Trust In Tech Cologne

Data Analytics with Azure Sentinel and Microsoft Threat Protection

Christian Müller (@ChrisOnSecurity)

29. April 2020

About me

Christian Müller

Security Consultant @ infoWAN

Regensburg, Germany

@ChrisOnSecurity

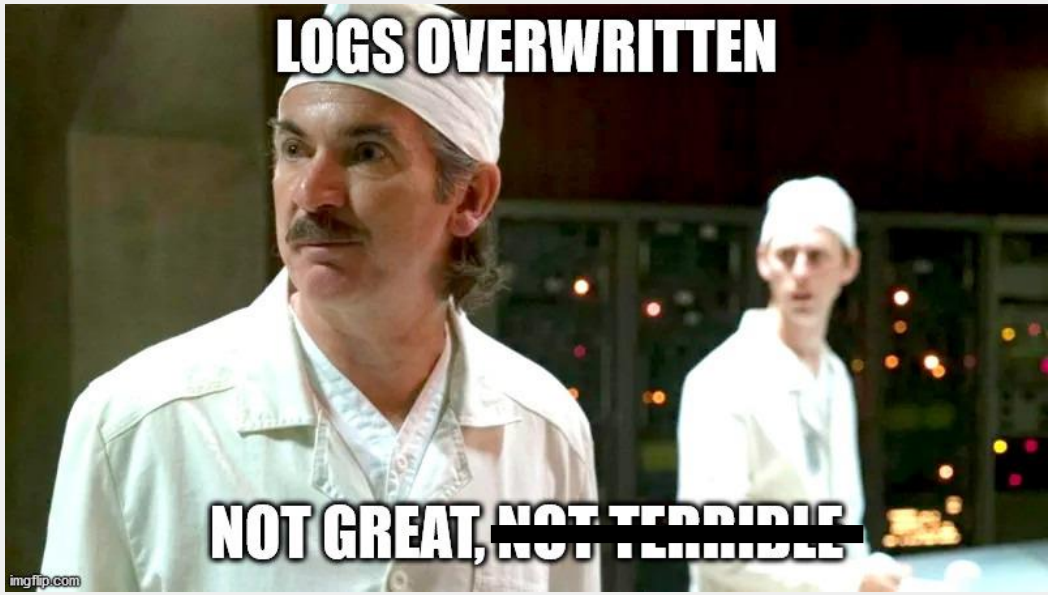
www.chrisonsecurity.net

Agenda

- Why data is so important for IT security
- Step 1: Collect all the things!
- Step 2: Closing the Microsoft 365 perimeter
- Step 3: I have all the data I wanted, what now?
- Closing

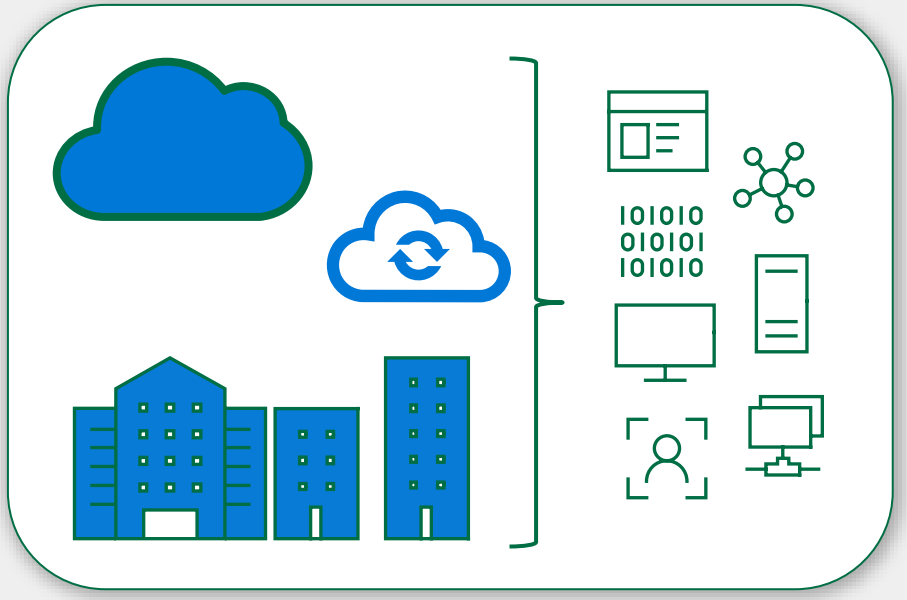
Why is data so important for IT security?

- Lost data can’t be restored in most cases
- You’re basically blind
- Being in this situation should be avoided
- No data = no investigation
- [I am not going to talk about compliance ;)]



Why is data so important for IT security?

