100 CUSTOM SIEM RULES FOR CLIENT ONBOARDING

BY IZZMIER IZZUDDIN

AUTHENTICATION AND ACCESS CONTROL

Rule Name	Description	Correlated Log Source(s)
1. Multiple Failed Login Attempts	Detects multiple failed login attempts from the same user or IP.	Firewall, IDS, VPN Logs, Authentication Server Logs (e.g., RADIUS, Active Directory)
2. Successful Login After Multiple Failures	Flags a successful login following a series of failed login attempts.	Firewall, IDS, VPN Logs, Authentication Server Logs (e.g., RADIUS, Active Directory)
3. Impossible Travel	Alerts on logins from distant geographic locations within a short timeframe.	VPN Logs, IDS/IPS, User Workstation Logs, Cloud Access Device Logs
4. Login from New Device or Location	Detects a user logging in from a new device or an unusual location.	Authentication Server Logs (e.g., Active Directory), EDR, VPN Logs
5. High Volume of Logins in a Short Period	Flags an unusually high number of login attempts from a single account or IP.	Firewall, IDS, Authentication Server Logs (e.g., RADIUS, Active Directory)
6. Account Lockout Events	Triggers when user accounts are repeatedly locked out.	Authentication Server Logs (e.g., Active Directory, RADIUS), VPN Logs
7. Dormant Account Login	Detects logins from accounts that have been inactive for a long time.	Authentication Server Logs (e.g., Active Directory, RADIUS), VPN Logs
8. Shared Account Usage	Flags simultaneous logins to a shared account from multiple locations.	Firewall, IDS, VPN Logs, Authentication Server Logs (e.g., Active Directory)
9. Multiple Password Changes	Detects multiple password changes for the same account in a short timeframe.	Authentication Server Logs (e.g., Active Directory), Identity Management System Logs
10. Unusual Authentication Protocol Usage	Triggers when uncommon protocols are used for	Authentication Server Logs (e.g., Active

	authentication (e.g., NTLM over HTTP).	Directory, RADIUS), Proxy Server Logs

1. Multiple Failed Login Attempts

Description: Detects multiple failed login attempts from the same user or IP.
AQL Query:

```
SELECT "Event Name", "Source IP", "Username"
FROM events
WHERE "Event Name" = 'Authentication Failure'
GROUP BY "Source IP", "Username"
HAVING COUNT(*) >= 5 AND TIME_WINDOW <= 10 MINUTES
```

2. Successful Login After Multiple Failures

Description: Flags a successful login following a series of failed login attempts.
AQL Query:

```
SELECT "Event Name", "Source IP", "Username"
FROM events
WHERE "Event Name" IN ('Authentication Failure', 'Successful Login')
GROUP BY "Source IP", "Username"
HAVING COUNT_IF("Event Name" = 'Authentication Failure') >= 5
AND COUNT_IF("Event Name" = 'Successful Login') >= 1
AND TIME_WINDOW <= 1 MINUTE
```

3. Impossible Travel

Description: Alerts on logins from distant geographic locations within a short timeframe.
AQL Query:

```
SELECT "Username", "Source Geolocation", "Event Time"
FROM events
WHERE "Event Name" = 'Successful Login'
GROUP BY "Username"
HAVING GEO_DISTANCE(Source_Geolocation_A, Source_Geolocation_B) /
TIME_DIFFERENCE(Event_Time_A, Event_Time_B) > 1000
```

4. Login from New Device or Location

Description: Detects a user logging in from a new device or an unusual location.
AQL Query:

```
SELECT "Username", "Source IP", "User Agent"
FROM events
WHERE "Event Name" = 'Successful Login'
GROUP BY "Username", "Source IP", "User Agent"
HAVING COUNT_IF("Source IP") = 1 OR COUNT_IF("User Agent") = 1
```

5. High Volume of Logins in a Short Period

Description: Flags an unusually high number of login attempts from a single account or IP.
AQL Query:

```
SELECT "Username", "Source IP", COUNT(*)
FROM events
WHERE "Event Name" = 'Login Attempt'
GROUP BY "Username", "Source IP"
HAVING COUNT(*) > 20 AND TIME_WINDOW <= 10 MINUTES
```

6. Account Lockout Events

Description: Triggers when user accounts are repeatedly locked out.
AQL Query:

```
SELECT "Event Name", "Username"
FROM events
WHERE "Event Name" = 'Account Lockout'
GROUP BY "Username"
HAVING COUNT(*) >= 3 AND TIME_WINDOW <= 30 MINUTES
```

7. Dormant Account Login

Description: Detects logins from accounts that have been inactive for a long time.
AQL Query:

```
SELECT "Username", "Last Login Time"
FROM events
WHERE "Event Name" = 'Successful Login'
AND DAYS_SINCE("Last Login Time") >= 90
GROUP BY "Username"
```

8. Shared Account Usage

Description: Flags simultaneous logins to a shared account from multiple locations.
AQL Query:

```
SELECT "Username", "Source IP"
FROM events
WHERE "Event Name" = 'Successful Login'
GROUP BY "Username"
HAVING COUNT(DISTINCT "Source IP") > 1 AND TIME_WINDOW <= 5 MINUTES
```

9. Multiple Password Changes

Description: Detects multiple password changes for the same account in a short timeframe.
AQL Query:

```
SELECT "Event Name", "Username"
FROM events
WHERE "Event Name" = 'Password Change'
GROUP BY "Username"
HAVING COUNT(*) >= 3 AND TIME_WINDOW <= 10 MINUTES
```

10. Unusual Authentication Protocol Usage

Description: Triggers when uncommon protocols are used for authentication (e.g., NTLM over HTTP).
AQL Query:

```
SELECT "Event Name", "Protocol", "Source IP", "Destination IP"
FROM events
WHERE "Event Name" = 'Authentication Attempt'
AND "Protocol" = 'NTLM over HTTP'
GROUP BY "Source IP", "Destination IP"
```

PRIVILEGE ESCALATION

Rule Name	Description	Correlated Log Source(s)
11. Privilege Escalation Detected	Detects users being added to privileged groups like Domain Admins.	Active Directory Logs, Identity Management System Logs, Windows Event Logs
12. User Account Changes	Flags when user accounts are modified (e.g., role changes, group additions).	Active Directory Logs, Identity Management System Logs, Windows Event Logs
13. Service Account Misuse	Detects logins or changes to service accounts by unauthorised users.	EDR, Authentication Logs, Windows Event Logs, Identity Management System Logs
14. Multiple Failed Admin Logins	Triggers for failed admin logins, suggesting privilege escalation attempts.	Authentication Logs, Firewall, IDS/IPS, VPN Logs, Windows Event Logs
15. Group Policy Modifications	Detects changes to Group Policy Objects (GPOs).	Windows Event Logs, Group Policy Logs, Active Directory Logs
16. Privilege Escalation via Sudo	Alerts when non-privileged users execute sudo commands without prior permission.	Linux/Unix System Logs, EDR, Syslog, Authentication Logs
17. Creation of a New Privileged Account	Flags the creation of new accounts with admin privileges.	Active Directory Logs, Identity Management System Logs, Windows Event Logs
18. Critical Role Reassignment	Detects when sensitive roles (e.g., security manager) are reassigned.	Active Directory Logs, Identity Management System Logs, Windows Event Logs
19. Password Reset for Privileged Accounts	Monitors password resets for admin accounts to detect malicious intent.	Active Directory Logs, Identity Management System Logs, Windows Event Logs
20. Access to Sensitive Applications by Non-Admins	Alerts when non-admins access applications like SIEM, backup tools, or HR systems.	Application Logs, Authentication Logs, EDR

