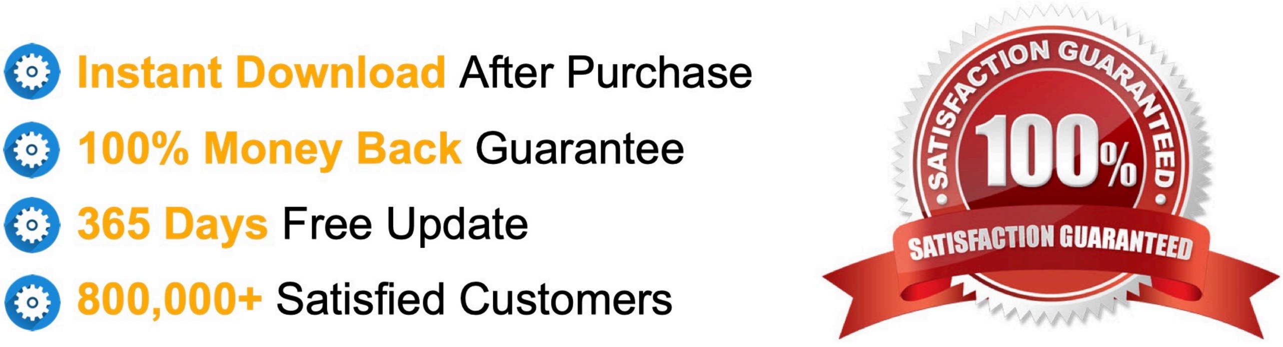
PCDRA Q&As

Palo Alto Networks Certified Detection and Remediation Analyst

Pass Palo Alto Networks PCDRA Exam with 100% Guarantee

Following Questions and Answers are all new published by Palo Alto Networks Official Exam Center


Instant Download After Purchase
100% Money Back Guarantee
365 Days Free Update
800,000+ Satisfied Customers
SATISFACTION GUARANTEED
100%
SATISFACTION GUARANTEED

QUESTION 1

Which function describes the removal of a specific file from its location on a local or removable drive to a protected folder to prevent the file from being executed?

A. Search and destroy

B. Isolation

C. Quarantine

D. Flag for removal

Correct Answer: C

Explanation: The function that describes the removal of a specific file from its location on a local or removable drive to a protected folder to prevent the file from being executed is quarantine. Quarantine is a feature of Cortex XDR that allows you to isolate malicious or suspicious files from the endpoint and prevent them from running or spreading. You can quarantine files manually from the Cortex XDR console, or automatically based on the malware analysis profile or the remediation suggestions. When you quarantine a file, the Cortex XDR agent encrypts the file and moves it to a hidden folder under the agent installation directory. The file is also renamed with a random string and a .quarantine extension. You can view, restore, or delete the quarantined files from the Cortex XDR console. References: Quarantine Files Manage Quarantined Files

QUESTION 2

What kind of malware uses encryption, data theft, denial of service, and possibly harassment to take advantage of a victim?

A. Ransomware

B. Worm

C. Keylogger

D. Rootkit

Correct Answer: A

Explanation: The kind of malware that uses encryption, data theft, denial of service, and possibly harassment to take advantage of a victim is ransomware. Ransomware is a type of malware that encrypts the victim\\'s files or blocks access to

their system, and then demands a ransom for the decryption key or the restoration of access. Ransomware can also threaten to expose or delete the victim\\'s data if the ransom is not paid. Ransomware can cause significant damage and

disruption to individuals, businesses, and organizations, and can be difficult to remove or recover from. Some examples of ransomware are CryptoLocker, WannaCry, Ryuk, and REvil.

References:

12 Types of Malware + Examples That You Should Know - CrowdStrike What is Malware? Malware Definition, Types

and Protection 12+ Types of Malware Explained with Examples (Complete List)

QUESTION 3

Which Type of IOC can you define in Cortex XDR?

