Vendor: Cisco

Exam Code: 350-201

Exam Name: Performing CyberOps Using Core Security Technologies

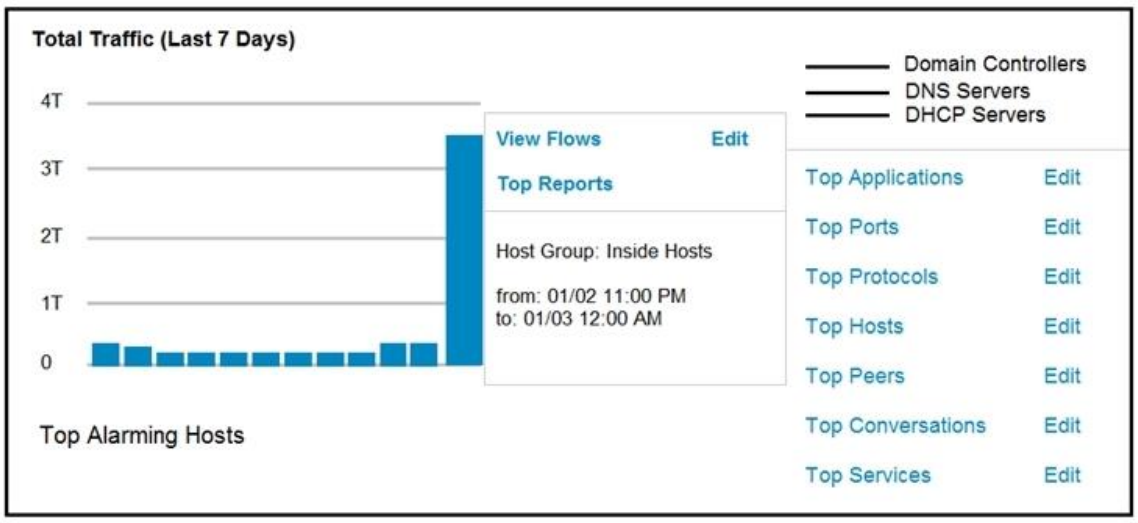
Version: DEMO

QUESTION 1
An engineer is moving data from NAS servers in different departments to a combined storage database so that the data can be accessed and analyzed by the organization on-demand. Which data management process is being used?

A. data clustering
B. data regression
C. data ingestion
D. data obfuscation

Answer: C
Explanation:
Technically, data ingestion is the process of transferring data from any source. But that's not always the case as businesses have multiple units, each having its own applications, file types, and systems. To make business decisions, companies port-in data from these heterogeneous sources onto a single storage medium, typically a data warehouse or a data mart after passing it through the Extract, Transfer, Load (ETL) process.
https://dataintegrationinfo.com/what-is-data-ingestion

QUESTION 2
Refer to the exhibit. An engineer notices a significant anomaly in the traffic in one of the host groups in Cisco Secure Network Analytics (Stealthwatch) and must analyze the top data transmissions. Which tool accomplishes this task?



A. Top Peers
B. Top Hosts
C. Top Conversations
D. Top Ports

Answer: C
Explanation:
Top Host doesn't show any "top data transmission" deteails, it shows WHO has more traffic. Top Conversations show WHAT data transmissions (ports, protocols, peer) are highest.

QUESTION 3
Refer to the exhibit. Where are the browser page rendering permissions displayed?

```
pragma: no-cache
server: Apache
status: 200
strict-transport-security: max-age=31536000
vary: Accept-Encoding
x-content-type-options: nosniff
x-frame-options: SAMEORIGIN
x-test-debug: nURL=www.cisco.com,realm=0,isRealm=0,realDomain=0,shortrealm=0
x-xss-protection: 1; mode=block
```

A. x-frame-options
B. x-xss-protection
C. x-content-type-options
D. x-test-debug

Answer: A
Explanation:
Conten-type: media type of the source and charset provided to the client or sent from the client
X-Frame-Options: HTTP response header can be used to indicate whether or not a browser should be allowed to render a page in a frame, iframe, embed or object.
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options#browser_compatibility

