Paloalto-Networks

Exam Questions PCCET

Palo Alto Networks Certified Cybersecurity Entry-level Technician

NEW QUESTION 1
Which model would a customer choose if they want full control over the operating system(s) running on their cloud computing platform?

A. SaaS
B. DaaS
C. PaaS
D. IaaS

Answer: D

NEW QUESTION 2
Which security component should you configure to block viruses not seen and blocked by the perimeter firewall?

A. endpoint antivirus software
B. strong endpoint passwords
C. endpoint disk encryption
D. endpoint NIC ACLs

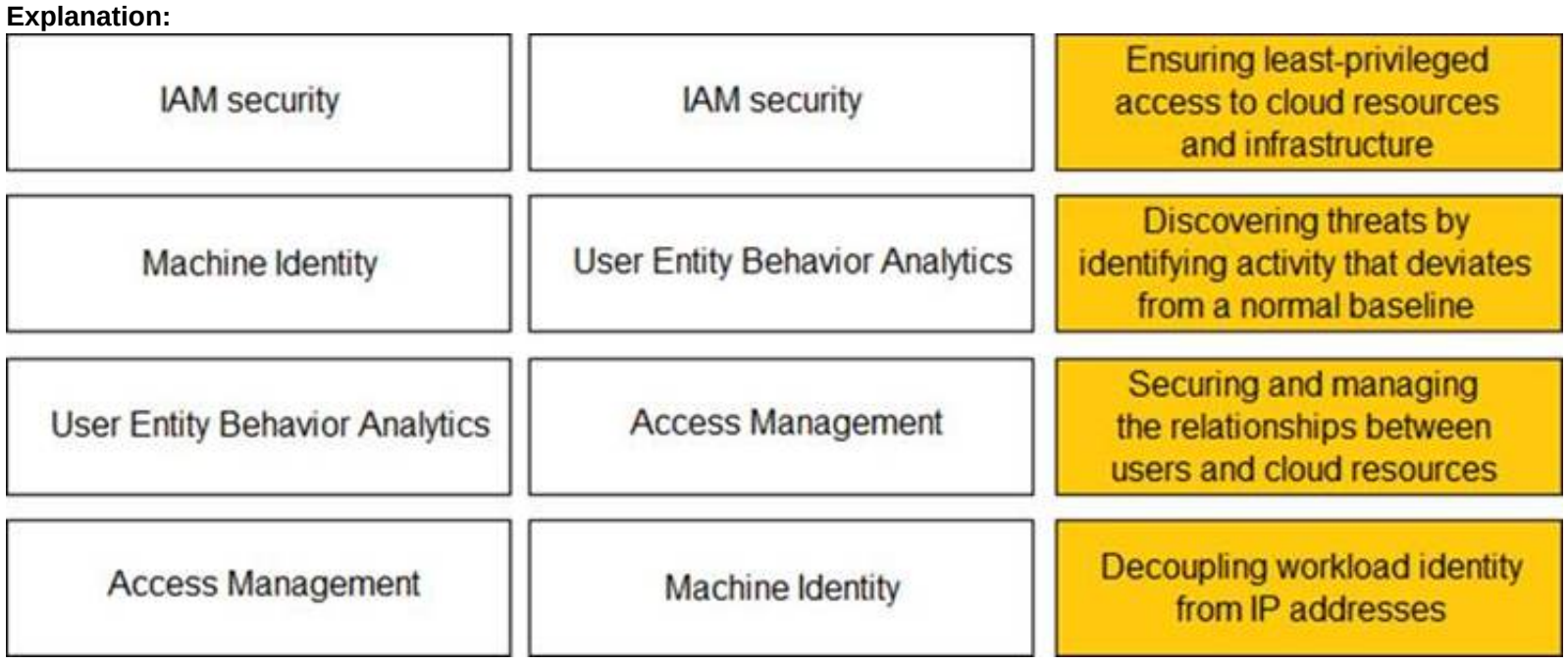
Answer: A

NEW QUESTION 3
Match the Identity and Access Management (IAM) security control with the appropriate definition.

A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 4
The customer is responsible only for which type of security when using a SaaS application?

A. physical
B. platform
C. data
D. infrastructure

Answer: C

NEW QUESTION 5
In which situation would a dynamic routing protocol be the quickest way to configure routes on a router?

A. the network is large
B. the network is small
C. the network has low bandwidth requirements
D. the network needs backup routes

Answer: A

Explanation:
A static routing protocol requires that routes be created and updated manually on a router or other network device. If a static route is down, traffic can't be automatically rerouted unless an alternate route has been configured. Also, if the route is congested, traffic can't be automatically rerouted over the less congested alternate route. Static routing is practical only in very small networks or for very limited, special-case routing scenarios (for example, a destination that's used as a backup route or is reachable only via a single router). However, static routing has low bandwidth requirements (routing information isn't broadcast across the network) and some built-in security (users can route only to destinations that are specified in statically defined routes).