A. destination port

B. e-mail address

C. full path

D. App-ID

Correct Answer: C

Explanation: Cortex XDR allows you to define IOCs based on various criteria, such as file hashes, registry keys, IP addresses, domain names, and full paths. A full path IOC is a specific location of a file or folder on an endpoint, such as C:\Windows\System32\calc.exe. You can use full path IOCs to detect and respond to malicious files or folders that are located in known locations on your endpoints12. Let\\'s briefly discuss the other options to provide a comprehensive explanation:

A. destination port: This is not the correct answer. Destination port is not a type of IOC that you can define in Cortex XDR. Destination port is a network attribute that indicates the port number to which a packet is sent. Cortex XDR does not support defining IOCs based on destination ports, but you can use XQL queries to filter network events by destination ports3.

B. e-mail address: This is not the correct answer. E-mail address is not a type of IOC that you can define in Cortex XDR. E-mail address is an identifier that is used to send and receive e-mails. Cortex XDR does not support defining IOCs based on e-mail addresses, but you can use the Cortex XDR - IOC integration with Cortex XSOAR to ingest IOCs from various sources, including e-mail addresses4.

D. App-ID: This is not the correct answer. App-ID is not a type of IOC that you can define in Cortex XDR. App-ID is a feature of Palo Alto Networks firewalls that identifies and controls applications on the network. Cortex XDR does not support defining IOCs based on App- IDs, but you can use the Cortex XDR Analytics app to create custom rules that use App- IDs as part of the rule logic5. In conclusion, full path is the type of IOC that you can define in Cortex XDR. By using full path IOCs, you can enhance your detection and response capabilities and protect your endpoints from malicious files or folders. References: Create an IOC Rule XQL Reference Guide: Network Events Schema Cortex XDR - IOC Cortex XDR Analytics App PCDRA: Which Type of IOC can define in Cortex XDR?

QUESTION 4

A file is identified as malware by the Local Analysis module whereas WildFire verdict is Benign, Assuming WildFire is accurate. Which statement is correct for the incident?

A. It is true positive.

B. It is false positive.

C. It is a false negative.

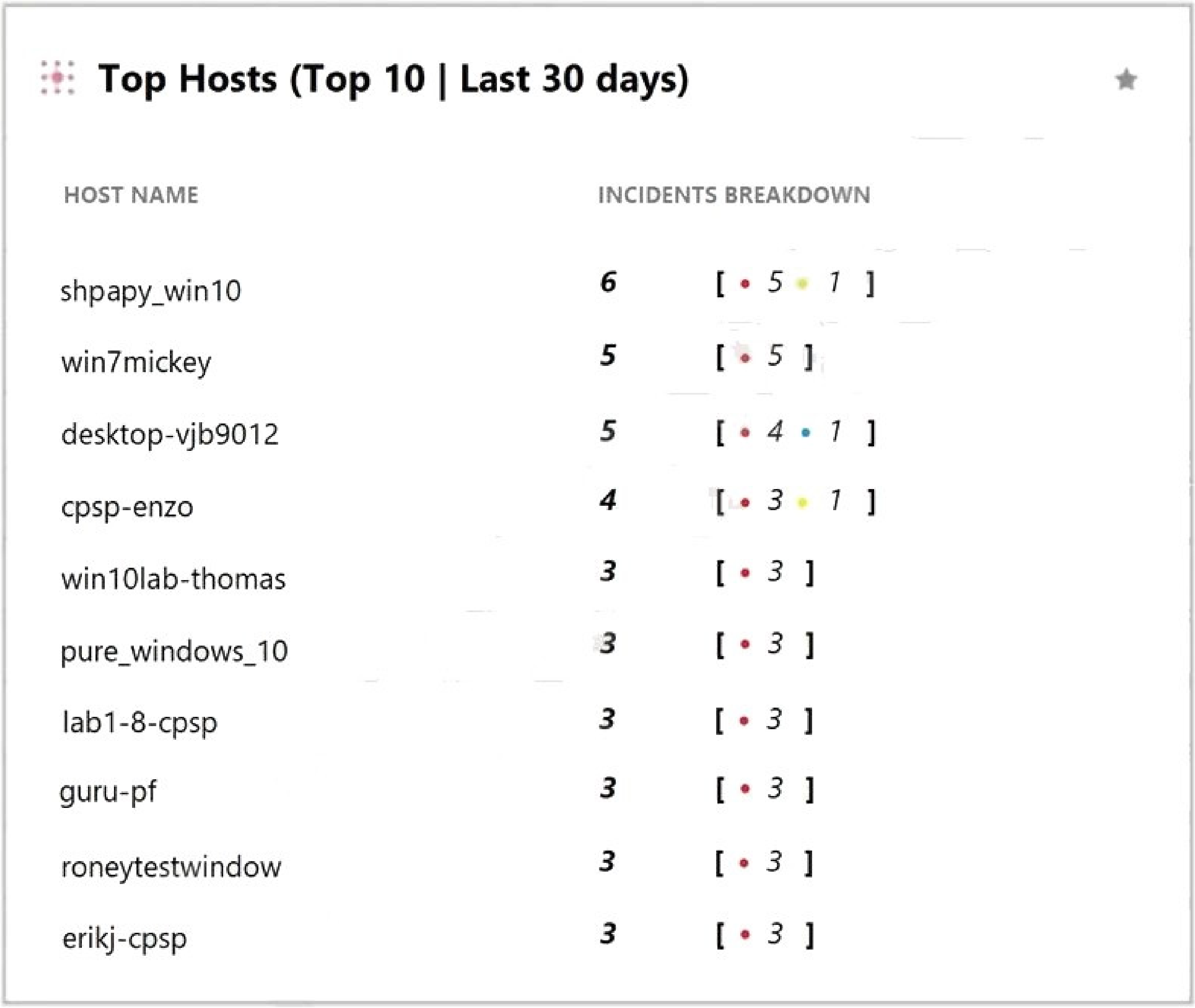
D. It is true negative.

