

ATT&CKing the Sentinel

Deploying a threat hunting capability on Azure Sentinel using Sysmon
and MITRE ATT&CK



Hi there!




Edoardo Gerosa

Vigilant Service Lead @ Deloitte AG

Consulted at banks, pharmaceuticals and tech companies

 @netevert

 github.com/netevert

 edoardogerosa@deloitte.ch



Olaf Hartong

Blue Team Specialist Leader @ Deloitte NL

Consulted at banks, educational institutions and governmental organisations

 @olafhartong

 github.com/olafhartong

 ohartong@deloitte.nl

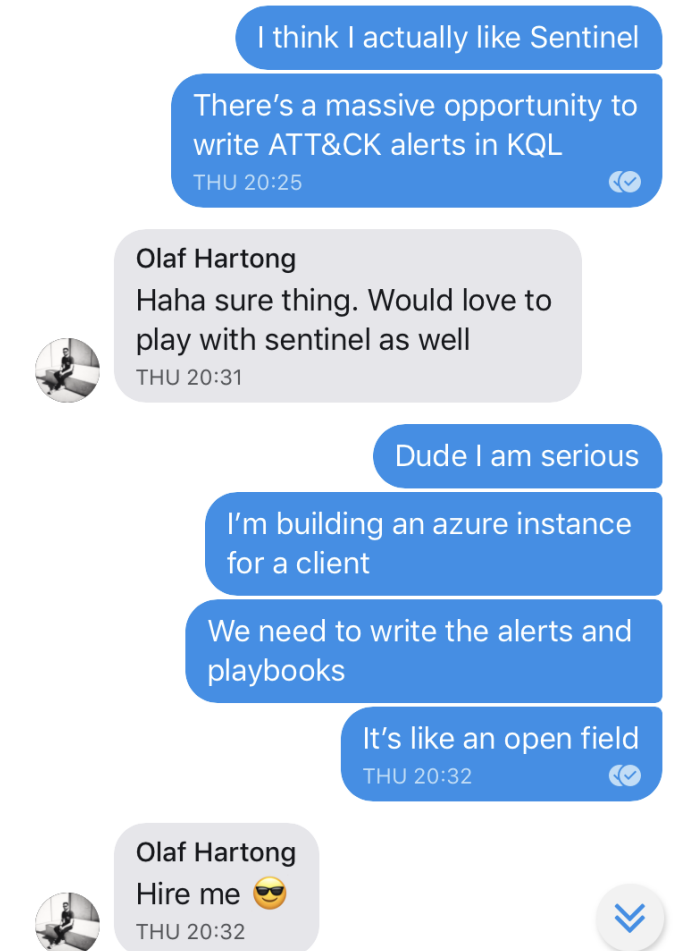
Before we start

- DISCLAIMER: The tool presented is not a magic bullet. It will require tuning and real investigative work to be truly effective in your environment
- Sentinel is still in public preview ... much will change in the coming year
- Although we will talk about limitations of Sentinel in a threat hunting context, Microsoft has been proactive in reaching out to us to collect feedback ... credit where due
- We are not Azure Sentinel experts, we likely cannot answer all questions about the platform itself

What are we talking about

We'd like to share a tale of discovery and experimentation...

(which began with a misunderstanding)



What are we talking about

...that ended in yet another GitHub project

Sentinel ATT&CK aims to simplify the rapid deployment of a threat hunting capability that leverages Sysmon and MITRE ATT&CK on Azure Sentinel

Why?

- The Endpoint is often used as an entry point into a network, whether it lives in the cloud or on-prem
- Endpoint Detection & Remediation (EDR) solutions are great, however often quite costly
- There is an alternative approach to the detection aspect, using an adversarial framework
- It allows you to leverage a data platform that is easy to deploy and, out of the box, quite powerful

Project background

Sentinel-ATT&CK borrows ideas from successful threat hunting projects

 [sysmon-modular](#)

A repository of sysmon configuration modules

● PowerShell ★ 510 🍴 78

- A Sysmon configuration repository, set up in a modular fashion for easy maintenance
- Helps generate tailored configurations
- Mapped to the MITRE ATT&CK framework
- Frequently updated based on threat reports or new attacker techniques

 [ThreatHunting](#)

A Splunk app mapped to MITRE ATT&CK to guide your threat hunts

● Python ★ 340 🍴 50

- Splunk App providing an investigative workflow approach for Threat Hunters
- Based on ML (Mandatory Learning) to help hunters to get to know their environment
- No false positives are assumed, just triggers
- Supplies the user with tools to contextualise and investigate these events

MITRE ATT&CK

A lightning overview

“ A framework for describing the behaviour of cyber adversaries operating within enterprise networks ”



- Comprehensive library of "what to look for"
- Threat model & framework
- Library of attacker activity (TTPs) covering 245 techniques
 - Windows: 211
 - Linux: 126
 - Mac: 145






Found @ <https://attack.mitre.org>

Sysmon

Another lightning overview

- Sysmon is a free, powerful host-level tracing tool, developed by a small team of Microsoft employees
- Initially developed for internal use at Microsoft
- Sysmon uses a device driver and a service that runs in the background and loads early in the boot process
- Monitors 22 events ranging from process creation, file timestamp changes, network connections, registry events and DNS events