Collect all the things!

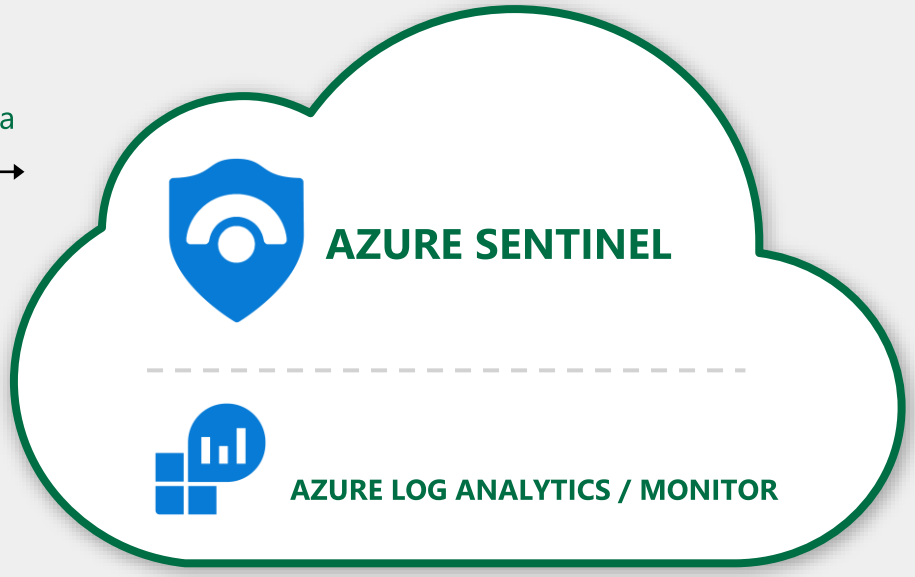


AZURE + MICROSOFT 365
Security Alerts, Activity & Audit Data

COLLECTORS
Windows, Linux, Syslog

TAXII + MS Graph
Threat Indicators & Graph API Calls

APIs
Custom Logs



Collect all the things! – Create Sentinel Workspace

ChrisOnSecurity

Home > Azure Sentinel workspaces

1

Azure Sentinel workspaces

Microsoft

+ Add Refresh

Home > Azure Sentinel workspaces > Choose a workspace to add to Azure Sentinel

Choose a workspace to add to Azure Sentinel

Search workspaces

+ Create a new workspace

2

Create Log Analytics workspace

Basics Pricing tier Tags Review + Create

3

With Azure logs, you can easily store, retain, and query your Azure and other resources for valuable insights and monitoring. Azure Logs workspace is the logical storage unit where your various logs are stored. Learn more

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * : Visual Studio Enterprise – MPN

Resource group * : rg-monitoring-vsempn

Create new

Instance details

Name * : DEMO-NAME

Region * : (Europe) West Europe

Basics Pricing tier Tags Review + Create

4

The cost of your workspace depends on the pricing tier and what solutions you use.
To learn more about Log Analytics pricing click here

Pricing tier

You can change to a Capacity Reservation tier after your workspace is created. Learn more
To learn more about access to legacy pricing tiers click here
To use Operations Management Suite entitlements choose "Per Node (OMS)".

Pricing tier * : Pay-as-you-go (Per GB 2018)

Pay-as-you-go (Per GB 2018)

Collect all the things! – Basics

ChrisOnSecurity

Search (Ctrl+/)

General
- Overview
- Logs
- News & guides

Threat management
- Incidents
- Workbooks
- Hunting
- Notebooks

Configuration
- Data connectors
- Analytics
- Playbooks
- Community
- Settings

Refresh

39 Connectors | 11 Connected | 1 Coming soon

Search by name or provider | PROVIDERS : Microsoft | DATA TYPES : All

Status	Connector name
	Azure Active Directory Microsoft
	Azure Active Directory Identity Protection Microsoft
	Azure Activity Microsoft
	Azure Advanced Threat Protection (Preview) Microsoft
	Azure Security Center Microsoft
	Microsoft Cloud App Security Microsoft
	Microsoft Defender Advanced Threat Protection (Preview) Microsoft
	Office 365 Microsoft
	Security Events Microsoft
	Threat Intelligence Platforms (Preview) Microsoft
	Windows Firewall

