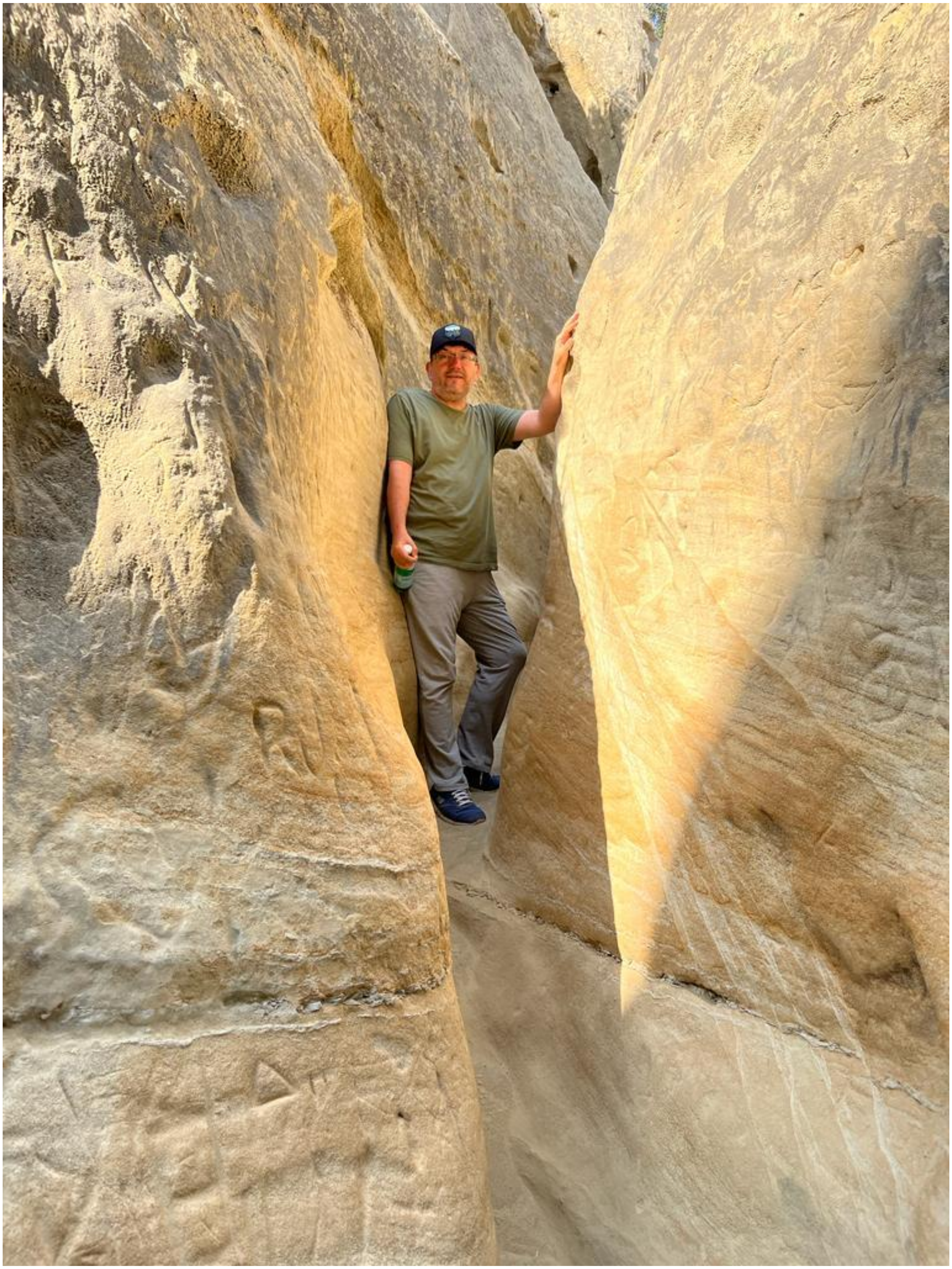
Extraordinary SOC SIEM Use Cases

Dr. Ertuğrul AKBAŞ

ertugrul.akbas@surelogsiem.com



1. Starting from today, can you retrieve the list of failed sessions on the firewall within 3–5 minutes, going back 180 days?

