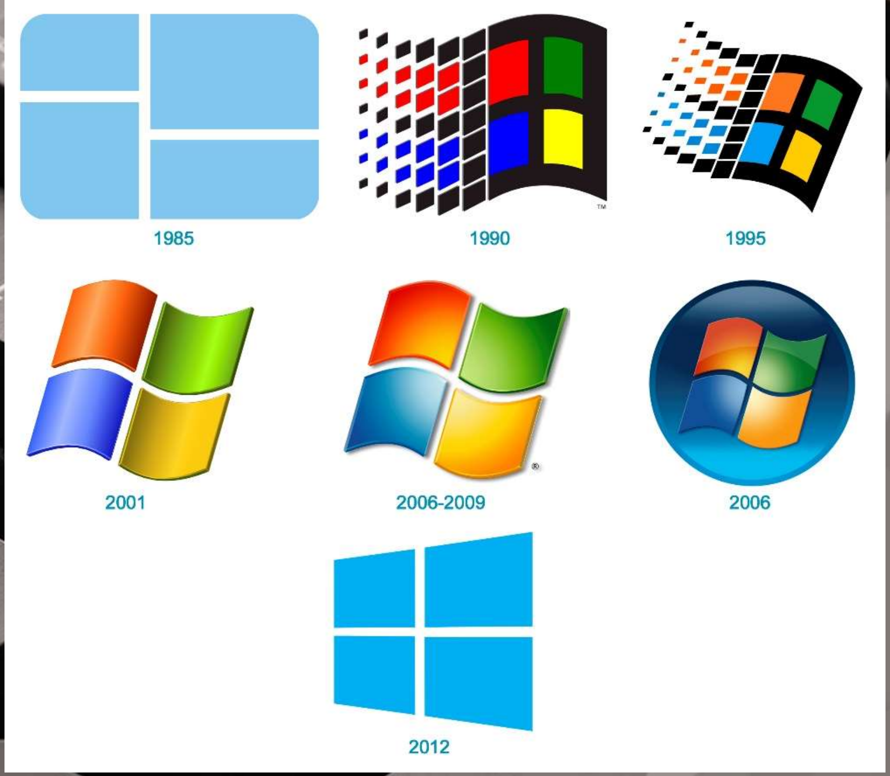


Microsoft

# Windows Logs

Mahesh Pavaskar

# Content

1. Why logs are important?
2. Where logs are stored?
3. How log looks & important fields in logs
4. Types of logs?
5. Possible Data sources based on types of logs
6. EventViewer
7. How to send logs towards syslog server / Collector / SIEM
8. Important EventID in Windows – might be useful to write security use cases

# Why logs are important?

- To trace the activity
- Analyse the logs and identify the suspicious behaviour
- Prevent attacker before more damage to organization
- Behavioural analysis
- Anomaly detection
- Outlier