QUESTION 4
Refer to the exhibit. An employee is a victim of a social engineering phone call and installs remote access software to allow an "MS Support" technician to check his machine for malware. The employee becomes suspicious after the remote technician requests payment in the form of gift cards. The employee has copies of multiple, unencrypted database files, over 400 MB each, on his system and is worried that the scammer copied the files off but has no proof of it. The remote technician was connected sometime between 2:00 pm and 3:00 pm over https.
What should be determined regarding data loss between the employee's laptop and the remote technician's system?

```
Max (K)     Retain      OverflowAction       Entries        Log
-------     ------      --------------       --------       ---
15,168           0      OverwriteAsNeeded    20,792         Application
15,168           0      OverwriteAsNeeded    12,559         System
15,360           0      OverwriteAsNeeded    11,173         Windows PowerShell
```

A. No database files were disclosed
B. The database files were disclosed
C. The database files integrity was violated
D. The database files were intentionally corrupted, and encryption is possible

Answer: A
Explanation:
Anydesk access through HTTPS web client can only send files but not download from the sysem.

QUESTION 5
What is a principle of Infrastructure as Code?

A. System maintenance is delegated to software systems
B. Comprehensive initial designs support robust systems
C. Scripts and manual configurations work together to ensure repeatable routines
D. System downtime is grouped and scheduled across the infrastructure

Answer: A
Explanation:
Infrastructure as code (IaC) is a software-based IT methodology for codifying and maintaining IT infrastructure.

QUESTION 6
Refer to the exhibit. A security analyst needs to investigate a security incident involving several suspicious connections with a possible attacker. Which tool should the analyst use to identify the source IP of the offender?

TCP	192.168.1.8:54580	vk-in-f108:imaps	ESTABLISHED
TCP	192.168.1.8:54583	132.245.61.50:https	ESTABLISHED
TCP	192.168.1.8:54916	bay405-m:https	ESTABLISHED
TCP	192.168.1.8:54978	vu-in-f188:5228	ESTABLISHED
TCP	192.168.1.8:55094	72.21.194.109:https	ESTABLISHED
TCP	192.168.1.8:55401	wonderhowto:http	ESTABLISHED
TCP	192.168.1.8:55730	mia07s34-in-f78:https	TIME WAIT
TCP	192.168.1.8:55824	a23-40-191-15:https	CLOSE_WAIT
TCP	192.168.1.8:55825	a23-40-191-15:https	CLOSE_WAIT
TCP	192.168.1.8:55846	mia07s25-in-f14:https	TIME_WAIT
TCP	192.168.1.8:55847	a184-51-150-89:http	CLOSE_WAIT
TCP	192.168.1.8:55853	157.55.56.154:40028	ESTABLISHED
TCP	192.168.1.8:55879	atl14s38-in-f4:https	ESTABLISHED
TCP	192.168.1.8:55884	208-46-117-174:https	ESTABLISHED
TCP	192.168.1.8:55893	vx-in-f95:https	TIME_WAIT
TCP	192.168.1.8:55947	stackoverflow:https	ESTABLISHED
TCP	192.168.1.8:55966	stackoverflow:https	ESTABLISHED
TCP	192.168.1.8:55970	mia07s34-in-f78:https	TIME_WAIT
TCP	192.168.1.8:55972	191.238.241.80:https	TIME_WAIT
TCP	192.168.1.8:55976	54.239.26.242:https	ESTABLISHED
TCP	192.168.1.8:55979	mia07s35-in-f14:https	ESTABLISHED
TCP	192.168.1.8:55986	server11:https	TIME_WAIT
TCP	192.168.1.8:55988	104.16.118.182:http	ESTABLISHED

A. packet sniffer
B. malware analysis
C. SIEM

D. firewall manager

Answer: D
Explanation:
Netstat image is useless without the source of information that identified the possible attacker connections. An FMC as in "D. Firewall manager" would identify the attack based on IPS and show the IP. A sniffer does not have security intel to identify the offending IP.