2. Can you retrieve the list of all failed firewall sessions in the last 180 days within a few minutes?

3. Can you retrieve the list of devices that accessed the target IP address “X” within the last 12 months.

4. Can you retrieve the list of user access reports within the last 12 months for your user, which were not blocked by the firewall but were in the threat intelligence list, including the original log from the firewall.

5. Which databases did SA log in to and what queries did they execute in the last year?

6. Can you retrieve the list all activities performed by service account “X” in the last 6 months, including the firewall?

7. Can you retrieve the list of machines that have not generated any traffic in the last month.

8. List of users who accessed tables X or Y (containing personal data) or files A or B on the file server (containing personal data), followed by the list of all URLs and IP addresses accessed by these users in the last 12 months, including port information.

Finally, provide a list of other users who accessed these listed IPs or URLs in the last 12 months.

9. Example of a site that was discovered/revealed to be used for an attack long after: deftsecurity[.]com (similar to the SolarWinds incident). Provide a list of users from your system who accessed this site in the last 6 months.

10. Number of occurrences of hitting the monthly threat intelligence list in the last 6 months.

11. List of users who hit the monthly threat intelligence list the most in the last 6 months.

12. Users who were blocked by the firewall while accessing the same target domain simultaneously.

13. List of devices, along with source port and username, that accessed the sample IP address avsvmcloud[.]com in the last 12 months.

CORRELATION USE CASES

14. Detect if the hourly login fail/login success authentication rate exceeds 3%.

15. Generate an alert if a file containing personal data is copied to a shared path that is accessible to everyone, or if personal data is added to an existing file in the shared path that is being edited.

16. Identify if the hourly HTTP/DNS ratio is less than 1.

17. If the total number of login events during business hours is at least 3% higher than the total number of users, and more than 5% of these events are generated by the same repeating users, notify.

18. If the data row added to the monitored table in the last hour is anomalous compared to log history, then alert

19. Raise an alert if a machine is detected with a virus by the AV, and within 5 minutes, another machine is logged into, followed by the blocking of the logged-in machine within 5 minutes.

20. Alert if the same user logs in to multiple machines simultaneously, except for admin users or those in the whitelist.

21. If a user triggers a failed session event and repeats it between the 5th and 10th minute, with a 5–10 minute interval, raise an alert. (Operator support is needed for the condition where Event A does not occur within the first 5 minutes but occurs between the 5th and 10th minute.)

22. Raise an alert if the same user establishes a VPN connection to one machine and simultaneously performs a local login to another system.

23. Raise an alert if a user attempts three login failures within 30 minutes without any successful logins, especially if they are not an administrator or in the whitelist.

24. Raise an alert if a user downloads more than 50 MB in one minute or uploads more than 250 MB to the same target IP/Domain within 10 minutes, especially if the URL ends with zip, exe, or dat.

25. Raise an alert if a process is started on one machine and within 5 minutes, the same process starts on another machine with the same path as the first machine, and if one of these machines is blocked by the firewall within the next 5 minutes, and the users are different.

26. Raise an alert if a user creates a new user, and within 5 minutes, the created user performs a login failure, followed by the creation of another user by the user who created the initial user.

27. Do not generate an alarm if a user is created but deleted within 10 minutes without being used. However, raise an alert if the user is used before being deleted or deleted within the same day.

28. Raise an alert if the same IP first logs into a Linux server, then logs into a Windows server, and subsequently starts/stops a service on either of these servers.

29. Raise an alert if the same user attempts unsuccessful logins on two different machines within 15 minutes, and if within 5

minutes after the second unsuccessful login, there is an access request to an IP in the threat intelligence list from one of these machines.