# Where logs are stored?

- Windows

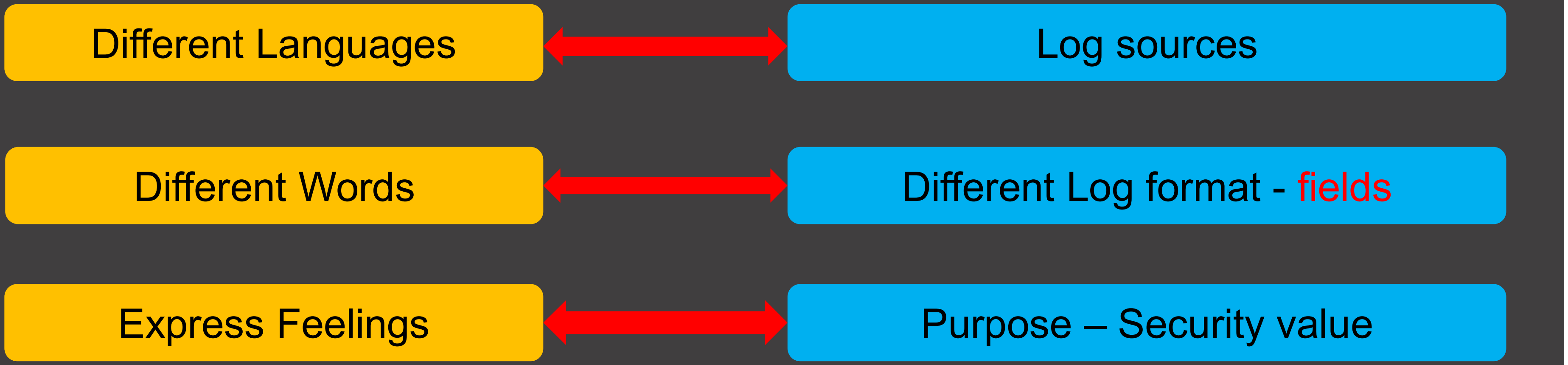
C:\Windows\System32\winevt\Logs

# How log looks & important fields in logs

- Original Format : XML

- Important Fields

Timestamp, Hostname,EventID,SubjectUser, TargetUser etc



Different Languages

Log sources

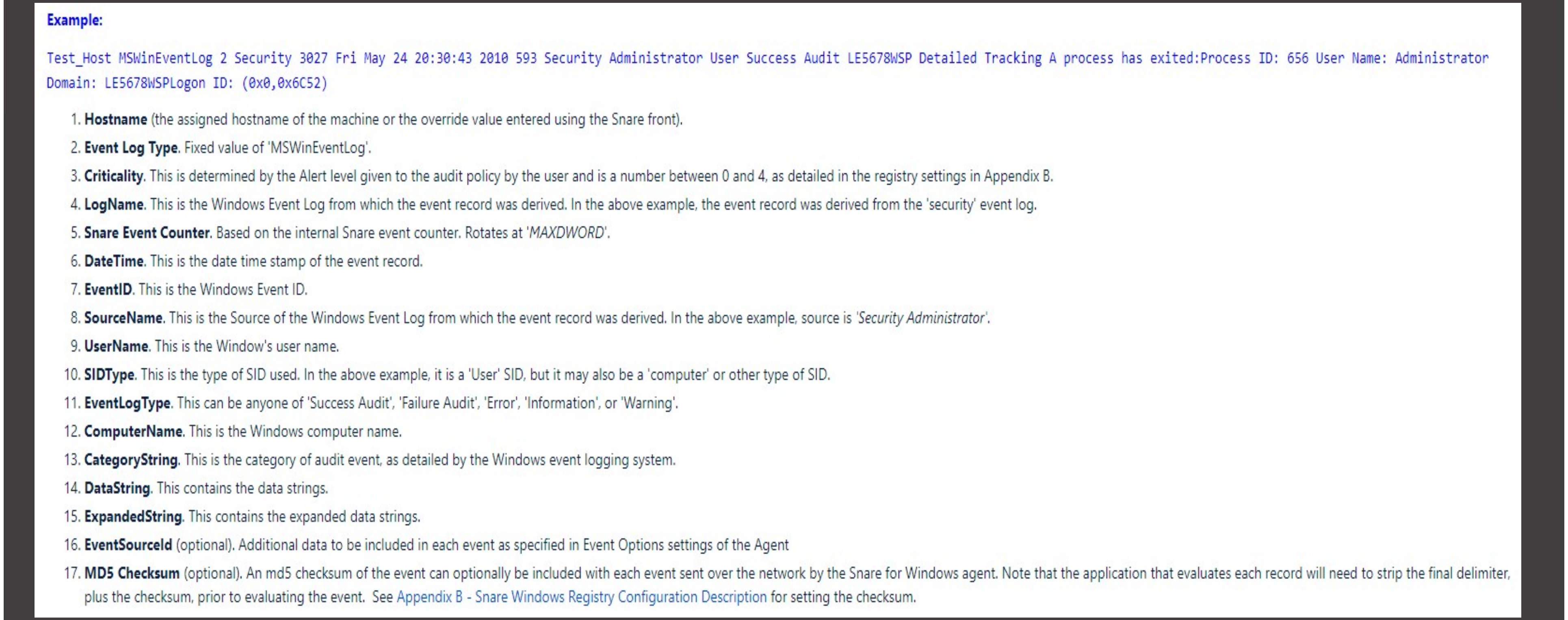
Different Words

Different Log format - fields

Express Feelings

Purpose – Security value

https://prophecyinternational.atlassian.net/wiki/spaces/WADOC/pages/1233224043/Appendix+A+-+Windows+Event+Output+Format