11. Privilege Escalation Detected

Description: Detects users being added to privileged groups like Domain Admins.
AQL Query:

```
SELECT "Event Name", "Target Group", "Username"
FROM events
WHERE "Event Name" = 'Group Membership Change'
AND "Target Group" IN ('Domain Admins', 'Enterprise Admins')
GROUP BY "Username"
```

12. User Account Changes

Description: Flags when user accounts are modified (e.g., role changes, group additions).
AQL Query:

```
SELECT "Event Name", "Username", "Modified Attribute"
FROM events
WHERE "Event Name" = 'User Account Modification'
GROUP BY "Username", "Modified Attribute"
```

13. Service Account Misuse

Description: Detects logins or changes to service accounts by unauthorised users.
AQL Query:

```
SELECT "Event Name", "Username", "Source IP"
FROM events
WHERE "Event Name" IN ('Successful Login', 'User Account Modification')
AND "Username" LIKE 'svc%'
AND "Source IP" NOT IN ('Authorised Management IPs')
GROUP BY "Username", "Source IP"
```

14. Multiple Failed Admin Logins

Description: Triggers for failed admin logins, suggesting privilege escalation attempts.
AQL Query:

```
SELECT "Event Name", "Username", "Source IP"
FROM events
WHERE "Event Name" = 'Authentication Failure'
AND "Username" IN ('Administrator', 'Admin', 'Root')
GROUP BY "Username", "Source IP"
HAVING COUNT(*) >= 5 AND TIME_WINDOW <= 10 MINUTES
```

15. Group Policy Modifications

Description: Detects changes to Group Policy Objects (GPOs).
AQL Query:

```
SELECT "Event Name", "Modified Object", "Username"
FROM events
WHERE "Event Name" = 'GPO Change'
GROUP BY "Modified Object", "Username"
```

16. Privilege Escalation via Sudo

Description: Alerts when non-privileged users execute sudo commands without prior permission.
AQL Query:

```
SELECT "Event Name", "Username", "Command"
FROM events
WHERE "Event Name" = 'Sudo Command Execution'
AND "Username" NOT IN ('Authorised Sudo Users')
GROUP BY "Username", "Command"
```

17. Creation of a New Privileged Account

Description: Flags the creation of new accounts with admin privileges.
AQL Query:

```
SELECT "Event Name", "Username", "Target Account"
FROM events
WHERE "Event Name" = 'Account Creation'
AND "Target Account" IN ('Admin', 'Domain Admin', 'Enterprise Admin')
GROUP BY "Target Account", "Username"
```

18. Critical Role Reassignment

Description: Detects when sensitive roles (e.g., security manager) are reassigned.
AQL Query:

```
SELECT "Event Name", "Target Role", "Username"
FROM events
WHERE "Event Name" = 'Role Assignment Change'
AND "Target Role" IN ('Security Manager', 'IT Admin', 'SIEM Manager')
GROUP BY "Target Role", "Username"
```

19. Password Reset for Privileged Accounts

Description: Monitors password resets for admin accounts to detect malicious intent.
AQL Query:

```
SELECT "Event Name", "Username", "Modified By"
FROM events
WHERE "Event Name" = 'Password Reset'
AND "Username" IN ('Admin', 'Domain Admin', 'Enterprise Admin')
GROUP BY "Username", "Modified By"
```

20. Access to Sensitive Applications by Non-Admins

Description: Alerts when non-admins access applications like SIEM, backup tools, or HR systems.
AQL Query:

```
SELECT "Event Name", "Application Name", "Username"
FROM events
WHERE "Application Name" IN ('Splunk', 'Backup Exec', 'Workday')
AND "Username" NOT IN ('Authorised Admins')
GROUP BY "Application Name", "Username"
```

NETWORK TRAFFIC AND RECONNAISSANCE

Rule Name	Description	Correlated Log Source(s)
21. Outbound Traffic to Known Malicious IPs	Matches traffic to IPs flagged in threat intelligence feeds.	Firewall Logs, IDS/IPS, Proxy Server Logs, Threat Intelligence Feeds
22. Port Scanning or Reconnaissance	Detects scanning behaviour by monitoring connections to multiple ports.	Firewall Logs, IDS/IPS, Network Monitoring Tools
23. Unusual Protocol Usage	Flags non-standard protocols (e.g., IRC, FTP) being used within the network.	Firewall Logs, IDS/IPS, Proxy Server Logs, Network Traffic Logs
24. High Volume of DNS Queries	Detects DNS tunnelling or command-and-control activity.	DNS Server Logs, Firewall Logs
25. Suspicious ICMP Traffic	Monitors excessive ICMP requests (e.g., ping sweeps).	Firewall Logs, IDS/IPS, Network Traffic Logs
26. External Connection Attempts from Internal Hosts	Flags internal hosts attempting to connect to external IPs.	Firewall Logs, Proxy Server Logs, VPN Logs
27. Internal Traffic to Non-Business Countries	Alerts on traffic to IPs in countries where the client has no business presence.	Firewall Logs, Proxy Server Logs
28. Unusual Traffic Spikes	Detects bandwidth spikes that could indicate data exfiltration or DDoS attacks.	Firewall Logs, IDS/IPS, Network Traffic Logs
29. Multiple Connection Attempts to Blocked Ports	Flags repeated attempts to connect to ports blocked by firewalls.	Firewall Logs, IDS/IPS
30. Suspicious Traffic to Cloud Services	Monitors unusual traffic to cloud services like AWS, Azure, or Google Drive.	Firewall Logs, Cloud Access Logs, Proxy Server Logs

21. Outbound Traffic to Known Malicious IPs

Description: Matches traffic to IPs flagged in threat intelligence feeds.
AQL Query:

```
SELECT "Event Name", "Destination IP", "Source IP"
FROM events
WHERE "Destination IP" IN ('Threat Intelligence IP List')
GROUP BY "Destination IP", "Source IP"
```

22. Port Scanning or Reconnaissance

Description: Detects scanning behavior by monitoring connections to multiple ports.
AQL Query:

```
SELECT "Event Name", "Source IP", "Destination Port"
FROM events
WHERE "Event Name" = 'Port Connection Attempt'
GROUP BY "Source IP"
HAVING COUNT(DISTINCT "Destination Port") >= 10 AND TIME_WINDOW <= 5 MINUTES
```