30. Raise an alert if the same user attempts at least 3 unsuccessful logins within 10 minutes without any successful logins in between.

31. If multiple usernames are subjected to brute force attacks or if, within 15 minutes of a brute force attack, one of the machines that was subjected to the attack successfully logs in (excluding machines where brute force was not attempted to avoid false positives), raise an alert. The expected outcome of this rule is as follows:

✔ Notify about users conducting brute force attacks

✔ Create a list of source IPs from machines where brute force was attempted

✔ Report machines where successful logins occurred

✔ Report the usernames used during successful logins

The reason for including this rule here is:

🔔 It can perform these four tasks simultaneously without using lists.

🔔 It can detect multiple usernames in a single step.

🔔 In large networks with thousands of devices, only the 100 devices that are subjected to brute force need to be monitored, reducing false positives.

🔔 It can identify the username that successfully cracks the password as a result of brute force.

🔔 It can achieve the above four points in a single rule, written within 3–5 minutes using the GUI.

32. DGA detection (ML)

33. If critical processes that should be secure in your network (winlogon.exe, svchost.exe, explorer.exe, lsm.exe, lsass.exe, csrss.exe, taskhost.exe, wininit.exe, smss.exe, smsvchost.exe) start processes that may be deceptive in terms of their names (could be perceived as the same by human eyes) and these processes are not among the allowed processes, raise an alert.

34. Raise an alert if there are users who have not logged in for more than 3 months.

35. Raise an alert if a user has been created and hasn’t been used for 72 hours.

36. Identify machines or users that have been idle for more than 30 days (40 days, 60 days, 90 days, … 365 days) and then appear on the network, and shut down the machine and disable the user.

37. If a user has not used VPN for at least 2 weeks (20 days, 30 days, 40 days, … 365 days) and within a short period of time, they perform remote interactive logon on more than one workstation, raise an alert.

38. If a port, other than standard proxy target ports, which has not been used for at least 30 days or more (40 days, 60 days, 90 days, … 365 days), starts to be used again and this port is greater than port 1024, and within 5 minutes, multiple requests are made to different destination IP addresses with requestMethod=POST, raise an alert. (Threshold, but not all SIEMs support it, so it is included here.)

39. If the same user performs two or more unsuccessful logins to the same machine within a day without any successful logins, identify and raise an alert.

40. If a locked user remains unlocked for more than 72 hours, raise an alert.

41. If an authentication error occurs simultaneously from the Oracle database user interface (Oracle Management Studio) and the console (SQL*Plus), raise an alert.

42. Learn the user agent information of each user, then warn if any other user agent information is detected.

43. Learn users' campus (University or distributed locations) information, then warn if any other campus location information is detected.

44. Learn users’ flat number or building location information, then warn if any other location information is detected.

45. Detects when a user is still logged on but someone else logs on with a different IP using the same username to any machine

46. After the Antivirus system detects the Virus on a machine, notify if a process starts on that machine before it is deleted, and also alert if this process occurs more than two times in 15 days.

47. Alert when a user is still logged on but someone else logs on with a different IP using the same username to any machine

48. Warn if the same user tries more than 3 unsuccessful sessions on the same machine for three days without any successful login

49. Detect when multiple logins are occurring with the same username but from different IP addresses.

50. Detect first Access to Critical Assets

51. Detect user Access at Unusual Times

52. If the user whose last login event is Authentication-Fail, and this user fails again after at least 5 minutes without any successful login.

53. Create rules around logins that hop to different points of the network after a failure occurs or use the same credentials across multiple assets. (Automated login attempts)

54. Alert, while a user’s VPN connection is in progress, a new VPN connection request is received with the same username.