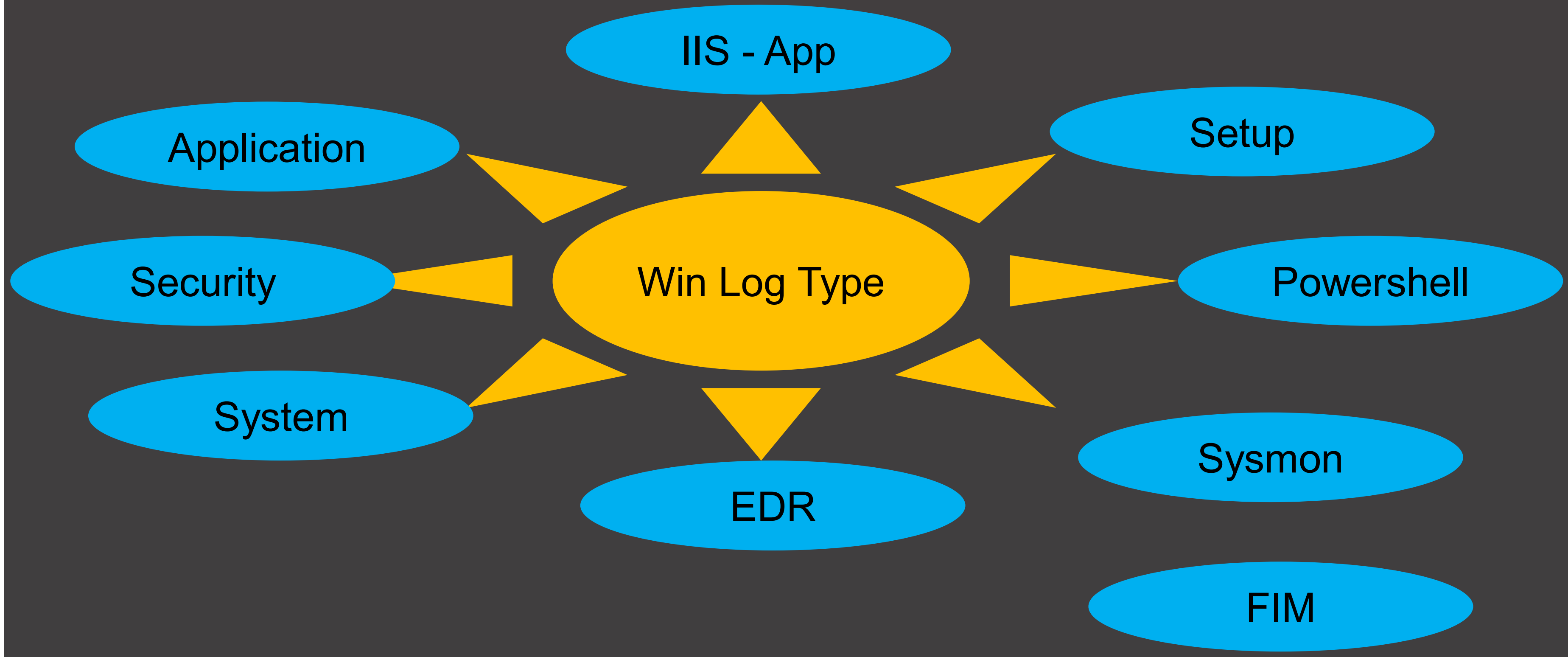


**Example:**

```
Test_Host MSWinEventLog 2 Security 3027 Fri May 24 20:30:43 2010 593 Security Administrator User Success Audit LE5678WSP Detailed Tracking A process has exited:Process ID: 656 User Name: Administrator
Domain: LE5678WSPLogon ID: (0x0,0x6C52)
```

1. **Hostname** (the assigned hostname of the machine or the override value entered using the Snare front).
2. **Event Log Type**. Fixed value of 'MSWinEventLog'.
3. **Criticality**. This is determined by the Alert level given to the audit policy by the user and is a number between 0 and 4, as detailed in the registry settings in Appendix B.
4. **LogName**. This is the Windows Event Log from which the event record was derived. In the above example, the event record was derived from the 'security' event log.
5. **Snare Event Counter**. Based on the internal Snare event counter. Rotates at '*MAXDWORD*'.
6. **DateTime**. This is the date time stamp of the event record.
7. **EventID**. This is the Windows Event ID.
8. **SourceName**. This is the Source of the Windows Event Log from which the event record was derived. In the above example, source is '*Security Administrator*'.
9. **UserName**. This is the Window's user name.
10. **SIDType**. This is the type of SID used. In the above example, it is a 'User' SID, but it may also be a 'computer' or other type of SID.
11. **EventLogType**. This can be anyone of 'Success Audit', 'Failure Audit', 'Error', 'Information', or 'Warning'.
12. **ComputerName**. This is the Windows computer name.
13. **CategoryString**. This is the category of audit event, as detailed by the Windows event logging system.
14. **DataString**. This contains the data strings.
15. **ExpandedString**. This contains the expanded data strings.
16. **EventSourceId** (optional). Additional data to be included in each event as specified in Event Options settings of the Agent
17. **MD5 Checksum** (optional). An md5 checksum of the event can optionally be included with each event sent over the network by the Snare for Windows agent. Note that the application that evaluates each record will need to strip the final delimiter, plus the checksum, prior to evaluating the event.  See Appendix B - Snare Windows Registry Configuration Description for setting the checksum.