Azure Active Directory

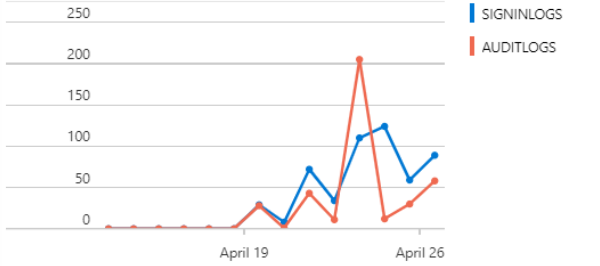
Connected (Status) | Microsoft (Provider) | 34 minutes ago (Last Log Received)

Description
Gain insights into Azure Active Directory by connecting Audit and Sign-in logs to Azure Sentinel to gather insights around Azure Active Directory scenarios. You can learn about app usage, conditional access policies, legacy auth relate details using our Sign-in logs. You can get information on your Self Service Password Reset (SSPR) usage, Azure Active Directory Management activities like user, group, role, app management using our Audit logs table.

Last data received
04/27/20, 01:45 PM

Related content
3 Workbooks | 2 Queries | 21 Analytic rules templates

Data received — Go to log analytics



Total data received 525 | Total data received 388

Open connector page

Collect all the things! – I want more data

ChrisOnSecurity

log-cos-unified...
Log Analytics workspace

Search (Ctrl+/)

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems

Settings

- Locks
- Export template
- Advanced settings

General

- Quick Start
- Workspace summary
- View Designer
- Workbooks
- Logs
- Solutions
- Saved searches
- Pricing tier
- Usage and estimated costs
- Properties
- Service Map

Workspace Data Sources

- Virtual machines
- Storage accounts logs

Advanced settings

log-cos-unified4sentinel

Refresh Logs

- Connected Sources
- Data
- Computer Groups

- Windows Servers
- Linux Servers
- Azure Storage
- System Center

Windows Servers

Attach any Windows server or client.

4 WINDOWS COMPUTERS CONNECTED

Download Windows Agent (64 bit) Download Windows Agent (32 bit)

You'll need the Workspace ID and Key to install the agent.

WORKSPACE ID

PRIMARY KEY

Regenerate

SECONDARY KEY

Regenerate

OMS Gateway

If you have machines with no internet connectivity to OMS, download the OMS Gateway to act as a proxy. Learn more.

Download OMS Gateway

Collect all the things! – I want more data

ChrisOnSecurity

Microsoft Edge

Administrator: Windows PowerShell

```
PS C:\temp> .\MMASetup-AMD64.exe /qn NOAPM=1 ADD_OPINSIGHTS_WORKSPACE=1 OPINSIGHTS_WORKSP
ACE_AZURE_CLOUD_TYPE=0 OPINSIGHTS_WORKSPACE_ID="############################" OPINSIGHTS
_WORKSPACE_KEY="############################" AcceptEndUserLicenseAgreement=1
```

Command line

Microsoft Monitoring Agent Setup

Azure Log Analytics

Connect the agent to an Azure Log Analytics workspace.

GUI

Workspace ID: ############################

Workspace Key: ••••••••••••••••••••••••••••••••

Azure Cloud: Azure Commercial

Your workspace ID and key are available within the Azure Log Analytics portal. The Log Analytics portal for Azure Commercial is at https://www.microsoft.com/oms/.

Click Advanced to provide HTTP proxy configuration.

Advanced

When you click Next, these properties will be validated by the Azure Log Analytics service.

< Back | Next > | Cancel

Collect all the things! – I want more data

ChrisOnSecurity

Microsoft Edge

Administrator: Windows PowerShell

```
PS C:\temp\Sysmon> .\Sysmon64.exe -i .\sysmonconfig-export.xml -accepteula

System Monitor v10.42 - System activity monitor
Copyright (C) 2014-2019 Mark Russinovich and Thomas Garnier
Sysinternals - www.sysinternals.com

Loading configuration file with schema version 4.22
Sysmon schema version: 4.23
Configuration file validated.
Sysmon64 installed.
SysmonDrv installed.
Starting SysmonDrv.
SysmonDrv started.
Starting Sysmon64..
Sysmon64 started.
PS C:\temp\Sysmon>
```

Sysmon

File Home Share View

This PC > Windows (C:) > temp > Sysmon

Search Sysmon

Name	Date modified	Type	Size
Eula.txt	4/27/2020 2:50 PM	Text Document	8 KB
Sysmon.exe	4/27/2020 2:50 PM	Application	3,626 KB
Sysmon64.exe	4/27/2020 2:50 PM	Application	1,972 KB
sysmonconfig-export.xml	4/27/2020 2:54 PM	XML Document	112 KB