55. Warn if a logged-off user evet detected without a logon event.

56. If a user tries to log in to another machine while logged in on one another machine, alert.

57. Notify if the mac address of the server changes.

58. Monitor each users VPN connections from unauthorized locations. (While sales personnel can travel to certain countries in the world, the locations where the developers and accounting personnel work are fixed)

59. Detecting login attempts to a database server from an unauthorized IP address or users.

60. If the mail gateway discovers an infected email, add the sender’s IP address to the list of suspect IPs, add the email’s attachment file name to the list of suspected files, and alert any access from this IP (directly blocking is risky on the firewall), additionally, alert if there are any file accesses with the same filename until mail gateway categories this IP clean.

61. Report all access to an external IP categorized as suspicious by the URL proxy until it is again removed from the suspicious category by the URL proxy. Do not report after leaving the suspect category.

62. If an Antivirus System detects a virus on a machine, add the IP of that machine to the infected machines list, and add the current user to the suspicious users' list and notify that IP and user activities until the Antivirus send the information that it has been cleaned for that machine.

63. When multiple failed login attempts from a single IP address occur within a short time frame, add the IP to a list of suspicious IPs' and users to the suspicious users' list. Then alert all the events of that IP address or users until a successful login event comes from that IP or one of the users. After a successful login event does not create an alert for that IP or user (successful event IP or user).

64. When a VPN connection is detected from a high-risk area, alert all events of this user until a VPN connection from a low-risk location with the same user. Do not alert after this VPN connection.

65. if multiple users accessing sensitive information (Monitoring Cloud Environments or File Servers) at the same time, alert. If someone accessed a file, then 5 minutes later, another user accessed the same file, this event flow will not generate an alert.

66. If multiple devices on the network are infected at the same time (At least 3–5 seconds)

67. If multiple users modifying system settings at the same time, alert

68. If a new device is being added while (at the same time) the firewall rules are being changed, alert.

69. Detect, if multiple users are accessing suspicious websites at the same time.

70. A user accesses a database, followed immediately by a user uploading a large file to a cloud storage service.

71.A user accesses a sensitive document, followed immediately by a user connecting to a VPN

72. Alert if more than half of the queries in the last hour to a selected table from the database belong to the same user.

73. If there are more than 15,000 events from at least 50 unique IPs within 3 minutes, and these events belong to a maximum of 10 different categories, notify “So, these 15,000 events are being grouped into a maximum of 10 categories”.

74. Alert if the ratio of unsuccessful sessions to successful sessions in the last hour exceeds 5%.

75. Alert if more than half of the data added in the last hour to a selected table from the database belongs to the same user.

76. If the data row added to the monitored table in the last hour is 10% more than the previous hour, then alert

77. Detect anomalies between the number of inserts in the logs and the number of rows added to the monitored critical table.

78. Detecting data loss: Monitor the logs of a database table for any anomalies between the number of inserts in the logs and the number of rows added to the table. If the number of inserts in the logs is significantly lower than the number of rows added to the table, this could indicate potential data loss or deletion.

79. Detecting database performance issues: Monitor the logs of a database table for any discrepancies between the number of inserts in the logs and the number of rows added to the table. If the number of inserts in the logs is significantly higher than the number of rows added to the table, this could indicate database performance issues, such as slow or failing queries.

80. Detecting unauthorized data access: Use logs to track access to a sensitive database table and compare the number of inserts in the logs to the number of rows added to the table. If there is a significant difference between the two, generate an alert to indicate potential unauthorized access to the data.

81. Detecting data tampering: Monitor the logs of a database table for any anomalies between the number of inserts in the logs

and the number of rows added to the table. If there is a discrepancy between the two numbers, generate an alert to notify security teams of potential data tampering.

82. Generate an alert if a file containing personal data is copied to a shared path that is accessible to everyone, or if personal data is added to an existing file in the shared path that is being edited.