# Types of logs?



Win Log Type

IIS - App

Application

Setup

Security

Powershell

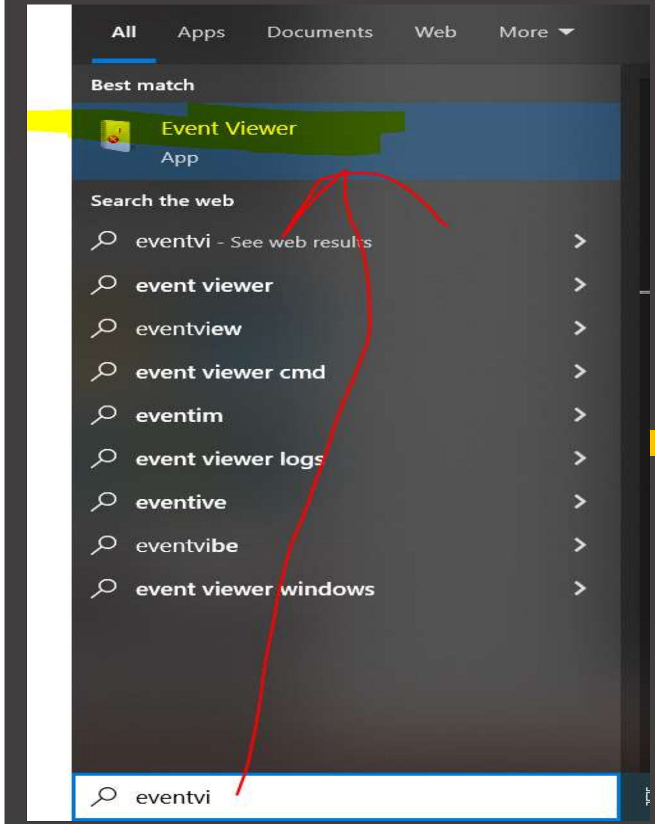
System

EDR

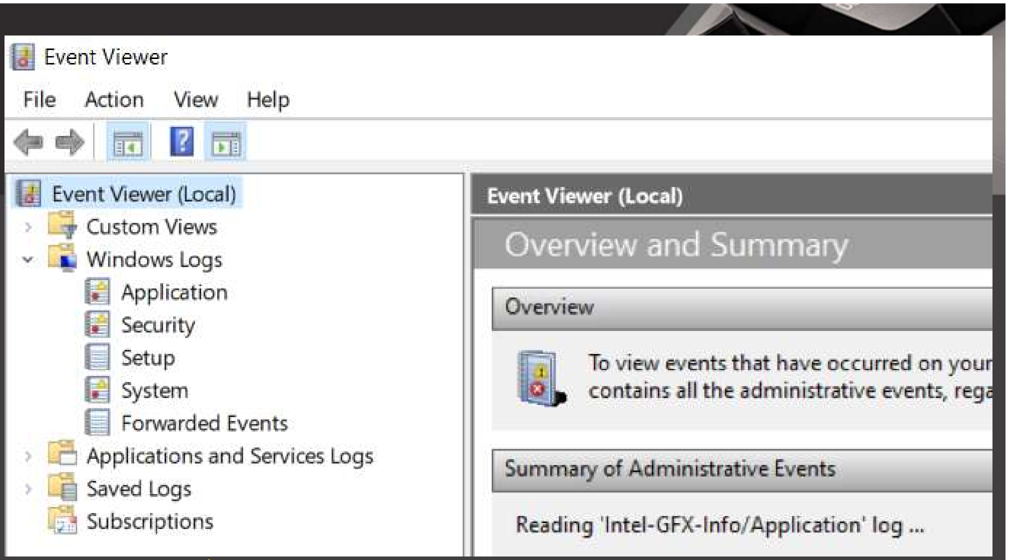
Sysmon

FIM

# EventViewer



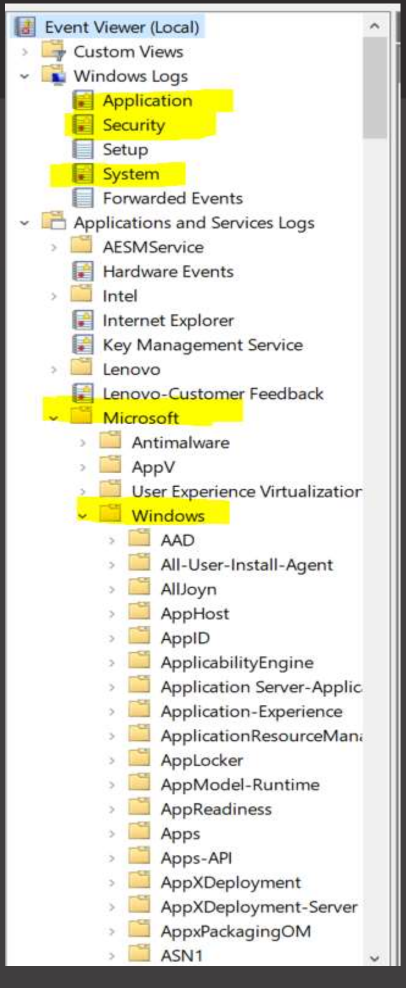
eventvi



To view events that have occurred on your
contains all the administrative events, rega

