**Veritas NetBackup and Microsoft Sentinel Integration Guide**

The integration between Veritas NetBackup and Microsoft Sentinel empowers security operations teams by providing valuable insights from Veritas NetBackup Anomaly Detection and Malware Scanning engines directly into Microsoft Sentinel.

### These insights provide the following advantages to Security and IT ops:

* Identification of early indicators of compromise such as malware or data anomaly detection including spikes in new uncompressible data or change in deduplication ratio, files modifications during backups, etc.
* Enhances capabilities for security operators to prioritize and expedite the investigation of potential security incidents with the help of insights from threats published by Veritas NetBackup.
* Enables NetBackup users to ingest alerts and other data into their Sentinel instance. With Analytic Rules, Sentinel can automatically create Sentinel incidents from incoming events.

Veritas NetBackup has developed a first-class, in-product integration with Microsoft Sentinel. Security insights will be pushed via NetBackup APIs directly into the Microsoft Sentinel workspace, eliminating any dependency on playbooks or the need to develop data connectors separately. The threat hunting queries with enrich anomaly events from NetBackup helps during Ransomware analysis and helps incident prioritization when security administrators deal with several thousand security events.

**Prerequisites**

Veritas NetBackup should be configured to send appropriate events to Microsoft Sentinel and must be running version 10.2 or higher.

Microsoft Sentinel and NetBackup should be configured to connect to API end points using an account with the relevant privileges necessary to perform the desired operations.

A workspace key and ID are required for NetBackup to connect to Sentinel. These are generated in Sentinel via its SIEM WebUI/API interface and stored and used by the NetBackup primary server.

**How NetBackup Sends Events to Microsoft Sentinel**

The figure below shows how NetBackup sends events to SIEM platforms using Microsoft Sentinel as an example. A workspace key and ID are required for NetBackup to connect to Sentinel. These are generated in Microsoft Sentinel via its SIEM WebUI/API interface and stored and used by the NetBackup primary server. Once NetBackup can connect to Microsoft Sentinel, NetBackup audits its own logs for the type(s) of alerts you’ve configured for forwarding to Microsoft Sentinel. The selected alerts are then sent to Microsoft Sentinel as audit alert broadcast messages.

A diagram of a software system

Description automatically generated

**Connecting Veritas NetBackup to Microsoft Sentinel**

The Microsoft Sentinel workspace to receive audit alerts from NetBackup must already exist before it can be selected as an audit alert target. The example workspace in the figure below is “sentinel1.” Search the Microsoft Sentinel documentation for accessing the “Log Analytics Agents Instructions” feature to display workspace IDs and keys as shown. Existing IDs and keys can be copied, or new ones generated as needed.

A screenshot of a computer

Description automatically generated

Once you have a copy of the workspace ID and key, you can configure the workspace in NetBackup as an audit event target. Login to NetBackup WebUI. SIEM targets can only be configured in the WebUI. Go to *Security -> Security events -> Audit event settings* as shown below.

A screenshot of a computer

Description automatically generated

Click the “Send audit events to log forwarding endpoints” checkbox, then click on “Select Endpoints” tab when it appears as shown below.

A screenshot of a computer

Description automatically generated

Click the “Microsoft Sentinel” checkbox, then the “Add a new credential” button.  Enter the workspace ID and key and save the changes. The new credential for Microsoft Sentinel appears as shown below. Click on the dot menu and select “Edit.”

A screenshot of a computer

Description automatically generated

Enter a tag (optional), description, workspace ID, and workspace primary key, as shown below. Click “Next.”  The credentials are updated.  Click “Save.”

A screenshot of a computer

Description automatically generated

NetBackup can now send audit events to Microsoft Sentinel as shown below.

A screenshot of a computer

Description automatically generated

Now that you have a target workspace to receive audit alerts, click “Edit” to select the audit event categories you want to forward to selected endpoints. By default, all categories are selected. Click the checkboxes of the audit categories to select/unselect them shown and click save.

A screenshot of a computer

Description automatically generated

NetBackup is now configured to send the audit events you selected to the Microsoft Sentinel workspace you specified. Only new audit alerts will be forwarded when they are generated. Click “Close.” A summary of your Microsoft Sentinel configuration is displayed, as shown below.

**For example - Anomaly Audit Event -** Contains the sentinel function which receives anomaly event data via Veritas NetBackup Web APIs and ingests into Microsoft Sentinel.

A screenshot of a computer

Description automatically generated

**How to use NetBackup alerts in Microsoft Sentinel**

**Query Data**

* + Users can query NetBackup data from sentinel using KQL queries in Sentinel.
  + Below simple KQL will return all NetBackup alerts.

**Analytics Rule Example 1:**

**Anomaly Detection and malware detection Alerts**

This query provides insights into anomaly detection and malware scanning alerts ingested by NetBackup into sentinel.

union NetBackupAlerts\_CL | where Category contains "ANOMOLY\_EXTENSION"

union NetBackupAlerts\_CL | where Category contains "MALWARE\_IMPACTED"

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

**Analytics Rule Example 2:**

**User login Alerts**

This query creates an automated rule to check for 10 or more login failures, indicating a potential security breach or unauthorized access to the systems.

*Query:*

*NetBackupAlerts\_CL  
| where operations contains "LOGIN" and Message contains "authentication failed"   
| summarize total=count() | where total > 10*

Once the data is available in Sentinel, Analytics rules can be set to run different use cases.

Using KQL language, we can write the scripts which fetches the desired data as per the use case. For example, there is need to create automated rule to check if there are 10 or more login failures in NetBackup, then this can be done using Analytics rules.

**I**n Microsoft Sentinel, under Analytics Tab- click on Create Scheduled rule.

Setup basic rule details as below

A screenshot of a computer

Description automatically generated

Query:

*let time\_span = ago(60m);*  
*NetBackupAlerts\_CL*  
*| where operation\_s contains "LOGIN" and Message contains "authentication failed"*  
*| extend userName =  split(userName\_s, "@")[0] | extend host =*  
*split(userName\_s, "@")[1]*  
*| where TimeGenerated >= time\_span*  
*| summarize count() by tostring(host)*

**Create Playbook for actions.**

From Microsoft Sentinel | Automation, click on Create | Playbook with incident trigger.

A screenshot of a computer

Description automatically generated

Once playbook is created, it will open logic app designer. Click on New Step and select HTTP.

A screenshot of a computer

Description automatically generated

* + Provide API details and Save.

A screenshot of a computer

Description automatically generated