NEW QUESTION 6
In which phase of the cyberattack lifecycle do attackers establish encrypted communication channels back to servers across the internet so that they can modify their attack objectives and methods?

A. exploitation
B. actions on the objective
C. command and control
D. installation

Answer: C

Explanation:
Command and Control: Attackers establish encrypted communication channels back to command-and-control (C2) servers across the internet so that they can modify their attack objectives and methods as additional
targets of opportunity are identified within the victim network, or to evade any new security countermeasures that the organization may attempt to deploy if attack artifacts are discovered.

NEW QUESTION 7
A native hypervisor runs:

A. with extreme demands on network throughput
B. only on certain platforms
C. within an operating system's environment
D. directly on the host computer's hardware

Answer: D

Explanation:
Type 1 (native or bare metal). Runs directly on the host computer's hardware Type 2 (hosted). Runs within an operating system environment

NEW QUESTION 8
Match each description to a Security Operating Platform key capability.

understanding the full context of attacks on a network		detect and prevent new, unknown threats with automation
a prevention architecture that exerts positive control based on applications		provide full visibility
a coordinated security platform that detects and accounts for the full scope of an attack		prevent all known threats
creation and delivery of near real-time protections to allow enterprises to scale defenses with technology rather than people		reduce the attack surface area

A. Mastered

B. Not Mastered

Answer: A

Explanation:
Reduce the attack surface: Best-of-breed technologies that are natively integrated provide a prevention architecture that inherently reduces the attack surface. This type of architecture allows organizations to exert positive control based on applications, users, and content, with support for open communication, orchestration, and visibility.
Prevent all known threats, fast: A coordinated security platform accounts for the full scope of an attack across the various security controls that compose the security posture, thus enabling organizations to quickly identify and block known threats.
Detect and prevent new, unknown threats with automation: Security that simply detects threats and requires a manual response is too little, too late. Automated creation and
delivery of near-real-time protections against new threats to the various security solutions in the organization's environments enable dynamic policy updates. These updates are
designed to allow enterprises to scale defenses with technology, rather than people.

NEW QUESTION 9
In which step of the cyber-attack lifecycle do hackers embed intruder code within seemingly innocuous files?

A. weaponization
B. reconnaissance
C. exploitation
D. delivery

Answer: A

Explanation:
"Weaponization: Next, attackers determine which methods to use to compromise a target endpoint. They may choose to embed intruder code within seemingly innocuous files such as a PDF or Microsoft Word document or email message."

NEW QUESTION 10
Which Palo Alto Networks tool is used to prevent endpoint systems from running malware executables such as viruses, trojans, and rootkits?

A. Expedition
B. Cortex XDR
C. AutoFocus
D. App-ID

Answer: B

NEW QUESTION 10
Which product from Palo Alto Networks enables organizations to prevent successful cyberattacks as well as simplify and strengthen security processes?

A. Expedition
B. AutoFocus
C. MineMeld
D. Cortex XDR

Answer: D

Explanation:
From a business perspective, XDR platforms enable organizations to prevent successful cyberattacks as well as simplify and strengthen security processes.

NEW QUESTION 11
Which type of IDS/IPS uses a baseline of normal network activity to identify unusual patterns or levels of network activity that may be indicative of an intrusion attempt?

A. Knowledge-based
B. Signature-based
C. Behavior-based
D. Database-based

Answer: C

Explanation:
IDSs and IPSs also can be classified as knowledge-based (or signature-based) or behavior-based (or statistical anomaly-based) systems:
A knowledge-based system uses a database of known vulnerabilities and attack profiles to identify intrusion attempts. These types of systems have lower false-alarm rates than behavior-based systems but must be continually updated with new attack signatures to be effective.
A behavior-based system uses a baseline of normal network activity to identify unusual patterns or levels of network activity that may be indicative of an intrusion attempt.
These types of systems are more adaptive than knowledge-based systems and therefore
may be more effective in detecting previously unknown vulnerabilities and attacks, but they have a much higher false-positive rate than knowledge-based systems