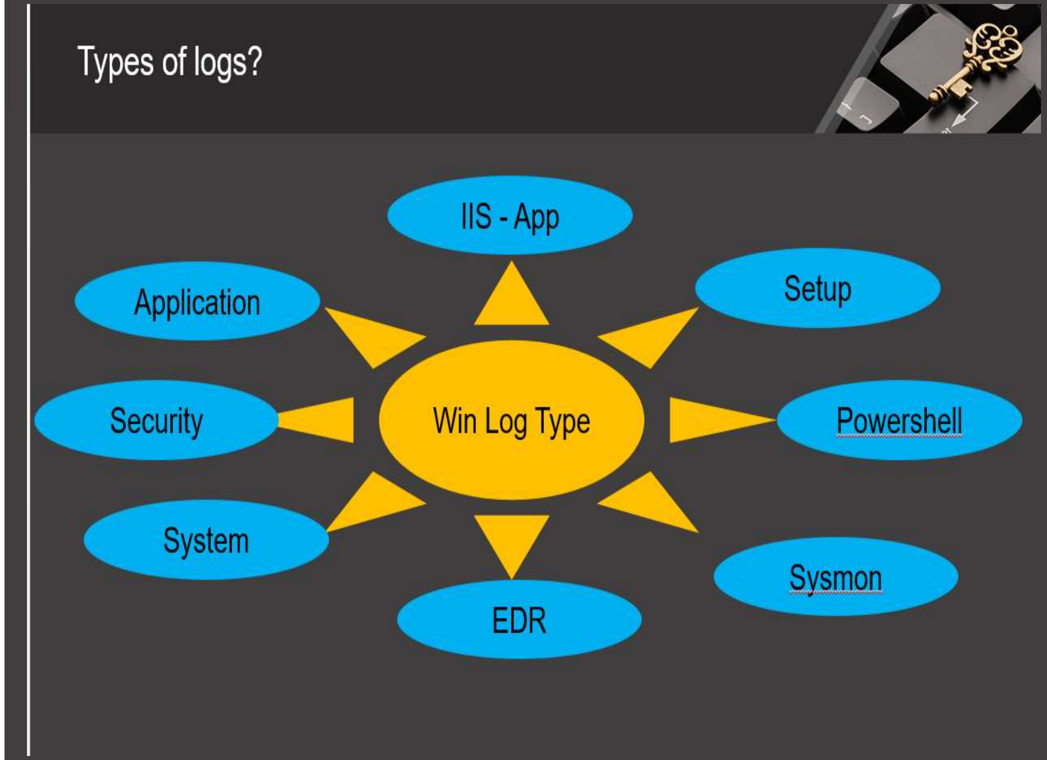
Reading 'Intel-GFX-Info/Application' log ...

# EventViewer



- Event Viewer (Local)
  - Custom Views
  - Windows Logs
    - Application
    - Security
    - Setup
    - System
    - Forwarded Events
  - Applications and Services Logs
    - AESMService
    - Hardware Events
    - Intel
    - Internet Explorer
    - Key Management Service
    - Lenovo
    - Lenovo-Customer Feedback
    - Microsoft
      - Antimalware
      - AppV
      - User Experience Virtualizatior
      - Windows
        - AAD
        - All-User-Install-Agent
        - AllJoyn
        - AppHost
        - AppID
        - ApplicabilityEngine
        - Application Server-Applic
        - Application-Experience
        - ApplicationResourceMan
        - AppLocker
        - AppModel-Runtime
        - AppReadiness
        - Apps
        - Apps-API
        - AppXDeployment
        - AppXDeployment-Server
        - AppxPackagingOM
        - ASN1