QUESTION 7
A threat actor attacked an organization's Active Directory server from a remote location, and in a thirty-minute timeframe, stole the password for the administrator account and attempted to access 3 company servers. The threat actor successfully accessed the first server that contained sales data, but no files were downloaded. A second server was also accessed that contained marketing information and 11 files were downloaded. When the threat actor accessed the third server that contained corporate financial data, the session was disconnected, and the administrator's account was disabled. Which activity triggered the behavior analytics tool?

A. accessing the Active Directory server
B. accessing the server with financial data
C. accessing multiple servers
D. downloading more than 10 files

Answer: B
Explanation:
If you have admin then it is normal to jump through many RDPs for many tasks, an admin in a financial server would be more suspicious. Accessing multiple servers would probably raise many False Positive alerts and disabled accounts.

QUESTION 8
A company recently completed an internal audit and discovered that there is CSRF vulnerability in 20 of its hosted applications. Based on the audit, which recommendation should an engineer make for patching?

A. Identify the business applications running on the assets
B. Update software to patch third-party software
C. Validate CSRF by executing exploits within Metasploit
D. Fix applications according to the risk scores

Answer: D
Explanation:
Cross-Site Request Forgery (CSRF) is a type of attack that occurs when a malicious web site, email, blog, instant message, or program causes a user's web browser to perform an unwanted action on a trusted site when the user is authenticated. A CSRF attack works because browser requests automatically include all cookies including session cookies. Therefore, if the user is authenticated to the site, the site cannot distinguish between legitimate authorized requests and forged authenticated requests.

QUESTION 9
An engineer is going through vulnerability triage with company management because of a recent malware outbreak from which 21 affected assets need to be patched or remediated. Management decides not to prioritize fixing the assets and accepts the vulnerabilities. What is the next step the

engineer should take?

A. Investigate the vulnerability to prevent further spread
B. Acknowledge the vulnerabilities and document the risk
C. Apply vendor patches or available hot fixes
D. Isolate the assets affected in a separate network

Answer: B
Explanation:
Acknowledge issues are those which, for whatever reason, you decide not to resolve at present. There are valid reasons for not immediately resolving a vulnerability, and they should be recorded, along with the reasoning for acknowledging it and a review date given. If the level of risk they present is sufficiently high, record the issue in a risk register.

QUESTION 10
Refer to the exhibit. How must these advisories be prioritized for handling?

Vulnerability #1	Vulnerability #2
A vulnerability in the Command Line Interpreter (CLI) of ACME Super Firewall (all models) could allow an attacker to execute a command which would overflow a buffer in memory. In order to carry out this attack, the attacker needs to fulfill all of the following conditions: a) Be logged in to the device over telnet or SSH, or through the local console b) Be logged in as a high-privileges administrative user In order to trigger the vulnerability, the attacker has to execute a command on the device and supply a specially crafted argument to such command. Once the command is executed, an internal stack-based buffer overflow will be triggered. This buffer overflow may lead to code execution within the process space of the CLI parser, or may crash the device. All software versions are affected Fixes are available now There are no workarounds or mitigations	A vulnerability in the web-based management interface of the ACME Big Router models 1010 and 1020 could allow an attacker to bypass authorization checks and then access sensitive information on the device, modify the device's configuration, impact the availability of the system, create administrative level and regular level users on the device. In order to exploit this vulnerability, the attacker needs to: a) Be able to reach port 80/tcp on an affected device b) The web-based management interface needs to be enabled on the device The attacker would then need to send a specially formed HTTP request to the web-based management interface of an affected system. The attacker does not need to log-in to the device before launching the attack. All software versions are affected There are no fixes available now Customers can disable the web-based management interface to prevent exploitation. Customers will still be able to manage, configure and monitor the device by using the Command Line Interface (CLI), but with reduced capabilities for monitoring.