23. Unusual Protocol Usage

Description: Flags non-standard protocols (e.g., IRC, FTP) being used within the network.
AQL Query:

```
SELECT "Event Name", "Protocol", "Source IP", "Destination IP"
FROM events
WHERE "Protocol" IN ('IRC', 'FTP', 'Telnet')
GROUP BY "Protocol", "Source IP", "Destination IP"
```

24. High Volume of DNS Queries

Description: Detects DNS tunneling or command-and-control activity.
AQL Query:

```
SELECT "Event Name", "Source IP", "Query Count"
FROM events
WHERE "Event Name" = 'DNS Query'
GROUP BY "Source IP"
HAVING COUNT(*) >= 100 AND TIME_WINDOW <= 10 MINUTES
```

25. Suspicious ICMP Traffic

Description: Monitors excessive ICMP requests (e.g., ping sweeps).
AQL Query:

```
SELECT "Event Name", "Source IP", "Destination IP"
FROM events
WHERE "Event Name" = 'ICMP Request'
GROUP BY "Source IP"
HAVING COUNT(*) >= 50 AND TIME_WINDOW <= 5 MINUTES
```

26. External Connection Attempts from Internal Hosts

Description: Flags internal hosts attempting to connect to external IPs.
AQL Query:

```
SELECT "Event Name", "Source IP", "Destination IP"
FROM events
WHERE "Destination IP" NOT IN ('Internal IP Range')
GROUP BY "Source IP", "Destination IP"
```

27. Internal Traffic to Non-Business Countries

Description: Alerts on traffic to IPs in countries where the client has no business presence.
AQL Query:

```
SELECT "Event Name", "Destination IP", "Source IP", "Country"
FROM events
WHERE "Country" NOT IN ('Authorised Country List')
GROUP BY "Destination IP", "Source IP", "Country"
```

28. Unusual Traffic Spikes

Description: Detects bandwidth spikes that could indicate data exfiltration or DDoS attacks.
AQL Query:

```
SELECT "Event Name", "Source IP", "Traffic Volume"
FROM events
WHERE "Event Name" = 'Traffic Volume'
GROUP BY "Source IP"
HAVING SUM("Traffic Volume") >= 1000000 AND TIME_WINDOW <= 10 MINUTES
```

29. Multiple Connection Attempts to Blocked Ports

Description: Flags repeated attempts to connect to ports blocked by firewalls.
AQL Query:

```
SELECT "Event Name", "Source IP", "Destination Port"
FROM events
WHERE "Event Name" = 'Blocked Port Connection Attempt'
GROUP BY "Source IP", "Destination Port"
HAVING COUNT(*) >= 5 AND TIME_WINDOW <= 10 MINUTES
```

30. Suspicious Traffic to Cloud Services

Description: Monitors unusual traffic to cloud services like AWS, Azure, or Google Drive.
AQL Query:

```
SELECT "Event Name", "Destination IP", "Source IP", "Service"
FROM events
WHERE "Service" IN ('AWS', 'Azure', 'Google Drive')
GROUP BY "Destination IP", "Source IP", "Service"
HAVING COUNT(*) >= 10 AND TIME_WINDOW <= 10 MINUTES
```

MALWARE AND EXPLOIT DETECTION

Rule Name	Description	Correlated Log Source(s)
31. Malicious File Uploads	Monitors file uploads and matches file hashes with known malware databases.	Web Server Logs, EDR, File Integrity Monitoring Logs
32. Execution of Obfuscated Scripts	Flags PowerShell or Bash scripts that use obfuscation techniques.	EDR, Sysmon, Windows/Linux Event Logs, PowerShell Logs
33. Known Exploit Payloads	Detects traffic or processes matching known exploit signatures.	IDS/IPS, Firewall Logs, Antivirus Logs
34. Unusual Binary Execution	Alerts on the execution of uncommon binaries (e.g., malware droppers).	EDR, Windows/Linux Event Logs, Application Logs
35. Ransomware Activity	Flags mass encryption of files, unusual file extensions, or deletion of backups.	EDR, Antivirus Logs, File Integrity Monitoring Logs, Backup Logs
36. Unusual File Permissions	Detects files with permissions that allow unauthorised access.	File System Logs, EDR, Windows/Linux Event Logs
37. Suspicious Scheduled Tasks	Alerts on new or modified scheduled tasks created by unauthorised users.	Windows/Linux Event Logs, EDR, Task Scheduler Logs
38. Malicious Process Chains	Monitors suspicious parent-child process relationships (e.g., cmd.exe launching powershell.exe).	EDR, Sysmon, Windows/Linux Event Logs
39. File Hashes Matching Known Threats	Matches file hashes in logs to threat intelligence feeds.	EDR, Antivirus Logs, File Integrity Monitoring Logs

40. Injected Code in Running Processes	Detects process injection techniques used by malware.	EDR, Sysmon, Windows/Linux Event Logs

31. Malicious File Uploads

Description: Monitors file uploads and matches file hashes with known malware databases.
AQL Query:

```
SELECT "Event Name", "File Hash", "Source IP", "Destination IP"
FROM events
WHERE "Event Name" = 'File Upload'
AND "File Hash" IN ('Threat Intelligence Hash List')
GROUP BY "File Hash", "Source IP", "Destination IP"
```

32. Execution of Obfuscated Scripts

Description: Flags PowerShell or Bash scripts that use obfuscation techniques.
AQL Query:

```
SELECT "Event Name", "Command Line Arguments", "Source IP"
FROM events
WHERE "Command Line Arguments" LIKE '%-EncodedCommand%'
OR "Command Line Arguments" LIKE '%base64%'
GROUP BY "Source IP", "Command Line Arguments"
```

33. Known Exploit Payloads

Description: Detects traffic or processes matching known exploit signatures.
AQL Query:

```
SELECT "Event Name", "Source IP", "Destination IP"
FROM events
WHERE "Event Name" IN ('Exploit Attempt Detected', 'Exploit Signature Match')
GROUP BY "Source IP", "Destination IP"
```

34. Unusual Binary Execution

Description: Alerts on the execution of uncommon binaries (e.g., malware droppers).
AQL Query:

```
SELECT "Event Name", "Binary Name", "Source IP"
FROM events
```

```
WHERE "Binary Name" NOT IN ('Allowed Binaries List')
GROUP BY "Source IP", "Binary Name"
```

35. Ransomware Activity

Description: Flags mass encryption of files, unusual file extensions, or deletion of backups.
AQL Query:

```
SELECT "Event Name", "Source IP", "File Extension", "Activity Type"
FROM events
WHERE "Activity Type" IN ('File Encryption', 'Backup Deletion')
OR "File Extension" IN ('.locked', '.encrypted')
GROUP BY "Source IP", "File Extension", "Activity Type"
```

36. Unusual File Permissions

Description: Detects files with permissions that allow unauthorised access.
AQL Query:

```
SELECT "Event Name", "File Path", "Permissions", "Source IP"
FROM events
WHERE "Permissions" LIKE '%777%'
OR "Permissions" LIKE '%Everyone%'
GROUP BY "File Path", "Source IP", "Permissions"
```