Sysmon v10.2

06/28/2019 • 13 minutes to read •     

By **Mark Russinovich** and **Thomas Garnier**

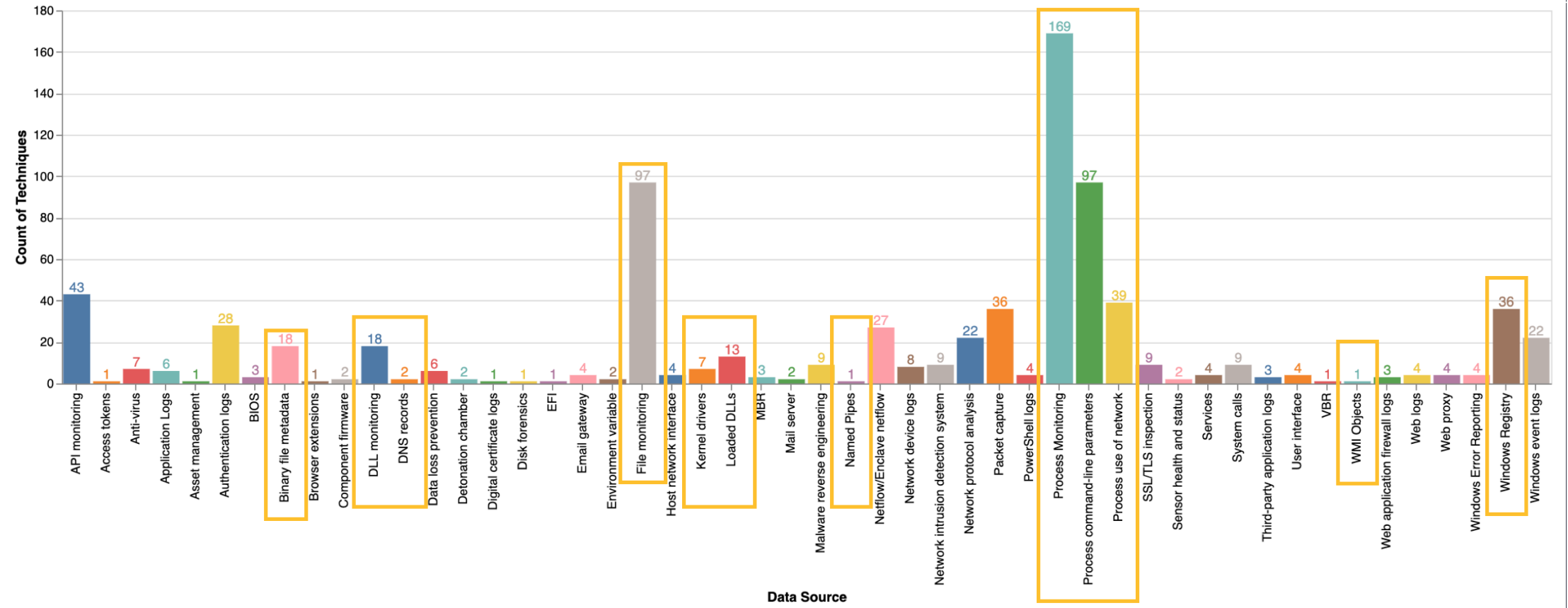
Published: June 28, 2019



[Download Sysmon](#) (1.4 MB)

Why combine ATT&CK and Sysmon

12 ATT&CK data sources can be collected with Sysmon



Project background

Armed with these ideas we began experimenting

(with not a lot of success)

#general
☆ | 👤 9 | 🔒 0 | Welcome

netevert 10:52 PM


there's one thing that is bothering me
Kevin runs the hunting query
it looks for processes
finds the calc.exe
so it should easily find our cscript.exe
i think we must've **BEEP!** some configuration

olafhartong 10:53 PM

yep
should parse it, now it doesnt

ragequit

Posted using /giphy (1 MB) ▾



I'm going to bed. Trying again tomorrow 😊


#general
☆ | 👤 9 | 🔒 0 | Welcome

netevert 10:40 PM

image.png ▾

NetEver @netevert · 10h

It's out! POCKINT: A portable OSINT Swiss professionals
github.com/netevert/pockint
Looking forward to the feedback and gaug repo 🙌
#DFIR #ThreatHunting #threatintel #infosec #osint #tools



Maarten Goet

@maarten_goet
MVP since 07 & RD since '15, CEH, CISSP, f @conviso, Speaker. Loving #Azure & maartengoet.org

netevert 10:46 PM

what the **BEEP!**
Kevin is running a threat hunti

olafhartong 10:46 PM

yeah, there aren't that many se

+ Message #general

netevert 10:26 PM

yeah
i just ran the query
myself too
it derped
yeah
BEEP!
image.png ▾

Run

Time range: Last 24 hours

SecurityEvent
| where ProcessId contains "1148"

Completed. Showing results from the last 24 hours.