83. Find the change in the 90th percentile of incoming traffic volume per source IP between two time periods

84. Detect spikes in incoming traffic volume per source IP

85. Detect spikes in outgoing traffic volume per destination IP

86. Detect abnormal increase in the number of connections per source IP

87. Detect abnormal increase in incoming traffic volume per source IP using percentile

88. Detect abnormal increase in outgoing traffic volume per destination IP using percentile

89. Find the standard deviation of incoming traffic volume per source IP

90. Find the average number of incoming packets per destination IP

91. Find the 90th percentile of incoming traffic volume per source IP

92. Find the 75th percentile of outgoing traffic volume per protocol

93. Find the average number of connections per source IP, broken down by connection type

94. Find the standard deviation of incoming traffic volume per destination port

95. Find the average number of packets per protocol and destination IP

96. Count the number of events by event type

97. Find the top 10 destination IPs that have the highest number of failed login attempts

98. Find the top 10 source IPs that have generated the highest volume of traffic

99. Find the top 10 source IPs that have generated the highest number of events

100. Find the top 10 destination IPs that have the highest number of events per protocol

101. Find the top 10 source IPs that have generated the highest volume of incoming traffic

102. Find the top 10 destination IPs that have received the highest volume of outgoing traffic

103. Find the top 10 source IPs that have generated the highest number of incoming packets

104. Find the top 10 destination IPs that have received the highest number of outgoing packets

105. Find the top 10 source IPs that have generated the highest number of incoming connections

106. Find the top 10 destination IPs that have received the highest number of outgoing connections

107. Find the top 10 protocols that have generated the highest volume of traffic

108. Find the top 10 protocols that have generated the highest number of packets

109. Warn if a user does something they've never done before

110. Warn if a user who has not had a VPN for at least 15 days (20,30,40…265 days) has remote interactive logon on more than one (1) workstation in a short time.

111. No Activity for more than 60 Days - This account has not logged in for over 60 days

112. Password changes for the same user more than 3 within 15 days

113. Warn if a user has visited the malicious categories on the proxy at least once a day for a week. (Bot Networks, Uncategorized, Malware, Spyware, Dynamic Dns, Encrypted Upload)

114. If there is a port usage, which is very rare

115. Detect the ratio of login success versus failure per user anomaly

116. Monitors all the logins and access for nonworking hours.

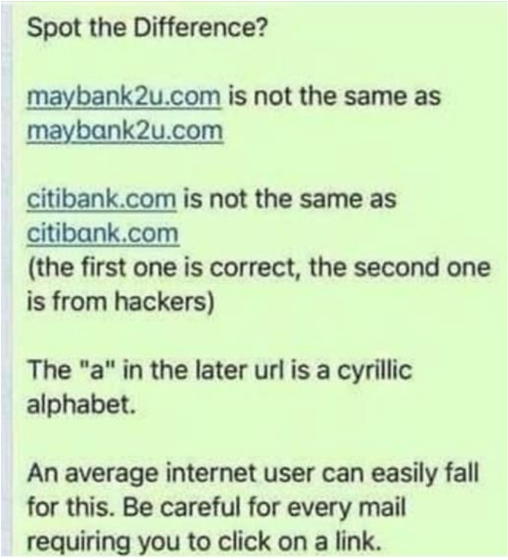
117. Checks the geo location to Find unusual behavior (Never seen before)

118. Warn if the time between two logins failed events of the same user is less than 1 minute

119. Warn if the VPN user has not made any VPN connection in the last week

120. Warn if the time between two login events of a non-admin user is less than 5 minutes

121. Mail Masquerade Detection Warn if an e-mail was received from e-mail addresses similar to the original e-mail address like ali.veli@citibank.com and ali.veli@citibɑnk.com



Spot the Difference?

maybank2u.com is not the same as maybɑnk2u.com

citibank.com is not the same as citibɑnk.com
(the first one is correct, the second one is from hackers)

The "a" in the later url is a cyrillic alphabet.

An average internet user can easily fall for this. Be careful for every mail requiring you to click on a link.

