1. Identify the Security Operations Center (SOC) Practitioner Personas that are most likely to be using Security Information and Event Management (SIEM) on a regular basis.

A. Security Analyst

Security Engineer

2. Identify the three features referred to as "table stakes" for Security Information and Event Management (SIEM).

A.Search, Detection, and Visualization

3. The rule language in Chronicle Security Information and Event Management (SIEM) was designed for what purpose?

A.Threat Detection

4. Aliasing applies to what kinds of entities in Chronicle Security Information and Event Management (SIEM)?

A.Users, Internet Protocol (IP) Addresses, Domains, and Indicators of Compromise (IOCs)

5. What three components make up the Chronicle Entity Context Graph (ECG)?

A.Entity Context, Global Context, and Local Context

6. What is the product name of the largest threat observatory, operated by Google, that plugs directly into Chronicle?

A. VirusTotal

7. There are rules that are created by the customer or owner of a Chronicle Security Information and Event Management (SIEM) tenant, and there are a group of rules developed by Uppercase based on Google threat intelligence. What is the Google-provided rules called?

A.Default Rules

8. Over what time span will Chronicle Security Information and Event Management (SIEM) re-evaluate Indicators of Compromise (IOCs) and create new correlations and alerts?

A. 1 year

9. Data from Chronicle can be transparently copied out into what data warehouse for further analytics?

A.Google BigQuery

10. When selecting a data source to forward to Chronicle Security Information and Event Management (SIEM), for what parsers can you expect the most rigorous testing?

A.Default Parsers

11. What does UDM stand for?

A.Unified Data Model

12. The UDM is designed to contain models for what two types of data?

A.Events and Entities

13. Chronicle Security Information and Event Management (SIEM) applies the schema at what point to ensure maximum performance and increase the number of pivots that can be done on data?

A.On write

14. What is the primary job of the Indexing service?

A.Index the telemetry for fast retrieval.

15. Which Chronicle Security Information and Event Management (SIEM) search method allows for a "grep" like functionality?

A.Raw Log Search

16. What are the two primary functions of the Partner Application Programming Interfaces (APIs)?

A.Provision new customers and parser tools

17. What are the required sections of a YARA-L rule?

A.Meta, events, and condition

18. Which optional field is required for a multi-event YARA-L rule?

A. Match

19. In YARA-L, what is the equivalent of #var > 0?

A.$var

20. For what kind of field will the nocase operator cause an error?

A.Enumerated Fields

21. What are the special operators that can act on a repeated field value in YARA-L?

A.ANY, ALL

22. What is the maximum time range for a match section of a multi-event rule in YARA-L?

A.48 hours

23. What two operators in YARA-L create a sliding window of time that will match events in a specific order?

A.before, after

24. What string function can be used to decode encoded command lines, especially in PowerShell?

A.strings.base64\_decode

25. When considering parsing in Chronicle Security Information and Event Management (SIEM), a data source must always be associated with what?

A.Metadata event type

26. What are the extract functions used in Google's Configuration-based Normalization?

A.JSON, XML, KV, GROK, and CSV

27. What are the two search modes available in Chronicle Security Information and Event Management (SIEM)?

A.Unified Data Model (UDM) Search and Raw Log Scan

28. On the Mandiant Advantage Threat Intelligence home page, high-level activity metrics for which types of threats are shown on the dashboard?

A.Actor, Malware, and Vulnerability

29. What is the minimum Mandiant Threat Intel subscription level that provides access to MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) tactics and techniques for Mandiant-tracked Actors and Malware?

A.Threat Intelligence Security Operations

30. If a prospect requires a keyword-driven solution for deep, dark, and open web reconnaissance, which Mandiant Threat Intelligence subscription should be considered?

A.Digital Threat Monitoring

31. What is the minimum Mandiant Threat Intelligence subscription level that provides full-narrative strategic to tactical analysis and access to 20+ report types from Mandiant frontline threat intelligence analysts?

