NCPROTECT™
DATA CONNECTOR FOR MICROSOFT SENTINEL®

Executive Summary

Microsoft Sentinel is a cloud-native SIEM that you can use for intelligent security analytics across your entire enterprise.

The NC Protect Data Connector for Microsoft Sentinel allows you to easily ingest user activity and protection logs and their associated “events” from NC Protect into Microsoft Sentinel.

Key Benefits

- Installed and configured from within the Microsoft Sentinel portal.
- Jump start threat investigation with just a few clicks using built-in Sentinel workbooks.
- Create custom reports and visualizations to analyze user activity and behavior tracked by NC Protect.
- Get advanced auditing capability by aggregating NC Protect access data with existing SIEM processes.
- Trigger real-time alerts and workflows on suspicious user activity.
- Report on guest activity within SharePoint.

PROACTIVE INFORMATION SECURITY TO PROTECT FROM THE INSIDE OUT

Today’s organizations must assume they will be compromised by a bad actor, disgruntled or even a negligent employee. We can no longer solely afford to settle for after the fact detection and user behavior analysis to detect a breach.

NC Protect’s real-time data security leverages attribute-based access control (ABAC) policies which take into consideration content and user context, to prevent both negligent and malicious data loss. It provides advanced information protection that’s simple, fast and scalable to protect and audit sensitive information access across the Microsoft 365 collaboration stack.

NC Protect also provides out of the box centralized reporting and auditing capabilities to:

- Report on the number of issues identified by classification level.
- Allow policy officers to review the results and - if needed - rescan, reclassify or reapply permissions.
- Log and track user activities and actions such as producing, editing or deleting data, and general access.
- Track any changes to NC Protect settings and policies, and who made them.

GET ADVANCED INSIGHT & ALERTS WITH NC PROTECT’S MICROSOFT SENTINEL INTEGRATION

You can also leverage the power of Microsoft Sentinel for deeper analysis and to automate downstream actions from the insights gained from the audit logs created by NC Protect and cross-correlate them with the rest of your investigation and reporting ecosystem.

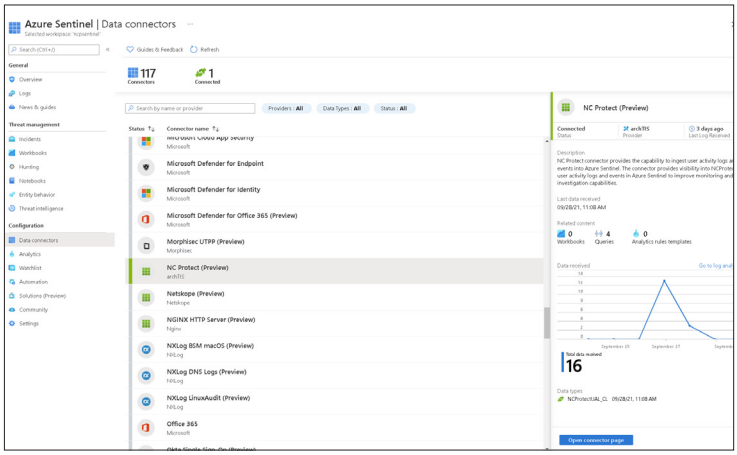
The NC Protect Data Connector for Microsoft Sentinel enables customers to easily ingest user activity and logs collected in NC Protect into Microsoft Sentinel to analyze the data at cloud scale, as well as trigger holistic alerts and remediation actions alongside the dynamic and real-time access controls of NC Protect.

Easily installed directly from the Microsoft Sentinel administration portal, the NC Protect Data Connector will immediately start ingesting information so you can investigate and respond to potential security incidents and suspicious user

GET ADVANCED INSIGHT & ALERTS WITH NC PROTECT'S MICROSOFT SENTINEL INTEGRATION

EASY TO INSTALL

The NC Protect Data Connector for Microsoft Sentinel is easy to install and configure directly from within the Microsoft Sentinel administration portal. Once configured and active in your Microsoft Sentinel instance, NC Protect data logs will flow into the pre-built workbooks (or your custom workbooks) for integration into your SIEM processes.



