QUESTION 76
Which network device breaks networks into separate broadcast domains?

A. Hub
B. Layer 2 switch
C. Router
D. Wireless access point

Answer: C
Explanation:
A layer 2 switch will break up collision domains but not broadcast domains. To break up broadcast domains you need a Layer 3 switch with vlan capabilities.

QUESTION 77
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

QUESTION 78
Which NGFW feature is used to provide continuous identification, categorization, and control of known and previously unknown SaaS applications?

A. User-ID
B. Device-ID
C. App-ID
D. Content-ID

Answer: C
Explanation:
App-IDTM technology leverages the power of the broad global community to provide continuous identification, categorization, and granular risk-based control of known and previously unknown SaaS applications, ensuring new applications are discovered automatically as they become popular.

QUESTION 79
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.

QUESTION 80
What does SOAR technology use to automate and coordinate workflows?

A. algorithms
B. Cloud Access Security Broker
C. Security Incident and Event Management
D. playbooks

Answer: D
Explanation:
SOAR tools ingest aggregated alerts from detection sources (such as SIEMs, network security tools, and mailboxes) before executing automatable, process-driven playbooks to enrich and respond to these alerts.

QUESTION 81
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.

QUESTION 82
Which three services are part of Prisma SaaS? (Choose three.)

A. Data Loss Prevention
B. DevOps
C. Denial of Service
D. Data Exposure Control
E. Threat Prevention

Answer: ADE

QUESTION 83
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.

QUESTION 84
Which of the following is an AWS serverless service?

A. Beta
B. Kappa
C. Delta
D. Lambda

Answer: D
Explanation:
Examples of serverless environments include Amazon Lambda and Azure Functions. Many PaaS offerings, such as Pivotal Cloud Foundry, also are effectively serverless even if they have not historically been marketed as such. Although serverless may appear to lack the container-specific, cloud native attribute, containers are extensively used in the underlying implementations, even if those implementations are not exposed to end users directly.

QUESTION 85
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).

QUESTION 86
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.

QUESTION 87
A user is provided access over the internet to an application running on a cloud infrastructure. The servers, databases, and code of that application are hosted and maintained by the vendor.
Which NIST cloud service model is this?

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

Answer: B
Explanation:
SaaS - User responsible for only the data, vendor responsible for rest.

QUESTION 88
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.

QUESTION 89
From which resource does Palo Alto Networks AutoFocus correlate and gain URL filtering intelligence?

A. Unit 52
B. PAN-DB
C. BrightCloud
D. MineMeld

Answer: B
Explanation:
When you enable URL Filtering, all web traffic is compared against the URL Filtering database, PAN- DB, which contains millions of URLs that have been grouped into about 65 categories.

QUESTION 90
Which of the following is a service that allows you to control permissions assigned to users in order for them to access and utilize cloud resources?

A. User-ID
B. Lightweight Directory Access Protocol (LDAP)
C. User and Entity Behavior Analytics (UEBA)
D. Identity and Access Management (IAM)

Answer: D
Explanation:
Identity and access management (IAM) is a software service or framework that allows organizations to define user or group identities within software environments, then associate permissions with them. The identities and permissions are usually spelled out in a text file, which is referred to as an IAM policy.

QUESTION 91
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.

QUESTION 92
What is used to orchestrate, coordinate, and control clusters of containers?

A. Kubernetes
B. Prisma Saas
C. Docker
D. CN-Series

Answer: A
Explanation:
As containers grew in popularity and used diversified orchestrators such as Kubernetes (and its derivatives, such as OpenShift), Mesos, and Docker Swarm, it became increasingly important to deploy and operate containers at scale.

https://www.dynatrace.com/news/blog/kubernetes-vs-docker/

QUESTION 93
Under which category does an application that is approved by the IT department, such as Office 365, fall?

A. unsanctioned
B. prohibited
C. tolerated
D. sanctioned

Answer: D