Correct Answer: B

Explanation: A false positive is a situation where a file or activity is incorrectly identified as malicious by a security tool, when in fact it is benign or harmless. A false positive can cause unnecessary alerts, disruptions, or remediation actions, and reduce the confidence and efficiency of the security system. In this question, a file is identified as malware by the Local Analysis module, whereas WildFire verdict is Benign, assuming WildFire is accurate. This means that the Local Analysis module has made a mistake and flagged a legitimate file as malicious, while WildFire has correctly determined that the file is safe. Therefore, this is an example of a false positive. The Local Analysis module is a feature of the Cortex XDR agent that uses a static set of pattern-matching rules and a statistical model to determine if an unknown file is likely to be malware. The Local Analysis module can provide a fast and offline verdict for files that are not yet analyzed by WildFire, but it is not as accurate or comprehensive as WildFire, which uses dynamic analysis and machine learning to examine the behavior and characteristics of files in a sandbox environment. WildFire verdicts are considered more reliable and authoritative than Local Analysis verdicts, and can override them in case of a discrepancy. Therefore, if a file is identified as malware by the Local Analysis module, but as Benign by WildFire, the WildFire verdict should be trusted and the Local Analysis verdict should be disregarded123 References: False positive (security) - Wikipedia Local Analysis WildFire Overview

QUESTION 5

What does the following output tell us?



Top Hosts (Top 10 | Last 30 days)

HOST NAME	INCIDENTS BREAKDOWN	
shpapy_win10	6	[• 5 • 1]
win7mickey	5	[• 5]
desktop-vjb9012	5	[• 4 • 1]
cpsp-enzo	4	[• 3 • 1]
win10lab-thomas	3	[• 3]
pure_windows_10	3	[• 3]
lab1-8-cpsp	3	[• 3]
guru-pf	3	[• 3]
roneytestwindow	3	[• 3]
erikj-cpsp	3	[• 3]

A. There is one low severity incident.

B. Host shpapy_win10 had the most vulnerabilities.

C. There is one informational severity alert.

D. This is an actual output of the Top 10 hosts with the most malware.

Correct Answer: D

Explanation: The output shows the top 10 hosts with the most malware in the last 30 days, based on the Cortex XDR data. The output is sorted by the number of incidents, with the host with the most incidents at the top. The output also shows the number of alerts, the number of endpoints, and the percentage of endpoints for each host. The output is generated by using the ACC (Application Command Center) feature of Cortex XDR, which provides a graphical representation of the network activity and threat landscape. The ACC allows you to view and analyze various widgets, such as the Top 10 hosts with the most malware, the Top 10 applications by bandwidth, the Top 10 threats by count, and more . References: Use the ACC to Analyze Network Activity Top 10 Hosts with the Most Malware

QUESTION 6

Cortex XDR Analytics can alert when detecting activity matching the following MITRE ATTandCKTM techniques.