37. Suspicious Scheduled Tasks

Description: Alerts on new or modified scheduled tasks created by unauthorised users.
AQL Query:

```
SELECT "Event Name", "Task Name", "Source IP", "User Account"
FROM events
WHERE "Event Name" = 'Scheduled Task Creation'
AND "User Account" NOT IN ('Authorised Users List')
GROUP BY "Task Name", "Source IP", "User Account"
```

38. Malicious Process Chains

Description: Monitors suspicious parent-child process relationships (e.g., cmd.exe launching powershell.exe).
AQL Query:

```
SELECT "Event Name", "Parent Process", "Child Process", "Source IP"
```

```
FROM events
WHERE "Parent Process" = 'cmd.exe'
AND "Child Process" IN ('powershell.exe', 'wscript.exe')
GROUP BY "Parent Process", "Child Process", "Source IP"
```

39. File Hashes Matching Known Threats

Description: Matches file hashes in logs to threat intelligence feeds.
AQL Query:

```
SELECT "Event Name", "File Hash", "Source IP"
FROM events
WHERE "File Hash" IN ('Threat Intelligence Hash List')
GROUP BY "File Hash", "Source IP"
```

40. Injected Code in Running Processes

Description: Detects process injection techniques used by malware.
AQL Query:

```
SELECT "Event Name", "Process Name", "Injected Code", "Source IP"
FROM events
WHERE "Injected Code" IS NOT NULL
GROUP BY "Process Name", "Injected Code", "Source IP"
```

DATA EXFILTRATION AND INSIDER THREATS

Rule Name	Description	Correlated Log Source(s)
41. Large File Transfers Outside Business Hours	Triggers on high-volume file uploads during non-working hours.	File System Logs, EDR, Network Traffic Logs, VPN Logs
42. Sensitive File Access Patterns	Flags unusual access to sensitive files (e.g., financial or customer data).	File Access Logs, EDR, Application Logs, File Integrity Monitoring Logs
43. Use of Personal Cloud Storage	Detects file uploads to personal cloud services (e.g., Google Drive).	Proxy Server Logs, Firewall Logs, Cloud Service Logs
44. Mass File Deletions	Alerts on bulk deletions of files, which could indicate insider sabotage.	File System Logs, EDR, Backup Logs
45. Unusual Database Queries	Flags unauthorised or anomalous SQL queries accessing sensitive data.	Database Logs, Web Application Firewall Logs, Application Logs
46. Email Forwarding to External Domains	Detects emails automatically forwarded to external, non-business domains.	Email Server Logs, SMTP Logs
47. Printing Large Volumes of Sensitive Data	Monitors mass printing of confidential files.	Printer Logs, File Access Logs
48. USB Device Usage on Critical Systems	Flags file transfers to USB devices on sensitive systems.	USB Device Logs, EDR, Windows/Linux Event Logs
49. Anomalous Encryption Activity	Detects unexpected encryption activity on critical systems.	EDR, File Integrity Monitoring Logs, Antivirus Logs
50. Access to Backup Servers	Monitors unauthorised access to backup or disaster recovery systems.	Backup Server Logs, EDR, Authentication Logs

41. Large File Transfers Outside Business Hours

Description: Triggers on high-volume file uploads during non-working hours.
AQL Query:

```
SELECT "Event Name", "Source IP", "Destination IP", "File Sise"
FROM events
WHERE "Event Name" = 'File Upload'
AND "File Sise" > 100MB
```

```
AND "Timestamp" NOT BETWEEN '08:00:00' AND '18:00:00'
GROUP BY "Source IP", "Destination IP", "File Sise"
```

42. Sensitive File Access Patterns

Description: Flags unusual access to sensitive files (e.g., financial or customer data).
AQL Query:

```
SELECT "Event Name", "File Path", "User Account", "Source IP"
FROM events
WHERE "File Path" LIKE '%/sensitive_data/%'
AND "User Account" NOT IN ('Authorised Users List')
GROUP BY "File Path", "User Account", "Source IP"
```

43. Use of Personal Cloud Storage

Description: Detects file uploads to personal cloud services (e.g., Google Drive).
AQL Query:

```
SELECT "Event Name", "Destination URL", "Source IP"
FROM events
WHERE "Event Name" = 'File Upload'
AND "Destination URL" LIKE '%drive.google.com%' OR '%dropbox.com%' OR
'%onedrive.com%'
GROUP BY "Destination URL", "Source IP"
```

44. Mass File Deletions

Description: Alerts on bulk deletions of files, which could indicate insider sabotage.
AQL Query:

```
SELECT "Event Name", "File Path", "User Account", "Source IP"
FROM events
WHERE "Event Name" = 'File Deletion'
GROUP BY "User Account"
HAVING COUNT("File Path") > 50
```

45. Unusual Database Queries

Description: Flags unauthorised or anomalous SQL queries accessing sensitive data.
AQL Query:

```
SELECT "Event Name", "Query", "Database Name", "User Account", "Source IP"
FROM events
```

```
WHERE "Event Name" = 'Database Query'
AND ("Query" LIKE '%DROP%' OR "Query" LIKE '%SELECT *%')
AND "User Account" NOT IN ('Authorised Users List')
GROUP BY "Query", "User Account", "Database Name", "Source IP"
```

46. Email Forwarding to External Domains

Description: Detects emails automatically forwarded to external, non-business domains.
AQL Query:

```
SELECT "Event Name", "Forwarding Address", "User Account", "Source IP"
FROM events
WHERE "Event Name" = 'Email Forwarding Setup'
AND "Forwarding Address" NOT LIKE '%@yourcompanydomain.com%'
GROUP BY "Forwarding Address", "User Account", "Source IP"
```

47. Printing Large Volumes of Sensitive Data

Description: Monitors mass printing of confidential files.
AQL Query:

```
SELECT "Event Name", "File Name", "Printer Name", "User Account"
FROM events
WHERE "Event Name" = 'File Print'
AND "File Name" LIKE '%confidential%' OR '%financial%'
GROUP BY "Printer Name", "User Account"
HAVING COUNT("File Name") > 20
```

48. USB Device Usage on Critical Systems

Description: Flags file transfers to USB devices on sensitive systems.
AQL Query:

```
SELECT "Event Name", "USB Device Name", "Source IP", "User Account"
FROM events
WHERE "Event Name" = 'USB File Transfer'
AND "Source IP" IN ('Critical Systems List')
GROUP BY "USB Device Name", "Source IP", "User Account"
```

49. Anomalous Encryption Activity

Description: Detects unexpected encryption activity on critical systems.
AQL Query:

```
SELECT "Event Name", "Encryption Type", "Source IP", "File Path"
FROM events
WHERE "Event Name" = 'File Encryption'
AND "Source IP" IN ('Critical Systems List')
GROUP BY "Encryption Type", "Source IP", "File Path"
```

50. Access to Backup Servers

Description: Monitors unauthorised access to backup or disaster recovery systems.
AQL Query:

```
SELECT "Event Name", "User Account", "Source IP"
FROM events
WHERE "Event Name" = 'Login Attempt'
AND "Destination IP" IN ('Backup Server List')
AND "User Account" NOT IN ('Authorised Users List')
GROUP BY "User Account", "Source IP"
```