Quick access
Desktop
Downloads
Documents
Pictures
Sysmon
temp
This PC
Network

4 items

Sysmon v11.0

04/28/2020 • 13 minutes to read •

By Mark Russinovich and Thomas Garnier

Published: April 28, 2020

Download Sysmon **(1.7 MB)**

Collect all the things! – Get diagnostics

ChrisOnSecurity

Home > Microsoft Intune | Diagnostics settings

Microsoft Intune | Diagnostics settings

Search (Ctrl+/)

- Device configuration
- Device security
- Devices
- Client apps
- E-books
- Conditional access
- Exchange access
- Users
- Groups
- Roles
- Software updates
- Reports
- Policy sets

Monitoring

- Diagnostics settings
- Audit logs

Refresh Provide feedback

Diagnostic settings are used to configure streaming export of platform logs and metrics for a resource to the destination of your choice. You may create up to five different diagnostic settings to send different logs and metrics to independent destinations. Learn more about diagnostics settings

Diagnostics settings

Name	Storage account	Event hub	Log Analytics workspace	Edit setting
DefaultDiagnostics	-	-	log-cos-unified4sentinel	Edit setting

+ Add diagnostic setting

Click 'Add Diagnostic setting' above to configure the collection of the following data:

- AuditLogs
- OperationalLogs
- DeviceComplianceOrg

Diagnostic settings name DefaultDiagnostics

Category details

log

- [x] AuditLogs
- [x] OperationalLogs
- [x] DeviceComplianceOrg

Destination details

- [x] Send to Log Analytics

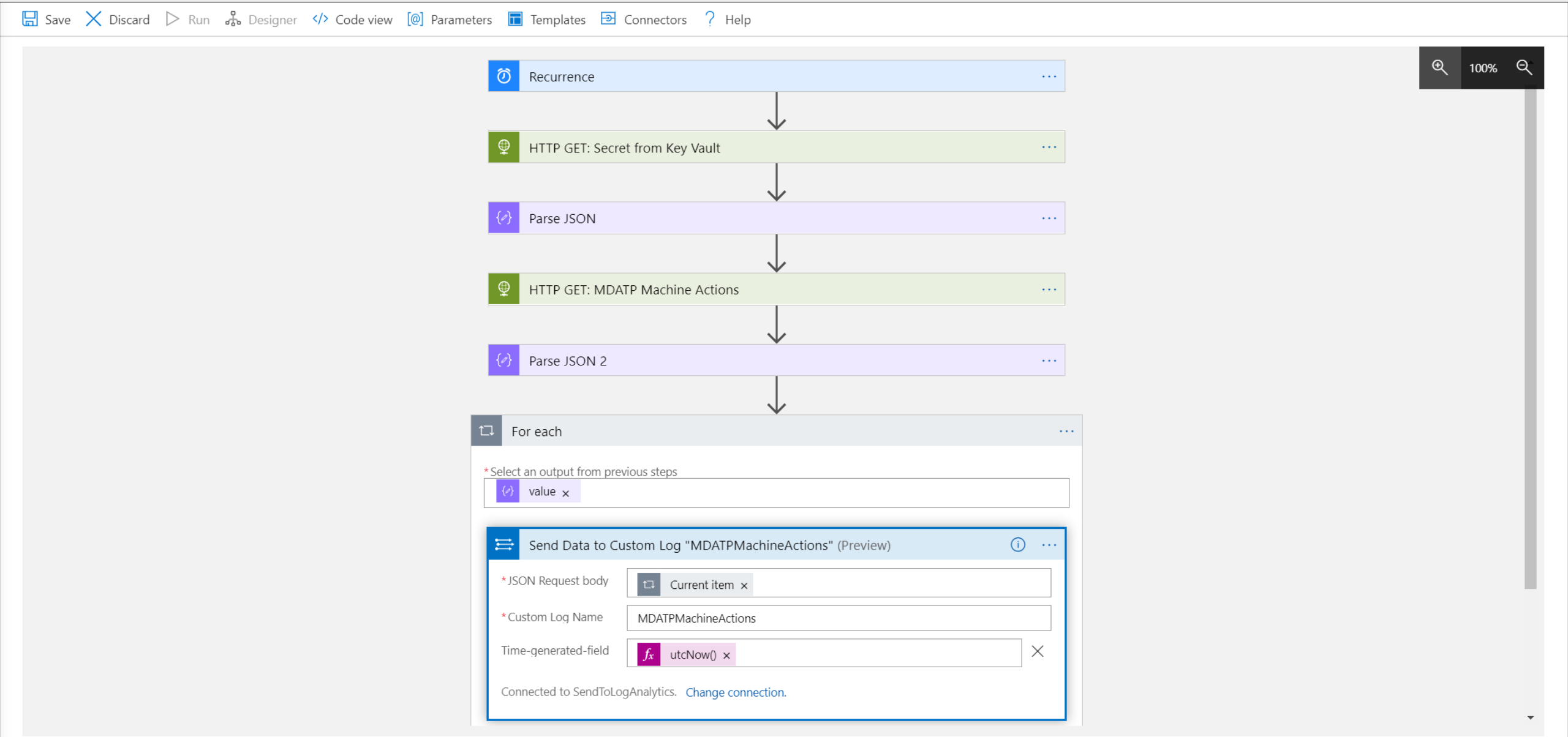
Subscription: Visual Studio Enterpri...