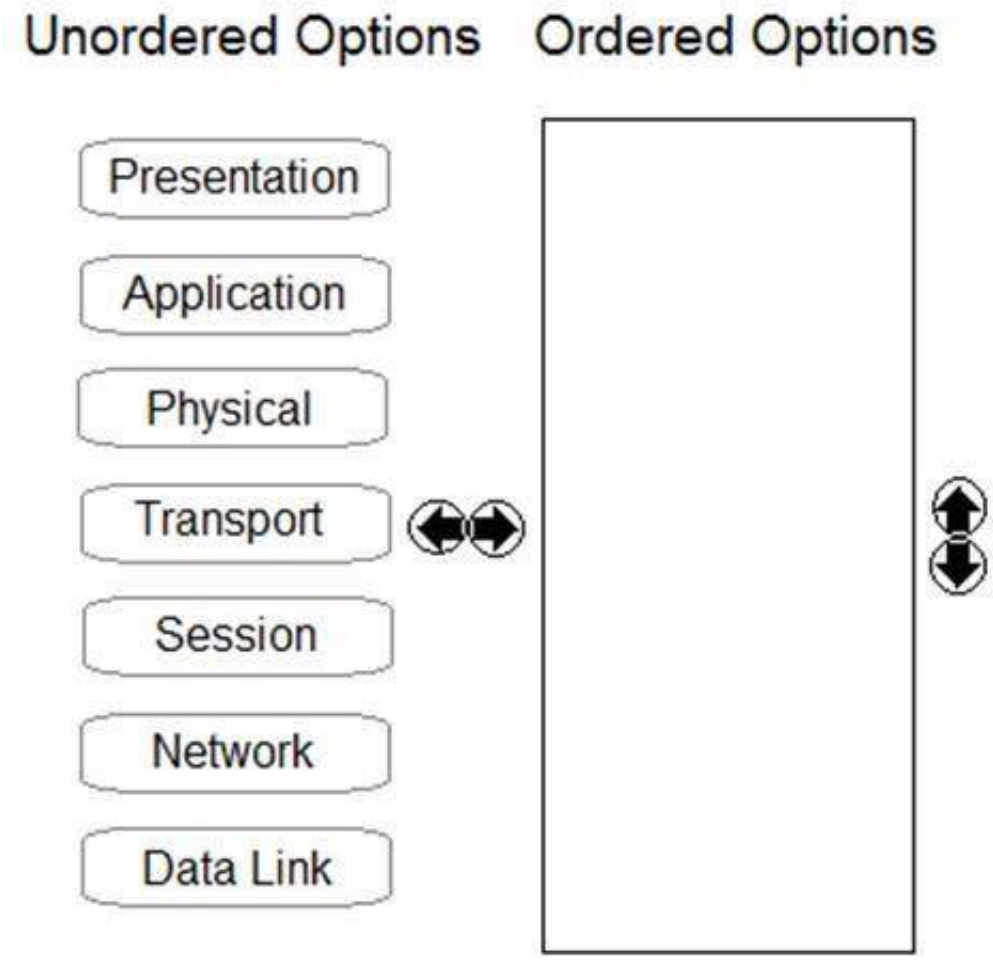
NEW QUESTION 13
Which attacker profile uses the internet to recruit members to an ideology, to train them, and to spread fear and include panic?