A. Exfiltration, Command and Control, Collection

B. Exfiltration, Command and Control, Privilege Escalation

C. Exfiltration, Command and Control, Impact

D. Exfiltration, Command and Control, Lateral Movement

Correct Answer: D

Explanation: Cortex XDR Analytics is a feature of Cortex XDR that leverages machine learning and behavioral analytics to detect and alert on malicious activity across the network and endpoint layers. Cortex XDR Analytics can alert when detecting activity matching the following MITRE ATTandCKTM techniques: Exfiltration, Command and Control, Lateral Movement, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, and Collection. However, among the options given in the question, the correct answer is D, Exfiltration, Command and Control, Lateral Movement. These are three of the most critical techniques that indicate an advanced and persistent threat (APT) in the environment. Exfiltration refers to the technique of transferring data or information from the compromised system or network to an external location controlled by the adversary. Command and Control refers to the technique of communicating with the compromised system or network to provide instructions, receive data, or update malware. Lateral Movement refers to the technique of moving from one system or network to another within the same environment, usually to gain access to more resources or data. Cortex XDR Analytics can alert on these techniques by analyzing various data sources, such as network traffic, firewall logs, endpoint events, and threat intelligence, and applying behavioral models, anomaly detection, and correlation rules. Cortex XDR Analytics can also map the alerts to the corresponding MITRE ATTandCKTM techniques and provide additional context and visibility into the attack chain1234 References: Cortex XDR Analytics MITRE ATTandCKTM Cortex XDR Analytics MITRE ATTandCKTM Techniques Cortex XDR Analytics Alert Categories

QUESTION 7

When using the "File Search and Destroy" feature, which of the following search hash type is supported?

A. SHA256 hash of the file

B. AES256 hash of the file

C. MD5 hash of the file

D. SHA1 hash of the file

Correct Answer: A

Explanation: The File Search and Destroy feature is a capability of Cortex XDR that allows you to search for and delete malicious or unwanted files across your endpoints. You can use this feature to quickly respond to incidents, remediate

threats, and enforce compliance policies. To use the File Search andDestroy feature, you need to specify the file name and the file hash of the file you want to search for and delete. The file hash is a unique identifier of the file that is

generated by a cryptographic hash function. The file hash ensures that you are targeting the exact file you want, and not a file with a similar name or a different version. The File Search and Destroy feature supports the SHA256 hash type,

which is a secure hash algorithm that produces a 256-bit (32-byte) hash value. The SHA256 hash type is widely used for file integrity verification and digital signatures. The File Search and Destroy feature does not support other hash types,

such as AES256, MD5, or SHA1, which are either encryption algorithms or less secure hash algorithms. Therefore, the correct answer is A, SHA256 hash of the file1234

References:

File Search and Destroy

What is a File Hash?

SHA-2 - Wikipedia

When using the "File Search and Destroy" feature, which of the following search hash type is supported?

QUESTION 8

A Linux endpoint with a Cortex XDR Pro per Endpoint license and Enhanced Endpoint Data enabled has reported malicious activity, resulting in the creation of a file that you wish to delete. Which action could you take to delete the file?

A. Manually remediate the problem on the endpoint in question.

B. Open X2go from the Cortex XDR console and delete the file via X2go.

C. Initiate Remediate Suggestions to automatically delete the file.

D. Open an NFS connection from the Cortex XDR console and delete the file.

Correct Answer: C

Explanation: The best action to delete the file on the Linux endpoint is to initiate Remediation Suggestions from the Cortex XDR console. Remediation Suggestions are a feature of Cortex XDR that provide you with recommended actions to

undo the effects of malicious activity on your endpoints. You can view the remediation suggestions for each alert or incident in the Cortex XDR console, and decide whether to apply them or not. Remediation Suggestions can help you restore

the endpoint to its original state, remove malicious files or processes, or fix registry or system settings. Remediation Suggestions are based on the forensic data collected by the Cortex XDR agent and the analysis performed by Cortex XDR.