COMPLIANCE MONITORING

Rule Name	Description	Correlated Log Source(s)
51. PII Data Access Monitoring	Detects unauthorised access to personal identifiable information (PII).	Database Logs, File Access Logs, EDR, Application Logs
52. Access to Financial Records	Flags access to financial systems or sensitive accounting data.	Financial System Logs, Database Logs, Application Logs
53. Non-Encrypted Traffic Containing Sensitive Data	Monitors for unencrypted transmission of sensitive information.	Network Traffic Logs, Proxy Server Logs, IDS/IPS
54. Failed Access to Secure Databases	Detects failed attempts to access PCI-DSS or HIPAA-regulated systems.	Database Logs, Authentication Logs
55. Policy Violations in Logins	Flags use of non-compliant systems for business purposes.	Authentication Logs, Proxy Server Logs

51. PII Data Access Monitoring

Description: Detects unauthorised access to personal identifiable information (PII).
AQL Query:

```
SELECT "Event Name", "File Path", "User Account", "Source IP"
FROM events
WHERE "File Path" LIKE '%/PII_Data/%'
AND "User Account" NOT IN ('Authorised Users List')
GROUP BY "File Path", "User Account", "Source IP"
```

52. Access to Financial Records

Description: Flags access to financial systems or sensitive accounting data.
AQL Query:

```
SELECT "Event Name", "File Path", "User Account", "Source IP"
FROM events
WHERE "File Path" LIKE '%/financial_data/%' OR '%/accounting/%'
AND "User Account" NOT IN ('Authorised Users List')
GROUP BY "File Path", "User Account", "Source IP"
```

53. Non-Encrypted Traffic Containing Sensitive Data

Description: Monitors for unencrypted transmission of sensitive information.
AQL Query:

```
SELECT "Event Name", "Protocol", "Source IP", "Destination IP"
FROM events
WHERE "Protocol" IN ('HTTP', 'FTP')
AND "File Path" LIKE '%sensitive%'
GROUP BY "Protocol", "Source IP", "Destination IP"
```

54. Failed Access to Secure Databases

Description: Detects failed attempts to access PCI-DSS or HIPAA-regulated systems.
AQL Query:

```
SELECT "Event Name", "Database Name", "User Account", "Source IP"
FROM events
WHERE "Event Name" = 'Failed Database Access'
AND "Database Name" IN ('PCI-DSS', 'HIPAA Systems')
GROUP BY "Database Name", "User Account", "Source IP"
```

55. Policy Violations in Logins

Description: Flags use of non-compliant systems for business purposes.
AQL Query:

```
SELECT "Event Name", "User Account", "Source IP", "Device Type"
FROM events
WHERE "Event Name" = 'Login Attempt'
AND "Device Type" NOT IN ('Compliant Devices List')
GROUP BY "User Account", "Source IP", "Device Type"
```

APPLICATION AND ENDPOINT MONITORING

Rule Name	Description	Correlated Log Source(s)
56. Unusual Application Behaviour	Detects applications consuming excessive CPU, memory, or network resources.	EDR, Sysmon, Application Logs, Performance Monitoring Logs
57. Execution of Unsigned Binaries	Flags the execution of binaries that are not signed or verified.	EDR, Windows/Linux Event Logs, Application Logs
58. Multiple Application Crashes	Alerts when critical applications crash repeatedly within a short timeframe.	Application Logs, Event Logs, EDR
59. New Software Installations	Detects unauthorised software installations on endpoints or servers.	Endpoint Logs, EDR, Application Logs
60. Access to Unauthorised Applications	Monitors attempts to access restricted applications or tools.	Application Logs, Proxy Server Logs
61. Shadow IT Detection	Flags use of unapproved third-party software or services.	Network Traffic Logs, Proxy Server Logs
62. Abnormal Endpoint Communication	Alerts on devices communicating with unusual or high-risk endpoints.	EDR, Network Traffic Logs
63. Unusual Registry Modifications	Monitors changes to critical registry keys that may indicate malware or persistence techniques.	Windows Event Logs, Sysmon, EDR
64. Endpoint Connections to Non-Business VPNs	Detects devices connecting to unauthorised VPN services.	VPN Logs, Network Traffic Logs, EDR
65. Execution of Dual-Use Tools	Flags tools like Mimikatz, BloodHound, or Metasploit that are used for both admin tasks and attacks.	EDR, Sysmon, Antivirus Logs, Windows/Linux Event Logs

56. Unusual Application Behaviour

Description: Detects applications consuming excessive CPU, memory, or network resources.
AQL Query:

```
SELECT "Event Name", "Application Name", "CPU Usage", "Memory Usage", "Network Usage"
FROM events
WHERE "CPU Usage" > 80 OR "Memory Usage" > 80 OR "Network Usage" > 80
```

```
GROUP BY "Application Name"
```

57. Execution of Unsigned Binaries

Description: Flags the execution of binaries that are not signed or verified.
AQL Query:

```
SELECT "Event Name", "File Name", "Signature Status", "Source IP"
FROM events
WHERE "Signature Status" = 'Unsigned'
GROUP BY "File Name", "Source IP"
```

58. Multiple Application Crashes

Description: Alerts when critical applications crash repeatedly within a short timeframe.
AQL Query:

```
SELECT "Event Name", "Application Name", "Crash Count", "Source IP"
FROM events
WHERE "Event Name" = 'Application Crash'
GROUP BY "Application Name"
HAVING COUNT("Crash Count") > 5
```

59. New Software Installations

Description: Detects unauthorised software installations on endpoints or servers.
AQL Query:

```
SELECT "Event Name", "Software Name", "Source IP", "User Account"
FROM events
WHERE "Event Name" = 'Software Installation'
AND "User Account" NOT IN ('Authorised Users List')
GROUP BY "Software Name", "Source IP"
```

60. Access to Unauthorised Applications

Description: Monitors attempts to access restricted applications or tools.
AQL Query:

```
SELECT "Event Name", "Application Name", "User Account", "Source IP"
FROM events
WHERE "Application Name" IN ('Restricted Applications List')
AND "User Account" NOT IN ('Authorised Users List')
GROUP BY "Application Name", "User Account", "Source IP"
```

61. Shadow IT Detection

Description: Flags use of unapproved third-party software or services.
AQL Query:

```
SELECT "Event Name", "Application Name", "Source IP", "User Account"
FROM events
WHERE "Application Name" NOT IN ('Approved Applications List')
GROUP BY "Application Name", "Source IP", "User Account"
```

62. Abnormal Endpoint Communication

Description: Alerts on devices communicating with unusual or high-risk endpoints.
AQL Query:

```
SELECT "Event Name", "Source IP", "Destination IP"
FROM events
WHERE "Destination IP" NOT IN ('Approved IP List')
GROUP BY "Source IP", "Destination IP"
```

63. Unusual Registry Modifications

Description: Monitors changes to critical registry keys that may indicate malware or persistence techniques.
AQL Query:

```
SELECT "Event Name", "Registry Key", "Modification Type", "Source IP"
FROM events
WHERE "Registry Key" IN ('Critical Registry Keys List')
GROUP BY "Registry Key", "Modification Type", "Source IP"
```