A. cybercriminals

B. state-affiliated groups
C. hacktivists
D. cyberterrorists

Answer: D

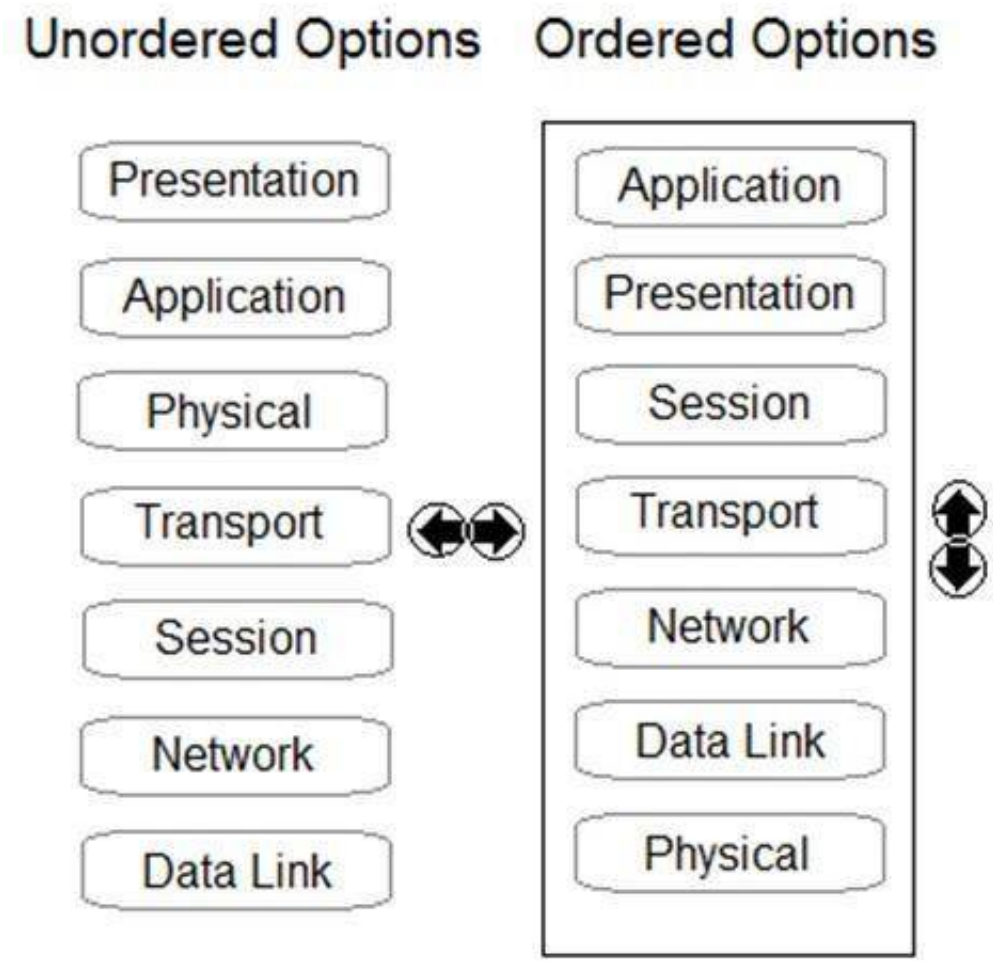
NEW QUESTION 16
Order the OSI model with Layer7 at the top and Layer1 at the bottom.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 19
Which pillar of Prisma Cloud application security does vulnerability management fall under?

A. dynamic computing
B. identity security
C. compute security

D. network protection

Answer: C

Explanation:
Prisma Cloud comprises four pillars:
Visibility, governance, and compliance. Gain deep visibility into the security posture of multicloud environments. Track everything that gets deployed with an automated asset inventory, and maintain compliance with out-of-the-box governance policies that
enforce good behavior across your environments.
Compute security. Secure hosts, containers, and serverless workloads throughout the application lifecycle. Detect and prevent risks by integrating vulnerability intelligence into your integrated development environment (IDE), software configuration management (SCM), and CI/CD workflows. Enforce machine learning-based runtime protection to protect applications and workloads in real time.
Network protection. Continuously monitor network activity for anomalous behavior, enforce microservice-aware micro-segmentation, and implement industry-leading firewall protection. Protect the network perimeter and the connectivity between containers and hosts.
Identity security. Monitor and leverage user and entity behavior analytics (UEBA) across your environments to detect and block malicious actions. Gain visibility into and enforce governance p

NEW QUESTION 23
In which two cloud computing service models are the vendors responsible for vulnerability and patch management of the underlying operating system? (Choose two.)

A. SaaS
B. PaaS
C. On-premises
D. IaaS

Answer: AB

NEW QUESTION 28
During the OSI layer 3 step of the encapsulation process, what is the Protocol Data Unit (PDU) called when the IP stack adds source (sender) and destination (receiver) IP addresses?

A. Frame
B. Segment
C. Packet
D. Data

Answer: C

Explanation:
The IP stack adds source (sender) and destination (receiver) IP addresses to the TCP segment (which now is called an IP packet) and notifies the server operating system that it has an outgoing message ready to be sent across the network.

NEW QUESTION 31
Which Palo Alto subscription service identifies unknown malware, zero-day exploits, and advanced persistent threats (APTs) through static and dynamic analysis in a scalable, virtual environment?

A. DNS Security
B. URL Filtering
C. WildFire
D. Threat Prevention

Answer: C

Explanation:
"The WildFire cloud-based malware analysis environment is a cyber threat prevention service that identifies unknown malware, zero-day exploits, and advanced persistent threats (APTs) through static and dynamic analysis in a scalable, virtual environment. WildFire automatically disseminates updated protections in near-real time to immediately prevent threats from spreading; this occurs without manual intervention"

NEW QUESTION 34
Which term describes data packets that move in and out of the virtualized environment from the host network or a corresponding traditional data center?

A. North-South traffic
B. Intrazone traffic
C. East-West traffic
D. Interzone traffic

Answer: A

NEW QUESTION 37
Which not-for-profit organization maintains the common vulnerability exposure catalog that is available through their public website?

A. Department of Homeland Security
B. MITRE
C. Office of Cyber Security and Information Assurance
D. Cybersecurity Vulnerability Research Center

Answer:

B

NEW QUESTION 38
Which method is used to exploit vulnerabilities, services, and applications?