A. The highest priority for handling depends on the type of institution deploying the devices
B. Vulnerability #2 is the highest priority for every type of institution
C. Vulnerability #1 and vulnerability #2 have the same priority
D. Vulnerability #1 is the highest priority for every type of institution

Answer: B
Explanation:
All that is needed is port 80 access on #2 whereas #1 requires a login by a privileged account to exploit.

QUESTION 11
The incident response team receives information about the abnormal behavior of a host. A malicious file is found being executed from an external USB flash drive. The team collects and documents all the necessary evidence from the computing resource. What is the next step?

A. Conduct a risk assessment of systems and applications
B. Isolate the infected host from the rest of the subnet
C. Install malware prevention software on the host
D. Analyze network traffic on the host's subnet

Answer: B
Explanation:
Short-term containment - limiting damage before the incident gets worse, usually by isolating network segments, taking down hacked production server and routing to failover.

QUESTION 12
An organization had several cyberattacks over the last 6 months and has tasked an engineer with looking for patterns or trends that will help the organization anticipate future attacks and mitigate them. Which data analytic technique should the engineer use to accomplish this task?

A. diagnostic
B. qualitative
C. predictive
D. statistical

Answer: C
Explanation:
What Is Predictive Analytics?
When you know what happened in the past and understand why it happened, you can then begin to predict what is likely to occur in the future based on that information. Predictive analytics takes the investigation a step further, using statistics, computational modeling, and machine learning to determine the probability of various outcomes.

What Is Diagnostic Analytics?
Once you know what happened, you'll want to know why it happened. That's where diagnostic analytics comes in. Understanding why a trend is developing or why a problem occurred will make your business intelligence actionable. It prevents your team from making inaccurate guesses, particularly related to confusing correlation and causality.

QUESTION 13
An employee abused PowerShell commands and script interpreters, which lead to an indicator of compromise (IOC) trigger. The IOC event shows that a known malicious file has been executed, and there is an increased likelihood of a breach. Which indicator generated this IOC event?

A. ExecutedMalware.ioc
B. Crossrider.ioc
C. ConnectToSuspiciousDomain.ioc
D. W32 AccesschkUtility.ioc

Answer: A
Explanation:
Crossrider is a an Adware variant that targets Mac with the intent of displaying ads. It also changes the default home page of Safari and Chrome browsers.
W32.AccesschkUtility.ioc
Accesscheck is a Windows utility that lets users check for access rights on resources including files, directories, registry keys, global objects and Windows services. This utility could be used by

malware or threat actors with malicious intent such as collection of information necessary for privilege escalation on the compromised host. This indicator monitors for accesschk tool used with suspicious options that suppress errors and dialog boxes.
ExecutedMalware.ioc
A known malicious file was executed. This increases the likelihood of a successful breach and this event should be promptly investigated.

QUESTION 14
Refer to the exhibit. IDS is producing an increased amount of false positive events about brute force attempts on the organization's mail server. How should the Snort rule be modified to improve performance?

