. Ability to tunnel legacy protocols

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #16 *Topic 1*

Which command can be used on a Linux system to search a file for a string of data and return the results to the screen?

A. type

B. cat

C. grep

D. tail

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #17 *Topic 1*

How could Wireshark be utilized in an attack against devices at Purdue levels 0 or 1?

A. Capture serial and fieldbus communications sent by networked devices

B. Capture communications between chips on a board

C. Detect open ports on a device by sending packets and analyzing the responses

D. Detect asymmetrical keys by identifying randomness in a data dump

E. Brute force crypto keys in an encrypted pcap file

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #18 *Topic 1*

What is a benefit of log aggregation?

A. Simplifies initial setup of logging in the environment

B. Reduces system load on logging devices

C. Eliminates the need for baselining normal log activity

D. Assists in analysis of log data from multiple sources

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #19 *Topic 1*

Which command would indicate that a user is attempting to alter the permissions on a Linux file?

A. attrib

B. chmod

C. pwd

D. md

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #20 *Topic 1*

Which type of process performs an action on a set quantity of material at one station before moving it to the next station for another action to be performed on it?

A. Batch

B. Hybrid

C. Continuous

D. Discrete

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #21 *Topic 1*

An organization wants to use Active Directory to manage systems within its Business and Control system networks. Which of the following is the recommended security practice?

A. Shared Active Directory domain with separate domain controllers for the Business and Control system networks

B. An Active Directory domain for the Business network and a Windows workgroup with a domain controller for the Control system network

C. Separate Active Directory domains for the Business and Control system networks

D. Shared Active Directory domain with fully functional domain controllers for the Business network and a Read-Only Domain Controller for the Control system network

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #22 *Topic 1*

Which of the following types of network devices sends traffic only to the intended recipient node?

A. Ethernet hub

B. Wireless access point

C. Ethernet switch

D. Wireless bridge

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #23 *Topic 1*

What is a use of Network Address Translation?

A. To maximize Firewall functionality

B. To make access list configuration easier

C. To hide private network addresses

D. To enable network routing functionality

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #24 *Topic 1*

According to the DHS suggested patch decision tree, what should the next step be if there is a vulnerability with an available patch, but without an available workaround?

A. Determine if the vulnerability affects the ICS

B. Determine if the operational needs are greater than the risk

C. Test and apply the patch

D. Identify the vulnerability and the available patch

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #25 *Topic 1*

What is a benefit of MECM over WSUS?

A. Hardware and software inventory control

B. Lower configuration and management overhead

C. Minimal system resource use

D. Lower operating and product cost

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #26 *Topic 1*

An attacker uses SQL injection to access the application which has access to all of DrilLogic's documentation and was able to exfiltrate the data. Which control would have prevented this?

A. Input sanitization

B. Encrypt data in motion

C. Strong password enforcement

D. Encrypt data at rest

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #27 *Topic 1*

What should be considered when implementing fieldbus protocols over an Ethernet network?

A. Communications between machines are limited to one host at a time

B. Different protocols cannot route across the same infrastructure

C. The network cannot be segmented into smaller subnets or VLANs

D. Different protocols will need a bridging device to talk to each other

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #28 *Topic 1*

What is a recommended practice for configuring enforcement boundary devices in an ICS control network?

A. Create a rule which drops inbound packets containing a source address from within the protected network

B. Enable full packet collection for all allowed and denied traffic rules on next-generation firewalls

C. Create one rule for each authorized conversation in a stateless access control list

D. Use an egress policy that allows everything out except for that which is explicitly denied

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #29 *Topic 1*

What approach can an organization use to make sure that high consequence, low probability risks are considered during risk analysis?

A. Prioritize risks based on impact

B. Give frequency a higher weight

C. Prioritize risks based on mitigation cost

D. Give likelihood a higher weight

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #30 *Topic 1*

Which resource includes a standardized categorization of common software vulnerabilities?

A. CWE

B. CVSS

C. CSC

D. CIP

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #31 *Topic 1*

Which of the following is a team of incident responders that often coordinate with organizations and law enforcement to reduce risks and advise on security threats?

A. CVE

B. COBIT

C. CERT

D. CVSS

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #32 *Topic 1*

Which of the following is a containment task within the six step incident handling process?

