Section Quiz

Candidate: Dunkan Gibson (dunkan.gibson)
Date: 4/18/2022 7:27:20 pm • Time spent: 03:38

Score: 80%

Passing Score: 80%

Question 1: ✓ Correct

Which of the following components are the SIEM's way of letting the IT team know that a pre-established parameter is not within the acceptable range?

○ Sensors

○ Trends

➡ ● Alerts

○ Dashboard

EXPLANATION

Alerts are the SIEM's way of letting the IT team know that a pre-established parameter is not within the acceptable range. An alert is intended to get the attention of the IT person, or persons, monitoring the network. A best practice in this area is 24-hour monitoring.

Sensors are set up at critical endpoints, services, and other vulnerable locations. These sensors are programmed to send customized alerts to the SIEM if certain parameters are not within the acceptable range.

The dashboard consists of customizable information screens that show real-time security and network information.

Trends are patterns of activity discovered and reported to the SIEM.

REFERENCES

12.3.3 SIEM and Log Management Facts

q_siem_logmgmt_alert_secp7.question.fex

Question 2: ✓ Correct

Some users report that frequent system crashes have started happening on their workstations. Upon further investigation, you notice that these users all have the same application installed that has been recently updated. Where would you go to conduct a root cause analysis?

○ Firewall log

○ Network log

➡ ● Application log

○ Security log

EXPLANATION

You would choose the application log. Most applications produce some type of event logging. These logs show application access, crashes, updates, and any other relevant information that could be valuable in conducting a root cause analysis. The application may be crashing or not performing correctly, and this could be tied to suspicious activity that may indicate malicious intent.

Network logs tell you what is coming into and leaving your network. A firewall log identifies traffic that has been allowed or denied through a firewall. A security log records information related to logons, such as incorrect passwords being used and the user right usage.

REFERENCES

12.3.3 SIEM and Log Management Facts

q_siem_logmgmt_applogs_secp7.question.fex

▾ Question 3: ✓ Correct

You suspect cache poisoning or spoofing has occurred on your network. Users are complaining of strange web results and being redirected to undesirable sites. Which log would help you determine what is going on?

- ○ Security logs
- ➡ ● DNS logs
- ○ Network logs
- ○ Application logs

EXPLANATION

You would take a look at the DNS logs for DNS cache poisoning. After this, you can begin monitoring DNS query traffic.

Network logs cannot help you with spoofed host name resolution.

Application logs do not help you determine DNS poisoning.

Security logs do little to help you identify spoofing.

REFERENCES

☰ 12.3.3 SIEM and Log Management Facts

q_siem_logmgmt_dnslogs_secp7.question.fex

Question 4: ✓ Correct

You suspect a bad video driver is causing a user's system to randomly crash and reboot. Where would you go to identify and confirm your suspicions?

○ SIP logs

○ Syslog

➡ ● Dump files

○ Application logs

EXPLANATION

You would choose dump files. Dump files are created when an application, OS, or other computer function stops abruptly. These files help IT admins perform root-cause analysis and can also give clues as to the crash's origin. This could be something as commonplace as a bad driver or hardware component. Or, unfortunately, it may prove to be the result of a malicious act.

Syslog is a protocol that defines how log messages are sent from one device to a logging server on an IP network. The sending device sends a small text message to the syslog receiver (the logging server).

App logs show application access, crashes, updates, and any other relevant information that could be valuable in determining root-cause analysis.

Session Information Protocol (SIP) logs contain key information about where a phone call was initiated and what the communication's intent was.

REFERENCES

12.3.3 SIEM and Log Management Facts

q_siem_logmgmt_dump_secp7.question.fex

Question 5: ✓ Correct

Which of the following is a standard for sending log messages to a central logging server?

➡ ● Syslog

○ OVAL

○ Nmap

○ LC4

EXPLANATION

Syslog is a protocol that defines how log messages are sent from one device to a logging server on an IP network. The sending device sends a small text message to the syslog receiver (the logging server).