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 143 ( msg:"PROTOCOL-
IMAP login brute force attempt";
flow:to_server,established,no_stream;
content:"LOGIN",fast_pattern,nocase; detection_filter:track
by_dst, count 5, seconds 900; metadata:ruleset community;
service:imap; reference:url,attack.mitre.org/techniques/T1110;
classtype:suspicious-login; sid:2273; rev:12; )
```

A. Block list of internal IPs from the rule
B. Change the rule content match to case sensitive
C. Set the rule to track the source IP
D. Tune the count and seconds threshold of the rule

Answer: C
Explanation:
Step 1 Identify Potential Locations for Sensors - To properly tune IDS sensors, the first step is to identify network locations where the sensors can be placed for maximum efficiency.
https://www.ccexpert.us/ccie-security/ids-tuning.html

QUESTION 15
A company's web server availability was breached by a DDoS attack and was offline for 3 hours because it was not deemed a critical asset in the incident response playbook. Leadership has requested a risk assessment of the asset. An analyst conducted the risk assessment using the threat sources, events, and vulnerabilities. Which additional element is needed to calculate the risk?

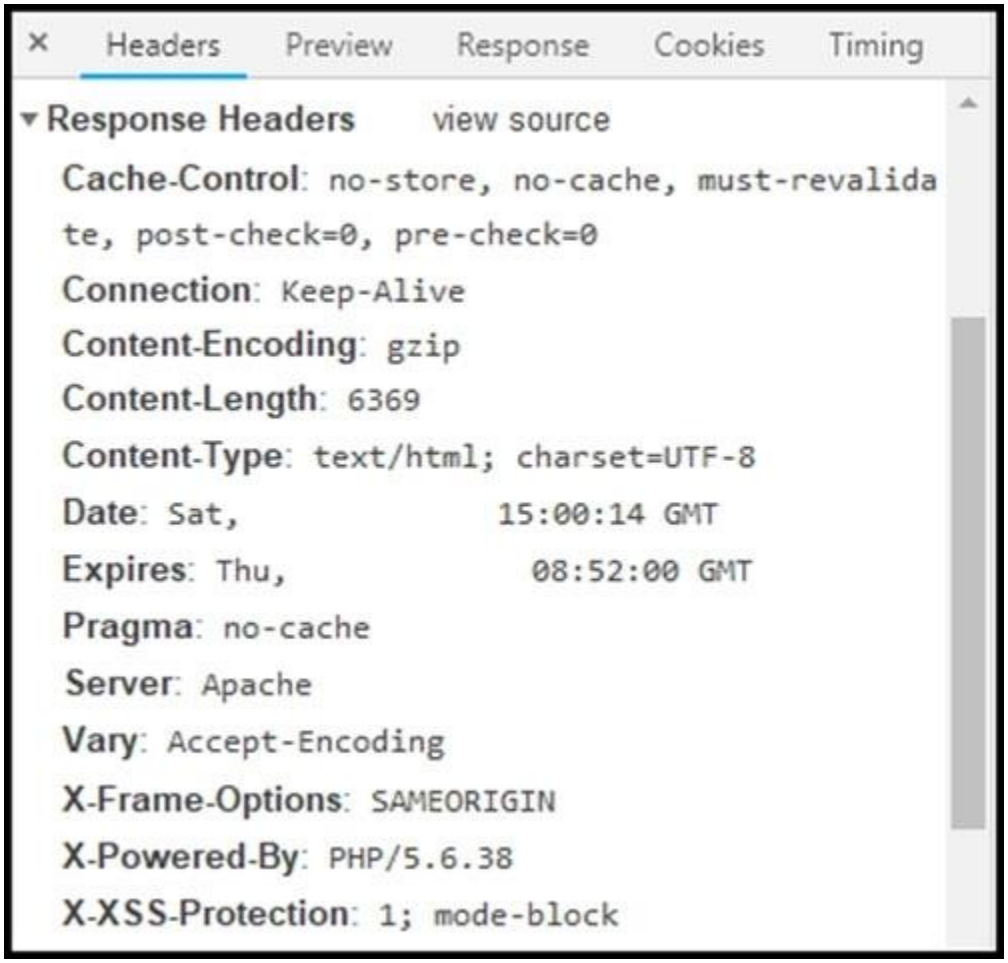
A. assessment scope
B. event severity and likelihood
C. incident response playbook
D. risk model framework

Answer: B
Explanation:
To conduct an assessment the following steps are required:
1) Identify threat sources and events
2) Identify vulnerabilities and predisposing conditions

3) Determine likelihood of occurrence
4) Determine magnitude of impact
5) Determine risk

https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf (page 32)

QUESTION 16
Refer to the exhibit. Where are the browser page rendering permissions displayed?



A. X-Frame-Options
B. X-XSS-Protection
C. Content-Type
D. Cache-Control

Answer: A
Explanation:
Conten-type: media type of the source and charset provided to the client or sent from the client
X-Frame-Options: HTTP response header can be used to indicate whether or not a browser should be allowed to render a page in a frame, iframe, embed or object.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**