



-Expert Verified, Online, **Free**.



CERTIFICATION TEST

-CertificationTest.net - Cheap & Quality Resources With Best Support

Question #1

Topic 1

Which methodology does Identity Threat Detection and Response (ITDR) use?

- A. Behavior analysis
- B. Comparison of alerts to signatures
- C. Manual inspection of user activities
- D. Rule-based activity prioritization

Suggested Answer: A

Explanation: ITDR uses behavior analysis to detect anomalies and suspicious activities associated with identities. This approach allows systems to spot deviations from normal user behavior, which may indicate credential misuse, lateral movement, or privilege escalation – common in identity-based attacks.

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

Which technology grants enhanced visibility and threat prevention locally on a device?

- A. EDR
- B. IDS
- C. SIEM
- D. DLP

Suggested Answer: A

Explanation: Endpoint Detection and Response (EDR) provides enhanced visibility and threat prevention locally on a device by monitoring, detecting, and responding to threats in real-time at the endpoint level. It collects data directly from endpoints and applies analytics to detect malicious behavior.

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

What are two examples of an attacker using social engineering? (Choose two.)

- A. Convincing an employee that they are also an employee
- B. Leveraging open-source intelligence to gather information about a high-level executive
- C. Acting as a company representative and asking for personal information not relevant to the reason for their call
- D. Compromising a website and configuring it to automatically install malicious files onto systems that visit the page

Suggested Answer: A, C

Explanation: Pretending to be a fellow employee is a classic social engineering tactic to build trust and manipulate the victim. Posing as a company representative to extract irrelevant personal information is another social engineering method used to deceive and gain unauthorized access. Other options are related to reconnaissance and exploitation, not direct social manipulation.

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

Which two services does a managed detection and response (MDR) solution provide? (Choose two.)

- A. Improved application development
- B. Incident impact analysis
- C. Periodic firewall updates
- D. Proactive threat hunting

Suggested Answer: *B, D*

Explanation: Incident impact analysis helps organizations understand the scope and severity of detected threats. Proactive threat hunting involves actively searching for threats that may have evaded automated detection, a core function of MDR services. Other options are unrelated to MDR; application development and firewall updates fall outside its scope.

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

What role do containers play in cloud migration and application management strategies?

- A. They enable companies to use cloud-native tools and methodologies.
- B. They are used for data storage in cloud environments.
- C. They serve as a template manager for software applications and services.
- D. They are used to orchestrate virtual machines (VMs) in cloud environments.

Suggested Answer: A

Explanation: Containers package applications and their dependencies into a lightweight, portable unit. This makes them ideal for cloud migration and application management because they support cloud-native architectures, enabling consistent deployment and scaling across different environments.

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

An administrator finds multiple gambling websites in the network traffic log.

What can be created to dynamically block these websites?

- A. URL category
- B. Custom signatures
- C. Decryption policy
- D. Application group

Suggested Answer: A

Explanation: A URL category allows an administrator to group websites (such as gambling sites) and apply security policies to dynamically block them. Palo Alto Networks firewalls support both predefined and custom URL categories for granular web filtering.

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

Which security function enables a firewall to validate the operating system version of a device before granting it network access?

- A. Sandboxing
- B. Stateless packet inspection
- C. Host intrusion prevention system (HIPS)
- D. Identity Threat Detection and Response (ITDR)

Suggested Answer: C

Explanation: HIPS can enforce host-based policies, including validating the operating system version and patch level before allowing network access. It ensures devices comply with security posture requirements to reduce risk.

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

Which scenario highlights how a malicious Portable Executable (PE) file is leveraged as an attack?

- A. Setting up a web page for harvesting user credentials
- B. Laterally transferring the file through a network after being granted access
- C. Embedding the file inside a .pdf to be downloaded and installed
- D. Corruption of security device memory spaces while file is in transit

Suggested Answer: *C*

Explanation: A malicious PE file embedded inside another file type (like a .pdf) is a common attack tactic. When the user downloads and opens the file, the PE file (executable) runs, triggering the malicious payload. This method leverages social engineering and file obfuscation to bypass defenses.

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

Which statement describes advanced malware?