# Possible Data sources based on types of logs



## Types of logs?

Win Log Type

IIS - App

Setup

Powershell

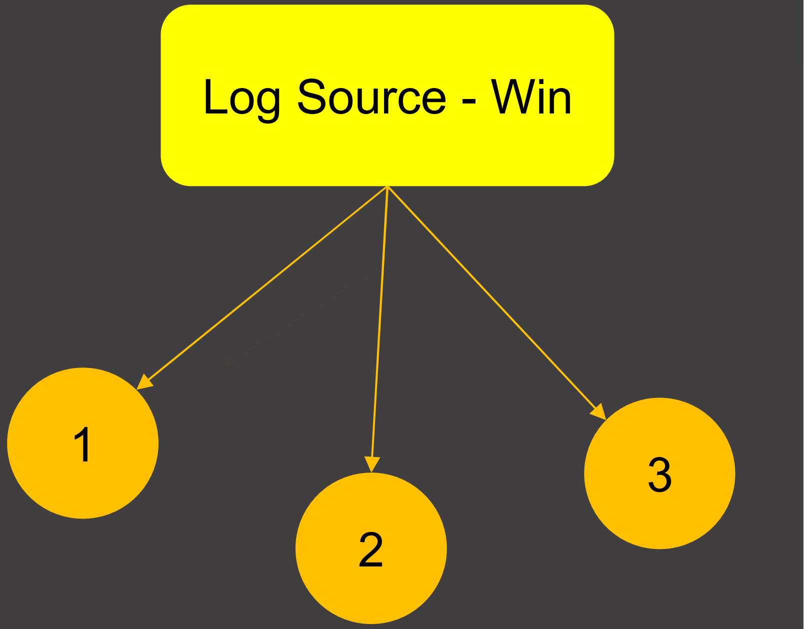
Sysmon

EDR

System

Security

Application



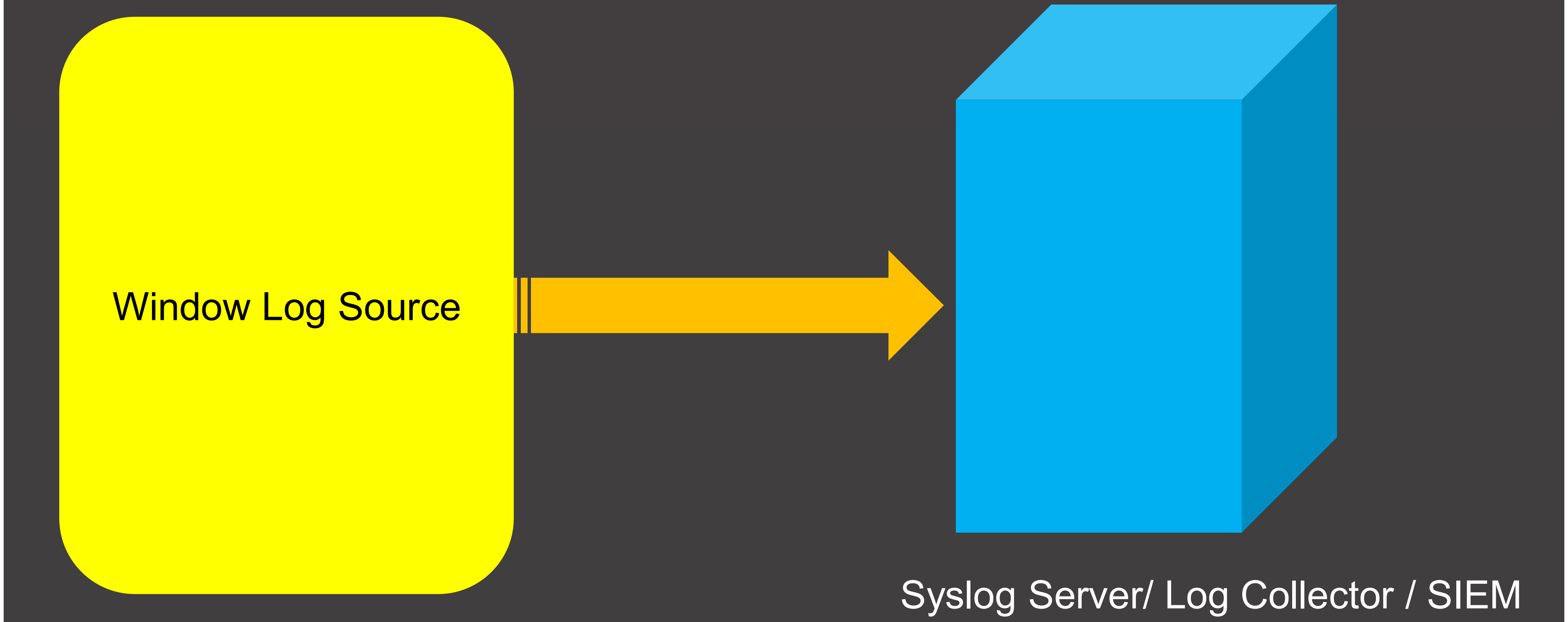
Log Source - Win

1

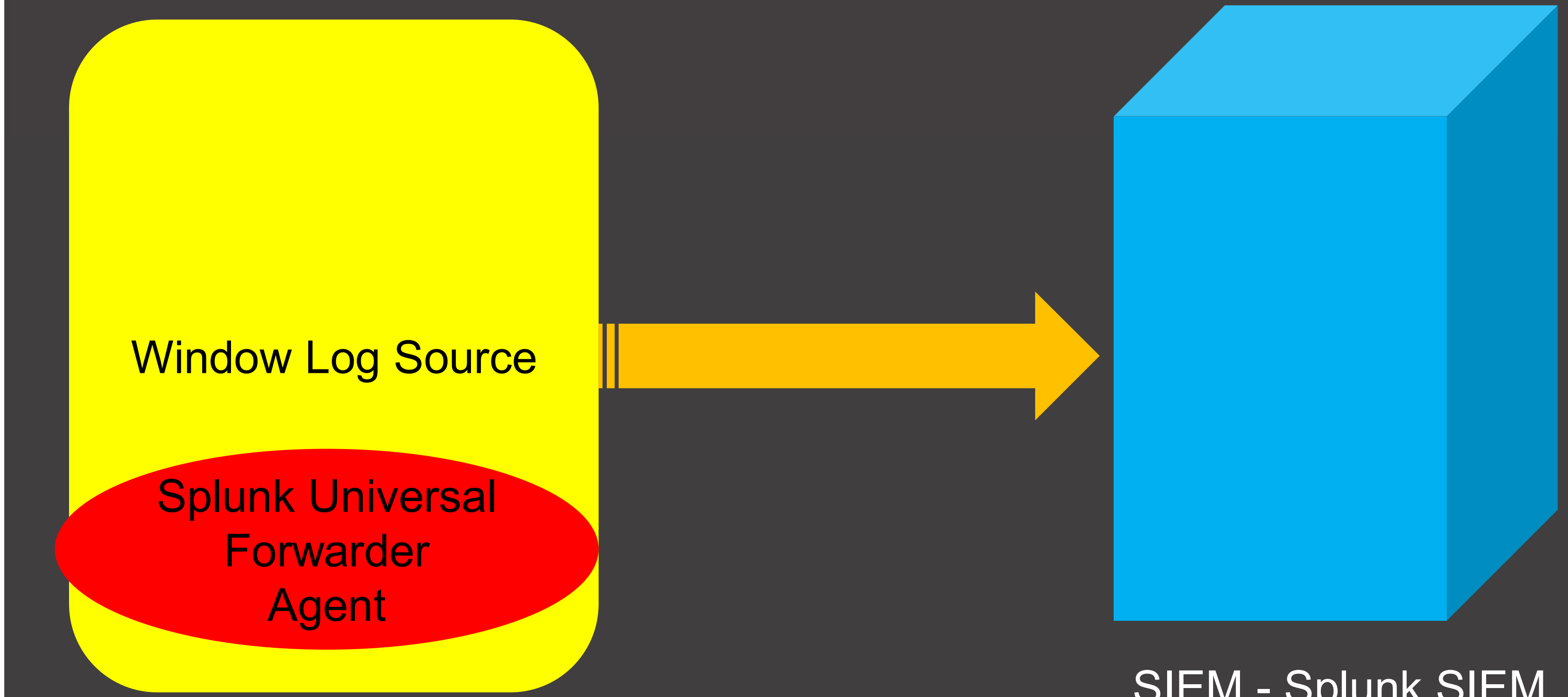
2

3

# How to send logs towards syslog server / Collector / SIEM



# Windows logs to Splunk SIEM

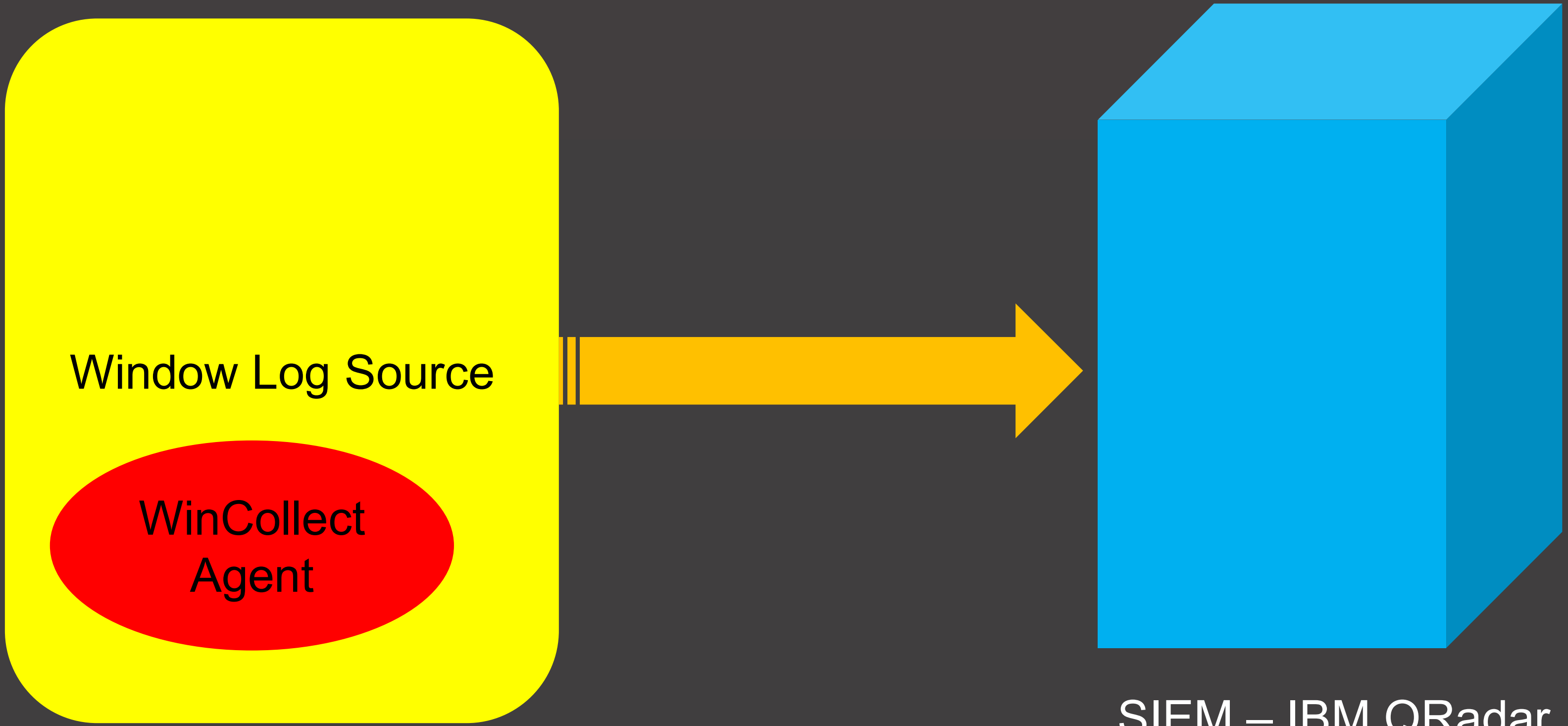


