Objective

What are we trying to achieve?

Detect when the Security Event Log is cleared.

Justification

Why are we trying to detect this activity?

Threat actors sometimes clear event logs to hamper investigations and incident response.

Analysis

How should the event be analysed?

Attempt to identify the user and any contextual activity that could indicate what the user was doing around the time of the log being cleared (e.g. by using process execution events).

Key Fields

SIEM Fieldname	Raw Log	Description
Hostname	Computer	Hostname where the log was cleared
Username	Account Name	Username that cleared the log
Domain	Domain Name	Domain of the user that cleared the log

Correlation Criteria

Description of how it detects.

Triggers whenever an EID 1102 occurs unless the host and user combination is allowlisted.

Limitations and Bypasses

Any known limitations or bypasses.

Does not apply to clearing of the System or Application Log. Does not detect log flooding. Does not detect more advanced methods of clearing the log without creating an EID 1102 (for examples see Reference 3).

Allowlisting

How should entities be allowlisted?

Hostname and Username tuple

Event Sources

List the event sources required.

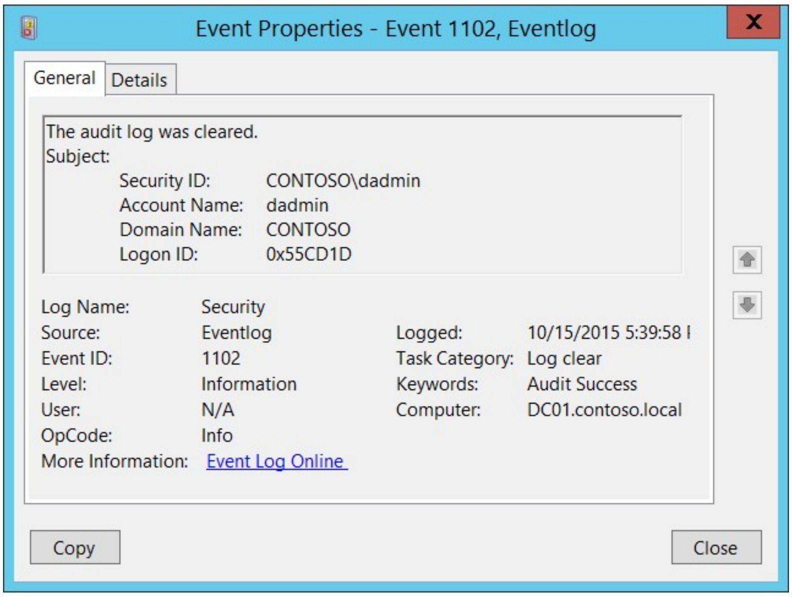
Windows Events, EID 1102

Testing

Document testing and results.

From an elevated command prompt:

```
C:\> wevtutil cl security
```



The audit log was cleared.
Subject:
Security ID: CONTOSO\dadmin
Account Name: dadmin
Domain Name: CONTOSO
Logon ID: 0x55CD1D

Log Name: Security
Source: Eventlog
Logged: 10/15/2015 5:39:58
Event ID: 1102
Task Category: Log clear
Level: Information
Keywords: Audit Success
User: N/A
Computer: DC01.contoso.local
OpCode: Info
More Information: Event Log Online

References

1. https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-1102
2. https://attack.mitre.org/techniques/T1070/001/
3. https://svch0st.medium.com/event-log-tampering-part-1-disrupting-the-eventlog-service-8d4b7d67335c