A. encryption
B. port scanning
C. DNS tunneling
D. port evasion

Answer: D

Explanation:
Attack communication traffic is usually hidden with various techniques and tools, including:
Encryption with SSL, SSH (Secure Shell), or some other custom or proprietary encryption Circumvention via proxies, remote access tools, or tunneling. In some instances, use of cellular networks enables complete circumvention of the target network for attack C2 traffic. Port evasion using network anonymizers or port hopping to traverse over any available open ports
Fast Flux (or Dynamic DNS) to proxy through multiple infected endpoints or multiple, ever-changing C2 servers to reroute traffic and make determination of the true destination or attack source difficult
DNS tunneling is used for C2 communications and data infiltration

NEW QUESTION 40
Which Palo Alto Networks tools enable a proactive, prevention-based approach to network automation that accelerates security analysis?

A. MineMeld
B. AutoFocus
C. WildFire
D. Cortex XDR

Answer: B

Explanation:
"Palo Alto Networks AutoFocus enables a proactive, prevention-based approach to network security that puts automation to work for security professionals. Threat intelligence from the service is made directly accessible in the Palo Alto Networks platform, including PAN-OS software and Panorama. AutoFocus speeds the security team’s existing workflows, which allows for in-depth investigation into suspicious activity, without additional specialized resources."

NEW QUESTION 45
Which type of malware replicates itself to spread rapidly through a computer network?

A. ransomware
B. Trojan horse
C. virus
D. worm

Answer: D

Explanation:
A worm replicates through the network while a virus replicates, not necessarily to spread through the network.

NEW QUESTION 46
On an endpoint, which method is used to protect proprietary data stored on a laptop that has been stolen?

A. operating system patches
B. full-disk encryption
C. periodic data backups
D. endpoint-based firewall

Answer: B

NEW QUESTION 47
Which three layers of the OSI model correspond to the Application Layer (L4) of the TCP/IP model?

A. Session, Transport, Network
B. Application, Presentation, and Session
C. Physical, Data Link, Network
D. Data Link, Session, Transport

Answer: B

Explanation:
Application (Layer 4 or L4): This layer loosely corresponds to Layers 5 through 7 of the OSI model. Transport (Layer 3 or L3): This layer corresponds to Layer 4 of the OSI model.
Internet (Layer 2 or L2): This layer corresponds to Layer 3 of the OSI model.
Network Access (Layer 1 or L1): This layer corresponds to Layers 1 and 2 of the OSI model

NEW QUESTION 51

Which analysis detonates previously unknown submissions in a custom-built, evasion-resistant virtual environment to determine real-world effects and behavior?

A. Dynamic
B. Pre-exploit protection
C. Bare-metal
D. Static

Answer: A

Explanation:
The WildFire cloud-based malware analysis environment is a cyber threat prevention service that identifies unknown malware, zero-day exploits, and advanced persistent threats (APTs) through static and dynamic analysis in a scalable, virtual environment.

NEW QUESTION 52
In an IDS/IPS, which type of alarm occurs when legitimate traffic is improperly identified as malicious traffic?

A. False-positive
B. True-negative
C. False-negative
D. True-positive

Answer: A

Explanation:
In anti-malware, a false positive incorrectly identifies a legitimate file or application as malware. A false negative incorrectly identifies malware as a legitimate file or application. In intrusion detection, a false positive incorrectly identifies legitimate traffic as a threat, and a false negative incorrectly identifies a threat as legitimate traffic.

NEW QUESTION 56
What are two key characteristics of a Type 1 hypervisor? (Choose two.)

A. is hardened against cyber attacks
B. runs without any vulnerability issues
C. runs within an operating system
D. allows multiple, virtual (or guest) operating systems to run concurrently on a single physical host computer