The Open Vulnerability and Assessment Language (OVAL) is an international standard for testing, analyzing, and reporting the security vulnerabilities of a system.

LC4 (previously called LOphtcrack) is a password-cracking tool.

Nmap is a network mapping tool that performs ping and port scans.

REFERENCES

12.3.3 SIEM and Log Management Facts

q_siem_logmgmt_syslog_01_secp7.question.fex

▼ Question 6: ✗ Incorrect

You are concerned that an attacker can gain access to your web server, make modifications to the system, and alter the log files to hide his or her actions. Which of the following actions would best protect the log files?

- ○ Encrypt the log files.
- ● ~~Take a hash of the log files.~~
- ➡ ○ Use syslog to send log entries to another server.
- ○ Configure permissions on the log files to prevent access.

EXPLANATION

The best protection is to save log files to a remote server. In this way, compromise of a system does not provide access to the log files for that system.

Configuring permissions on the log files would allow access for only the specified user accounts. However, if an attacker has gained access to the system, he or she might also have access to the user accounts that have been given access to the log files. Encrypting the log files protects the contents from being read, but this does not prevent the files from being deleted. Hashing of log files ensures integrity and that the files have not been altered since they were created.

REFERENCES

12.3.3 SIEM and Log Management Facts

q_siem_logmgmt_syslog_02_secp7.question.fex

Question 7: ✓ Correct

Over the past few days, a server has gone offline and rebooted automatically several times. You would like to see a record of when each of these restarts has occurred.

Which log type should you check?

- ○ Firewall
- ○ Performance
- ○ Security
- ➡ ● System

EXPLANATION

A system log records operating system, system, and hardware events. The system log contains entries for when the system was shut down or started, when new hardware was added, and when new services were started as well.

A performance log records information about the use of system resources, such as the processor, memory, disk, or network utilization. A firewall log identifies traffic that has been allowed or denied through a firewall. A security log records information related to logons, such as incorrect passwords being used and user right usage.

REFERENCES

12.3.3 SIEM and Log Management Facts

q_siem_logmgmt_system_secp7.question.fex

▼ Question 8: ✓ Correct

Which log file type is one of the most tedious to parse but can tell you exactly when users log onto your site and what their location is?

- ➡ ● Web server logs
- ○ Event logs
- ○ Authentication logs
- ○ System logs

EXPLANATION

Web server logs are one of the most tedious of all logs to parse. However, these logs can tell you exactly when users log onto your site and what their location is.

Authentication logs are vital to a network's security. Authentication servers may be Active Directory-based or OpenLDAP depending on your network structure.

System logs are produced by an operating system.

Event logs show application access, crashes, updates, and any other relevant information that could be valuable in determining root-cause analysis.

REFERENCES

12.3.3 SIEM and Log Management Facts

q_siem_logmgmt_web_secp7.question.fex

▾ Question 9: ✓ Correct

You would like to get a feel for the amount of bandwidth you are using in your network. What is the first thing you should do?

➡ ● Establish a baseline.

○ Choose a protocol.

○ Create data points.

○ Set intervals.

EXPLANATION

You would choose to establish a baseline. Baselines provide a reference for normal and abnormal activity.

After establishing a baseline, you would create data points.

To help create data points, you can set up intervals in minutes, hours, days, weeks, months, or years. Longer monitor runs equal more data points.

There is no need to define a protocol.

REFERENCES

12.3.10 Monitoring Data and Metadata Facts

q_mon_metadata_baseline_secp7.question.fex

▼ Question 10: ✕ Incorrect

You are worried about email spoofing. What can be put throughout an email's header that provides the originating email account or IP address and not a spoofed one?

● ~~Metadata~~

○ Timestamp

➡ ○ X-headers

○ Data points

EXPLANATION

You would choose x-headers. Do this with security devices that are designed for this purpose. These devices put X-headers throughout an email's header and provide the originating email account and IP address, not the spoofed one.

REFERENCES

12.3.10 Monitoring Data and Metadata Facts

q_mon_metadata_xheader_secp7.question.fex