Log Analytics workspace: log-cos-unified4senti...

- [ ] Archive to a storage account
- [ ] Stream to an event hub

Collect all the things! – Ingest other data via Logic Apps

ChrisOnSecurity



Collect all the things! – Ingest other data via Logic Apps

DEMO

M365: Closing the perimeter

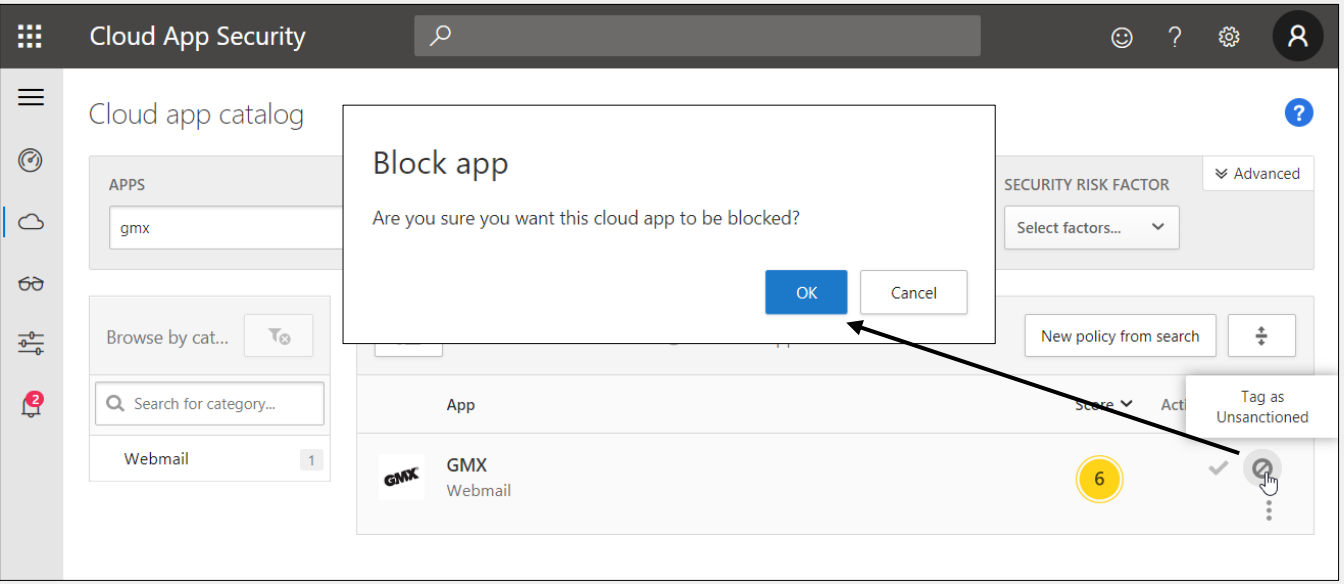
- Azure AD / OAuth2.0 apps can be secured via Conditional Access and MCAS Session Control to prevent data leakage
- But what about:
  - other cloud apps (Dropbox, web mailer, etc.)?
  - USB exfiltration?