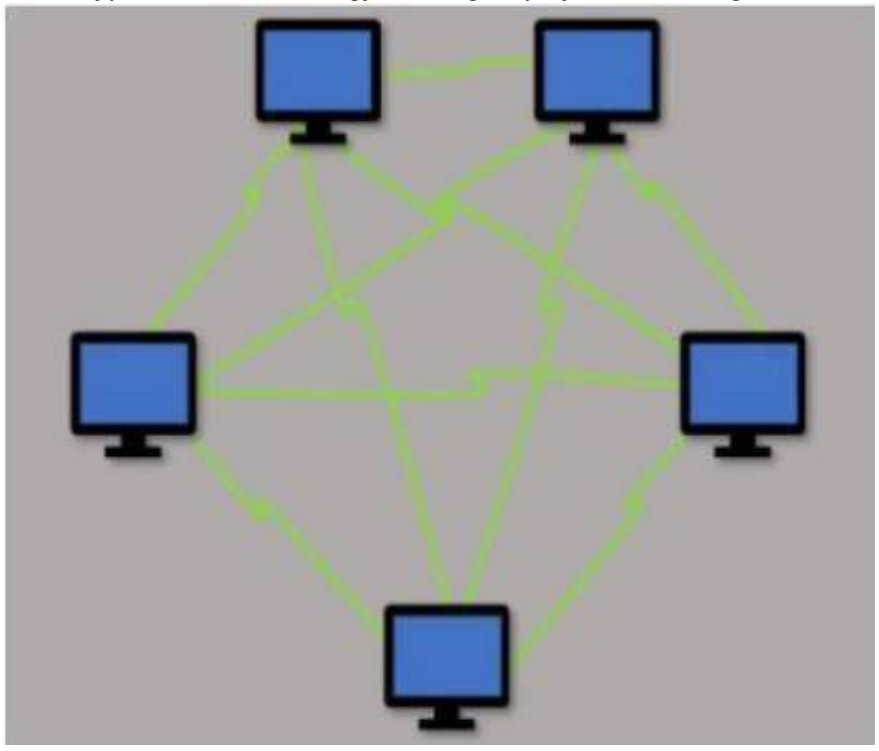
Answer: CD

NEW QUESTION 59
Which network analysis tool can be used to record packet captures?

A. Smart IP Scanner
B. Wireshark
C. Angry IP Scanner
D. Netman

Answer: B

NEW QUESTION 61
Which type of LAN technology is being displayed in the diagram?



A. Star Topology
B. Spine Leaf Topology
C. Mesh Topology
D. Bus Topology

Answer: A

NEW QUESTION 66
Which Palo Alto Networks subscription service complements App-ID by enabling you to configure the next- generation firewall to identify and control access to websites and to protect your organization from websites hosting malware and phishing pages?

A. Threat Prevention
B. DNS Security
C. WildFire
D. URL Filtering

Answer: D

Explanation:
The URL Filtering service complements App-ID by enabling you to configure the next-generation firewall to identify and control access to websites and to protect your organization from websites that host malware and phishing pages.

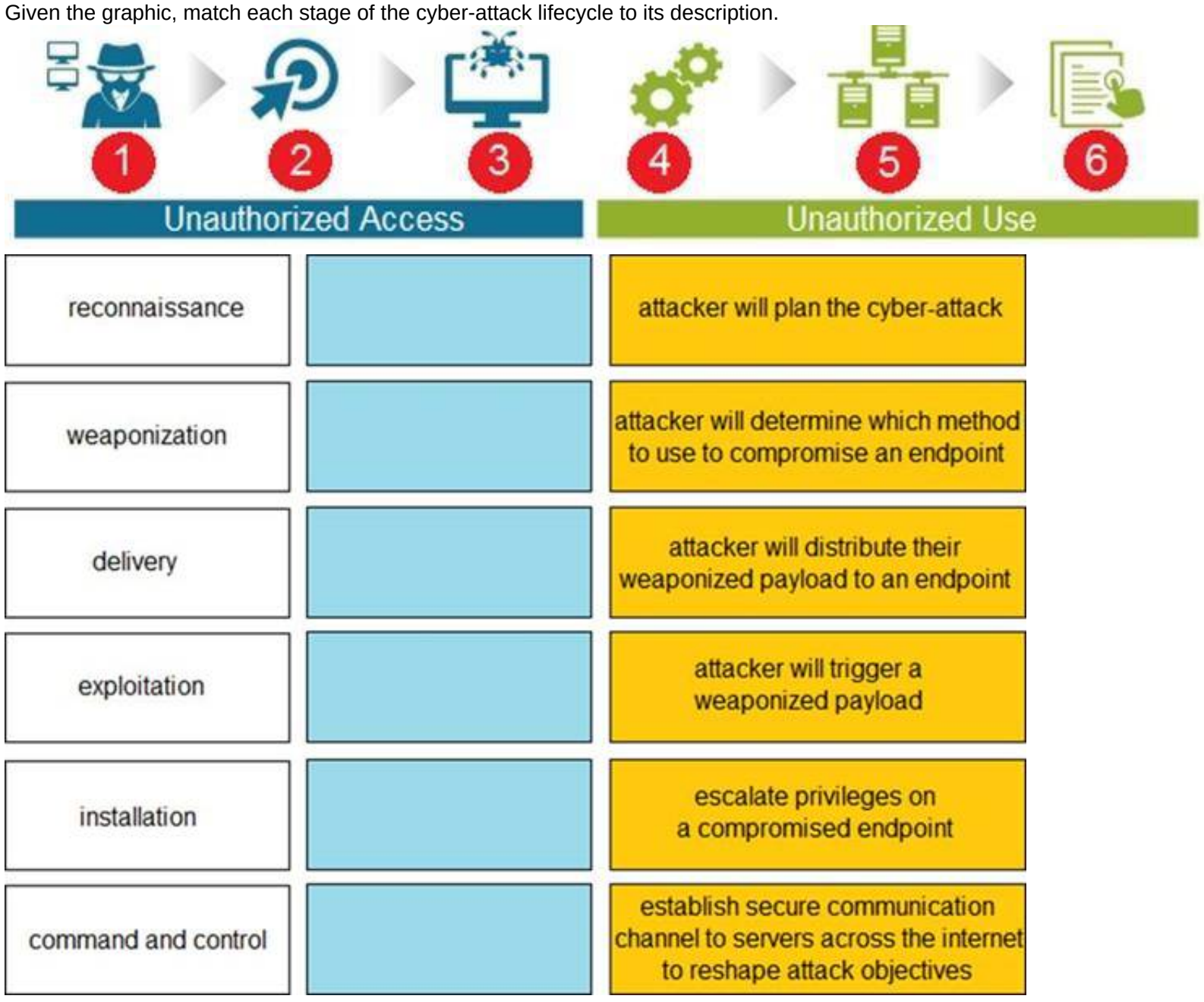
NEW QUESTION 70
Which IoT connectivity technology is provided by satellites?