Window Log Source

Splunk Universal Forwarder Agent

SIEM - Splunk SIEM

# Windows logs to IBM QRadar SIEM



Window Log Source

WinCollect Agent

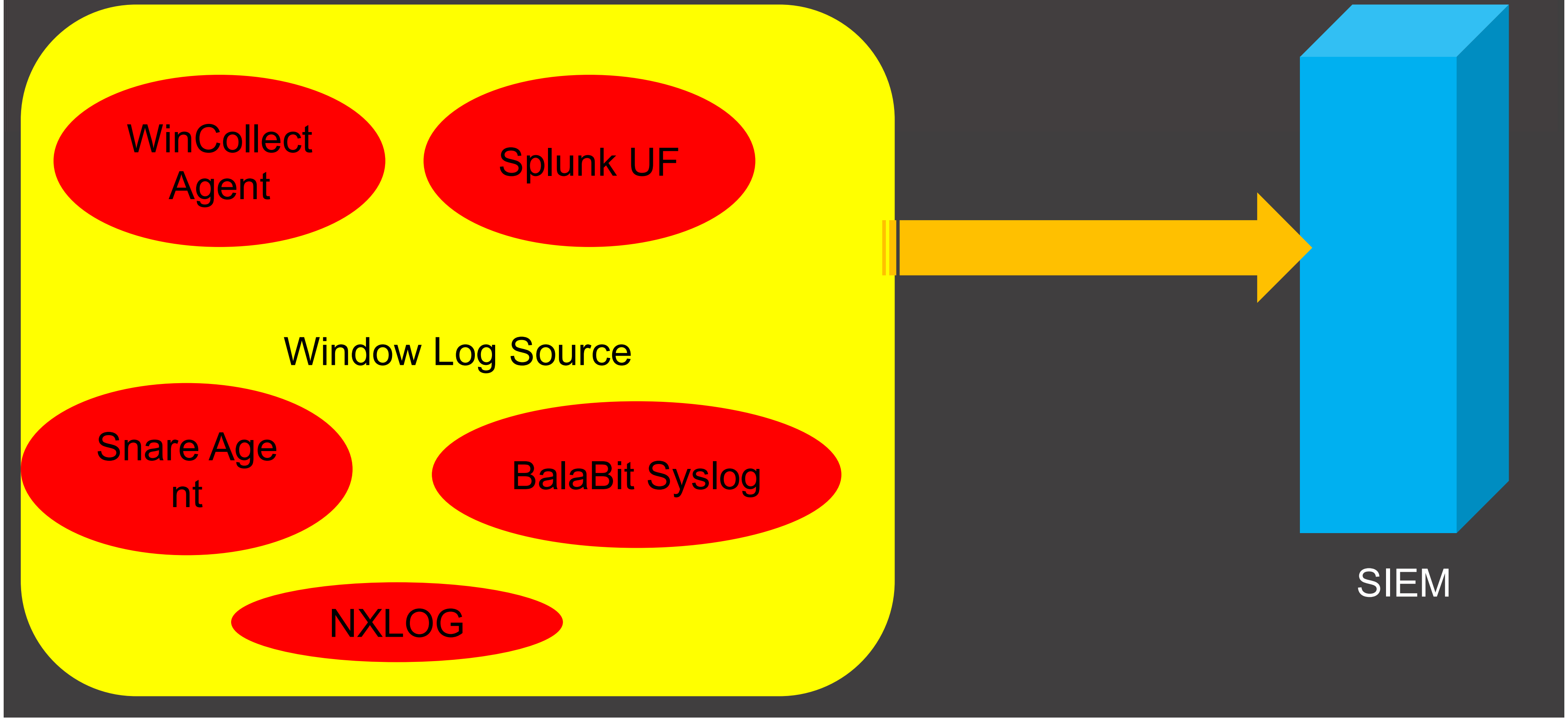
SIEM – IBM QRadar

# Solutions

- Agent Based Solution – Push
- Agentless Solution – Pull logs

Note : Each solution has pros and cons…

# Vendors in market who provide agents



WinCollect Agent

Splunk UF

Window Log Source

Snare Age
nt

BalaBit Syslog

NXLOG

SIEM

# Important EventID in Windows – might be useful to write security use cases

- https://prophecyinternational.atlassian.net/wiki/spaces/WADOC/pages/1233224059/Appendix+C+-+Audit+Policies+and+Security+Event+IDs

- https://andreafortuna.org/2019/06/12/windows-security-event-logs-my-own-cheatsheet/

# Thank you