A. Checking to ensure that the most recent patches were deployed to a web application server

B. Creating a forensic image of a compromised workstation

C. Re-imaging a workstation that was exhibiting worm-like behaviour

D. Validate fix using a vulnerability scan of the hosts within the DMZ

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #33 *Topic 1*

How are general purpose Programmable Logic Controllers (PLC) different than smart field devices?

A. Smart field devices cannot be controlled centrally from a management server

B. Programmable Logic Controllers are usually microcontroller-based

C. Programmable Logic Controllers have a more limited purpose and function

D. Smart field devices contain their own control logic that cannot be changed

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #34 *Topic 1*

An attacker crafts an email that will send a user to the following site if they click a link in the message. What else is necessary for this type of attack to work? hmi.giac.org/disconnect?sensor=812

A. The attacker must obtain a session cookie from an authorized HMI user

B. The user clicking the link must be an administrator on the network

C. The user must be authenticated to the HMI interface before clicking the link

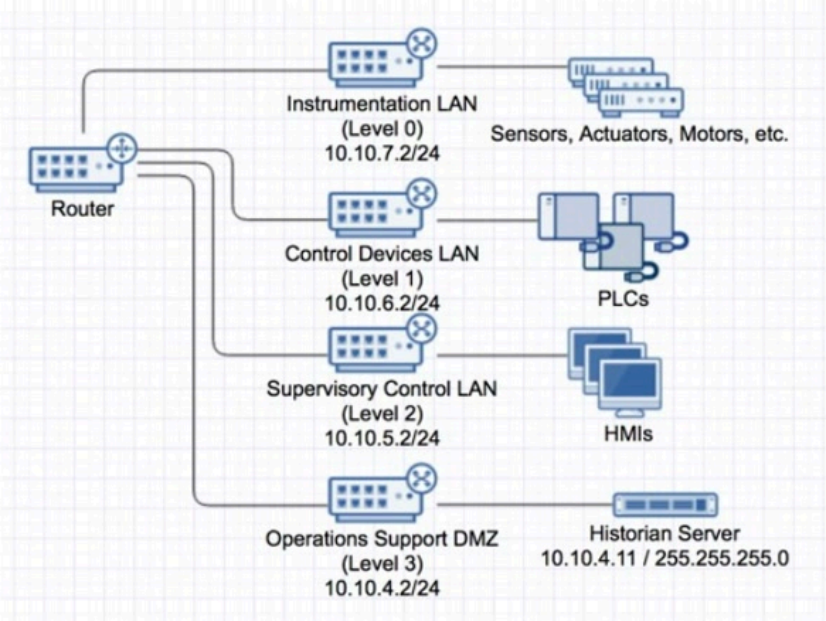
D. The attacker must enclose the URL parameter with <script> tags to run the code

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #35 *Topic 1*

What can be configured on the router so that it can most effectively implement and enforce zones for the shown subnets?



A. MAC-based port security

B. Access control lists

C. Secure Shell

D. 802.1x protocol

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #36 *Topic 1*

Which type of device is the following configuration setting from? deny modbus function write-multiple-holdingregisters

A. Network firewall

B. NIDS

C. SIEM

D. Application firewall

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #37 *Topic 1*

What type of physical security control is a procedure that details what to do in the event of a security breach?

A. Responsive

B. Detective

C. Delaying

D. Deterrence

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #38 *Topic 1*

For a SQL injection login authentication bypass to work on a website, it will contain a username comparison that the database finds to be true. What else is required for the bypass to work?

A. An unencrypted login page

B. The database's comment characters

C. Two pipe characters (||)

D. The correct password

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #39 *Topic 1*

Which of the following devices would indicate an enforcement boundary?

A. An application with a login screen

B. A workstation with antivirus

C. A router with ACLs

D. A switch with VLANs

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #40 *Topic 1*

What is a recommended practice for securing historians and databases whose purpose is to feed data back into the control processes?

A. Audit both successful and failed login attempts to databases

B. Facilitate auditing by placing historians and databases in the same DMZ

C. Use a dedicated domain admin user account to manage databases

D. Use reliable network protocols like HTTP for remote management

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!