- A. It operates openly and can be detected by traditional antivirus.
- B. It lacks the ability to exfiltrate data or persist within a system.
- C. It is designed to avoid detection and adapt.
- D. It can operate without consuming resources.

Suggested Answer: C

Explanation: Advanced malware is specifically engineered to evade traditional security tools, adapt to different environments, and often includes features for persistence, obfuscation, and data exfiltration, making it difficult to detect and remove.

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

Which technology helps Security Operations Center (SOC) teams identify heap spray attacks on company-owned laptops?

- A. CSPM
- B. ASM
- C. EDR
- D. CWP

Suggested Answer: *C*

Explanation: Endpoint Detection and Response (EDR) monitors endpoint behavior in real time and can detect memory-based attacks like heap spraying, which is a technique used to exploit vulnerabilities. EDR tools help SOC teams quickly identify, analyze, and respond to such threats on company-owned laptops.

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

What are two common lifecycle stages for an advanced persistent threat (APT) that is infiltrating a network? (Choose two.)

- A. Lateral movement
- B. Communication with covert channels
- C. Deletion of critical data
- D. Privilege escalation

Suggested Answer: A, D

Explanation: Lateral movement is a key stage where the attacker moves across the network to find valuable targets. Privilege escalation involves gaining higher access rights to expand control within the compromised environment. Communication with covert channels is a tactic used during persistence or exfiltration, while deletion of critical data is not a standard APT lifecycle stage – it's more characteristic of destructive attacks.

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

A high-profile company executive receives an urgent email containing a malicious link. The sender appears to be from the IT department of the company, and the email requests an update of the executive's login credentials for a system update.

Which type of phishing attack does this represent?

- A. Whaling
- B. Vishing
- C. Pharming
- D. Angler phishing

Suggested Answer: A

Explanation: Whaling is a targeted phishing attack aimed at high-profile individuals, such as executives. The attacker impersonates a trusted entity (e.g., IT department) to trick the executive into revealing sensitive credentials. This is a form of spear phishing specifically focused on "big fish" targets.

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

Which next-generation firewall (NGFW) deployment option provides full application visibility into Kubernetes environments?

- A. Virtual
- B. Container
- C. Physical
- D. SASE

Suggested Answer: *B*

Explanation: A container-based NGFW is specifically designed to integrate with Kubernetes environments, providing full application visibility and control within containerized workloads. It operates at the pod level, making it ideal for securing dynamic microservices architectures.

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

Which type of firewall should be implemented when a company headquarters is required to have redundant power and high processing power?

- A. Cloud
- B. Physical
- C. Virtual
- D. Containerized

Suggested Answer: *B*

Explanation: A physical firewall is ideal for environments like a company headquarters that require redundant power, high throughput, and dedicated hardware for maximum reliability and performance. It supports more robust failover and scalability compared to virtual or containerized options.

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

Which statement describes the process of application allow listing?

- A. It allows only trusted files, applications, and processes to run.
- B. It creates a set of specific applications that do not run on the system.
- C. It encrypts application data to protect the system from external threats.
- D. It allows safe use of applications by scanning files for malware.

Suggested Answer: A

Explanation: Application allow listing is a security practice that permits only pre-approved (trusted) applications, files, and processes to run on a system. This approach helps prevent unauthorized or malicious software from executing, thereby reducing the attack surface.

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

Which component of the AAA framework verifies user identities so they may access the network?

- A. Allowance
- B. Authorization
- C. Accounting
- D. Authentication

Suggested Answer: *D*

Explanation: Authentication is the component of the AAA (Authentication, Authorization, and Accounting) framework that verifies user identities (e.g., via passwords, certificates, or biometrics) before granting access to network resources.

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

Which capability does Cloud Security Posture Management (CSPM) provide for threat detection within Prisma Cloud?