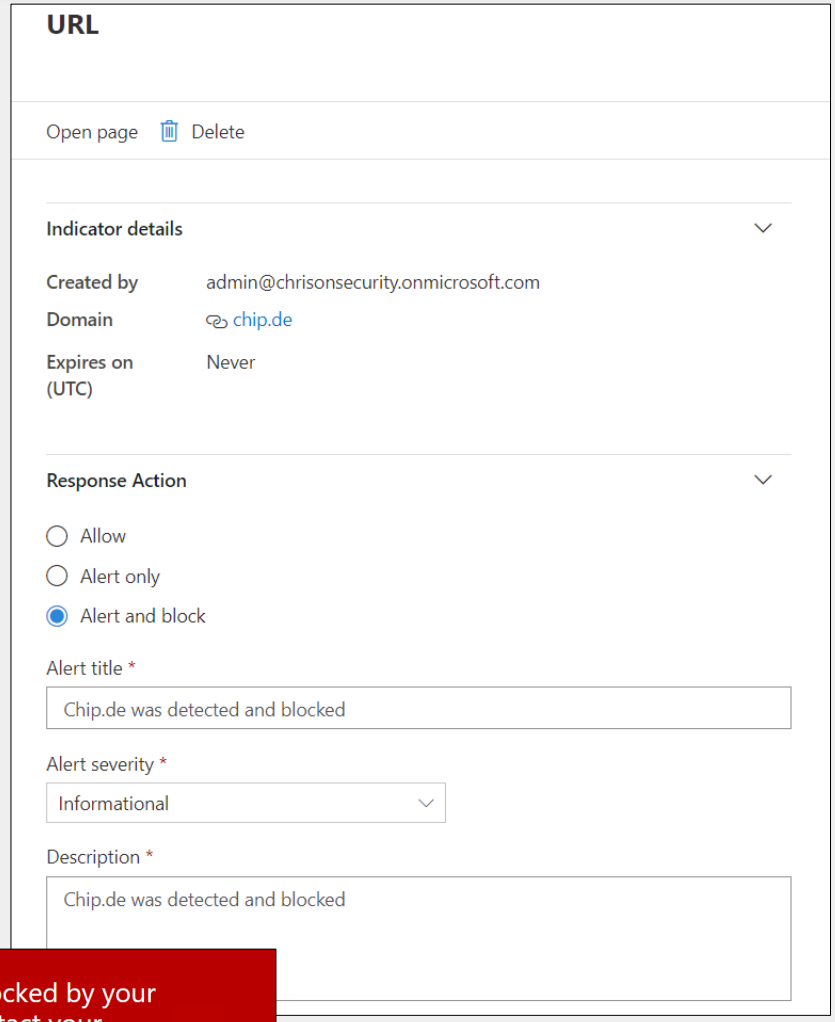
M365: Closing the perimeter for other cloud apps

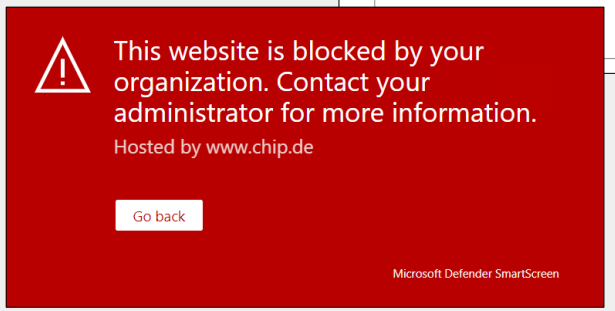
ChrisOnSecurity

How: MCAS cloud discovery + MDATP

- MCAS syncs to MDATP which enforced blocking
- Missing apps can be blocked with custom MDATP indicators