The other options are incorrect for the following reasons:

A is incorrect because manually remediating the problem on the endpoint is not a convenient or efficient way to delete the file. Manually remediating the problem would require you to access the endpoint directly, log in as root, locate the file,

and delete it. This would also require you to have the necessary permissions and credentials to access the endpoint, and to know the exact path and name of the file. Manually remediating the problem would also not provide you with any

audit trail or confirmation of the deletion.

B is incorrect because opening X2go from the Cortex XDR console is not a supported or secure way to delete the file. X2go is a third-party remote desktop software that allows you to access Linux endpoints from a graphical user interface.

However, X2go is not integrated with Cortex XDR, and using it would require you to install and configure it on both the Cortex XDR console and the endpoint. Using X2go would also expose the endpoint to potential network attacks or

unauthorized access, and would not provide you with any audit trail or confirmation of the deletion.

D is incorrect because opening an NFS connection from the Cortex XDR console is not a feasible or reliable way to delete the file. NFS is a network file system protocol that allows you to access files on remote servers as if they were local.

However, NFS is not integrated with Cortex XDR, and using it would require you to set up and maintain an NFS server and client on both the Cortex XDR console and the endpoint. Using NFS would also depend on the network availability

and performance, and would not provide you with any audit trail or confirmation of the deletion.

References:

Remediation Suggestions

Apply Remediation Suggestions

QUESTION 9

Which of the following Live Terminal options are available for Android systems?

A. Live Terminal is not supported.

B. Stop an app.

C. Run APK scripts.

D. Run Android commands.

Correct Answer: D

Explanation: Cortex XDR supports Live Terminal for Android systems, which allows you to remotely access and manage Android endpoints using a command-line interface. You can use Live Terminal to run Android commands, such as adb shell, adb logcat, adb install, and adb uninstall. You can also use Live Terminal to view and modify files, directories, and permissions on the Android endpoints. Live Terminal for Android systems does not support stopping an app or running APK scripts. References: Cortex XDR documentation portal Initiate a Live Terminal Session Live Terminal Commands

QUESTION 10

If you have an isolated network that is prevented from connecting to the Cortex Data Lake, which type of Broker VM setup can you use to facilitate the communication?

A. Broker VM Pathfinder

B. Local Agent Proxy

C. Local Agent Installer and Content Caching

D. Broker VM Syslog Collector

Correct Answer: B

Explanation: If you have an isolated network that is prevented from connecting to the Cortex Data Lake, you can use the Local Agent Proxy setup to facilitate the communication. The Local Agent Proxy is a type of Broker VM that acts as a proxy server for the Cortex XDR agents that are deployed on the isolated network. The Local Agent Proxy enables the Cortex XDR agents to communicate securely with the Cortex Data Lake and the Cortex XDR management console over the internet, without requiring direct access to the internet from the isolated network. The Local Agent Proxy also allows the Cortex XDR agents to download installation packages and content updates from the Cortex XDR management console. To use the Local Agent Proxy setup, you need to deploy a Broker VM on the isolated network and configure it as a Local Agent Proxy. You also need to deploy another Broker VM on a network that has internet access and configure it as a Remote Agent Proxy. The Remote Agent Proxy acts as a relay between the Local Agent Proxy and the Cortex Data Lake. You also need to install a strong cipher SHA256-based SSL certificate on both the Local Agent Proxy and the Remote Agent Proxy to ensure secure communication. You can read more about the Local Agent Proxy setup and how to configure it here1 and here2. References: Local Agent Proxy Configure the Local Agent Proxy Setup

QUESTION 11

How can you pivot within a row to Causality view and Timeline views for further investigate?