- A. Real-time protection from threats
- B. Alerts for new code introduction
- C. Integration with threat feeds
- D. Continuous monitoring of resources

Suggested Answer: D

Explanation: Cloud Security Posture Management (CSPM), including Prisma Cloud's offering, continuously monitors all cloud resources – such as compute instances, storage, network configurations, and identities – to detect misconfigurations, vulnerabilities, and potential threats in near real time. Reference: <https://www.paloaltonetworks.com/prisma/cloud/cloud-security-posture-management>

🗉 👤 jarzynvip Most Recent 1 month, 1 week ago

Selected Answer: D

D. Continuous monitoring of resources

Explanation: Cloud Security Posture Management (CSPM) in Prisma Cloud provides continuous visibility and continuous monitoring across multi-cloud environments. It continuously audits cloud resources, configurations, and activity logs to detect misconfigurations, compliance drift, and potential security threats.

upvoted 1 times

Which type of system collects data and uses correlation rules to trigger alarms?

- A. SIM
- B. SIEM
- C. UEBA
- D. SOAR

Suggested Answer: *B*

Explanation: A Security Information and Event Management (SIEM) system collects data from various sources (logs, events, etc.) and uses correlation rules to analyze this data and trigger alarms when suspicious or predefined patterns are detected.

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

What is the purpose of host-based architectures?

- A. They share the work of both clients and servers.
- B. They allow client computers to perform most of the work.
- C. They divide responsibilities among clients.
- D. They allow a server to perform all of the work virtually.

Suggested Answer: *D*

Explanation: In a host-based architecture, the server (host) handles all processing tasks, while the client mainly provides input/output. This centralizes control, processing, and data storage on the server, reducing the client's role to that of a terminal.

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

What is the function of an endpoint detection and response (EDR) tool?

- A. To provide organizations with expertise for monitoring network devices
- B. To ingest alert data from network devices
- C. To monitor activities and behaviors for investigation of security incidents on user devices
- D. To integrate data from different products in order to provide a holistic view of security posture

Suggested Answer: C

Explanation: Endpoint Detection and Response (EDR) tools monitor, record, and analyze endpoint activity to detect suspicious behavior, investigate incidents, and respond to threats on user devices such as laptops and desktops.

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

What type of attack redirects the traffic of a legitimate website to a fake website?

- A. Watering hole
- B. Pharming
- C. Spear phishing
- D. Whaling

Suggested Answer: B

Explanation: Pharming is an attack that redirects traffic from a legitimate website to a malicious fake website, typically by corrupting the DNS system or modifying host files, with the intent of stealing user credentials or sensitive data.

 **jarzynvip** Most Recent 1 month ago

Selected Answer: B

A watering hole attack compromises a legitimate, trusted website that a specific target group frequently visits to infect their devices with malware, whereas pharming manipulates DNS routing or host files to secretly redirect users typing a correct URL to a fake, malicious replica.

upvoted 2 times

Which security tool provides policy enforcement for mobile users and remote networks?

- A. Service connection
- B. Prisma Access
- C. Prisma Cloud
- D. Digital experience management

Suggested Answer: *B*

Explanation: Prisma Access is a cloud-delivered security platform that provides policy enforcement, secure access, and threat prevention for mobile users and remote networks, ensuring consistent security regardless of location.

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

Which two descriptions apply to an XDR solution? (Choose two.)

- A. It employs machine learning (ML) to identify threats.
- B. It is designed for reporting on key metrics for cloud environments.
- C. It ingests data from a wide spectrum of sources.
- D. It is focused on single-vector attacks on specific layers of defense.

Suggested Answer: A, C

Explanation: XDR (Extended Detection and Response) uses machine learning (ML) to detect threats by identifying patterns and anomalies. XDR ingests data from multiple sources – including endpoints, networks, servers, and cloud workloads – to provide a unified and correlated view of threats across the environment.

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

What differentiates SOAR from SIEM?

- A. SOAR platforms focus on analyzing network traffic.
- B. SOAR platforms integrate automated response into the investigation process.
- C. SOAR platforms collect data and send alerts.
- D. SOAR platforms filter alerts with their broader coverage of security incidents.

Suggested Answer: B

Explanation: SOAR (Security Orchestration, Automation, and Response) differs from SIEM by adding automated incident response and workflow orchestration to the detection and alerting capabilities found in SIEM. This enables faster and more efficient handling of security incidents.

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

Which of the Cloud-Delivered Security Services (CDSS) will detect zero-day malware by using inline cloud machine learning (ML) and sandboxing?