A. 4G/LTE
B. VLF
C. L-band
D. 2G/2.5G

Answer: C

Explanation:
2G/2.5G: 2G connectivity remains a prevalent and viable IoT connectivity option due to the low cost of 2G modules, relatively long battery life, and large installed base of 2G sensors and M2M applications.
3G: IoT devices with 3G modules use either Wideband Code Division Multiple Access (W-CDMA) or Evolved High Speed Packet Access (HSPA+ and Advanced HSPA+) to
achieve data transfer rates of 384Kbps to 168Mbps.
4G/Long-Term Evolution (LTE): 4G/LTE networks enable real-time IoT use cases, such as autonomous vehicles, with 4G LTE Advanced Pro delivering speeds in excess of 3Gbps and less than 2 milliseconds of latency.
5G: 5G cellular technology provides significant enhancements compared to 4G/LTE networks and is backed by ultra-low latency, massive connectivity and scalability for IoT devices, more efficient use of the licensed spectrum, and network slicing for application traffic prioritization.

NEW QUESTION 71
Given the graphic, match each stage of the cyber-attack lifecycle to its description.

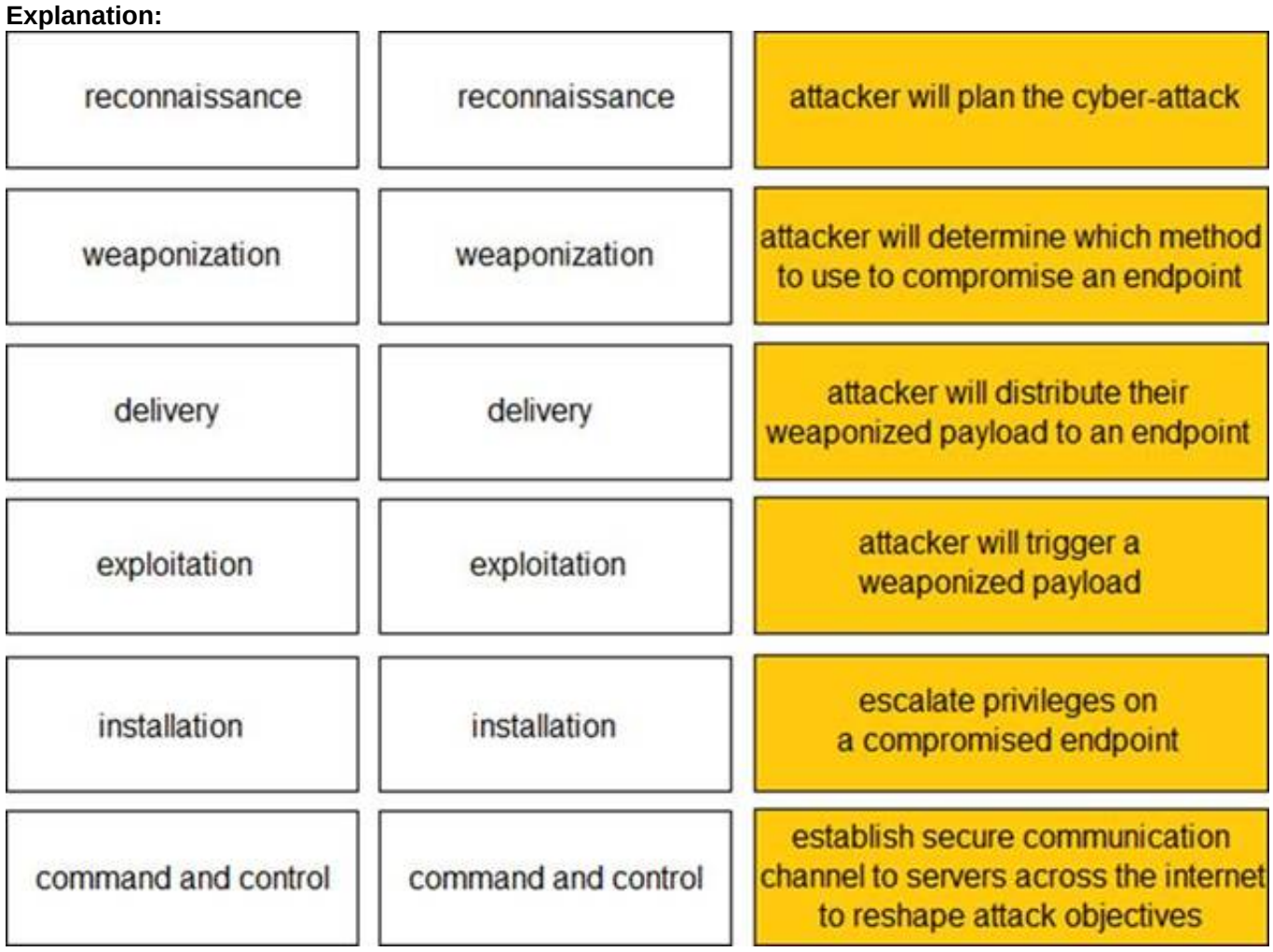


A. Mastered

B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 72
How does DevSecOps improve the Continuous Integration/Continuous Deployment (CI/CD) pipeline?

A. DevSecOps improves pipeline security by assigning the security team as the lead team for continuousdeployment
B. DevSecOps ensures the pipeline has horizontal intersections for application code deployment
C. DevSecOps unites the Security team with the Development and Operations teams to integrate security into the CI/CD pipeline
D. DevSecOps does security checking after the application code has been processed through the CI/CD pipeline

Answer: C

Explanation:
DevSecOps takes the concept behind DevOps that developers and IT teams should work together closely, instead of separately, throughout software delivery and extends it to include security and integrate automated checks into the full CI/CD pipeline. The integration of the CI/CD pipeline takes care of the problem of security seeming like an outside force and instead allows developers to maintain their usual speed without compromising data security

NEW QUESTION 73
Which tool supercharges security operations center (SOC) efficiency with the world's most comprehensive operating platform for enterprise security?