64. Endpoint Connections to Non-Business VPNs

Description: Detects devices connecting to unauthorised VPN services.
AQL Query:

```
SELECT "Event Name", "VPN Name", "Source IP", "User Account"
FROM events
WHERE "VPN Name" NOT IN ('Approved VPN List')
GROUP BY "VPN Name", "Source IP", "User Account"
```

65. Execution of Dual-Use Tools

Description: Flags tools like Mimikatz, BloodHound, or Metasploit that are used for both admin tasks and attacks.
AQL Query:

```
SELECT "Event Name", "Tool Name", "Source IP", "User Account"
FROM events
WHERE "Tool Name" IN ('Mimikatz', 'BloodHound', 'Metasploit')
GROUP BY "Tool Name", "Source IP", "User Account"
```

EMAIL SECURITY

Rule Name	Description	Correlated Log Source(s)
66. Phishing Email Detection	Alerts on emails containing malicious links or attachments.	Email Logs, Email Gateway Logs, Anti-Phishing Software
67. Mass Email Forwarding	Flags users forwarding large numbers of emails to external domains.	Email Logs, Email Server Logs
68. Spoofed Email Addresses	Detects emails sent with spoofed "From" fields mimicking internal users or domains.	Email Logs, Email Gateway Logs
69. Unusual Email Attachments	Monitors uncommon file types (e.g., .exe, .js) in email attachments.	Email Logs, Email Server Logs, Anti-Virus Logs
70. Multiple Failed Email Logins	Flags repeated failed login attempts on email systems.	Email Server Logs, Authentication Logs
71. Excessive Emails to External Domains	Detects mass outbound emails to non-business email addresses.	Email Logs, Outbound Email Logs
72. Access to Archived Emails	Flags unauthorised access to archived or historical email data.	Email Server Logs, Archive Access Logs
73. Malware Sent via Email Attachments	Matches email attachments with malware threat intelligence feeds.	Email Logs, Anti-Malware Logs
74. Keyword-Based DLP Email Monitoring	Detects emails containing sensitive keywords (e.g., "confidential", "passwords").	DLP Logs, Email Logs
75. Unusual Email Sending Patterns	Monitors users sending emails at unusual times or in unusual volumes.	Email Logs, Email Server Logs

66. Phishing Email Detection

Description: Alerts on emails containing malicious links or attachments.
AQL Query:

```
SELECT "Event Name", "Email Subject", "Sender Email", "URL", "Attachment Name"
FROM email_logs
WHERE "URL" IN ('Malicious URL Feed')
OR "Attachment Name" IN ('Malicious Hash Feed')
GROUP BY "Email Subject", "Sender Email", "URL", "Attachment Name"
```

67. Mass Email Forwarding

Description: Flags users forwarding large numbers of emails to external domains.
AQL Query:

```
SELECT "Event Name", "User Account", "Destination Email Domain", COUNT("Email ID")
AS Email_Count
FROM email_logs
WHERE "Event Name" = 'Email Forwarded'
AND "Destination Email Domain" NOT IN ('Approved Domains')
GROUP BY "User Account", "Destination Email Domain"
HAVING Email_Count > 50
```

68. Spoofed Email Addresses

Description: Detects emails sent with spoofed "From" fields mimicking internal users or domains.
AQL Query:

```
SELECT "Event Name", "Sender Email", "Source IP"
FROM email_logs
WHERE "Sender Email" LIKE '%@yourdomain.com'
AND "Source IP" NOT IN ('Internal IP Range')
GROUP BY "Sender Email", "Source IP"
```

69. Unusual Email Attachments

Description: Monitors uncommon file types (e.g., .exe, .js) in email attachments.
AQL Query:

```
SELECT "Event Name", "Email Subject", "Attachment Name", "User Account"
FROM email_logs
WHERE "Attachment Name" LIKE '%.exe' OR '%.js'
GROUP BY "Email Subject", "Attachment Name", "User Account"
```

70. Multiple Failed Email Logins

Description: Flags repeated failed login attempts on email systems.
AQL Query:

```
SELECT "Event Name", "User Account", "Source IP", COUNT("Event ID") AS Login_Attempts
FROM authentication_logs
WHERE "Event Name" = 'Failed Login'
AND "Service" = 'Email'
GROUP BY "User Account", "Source IP"
HAVING Login_Attempts > 5
```

71. Excessive Emails to External Domains

Description: Detects mass outbound emails to non-business email addresses.
AQL Query:

```
SELECT "Event Name", "User Account", "Destination Email Domain", COUNT("Email ID")
AS Email_Count
FROM email_logs
WHERE "Destination Email Domain" NOT IN ('Business Domains List')
GROUP BY "User Account", "Destination Email Domain"
HAVING Email_Count > 100
```

72. Access to Archived Emails

Description: Flags unauthorised access to archived or historical email data.
AQL Query:

```
SELECT "Event Name", "User Account", "File Path", "Source IP"
FROM access_logs
WHERE "File Path" LIKE '%/Archived_Emails/%'
AND "User Account" NOT IN ('Authorised Users List')
GROUP BY "File Path", "User Account", "Source IP"
```

73. Malware Sent via Email Attachments

Description: Matches email attachments with malware threat intelligence feeds.
AQL Query:

```
SELECT "Event Name", "Email Subject", "Attachment Name", "Sender Email"
FROM email_logs
WHERE "Attachment Hash" IN ('Malware Hash Feed')
GROUP BY "Email Subject", "Attachment Name", "Sender Email"
```

74. Keyword-Based DLP Email Monitoring

Description: Detects emails containing sensitive keywords (e.g., "confidential", "passwords").
AQL Query:

```
SELECT "Event Name", "Email Subject", "Body Content", "Sender Email"
FROM email_logs
WHERE "Body Content" LIKE '%confidential%' OR '%password%'
GROUP BY "Email Subject", "Body Content", "Sender Email"
```

75. Unusual Email Sending Patterns

Description: Monitors users sending emails at unusual times or in unusual volumes.
AQL Query:

```
SELECT "Event Name", "User Account", "Timestamp", COUNT("Email ID") AS Email_Count
FROM email_logs
WHERE HOUR("Timestamp") NOT BETWEEN 8 AND 18
GROUP BY "User Account", "Timestamp"
HAVING Email_Count > 50
```