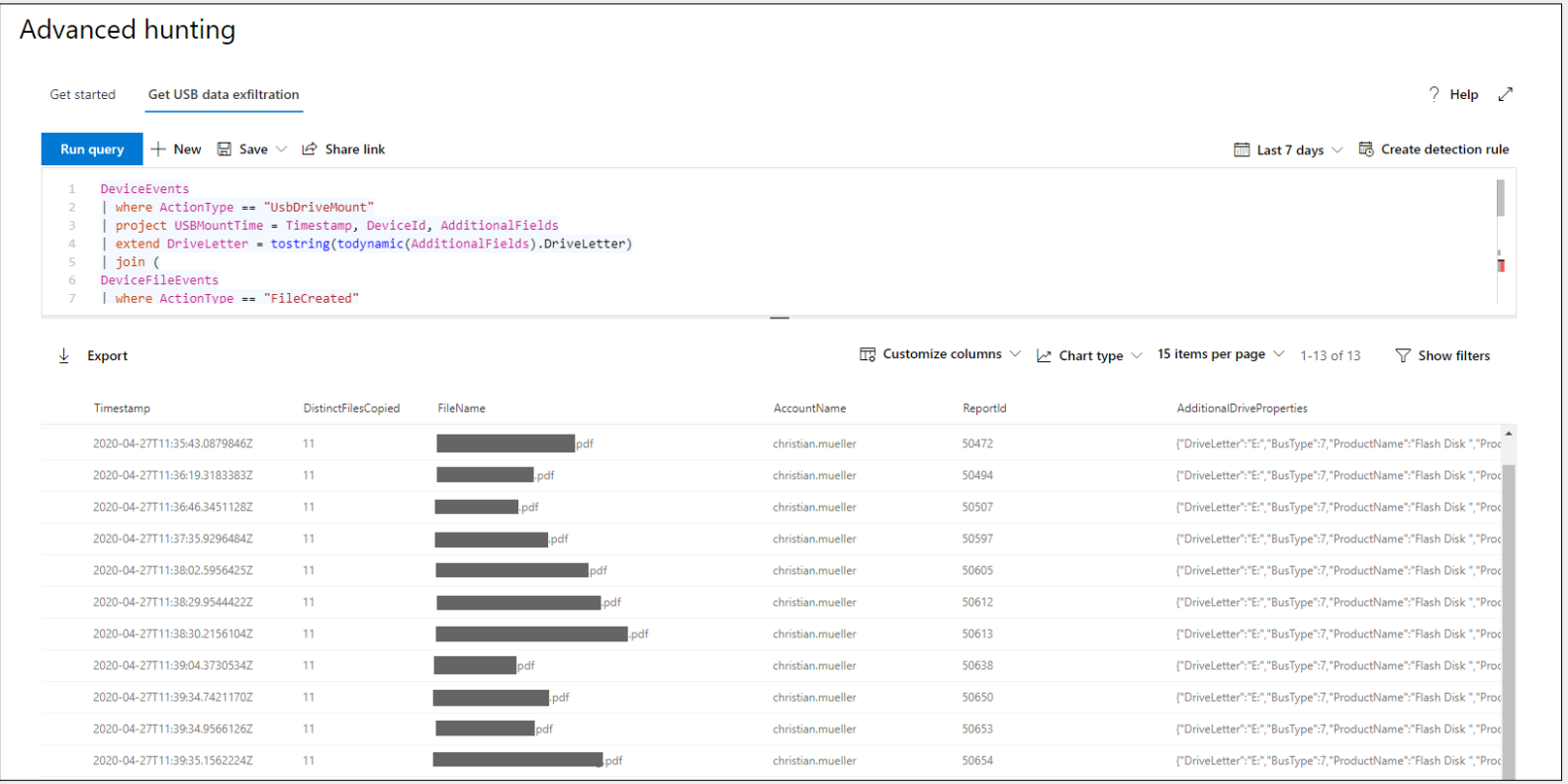


M365: Closing the perimeter for USB exfiltration

ChrisOnSecurity

How: MDATP

- MDATP offers various file and device events
- No active blocking at the moment but alerting




```
DeviceEvents
| where ActionType == "UsbDriveMount"
| project USBMountTime = Timestamp, DeviceId, AdditionalFields
| extend DriveLetter = tostring(todynamic(AdditionalFields).DriveLetter)
| join (
DeviceFileEvents
| where ActionType == "FileCreated"
| where FileName endswith ".docx" or FileName endswith ".pptx" or
FileName endswith ".pdf"
| parse FolderPath with DriveLetter '\\' *
| extend DriveLetter = tostring(DriveLetter)
)
on DeviceId, DriveLetter
| where (Timestamp - USBMountTime) between (0min .. 15min)
| summarize DistinctFilesCopied = dcount(SHA1),
Events=makeset(pack("AccountName", InitiatingProcessAccountName,
"Timestamp", Timestamp, "ReportId", ReportId, "FileName", FileName,
"AdditionalDriveProperties", AdditionalFields)) by DeviceId,
bin(Timestamp, 15m)
| where DistinctFilesCopied > 10
| mv-expand Events
| extend Timestamp = Events.Timestamp, FileName = Events.FileName,
AccountName = Events.AccountName, ReportId = Events.ReportId,
AdditionalDriveProperties = Events.AdditionalDriveProperties
```

I have all the data I wanted, what now?

- Parse data that is not yet useable
- Decide which information should be visualized
- Try to evaluate which data sets are stored for retention vs. immediate benefit
- While most can be stored over a longer period for future investigations, some events should trigger alerts / incidents / automated actions
- M365 and Sentinel Analytics trigger incidents per default
- Other sources require manual tasks

Parsing (Sysmon) events

ChrisOnSecurity

- Often data sources must be parsed for easier data management
- Those KQL queries can be saved as functions for easy re-use
- Sysmon parser: Azure Sentinel @ Github / sentinel-attack by BlueTeamLabs

All services > Azure Sentinel workspaces > Azure Sentinel | Logs

Azure Sentinel | Logs
Selected workspace: 'log-cos-unified4sentinel'

Sysmon*

log-cos-unified4sentinel | Run | Time range : Last 24 hours | Save | Copy link | New alert rule | Export | Pin to dashbo | Example queries | Query explorer

Tables | Filter

Search

Group by: Solution Filters: not s

- AuditLogs
- Informati...
- IntuneAu...
- Perf
- Protectio...
- SecurityA...
- SecurityE...
- SigninLogs
- Update
- UpdateS...
- LogManagement
- Security and Audit
- SecurityInsights
- SQL Advanced Threa...

```
let timeframe = "{time_range}";
let EventData = Event
| where Source == "Microsoft-Windows-Sysmon"
| extend RenderedDescription = tostring(split(RenderedDescription, ":")[0])
| project TimeGenerated, Source, EventID, Computer, UserName, EventData, RenderedDescription
| extend EvData = parse_xml(EventData)
| extend EventDetail = EvData.DataItem.EventData.Data
| project-away EventData, EvData
;
```

Results | Chart | Columns | Add bookmark | Display time (UTC+02:00)

Completed. Showing partial results from the last 24 hours.