- A. DNS security
- B. Advanced WildFire
- C. IoT security
- D. Advanced Threat Prevention

Suggested Answer: *B*

Explanation: Advanced WildFire is a Cloud-Delivered Security Service (CDSS) that detects zero-day malware using inline cloud machine learning (ML) and sandboxing techniques. It analyzes unknown files in real-time to identify and block new threats before they can cause harm.

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

What are two characteristics of an advanced persistent threat (APT)? (Choose two.)

- A. Multiple attack vectors
- B. Repeated pursuit of objective
- C. Reduced interaction time
- D. Tendency to isolate hosts

Suggested Answer: *A, B*

Explanation: Multiple attack vectors – APTs often use various methods (phishing, malware, lateral movement) to infiltrate and maintain access to a target. Repeated pursuit of objective – APTs are known for their persistent nature, involving continuous efforts over time to achieve their goals, such as data theft or surveillance.

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

Which product functions as part of a SASE solution?

- A. Cortex
- B. Prisma Cloud
- C. Kubernetes
- D. Prisma SD-WAN

Suggested Answer: *D*

Explanation: Prisma SD-WAN is a key component of a SASE (Secure Access Service Edge) solution. It provides intelligent routing, traffic optimization, and secure connectivity between users and applications, supporting the networking part of SASE alongside security services like those in Prisma Access.

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

Which statement describes a host-based intrusion prevention system (HIPS)?

- A. It analyzes network traffic to detect unusual traffic flows and new malware.
- B. It scans a Wi-Fi network for unauthorized access and removes unauthorized devices.
- C. It is placed as a sensor to monitor all network traffic and scan for threats.
- D. It is installed on an endpoint and inspects the device.

Suggested Answer: *D*

Explanation: A Host-Based Intrusion Prevention System (HIPS) is installed directly on an endpoint device (such as a server or workstation) and monitors local system activity, including processes, file access, and system calls, to detect and prevent malicious behavior.

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

Which MITRE ATT&CK tactic grants increased permissions to a user account for internal servers of a corporate network?

- A. Impact
- B. Privilege escalation
- C. Data exfiltration
- D. Persistence

Suggested Answer: B

Explanation: The Privilege Escalation tactic in the MITRE ATT&CK framework involves techniques used by attackers to gain higher-level permissions on a system or network, allowing greater access to internal servers and sensitive data.

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

Which type of portable architecture can package software with dependencies in an isolated unit?

- A. Containerized
- B. Serverless
- C. Air-gapped
- D. SaaS

Suggested Answer: A

Explanation: A containerized architecture packages software along with its dependencies, libraries, and configuration into an isolated unit called a container. This ensures consistent behavior across environments and simplifies deployment and scaling.

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

Which action is unique to the security orchestration, automation, and response (SOAR) platforms?

- A. Prioritizing alerts
- B. Enhancing data collection
- C. Using predefined workflows
- D. Correlating incident data

Suggested Answer: C

Explanation: SOAR platforms are unique in their ability to automate incident response through the use of predefined workflows. These workflows allow repetitive security tasks to be executed automatically, improving response speed and efficiency.

 **jarzynvip** Most Recent 1 month, 1 week ago

Selected Answer: C

The correct answer is C. Using predefined workflows.

Explanation:

C. Using predefined workflows (Playbooks/Runbooks): SOAR platforms are uniquely designed to execute automated, step-by-step responses across disparate security systems using predefined workflows to streamline incident management.

A, B, and D (Prioritizing alerts, Enhancing data collection, and Correlating incident data): These functions are standard core capabilities of Security Information and Event Management (SIEM) systems and traditional security analytics tools rather than being unique to SOAR.

upvoted 1 times

Which two processes are critical to a security information and event management (SIEM) platform? (Choose two.)

- A. Detection of threats using data analysis
- B. Automation of security deployments
- C. Ingestion of log data
- D. Prevention of cybersecurity attacks

Suggested Answer: A, C

Explanation: Detection of threats using data analysis – SIEM platforms analyze collected data to identify suspicious patterns and detect threats. Ingestion of log data – SIEM systems collect and centralize log data from various sources, which is essential for analysis, correlation, and alerting. Automation and prevention are more aligned with SOAR and firewall/EDR functionalities, not the core operations of SIEM.