A. Using the Open Card Only

B. Using the Open Card and Open Timeline actions respectively

C. You can\\'t pivot within a row to Causality view and Timeline views

D. Using Open Timeline Actions Only

Correct Answer: B

Explanation: To pivot within a row to Causality view and Timeline views for further investigation, you can use the Open Card and Open Timeline actions respectively. The Open Card action will open a new tab with the Causality view of the selected row, showing the causal chain of events that led to the alert. The Open Timeline action will open a new tab with the Timeline view of the selected row, showing the chronological sequence of events that occurred on the affected endpoint. These actions allow you to drill down into the details of each alert and understand the root cause and impact of the incident. References: Cortex XDR User Guide, Chapter 9: Investigate Alerts, Section: Pivot to Causality View and Timeline View PCDRA Study Guide, Section 3: Investigate and Respond to Alerts, Objective 3.1: Investigate alerts using the Causality view and Timeline view

QUESTION 12

In Cortex XDR management console scheduled reports can be forwarded to which of the following applications/services?

A. Salesforce

B. Jira

C. Service Now

D. Slack

Correct Answer: D

Explanation: Cortex XDR allows you to schedule reports and forward them to Slack, a cloud-based collaboration platform. You can configure the Slack channel, frequency, and recipients of the scheduled reports. You can also view the report

history and status in the Cortex XDR management console. References:

Scheduled Queries: This document explains how to create, edit, and manage scheduled queries and reports in Cortex XDR.

Forward Scheduled Reports to Slack: This document provides the steps to configure Slack integration and forward scheduled reports to a Slack channel.

QUESTION 13

Which search methods is supported by File Search and Destroy?

A. File Seek and Destroy

B. File Search and Destroy

C. File Seek and Repair

D. File Search and Repair

Correct Answer: B

Explanation: File Search and Destroy is a feature of Cortex XDR that allows you to search for and remove malicious files from endpoints. You can use this feature to find files by their hash, full path, or partial path using regex parameters. You can then select the files from the search results and destroy them by hash or by path. When you destroy a file by hash, all the file instances on the endpoint are removed. File Search and Destroy is useful for quickly responding to threats and preventing further damage. References: Search and Destroy Malicious Files Cortex XDR Pro Administrator Guide

QUESTION 14

Which of the following protection modules is checked first in the Cortex XDR Windows agent malware protection flow?

A. Hash Verdict Determination

B. Behavioral Threat Protection

C. Restriction Policy

D. Child Process Protection

Correct Answer: A

Explanation: The first protection module that is checked in the Cortex XDR Windows agent malware protection flow is the Hash Verdict Determination. This module compares the hash of the executable file that is about to run on the endpoint with a list of known malicious hashes stored in the Cortex XDR cloud. If the hash matches a malicious hash, the agent blocks the execution and generates an alert. If the hash does not match a malicious hash, the agent proceeds to the next protection module, which is the Restriction Policy1. The Hash Verdict Determination module is the first line of defense against malware, as it can quickly and efficiently prevent known threats from running on the endpoint. However, this module cannot protect against unknown or zero-day threats, which have no known hash signature. Therefore, the Cortex XDR agent relies on other protection modules, such as Behavioral Threat Protection, Child Process Protection, and Exploit Protection, to detect and block malicious behaviors and exploits that may occur during the execution of the file1. References: Palo Alto Networks Cortex XDR Documentation, File Analysis and Protection Flow

QUESTION 15

When selecting multiple Incidents at a time, what options are available from the menu when a user right-clicks the incidents? (Choose two.)

A. Assign incidents to an analyst in bulk.

B. Change the status of multiple incidents.

C. Investigate several Incidents at once.

D. Delete the selected Incidents.

Correct Answer: AB

Explanation: When selecting multiple incidents at a time, the options that are available from the menu when a user right-clicks the incidents are: Assign incidents to an analyst in bulk and Change the status of multiple incidents. These options allow the user to perform bulk actions on the selected incidents, such as assigning them to a specific analyst or changing their status to open, in progress, resolved, or closed. These options can help the user to manage and prioritize the incidents more efficiently and effectively. To use these options, the user needs to select the incidents from the incident table, right-click on them, and choose the desired option from the menu. The user can also use keyboard shortcuts to perform these actions, such as Ctrl+A to select all incidents, Ctrl+Shift+A to assign incidents to an analyst, and Ctrl+Shift+S to change the status of incidents12 References: Assign Incidents to an Analyst in Bulk Change the Status of Multiple Incidents