Task-12

[Bhumireddy Thanmaye 21BCI0013](mailto:bhumireddy.thanmaye2021@vitstudent.ac.in)

Task Objective : To get knowledge about Wincollect and standalone wincollect

**What is WinCollect?**

WinCollect is a Syslog event forwarder that administrators can use to forward events from Windows logs to QRadar. WinCollect can collect events from systems locally or be configured to remotely poll other Windows systems for events.

**What is WinCollect Standalone?**

WinCollect standalone is a deployment option for WinCollect that allows you to collect logs from Windows hosts that do not have the WinCollect software installed. In a stand-alone deployment, a Windows host with the WinCollect software installed polls the remote hosts and collects their logs. The collected logs are then sent to QRadar.

**How will the WinCollect Log File be ?**

WinCollect generates log event extended format (LEEF) messages during installation and configuration and writes them to a single log file. The server in the Status Server field receives the LEEF messages through the syslog. These messages report on the status of the WinCollect service, authorization token, configuration, and more.

**What is the type of logs ?**

Each log entry is tagged with an identifier that indicates the entry type:

* System - Indicates system information, such as the operating system that the agent is installed on, RAM and CPU information from the operating system, service start-up information, and WinCollect version information.
* Code - Indicates information about spillover and cache messages, file reader messages, authorization token messages, IP address or hostname information for the local host, issues with destinations, log source auto-creation, stand-alone mode messages, and thread or process start-up and shutdown messages. Use these entries to investigate the WinCollect configuration.
* Device - Created when WinCollect collects events, the protocols that run event log collection. The following issues are logged as device entries
  + Loading Plug-in
  + Connection issues
  + Permission or Authentication
  + Windows error codes (hex value codes provided by the operating system, such as 0x000005 access denied)
  + File path or location
  + Event log is overdue to be polled
  + Event log transactions
  + RPC is unavailable (unable to find the location that you specified)
  + Reopening due to falling too far behind (tuning messages)

**Why is WinCollect and WinCollect standalone Used for ?**

WinCollect and WinCollect standalone are used for a variety of purposes which security monitoring,compliance reports,it operations monitoring,etc

1. **Security monitoring:** WinCollect can be used to collect security logs from Windows hosts, such as event logs, firewall logs, and intrusion detection system (IDS) logs. This information can be used to detect and investigate security incidents.
2. **Compliance reporting:** WinCollect can be used to collect logs that are required for compliance with regulations, such as the Payment Card Industry Data Security Standard (PCI DSS) and the Health Insurance Portability and Accountability Act (HIPAA).
3. **IT operations monitoring:** WinCollect can be used to collect logs from Windows hosts to monitor the health of the IT infrastructure. This information can be used to identify and troubleshoot problems.

**How to use WinCollect?**

1. The WinCollect agent is installed on a Windows host.

2. The agent uses the Windows Event Log API to collect events from the Windows event logs.

3. The agent sends the collected events to QRadar over a secure connection.

4. QRadar stores the events in its database and makes them available for analysis.

The WinCollect agent can be configured to collect a variety of events which includes the below

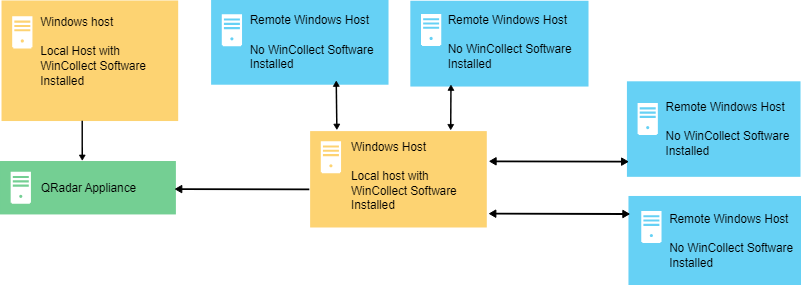
* Security events, such as login attempts, file access, and process creation.
* System events, such as hardware errors and software installation.
* Application events, such as errors and warnings.

WinCollect can also be configured to collect events from specific sources, such as specific event logs or specific Windows hosts.

The frequency at which WinCollect collects events can also be configured. This can be important for systems that generate a lot of events, such as systems that are used for logging security events.

* The WinCollect agent uses the Windows Event Log API to collect events from the Windows event logs. The Windows Event Log API is a set of functions that allow applications to access and manage the Windows event logs.
* The WinCollect agent sends the collected events to QRadar over a secure connection. The secure connection is typically a TLS (Transport Layer Security) connection.
* QRadar stores the events in its database and makes them available for analysis. QRadar uses a database to store the events that it collects. This database can be queried to retrieve specific events or to perform analysis on the events.

**WinCollect Standalone Example**



Stand-alone WinCollect mode has the following capabilities:

* Configure each WinCollect agent by using the WinCollect 10 Console.
* Update WinCollect software with the software update installer.
* Event storage to ensure that no events are dropped.
* Collects forwarded events from Microsoft Subscriptions.
* Filters events by using XPath queries or exclusion filters.
* Supports virtual machine installations.
* Send events to QRadar over TLS Syslog.
* Automatically create a local source at the time of agent installation.