Above: The NC Protect Data Connector can be installed right from Microsoft Sentinel

OUT OF THE BOX INSIGHTS

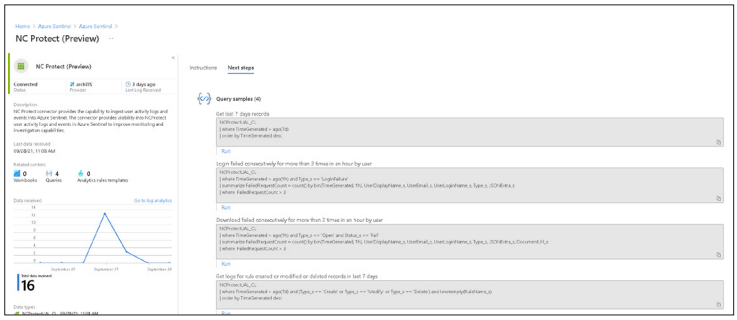
Integrating NC Protect's users activity logs with Microsoft Sentinel's reporting and visualization tools allows security officers to easily spot malicious activity and act accordingly.

The NC Protect Data Connector for Microsoft Sentinel comes with four ready to use queries, which allow you to analyze and understand user activity such as unsuccessful login attempts or download failures allowing administrators to gain better understanding of how users are behaving and serve as a starting point for investigation and alerts.

Prebuilt queries include:

- All data in last 7 days
- Login failed consecutively for more than 3 times in one hour by a user
- Downloads failed consecutively for more than 3 times in an hour by a user
- Get logs for policies created, modified or deleted in the last 7 days

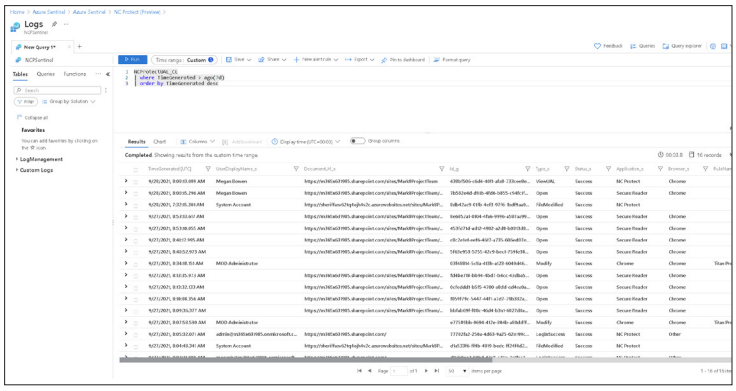
These queries are the basis of the prebuilt workbook that you can utilize out of the box, or use as a guide to building your own SIEM workbooks.



Above: The NC Protect Data Connector comes with ready to use sample queries, to jump start your auditing and analysis, and serve as a starting point for investigation and alerts.

TRIGGER ALERTS & REMEDIATION WORKFLOWS

Microsoft Sentinel enables administrators to analyze the raw log data provided by the NC Protect Data Connector to create reports and alerts that are vital for the active monitoring of digital access to the businesses digital assets in supported M365 applications. For example, set-up Sentinel alerts for suspicious access activity or blocked access to data in NC Protect to initiate further investigation in Microsoft Sentinel.



Above: Administrators can analyze raw data coming from NC Protect's user logs to create reports or alerts based on the scenarios that are most important to them.

REQUIREMENTS

A valid instance of NC Protect for Microsoft 365 is required in order use the NC Protect Data Connector for Microsoft Sentinel.

Get the NC Protect Data Connector for Microsoft Sentinel in Azure Marketplace here.

archTIS

archTIS.com | info@archtis.com Australia | United States | United Kingdom