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

***archTIS**

Microsoft Partner

Member of Microsoft Intelligent Security Association

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.

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.

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.

REQUIREMENTS

*archTIS

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

a (0+10)	Suides & Feedback () Refresh					
	117 Sensected					
guides	Search by name or provider Providers : All Data Types : All Status : All	III NC Protect (Preview)				
geneat	Status 1. Connector name 1.	Connected 24 archi15 (0.3 days ago				
	Interesting app security	Status Provider Last Log Receiv				
ks	Microsoft	Description				
	Microsoft Defender for Endpoint	NC Protect connector provides the capability to ingest user activity log events into Agure Sentinel. The connector provides visibility into NCPr				
ks		user activity logs and events in Azure Sentinel to improve monitoring investigation capabilities.				
havior	Microsoft Defender for identity	Last data received				
igence		09/28/21, 11:08 AM				
	Microsoft Defender for Office 365 (Preview) Microsoft	Related content				
a	Morphisec UTPP (Preview)					
	Morphisec	workbooks Queries wragets fores emplanes				
	NC Protect (Preview)	Data received Go to log a				
	and the second s					
040	Netskope (Preview)	12				
	Netskope					
	NGINX HTTP Server (Preview)					
	Nojinx Nojinx					
	NXLog BSM macOS (Preview) HoLog	September 25 September 27 Septe				
		16				
	NXLog DNS Logs (Preview) NRLog	110				
		Oata types				
	NXLog LinuxAudit (Preview) NoLog	NCProtectUAL_CL 09(28)(21, 11:08 AM				
	C Office 365					
	Office 365 Microsoft					

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

Home > Asure Sentinel > Asure Sentinel > NC Protect (Preview) ···						
III NC Protect (Preview)	Instructions Next streps					
Convected 21 architis © 2 days age Datus Provider Entring Received Description NC Protect conventor provides the capability to ingest user activity logs and	Construinter (a)					
event to Adva service. He survey private is stably avoid/funct investigation of advances. Landrase vocale stables (1) to Advances stables (1) to Advan	La La Ta Page 201 La La L					
Data monived Gan to log analysis 10 10 10 10 10 10 10 10 10 10	An An					
Superior 27 Superior 27 Superior 27 Superior 27	C - Lag for als much in a diff or Mind much is in T Age (1996) - Much (1997) - Much					

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.

Logs / ···									
P New Query 1* × +						0	reedback 😰 Querie	n 🕞 Query equ	Jore 👔
NCPSortinal	D Fun (Time range : Cue	tem 🜒 🔚 Sine 🗸 🕜 Share 🗸 🚽	New alertrule 🗸 🖙 Oport 🗸 🤌 Dinto debboard 🗇 D	loemat query					
Tables Queries Functions ···· < (P	KCP-VERCURE_CE Where TimeScreeneted Jonder by TimeScreene	> ego(2#) Joid desc							
favorites									
Tou can add favorites by clicking on the \$\overline\$ icon	Results Orant II Col	mmi 🗠 [I] Addoorkmark 🛛 🙆 Display	Stre (UTC=00.00) V (Oroup columns						
+ LogManagement	Completed. Showing results for	on the custom time range.						() 00.02.8 E	d 16 record
> Custom Loga	 TimeGenerated (UCQ) 	∇ UserCeplayName,s	7 Decement/H ₂	H.g V	Spile V	Pohis, a		V Brownes	∀ ≞
	> _ %/28/2021, 8:08:10.089	AM Meganilowen	https://w340a631985.dravepoint.com/sites;MarkBirojectReam	4385/505-c644-4011-a1a8-233ceelle	ViewUNL	Saccess	MC Protect	Chrome	
	> _ %28/2025 8.0035.296	AM Megan Dowen	https://m345a631985.abarepoint.com/abes/MarkiProjectReam/	18552e4d-d110-48d6-b855-c548c8	Open	Seccess	Secure Reader	Chrome	
	> _ %28/2025 23295.300	M System Account	$\label{eq:last_state} bitps://sheriifies/62tqtejhfv2c.asurevoloites.vet/sites/MarkIP_{\rm c}$	8db42ec9 01b 4ef3 92% 8d8ae5	Reflective	Seccess	AIC Protect		
	> _ %202020,#5338.602	rM	https://wilkiad/985.darepoint.com/sites/MafdItrojectleam/.	0005241404-040-9990-45813/99	Open	Saccess	Secure Reader	throme	
	> _ %27/2021, 0.53108.055	AM	https://w382a631985.abarepoint.com/sites/Ma68ProjectTeam/.	45352749422-0922-02483-001238	Open	Saccess	Secure Reader	Chrome	
	4/27/2021, 8:4812.005	AM	https://w382a631985.sharepcint.com/sites/MarkBirejectTeam/.	cll:2e1n1-ee15-4582-a735-605ed37n	Open	Secon	Secure Reader	Chrome	
	> _ %/27/2021, 8:4052.973	АМ	https://m345a601905.sharepoint.com/sites/MarkBhojet.floam/.	1940e93 5735-4249-beck 739fe8k	Open	Secces	Secure Reader	Chrome	
	> _ %/27/2021, 9.94.08.51.	M M00 Administrator		03518831-5c8a-4130-a/23-6043-8/6	Modily	Saccess	Chrome	Chrome	Y
	> _ %2//2021 #3835.913		https://wilklati/985.diarepoint.com/sites/MarkBirojectleam/.	594be718-0094-40d1-04cc-43dba5	Open	Saccess	Secure Reader	throme	
	> 1/27/2021, 0:0:32.03		https://w362a631985.abaropoint.com/abox/MarkBProjectRoam/	Ocfoddd1 b5/5-4700 a0dd od4or0a		Seccos	Secure Reader	Chrome	
	> 5/22/2021, 8:98:98.356		https://w38tats39905.sharepcint.com/sites/MarkBirejectReam/	859729c-5442-4481-a142-298382a	Open	Seccess	SecureReader	Cheome	
	× 0 5/27/2021 0.09/36/371		https://w385a631985.sharepoint.com/sites;MarkBrojectTeam/-	6666-691-80x-4688-63x1-682781x	Open	Saccess	Secure Reader	Chrome	
	> 0 %27/2021, 80758.580			e7758988-9694-412e-9848-4696897		Saccess	Chrome	Chrome	Y
	> _ %/27/2021, 8:05:32.07		https://m38ta631985.abarepcint.com/	17712142-2584-4463-9425-6211991		Seccess	NC PERMIT	Other	
	3 5/22/2020 8:04:48:341		http://sheriffan/52tplejhlv2c.anrowshoites.set/sites/MarkIP	d1d53266-8945-4335-beek 8248642	Redectified	Secon	N/C Protect		

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.

Get the NC Protect Data Connector for Microsoft Sentinel in Azure Marketplace <u>here</u>.

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

Copyright 2023 archTIS Limited. All rights reserved. archTIS, the archTIS logo and NC Protect logo are trademarks of archTIS Limited. Microsoft Sentinel and Microsoft are registered trademarks of Microsoft Corporation in the United States and/or other countries. All other product names mentioned herein are trademarks of their respective holders.