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

Which Palo Alto Networks solution has replaced legacy IPS solutions?

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

Suggested Answer: C

Explanation: Advanced Threat Prevention is the Palo Alto Networks solution that has replaced legacy Intrusion Prevention Systems (IPS). It offers inline, ML-powered threat detection and evasion-resistant inspection to block sophisticated threats in real time, going beyond traditional signature-based IPS.

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

Which type of system is a user entity behavior analysis (UEBA) tool?

- A. Correlating
- B. Active monitoring
- C. Archiving
- D. Sandboxing

Suggested Answer: B

Explanation: A User Entity Behavior Analysis (UEBA) tool performs active monitoring by continuously analyzing the behavior of users and entities to detect anomalies that may indicate insider threats, compromised accounts, or malicious activity. It uses machine learning and analytics to identify unusual patterns in real time.

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

What is a function of SSL/TLS decryption?

- A. It applies to unknown threat detection only.
- B. It reveals malware within web-based traffic.
- C. It protects users from social engineering.
- D. It identifies IoT devices on the internet.

Suggested Answer: *B*

Explanation: SSL/TLS decryption allows security tools to inspect encrypted traffic, enabling them to detect hidden malware, command-and-control communication, or data exfiltration that would otherwise bypass inspection if left encrypted.

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

Which feature is part of an intrusion prevention system (IPS)?

- A. API-based coverage of apps
- B. Automated security actions
- C. Protection of data at rest
- D. Real-time web filtering

Suggested Answer: B

Explanation: An Intrusion Prevention System (IPS) includes automated security actions, such as blocking malicious traffic, resetting connections, or alerting administrators when it detects suspicious activity, helping to stop attacks in real time.

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

What are two capabilities of identity threat detection and response (ITDR)? (Choose two.)

- A. Securing individual devices
- B. Matching risks to signatures
- C. Scanning for excessive logins
- D. Analyzing access management logs

Suggested Answer: *C, D*

Explanation: Scanning for excessive logins – ITDR identifies suspicious patterns such as unusual or excessive login attempts, which may indicate credential abuse. Analyzing access management logs – ITDR tools analyze identity-related logs, including authentication and authorization events, to detect threats tied to user behavior and access anomalies. Device security and signature matching are not core functions of ITDR; they fall under endpoint protection and traditional threat detection respectively.

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

Which type of attack involves sending data packets disguised as queries to a remote server, which then sends the data back to the attacker?

- A. DDoS
- B. DNS tunneling
- C. Command-and-control (C2)
- D. Port evasion

Suggested Answer: B

Explanation: DNS tunneling is an attack technique where data packets are disguised as DNS queries and sent to a remote server. That server, often under the attacker's control, responds with additional data or instructions, effectively creating a covert command-and-control (C2) channel over DNS.

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

Which service is encompassed by serverless architecture?

- A. Infrastructure as a Service (IaaS)
- B. Function as a Service (FaaS)
- C. Security as a Service (SaaS)
- D. Authentication as a Service (AaaS)

Suggested Answer: B

Explanation: Serverless architecture is primarily implemented through Function as a Service (FaaS), where developers write and deploy individual functions without managing the underlying infrastructure. The cloud provider handles scaling, resource allocation, and execution on demand.

 **jarzynvip** Most Recent 1 month, 1 week ago

Selected Answer: B

Function as a Service (FaaS) to podstawa architektury bezserwerowej (serverless). Umożliwia uruchamianie pojedynczych funkcji kodu w chmurze w odpowiedzi na konkretne zdarzenia, bez konieczności konfigurowania, zarządzania czy skalowania serwerów

upvoted 1 times

Which architecture model uses virtual machines (VMs) in a public cloud environment?

- A. Kubernetes
- B. Serverless
- C. Docker
- D. Host-based

Suggested Answer: *D*

Explanation: A host-based architecture uses virtual machines (VMs) to run workloads on a shared host, commonly found in public cloud environments. Each VM operates independently with its own OS, making this model suitable for traditional and isolated application deployments.