CLOUD SECURITY

Rule Name	Description	Correlated Log Source(s)
76. Unusual Cloud Login Locations	Detects logins to cloud services from unexpected geolocations.	Cloud Service Logs (AWS CloudTrail, Azure Activity Logs)
77. Multiple API Key Failures	Flags repeated failed API calls due to invalid keys.	API Logs, Cloud Service Logs
78. Mass Data Download from Cloud Storage	Detects large-scale data downloads from cloud platforms like AWS, Azure, or Google Cloud.	Cloud Storage Logs (AWS S3, Azure Blob Storage)
79. Publicly Exposed Cloud Buckets	Alerts on storage buckets that are configured as public.	Cloud Storage Logs (AWS S3, Azure Blob Storage), Cloud Security Logs
80. Unusual Cloud Resource Usage	Monitors spikes in cloud resource utilisation (e.g., CPU, bandwidth).	Cloud Platform Monitoring Logs, Cloud Service Logs
81. IAM Role Misuse in Cloud	Flags unauthorised use of Identity and Access Management (IAM) roles or permissions.	Cloud IAM Logs (AWS IAM, Azure Active Directory)
82. Unusual Cloud API Calls	Detects abnormal API call patterns to cloud management platforms.	Cloud API Logs, Cloud Service Logs
83. Cloud Instance Launch Outside Hours	Flags new cloud instances or virtual machines launched during off-hours.	Cloud Service Logs (AWS EC2, Azure VMs)
84. Configuration Changes in Cloud Security Groups	Monitors unauthorised changes to cloud security group settings.	Cloud Security Group Logs, Cloud Service Logs
85. Access to Restricted Cloud Services	Detects attempts to access cloud services that are restricted or not in use.	Cloud Access Logs, Cloud Service Logs

76. Unusual Cloud Login Locations

Description: Detects logins to cloud services from unexpected geolocations.
AQL Query:

```
SELECT "Event Name", "User Account", "Login Location", "Timestamp"
FROM cloud_authentication_logs
WHERE "Login Location" NOT IN ('Approved Geolocations')
```

```
GROUP BY "User Account", "Login Location"
```

77. Multiple API Key Failures

Description: Flags repeated failed API calls due to invalid keys.
AQL Query:

```
SELECT "Event Name", "API Key", "Source IP", COUNT("Event ID") AS Failure_Count
FROM cloud_api_logs
WHERE "Event Name" = 'API Key Failure'
GROUP BY "API Key", "Source IP"
HAVING Failure_Count > 5
```

78. Mass Data Download from Cloud Storage

Description: Detects large-scale data downloads from cloud platforms like AWS, Azure, or Google Cloud.
AQL Query:

```
SELECT "Event Name", "User Account", "Object Name", "Download Sise", "Timestamp"
FROM cloud_storage_logs
WHERE "Event Name" = 'Download'
AND "Download Sise" > 1000000000 -- Threshold in bytes (e.g., 1 GB)
GROUP BY "User Account", "Object Name", "Download Sise"
```

79. Publicly Exposed Cloud Buckets

Description: Alerts on storage buckets that are configured as public.
AQL Query:

```
SELECT "Bucket Name", "Access Control List", "Last Modified"
FROM cloud_storage_configuration
WHERE "Access Control List" = 'Public'
```

80. Unusual Cloud Resource Usage

Description: Monitors spikes in cloud resource utilisation (e.g., CPU, bandwidth).
AQL Query:

```
SELECT "Resource Type", "Resource ID", "Usage Metric", "Usage Value", "Timestamp"
FROM cloud_resource_logs
WHERE "Usage Metric" IN ('CPU', 'Bandwidth')
AND "Usage Value" > (SELECT AVG("Usage Value") * 2 FROM cloud_resource_logs)
```

81. IAM Role Misuse in Cloud

Description: Flags unauthorised use of Identity and Access Management (IAM) roles or permissions.
AQL Query:

```
SELECT "Event Name", "IAM Role", "User Account", "Source IP", "Timestamp"
FROM cloud_iam_logs
WHERE "Event Name" = 'Role Access'
AND "IAM Role" NOT IN ('Approved Roles List')
GROUP BY "IAM Role", "User Account", "Source IP"
```

82. Unusual Cloud API Calls

Description: Detects abnormal API call patterns to cloud management platforms.
AQL Query:

```
SELECT "Event Name", "API Endpoint", "User Account", COUNT("Event ID") AS
API_Call_Count
FROM cloud_api_logs
GROUP BY "API Endpoint", "User Account"
HAVING API_Call_Count > (SELECT AVG(API_Call_Count) * 3 FROM cloud_api_logs)
```

83. Cloud Instance Launch Outside Hours

Description: Flags new cloud instances or virtual machines launched during off-hours.
AQL Query:

```
SELECT "Event Name", "Instance ID", "User Account", "Timestamp"
FROM cloud_instance_logs
WHERE "Event Name" = 'Instance Launch'
AND HOUR("Timestamp") NOT BETWEEN 8 AND 18
GROUP BY "Instance ID", "User Account"
```

84. Configuration Changes in Cloud Security Groups

Description: Monitors unauthorised changes to cloud security group settings.
AQL Query:

```
SELECT "Event Name", "Security Group ID", "User Account", "Action Taken", "Timestamp"
FROM cloud_configuration_logs
WHERE "Event Name" = 'Security Group Modified'
AND "Action Taken" NOT IN ('Approved Actions List')
GROUP BY "Security Group ID", "User Account"
```

85. Access to Restricted Cloud Services

Description: Detects attempts to access cloud services that are restricted or not in use.
AQL Query:

```
SELECT "Event Name", "Service Name", "User Account", "Source IP", "Timestamp"
FROM cloud_service_logs
WHERE "Service Name" NOT IN ('Approved Services List')
GROUP BY "Service Name", "User Account"
```

FILE AND DATABASE MONITORING

Rule Name	Description	Correlated Log Source(s)
86. Mass File Access Attempts	Detects users accessing a large number of files in a short period.	File Access Logs, File System Logs
87. Unusual File Encryption Activity	Flags unexpected encryption of files, indicating ransomware.	Endpoint Detection Logs (EDR, XDR), File Access Logs
88. Database Table Dump Detected	Detects full table dumps or excessive SELECT queries in databases.	Database Logs (SQL Server, MySQL, Oracle)
89. Unauthorised Access to Critical Databases	Flags unauthorised access to databases storing sensitive data like PII.	Database Logs, Access Control Logs
90. Anomalous File Modifications	Alerts on unusual changes to critical files or configurations.	File Integrity Monitoring Logs, File Access Logs
91. Deletion of Security Logs	Monitors attempts to delete or alter security logs.	Security Logs, File Access Logs
92. File Uploads to Unauthorised Locations	Detects files being uploaded to unknown or restricted servers.	File Transfer Logs, Network Logs
93. File Sharing with Non-Business Domains	Flags files shared with external domains via collaboration tools.	Collaboration Tool Logs (e.g., OneDrive, Dropbox, Google Drive)
94. Database Access Outside Business Hours	Detects unusual database activity during non-working hours.	Database Logs
95. Backup File Deletion or Modification	Monitors unauthorised changes to backup files or directories.	Backup Logs, File Access Logs

86. Mass File Access Attempts

Description: Detects users accessing a large number of files in a short period.
AQL Query:

```
SELECT "Event Name", "User Account", COUNT("File Accessed") AS File_Access_Count,
"Timestamp"
FROM file_access_logs
WHERE "Event Name" = 'File Access'
GROUP BY "User Account", "Timestamp"
HAVING File_Access_Count > 50 -- Threshold for large access count
```