A. Prisma SAAS
B. WildFire
C. Cortex XDR
D. Cortex XSOAR

Answer: D

Explanation:
Cortex XSOAR enhances Security Operations Center (SOC) efficiency with the world's most comprehensive operating platform for enterprise security. Cortex XSOAR unifies case management, automation, real-time collaboration, and native threat intel management in the industry's first extended security orchestration, automation, and response (SOAR) offering.

NEW QUESTION 76
Which option is a Prisma Access security service?

A. Compute Security
B. Firewall as a Service (FWaaS)
C. Virtual Private Networks (VPNs)
D. Software-defined wide-area networks (SD-WANs)

Answer: B

Explanation:
Prisma Access provides firewall as a service (FWaaS) that protects branch offices from threats while also providing the security services expected from a next-generation firewall. The full spectrum of FWaaS includes threat prevention, URL filtering, sandboxing, and more.

NEW QUESTION 77
In a traditional data center what is one result of sequential traffic analysis?

A. simplifies security policy management
B. reduces network latency
C. causes security policies to be complex
D. improves security policy application ID enforcement

Answer: C

Explanation:
Multiple policies, no policy reconciliation tools: Sequential traffic analysis (stateful inspection, application control, intrusion prevention system (IPS), anti-malware, etc.) in traditional data center security solutions requires a corresponding security policy or profile, often using multiple management tools. The result is that your security policies become convoluted as you build and manage a firewall policy with source, destination, user, port, and action; an application control policy with similar rules; and any other threat prevention rules required. Multiple security policies that mix positive (firewall) and negative (application control, IPS, and anti-malware) control models can cause security holes by missing traffic and/or not identifying

NEW QUESTION 82
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

PCCET Practice Exam Features:

* PCCET Questions and Answers Updated Frequently

* PCCET Practice Questions Verified by Expert Senior Certified Staff

* PCCET Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* PCCET Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year