A.Threat Intelligence Fusion

32. Mandiant Threat Intelligence malware profiles include malware detections written in what language?

A.YARA

33. Which Mandiant Threat Intelligence Application Programming Interface (API) version four endpoint will return a list of all threat actors?

A. /v4/actor

34. Which Mandiant Threat Intelligence API version 4 endpoint will return information about vulnerabilities, including in a given period, by Identity Document (ID) or Common Vulnerabilities and Exposures (CVE)?

A. /v4/vulnerability

35. Which Mandiant Threat Intelligence Application Programming Interface (API) version 4 endpoint will return a list of indicators?

A. /v4/indicator

36. Mandiant Attack Surface Management (ASM) supports scanning for vulnerability exploitation that was demonstrated during the SolarWinds events publicized in December 2020. What kind of vulnerability exploitation was it?

A. Supply chain attack

37. When does Mandiant Attack Surface Management (ASM) require some form of authentication for discovery?

A. When integrating into Cloud Assets or third party tools

38. Mandiant Attack Surface Management (ASM) discovers technologies using what method?

A. NA

39. Which tab in the Mandiant Attack Surface Management (ASM) interface provides a high level exportable executive summary of the ASM solution's findings?

A. Executive Review

40. In Attack Surface Management, what is a seed?

A. A starting point for discovery

41. Which of the following are examples of issues that Mandiant Attack Surface Management (ASM) can identify?

A. Vulnerabilities

Misconfigurations

Expired Certificates

42. Which of the following is a currently supported outbound integration for Mandiant Attack Surface Management (ASM)?

A. JIRA

43. What part of an Entity page shows how Attack Surface Management (ASM) found this entity from the initial seed as well as the task that uncovered it?

A. Discovery Context

44. What collection scan settings can be supplied if custom input types are required?

A. Cookies, Ports, and Headers

45. What are the main types of actors used in Mandiant Security Validation?

A. Network

Endpoint

46. What happens to an Actor in a protected Theater after the conclusion of each test?

A. They are reverted to their original state.

47. The ability to automate drift detection, reducing manual efforts in standardization, is a function of what module of Mandiant Security Validation?

A. Advanced Environmental Drift Analysis

48. When considering a Proof of Concept (POC) of Mandiant Security Validation, in addition to the Success Criteria, what other customer information should be documented before the beginning of the POC?

A. Customer Validation Use Cases

Customer Network Infrastructure and Deployed Security Controls

Customer Internet Egress Internet Protocol (IP) Addresses

49. Which are the two MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) tactics that are not covered by Mandiant Security Validation?

A. Resource Development

Reconnaissance

50. How do you Sync integrations between your Director and Third party integrations?

A.Go to Settings > Integrations. Locate the integration you want to sync to the appropriate table. Click the vertical ellipses in the last column. Click Sync in the drop-down list. Wait for the sync to complete.

51. What is the name of the core Mandiant Security Validation component that is required for running actions against Network Security Controls, Linux, Mac, and Linux endpoint controls, and Email controls.

A.Actors

52. What is the scope of selecting the "All Environments" button when creating a playbook?

A. This function created within the playbook will run on all current environments as well as on all future environments.

53. Identify the use of blocks.

A. Repeatable actions

54. Who typically has sufficient rights to turn off the "simulator" mode?

A. Admin

55. What is the difference between Jobs and Connectors within Chronicle Security Orchestration, Automation, and Response (SOAR)?

A. Connectors are used to ingest cases into the platform. Jobs support healthcheck and synchonization tasks.

56. Where can you check all the Active System Modules?

A. License Management

57. How can a manual action within a playbook be identified?

A. Hand symbol

58. What allows you to create repetitive steps within a workflow and put together a string of inputs and outputs?

A.Blocks

59. Where can you find the execution log of an Alert?

A. Case

60. What can you find within the Chronicle Security Orchestration, Automation, and Response (SOAR) Marketplace?

A.Power Ups and Integrations