122. Masquerading Detection Detect system utilities, tasks, and services Masquerading. (T1036.003 Rename System Utilities Rename, T1036.004 Masquerade Task or Service)

123. Hunting malware and viruses by Detecting random strings

124. if the entropy of a file or directory is significantly higher than the baseline, it could indicate the presence of malware or unauthorized changes.

125. Processes Matching or Similar to System Processes in Unexpected Directories

126. Account Created with Name Similar to "Admin"

127. Account Created with Name Similar to "Administrator"

128. Account Created with Name Similar to the local service account naming convention

129. Newly-Registered Domains Visited (requires WHOIS enrichment)

130. Identifying Benign Websites Top 1 million Domains. If a domain has been created in the last 24 hours and this domain is in the top 1 million (Cisco Umbrella 1 million, , https//majestic.com/reports/majestic-million, https//tranco-list.eu/ , https//www.domcop.com/top-10-million-websites) list and not in our Whitelist, block it via NAC or Firewall.

131. Detect if the total (upload+download) amount of traffic for each user is abnormal based on the last week.

132. Detect if the same activity occurred for the last week/month for the same user or not

133. Warn if a user accesses a URL that they haven't accessed in the past week/month

134. Alert will be triggered when there are more than 3x admin logins than yesterday.

135. Alert will be triggered when there are more NX domain name responses than last week.

136. Allow/Block Ratio per System/User

137. GET/POST Ratio per System/User

138. Up/Down Bytes Ratio per System/User

139. Auth/Failed Auth per User

140. If the 90th percentile of network traffic from a specific IP address exceeds a certain threshold. This would mean that 90% of the network traffic from that IP address is below the threshold, and only 10% is above it. This rule can be used to Detect abnormal behavior, such as a DDoS attack, which would cause a spike in traffic from a specific IP.

141. Trigger an alert if the 99th percentile of authentication failure rate for a specific user or group of users exceeds a certain threshold.

142. Alert if the mean value of the authentication failure rate for a specific user or group of users exceeds a certain threshold.

143. Alert if the standard deviation of the login times for a specific user exceeds a certain threshold. This means that the login times are more variable than usual, which could be a sign of abnormal behavior, such as a compromised account being accessed from different locations or at different times.

144. If the standard deviation of the number of failed login attempts for a specific user exceeds a certain threshold. This means that the number of failed login attempts is more variable than usual, which could be a sign of abnormal behavior, such as a

brute force attack being launched from different IP addresses or at different times.

145. Identify a suspicious command that deletes shadow copies has been executed for process vssadmin.exe

146. Identify an employee who is accessing sensitive files outside of their normal job responsibilities, or who is sending large amounts of data outside of the organization.

147. Identify an account that has been accessed from multiple locations or devices at unusual times, or that has been used to access sensitive data or systems that the user does not normally access.

148. Identify a user who is attempting to access privileged accounts or systems without authorization, or who is attempting to use a privileged account to access sensitive data or systems.

149. Identify a privileged user who is accessing sensitive data or systems outside of their normal job responsibilities, or who is using privileged access to perform unauthorized actions.

150. Identify a privileged user who is sharing their account credentials with others, or who is using privileged accounts in an insecure way.

151. Identify a privileged user who is logging in from unusual locations or at unusual times, or who is using privileged accounts

to access sensitive data or systems that they do not normally access.

152. Identify a user who is copying large amounts of data to an external device or cloud storage account, or who is emailing sensitive data to a personal email account.

153. Identify a user who is accessing sensitive files outside of their normal job responsibilities or who is accessing files that they haven't accessed before.

154. Identify a user who is modifying sensitive files outside of their normal job responsibilities or who is modifying files that they haven't modified before.

155. Identify a user who is encrypting large numbers of files or who is encrypting sensitive files, which might indicate a security incident.

156. Identify a user who is deleting large numbers of files or who is deleting sensitive files, which might indicate a security incident.