 **jarzynvip** Most Recent 1 month, 1 week ago

Selected Answer: *D*

D. Host-based

Overview of Options:

Host-based: Uses full Virtual Machines (VMs) or instances running complete operating systems in a public cloud environment (such as AWS EC2 or Azure VMs). Kubernetes & Docker: Rely on containerization (OS-level virtualization) rather than managing standalone virtual machines directly.

Serverless: Eliminates the need to manage virtual machines, executing code dynamically on demand managed completely by the cloud provider.

upvoted 1 times

Which two statements apply to SaaS financial botnets? (Choose two.)

- A. They are larger than spamming or DDoS botnets.
- B. They are sold as kits that allow attackers to license the code.
- C. They are a defense against spam attacks.
- D. They are used by attackers to build their own botnets.

Suggested Answer: B, D

Explanation: SaaS financial botnets are often sold as kits, enabling attackers to license and reuse the malicious code easily. These kits allow attackers to build and operate their own botnets, often targeting financial data or systems. Financial botnets are typically smaller but more targeted than spamming or DDoS botnets. Botnets are not a defense mechanism, but rather a threat.

 **jarzynvip** Most Recent 1 month, 1 week ago

Selected Answer: B,D

The correct answers are B and D.

Explanation: B. They are sold as kits that allow attackers to license the code: Cybercriminals offer financial botnets under a Software-as-a-Service (SaaS) or crimeware-as-a-service model, providing licensing, updates, and attack infrastructure kits to buyer/attackers.

D. They are used by attackers to build their own botnets: These SaaS kits enable attackers to easily set up, customize, and operate their own botnets to target financial credentials and institutions.

Why the other options are incorrect:

A is incorrect: Financial botnets tend to be smaller, highly targeted networks rather than massive spamming or DDoS botnets.

C is incorrect: Botnets are offensive cyber threats used by attackers, not defensive tools against spam.

upvoted 1 times

What is an event-driven snippet of code that runs on managed infrastructure?

- A. API
- B. Serverless function
- C. Hypervisor
- D. Docker container

Suggested Answer: *B*

Explanation: A serverless function is an event-driven snippet of code that runs on managed infrastructure, typically as part of a Function as a Service (FaaS) model. It is executed in response to events such as HTTP requests or database changes, and the cloud provider handles the underlying infrastructure.

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

Which type of attack obscures its presence while attempting to spread to multiple hosts in a network?

- A. Advanced malware
- B. Smishing
- C. Reconnaissance
- D. Denial of service

Suggested Answer: A

Explanation: Advanced malware is designed to evade detection and persist within a system, often using stealthy techniques to spread laterally across multiple hosts in a network without triggering alerts, making it especially dangerous and difficult to remove.

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

What is a dependency for the functionality of signature-based malware detection?

- A. Frequent database updates
- B. Support of a DLP device
- C. API integration with a sandbox
- D. Enabling quality of service

Suggested Answer: A

Explanation: Signature-based malware detection relies on a constantly updated database of known threat signatures to identify malicious files or activity. Without frequent updates, it becomes ineffective against newly emerging threats.

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

When does a TLS handshake occur?

- A. Before establishing a TCP connection
- B. Only during DNS over HTTPS queries
- C. After a TCP handshake has been established
- D. Independently of HTTPS communications

Suggested Answer: C

Explanation: A TLS handshake occurs after the TCP handshake is complete. The TLS handshake is responsible for establishing a secure, encrypted session between client and server, including the negotiation of encryption algorithms and exchange of keys.

 **jarzynvip** Most Recent 1 month, 1 week ago

Selected Answer: C

C. After a TCP handshake has been established

Explanation:

TCP Handshake First: A TLS handshake requires a reliable connection to exchange encryption parameters, certificates, and keys. Therefore, the standard TCP three-way handshake (SYN, SYN-ACK, ACK) must be completed before the TLS handshake can begin.

Order of Execution:

1-TCP Handshake (Transport Layer)

2-TLS Handshake (Security/Presentation Layer)

3-Application Data Transfer (e.g., HTTP request/response)

upvoted 1 times