Drag a column header and drop it here to group by that column

TimeGenerated [Local Time]	RenderedDescription	event_creation_time	process_guid	process
4/28/2020, 1:01:03.047 PM	Process Create	2020-04-28T11:01:03.0430000Z	{7e28e3c1-0cef-5ea8-0000-00108adbf904}	6496
4/28/2020, 1:07:36.347 PM	Process Create	2020-04-28T11:07:36.3430000Z	{7e28e3c1-0e78-5ea8-0000-001039effc04}	3752
4/28/2020, 1:07:50.020 PM	Process Create	2020-04-28T11:07:50.0120000Z	{7e28e3c1-0e86-5ea8-0000-0010fdfdfc04}	6708
4/28/2020, 1:07:50.023 PM	Process Create	2020-04-28T11:07:50.0210000Z	{7e28e3c1-0e86-5ea8-0000-001071fefc04}	5584
4/28/2020, 1:08:06.583 PM	Process Create	2020-04-28T11:08:06.5790000Z	{7e28e3c1-0e96-5ea8-0000-0010762efd0...	4716

Page 1 of 200 | 50 items per page

Save

Name *
Sysmon

Save as
Function

Function Alias *
Sysmon

Save this query as a computer group

Category *
Activity

Save | Cancel

Parsing & visualization (Perfmon / Sysmon / MDATP / Updates)

DEMO

Monitoring heartbeat for data persistence

ChrisOnSecurity

All Agent Heartbeat info : Last 30 days

Computer	State	Environm...	OS	Azure Resource	Time	Heartbeat Trend
DESKTOP-B054GJQ	Unhealthy	Direct Agent	Windows		6 days ago	
DESKTOP-B054GJQ.chrisonsecurity.local	Unhealthy	Direct Agent	Windows		6 days ago	
COS-DC01.chrisonsecurity.local	Healthy	Direct Agent	Windows		0 seconds ago	
COS-HCL01.chrisonsecurity.local	Healthy	Direct Agent	Windows		0 seconds ago	
COS-CCL01	Healthy	Direct Agent	Windows		0 seconds ago	
COS-PCL01	Healthy	Direct Agent	Windows		0 seconds ago	

log-cos-unified4sentinel Status for Last 24 hours, Billable Tables have an average use of: 0.1 GiB per day

Search

Table Name	Table Entries	Table Size	Size per Entry	IsBillable	Last Record Received	Estimated Table Price
SecurityEvent	120.766I	134.398I	1.14KiB	True	32s	0
Event	15.907K	34.998M	2.25KiB	True	7s	0
Perf	115.085I	26.123M	238.02B	True	56s	0
AzureActivity	1.021K	1.257Mil	1.26KiB	False	19mins	0
Heartbeat	2.753K	1.251Mil	476.4B	False	17s	0
SecurityAlert	59	385.769I	6.54KiB	False	2.8hr	0

(Source: https://techcommunity.microsoft.com/t5/azure-sentinel/usage-reporting-for-azure-sentinel/ba-p/1267383)

Custom alerts & incidents

Other use cases for alerting:

- Alert on (suspicious) Active Directory changes
- Alert on systems under high load
- Alert on unresponsive systems
- Map external TI with Sysmon DNS / IP queries
- …

Alerting & response

DEMO

Useful links and references

- Become an Azure Sentinel Ninja: The complete level 400 training by Ofer Shezaf
- https://github.com/Azure/Azure-Sentinel
- Creating digital tripwires with custom threat intelligence feeds for Azure Sentinel
- Usage reporting for Azure Sentinel by Clive Watson
- Sysmon parser: Azure Sentinel @ Github / sentinel-attack by BlueTeamLabs
- Using KQL functions to speed up analysis in Azure Sentinel
- https://getshitsecured.com/2020/04/28/kusto-query-internals-azure-sentinel-reference/ by Huy
- https://github.com/SwiftOnSecurity/sysmon-config
- https://docs.microsoft.com/en-us/azure/sentinel/fusion

What we discussed today…

Thank you!