87. Unusual File Encryption Activity

Description: Flags unexpected encryption of files, indicating ransomware.
AQL Query:

```
SELECT "Event Name", "File Name", "Encryption Status", "User Account", "Timestamp"
FROM file_activity_logs
WHERE "Event Name" = 'File Encryption'
AND "Encryption Status" = 'Encrypted'
AND "Timestamp" BETWEEN NOW() - INTERVAL 30 MINUTE AND NOW()
GROUP BY "User Account", "File Name"
HAVING COUNT("File Name") > 10 -- Threshold for encryption attempts
```

88. Database Table Dump Detected

Description: Detects full table dumps or excessive SELECT queries in databases.
AQL Query:

```
SELECT "Event Name", "SQL Query", "User Account", "Timestamp"
FROM database_query_logs
WHERE "Event Name" = 'SQL Query'
AND ("SQL Query" LIKE '%SELECT%' OR "SQL Query" LIKE '/*dump*/%')
GROUP BY "User Account"
HAVING COUNT("SQL Query") > 20 -- Threshold for excessive queries
```

89. Unauthorised Access to Critical Databases

Description: Flags unauthorised access to databases storing sensitive data like PII.
AQL Query:

```
SELECT "Event Name", "User Account", "Database Name", "Access Level", "Timestamp"
FROM database_access_logs
WHERE "Database Name" IN ('PII_DB', 'Financial_DB')
AND "Access Level" NOT IN ('Admin', 'DBOwner')
GROUP BY "User Account", "Database Name"
```

90. Anomalous File Modifications

Description: Alerts on unusual changes to critical files or configurations.
AQL Query:

```
SELECT "Event Name", "File Path", "User Account", "Modification Type", "Timestamp"
FROM file_modification_logs
WHERE "Event Name" = 'File Modification'
AND "File Path" IN ('/etc/', '/var/log/', '/config/')
GROUP BY "User Account", "File Path"
```

HAVING COUNT("File Path") > 3 -- Threshold for unusual file modifications

91. Deletion of Security Logs

Description: Monitors attempts to delete or alter security logs.
AQL Query:

```
SELECT "Event Name", "User Account", "Log File", "Action Taken", "Timestamp"
FROM security_log_changes
WHERE "Event Name" = 'Log Deletion'
AND "Action Taken" = 'Delete'
GROUP BY "User Account", "Log File"
```

92. File Uploads to Unauthorised Locations

Description: Detects files being uploaded to unknown or restricted servers.
AQL Query:

```
SELECT "Event Name", "User Account", "File Path", "Destination", "Timestamp"
FROM file_upload_logs
WHERE "Event Name" = 'File Upload'
AND "Destination" NOT IN ('Approved Servers List')
GROUP BY "User Account", "Destination"
```

93. File Sharing with Non-Business Domains

Description: Flags files shared with external domains via collaboration tools.
AQL Query:

```
SELECT "Event Name", "File Name", "User Account", "Shared With", "Timestamp"
FROM file_sharing_logs
WHERE "Event Name" = 'File Shared'
AND "Shared With" NOT LIKE '%company.com'
GROUP BY "User Account", "File Name"
```

94. Database Access Outside Business Hours

Description: Detects unusual database activity during non-working hours.
AQL Query:

```
SELECT "Event Name", "User Account", "Database Name", "Timestamp"
FROM database_activity_logs
WHERE "Event Name" = 'Database Access'
AND HOUR("Timestamp") NOT BETWEEN 8 AND 18
```

```
GROUP BY "User Account", "Database Name"
```

95. Backup File Deletion or Modification

Description: Monitors unauthorised changes to backup files or directories.
AQL Query:

```
SELECT "Event Name", "File Path", "User Account", "Action Taken", "Timestamp"
FROM file_activity_logs
WHERE "Event Name" = 'File Modification' OR "Event Name" = 'File Deletion'
AND "File Path" LIKE '%/backup/%'
AND "Action Taken" = 'Delete'
GROUP BY "User Account", "File Path"
```

THREAT INTELLIGENCE INTEGRATION

Rule Name	Description	Correlated Log Source(s)
96. Traffic to Known Malicious IPs	Matches network traffic with known malicious IPs from threat feeds.	Network Logs, Firewall Logs, IDS/IPS Logs
97. Execution of Known Malware Hashes	Flags files or processes matching malware hashes in intelligence feeds.	Endpoint Detection Logs (EDR, XDR), Antivirus Logs
98. Communication with C2 Servers	Detects outbound traffic to known Command-and-Control (C2) servers.	Network Logs, Proxy Logs, Firewall Logs, IDS/IPS Logs
99. Access to Newly Registered Domains	Flags traffic to domains recently registered, which may indicate phishing or C2 activity.	DNS Logs, Network Logs
100. Unusual Access to TOR Exit Nodes	Alerts on traffic originating from or destined to TOR exit nodes.	Network Logs, Proxy Logs, Firewall Logs, IDS/IPS Logs

96. Traffic to Known Malicious IPs

Description: Matches network traffic with known malicious IPs from threat feeds.
AQL Query:

```
SELECT "Event Name", "Source IP", "Destination IP", "Timestamp"
FROM network_traffic_logs
WHERE "Destination IP" IN (SELECT "Malicious IP" FROM threat_intelligence_feeds)
GROUP BY "Source IP", "Destination IP"
```

97. Execution of Known Malware Hashes

Description: Flags files or processes matching malware hashes in intelligence feeds.
AQL Query:

```
SELECT "Event Name", "File Hash", "File Name", "User Account", "Timestamp"
FROM file_execution_logs
WHERE "File Hash" IN (SELECT "Malware Hash" FROM threat_intelligence_feeds)
GROUP BY "User Account", "File Name"
```

98. Communication with C2 Servers

Description: Detects outbound traffic to known Command-and-Control (C2) servers.
AQL Query:

```
SELECT "Event Name", "Source IP", "Destination IP", "Timestamp"
FROM network_traffic_logs
WHERE "Destination IP" IN (SELECT "C2 Server IP" FROM threat_intelligence_feeds)
GROUP BY "Source IP", "Destination IP"
```

99. Access to Newly Registered Domains

Description: Flags traffic to domains recently registered, which may indicate phishing or C2 activity.
AQL Query:

```
SELECT "Event Name", "Source IP", "Destination Domain", "Timestamp"
FROM network_traffic_logs
WHERE "Destination Domain" IN (SELECT "Domain" FROM newly_registered_domains
WHERE "Registration Date" > NOW() - INTERVAL 7 DAYS)
GROUP BY "Source IP", "Destination Domain"
```

100. Unusual Access to TOR Exit Nodes

Description: Alerts on traffic originating from or destined to TOR exit nodes.
AQL Query:

```
SELECT "Event Name", "Source IP", "Destination IP", "Timestamp"
FROM network_traffic_logs
WHERE "Destination IP" IN (SELECT "TOR Exit Node IP" FROM tor_exit_nodes)
OR "Source IP" IN (SELECT "TOR Exit Node IP" FROM tor_exit_nodes)
GROUP BY "Source IP", "Destination IP"
```