TABLE CHART

NO RESULTS FOUND (last 24 hours)

0 records watched for the selected time range

Need Help?
• [Select another time range.](#)
• [Add a custom time filter to your query.](#)

I refuse to believe that sysmon isn't properly parsed
we're doing something wrong

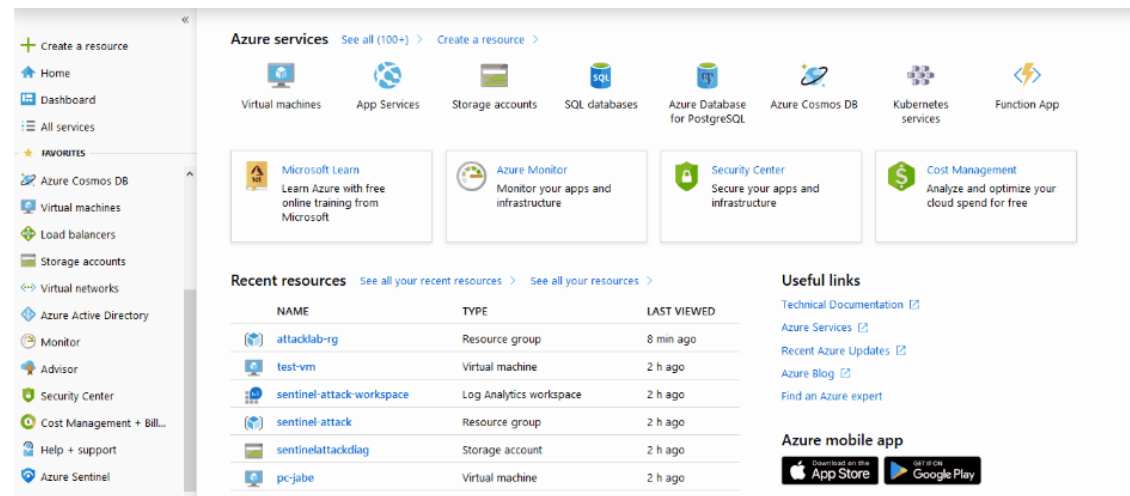
olafhartong 10:33 PM

well looks like it is

The platform

First impressions

Super fast deployment ... goodbye 4-month SIEM implementation projects



The platform

Azure Sentinel contains a number of excellent features

1. An easy-to-use query language

- Kusto Query Language (KQL)
- Read only
- Used to access and query log analytics workspaces via API or Web App

2. Incident grouping

- Grouping over time periods (default 24h)
- Incident grouping by case with Sentinel Fusion to reduce alert fatigue
- Ability to bake your own organisation's machine learning models

3. Threat response automation with Logic Apps

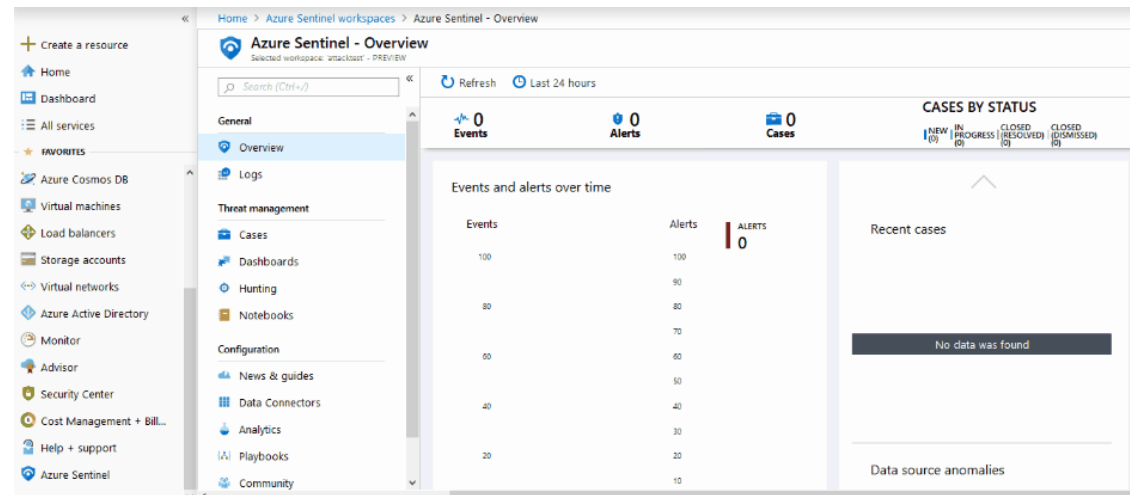
- Large amount of connectors (SNOW, Jira, Outlook, AD etc.)
- Ability to develop custom connectors
- Easy to use playbook designer

The problem

Setting up an ATT&CK-based hunting capability is not straightforward

Two aspects currently stand in the way:

1. Limited log onboarding documentation, with Sysmon/Operational logs currently being hidden



The problem

Setting up an ATT&CK-based hunting capability is not straightforward

2. By default Sysmon log data is unparsed and presented as XML

Completed. Showing results from the last 7 days. 00:00:09.734 2689 records Display time (UTC+02:00)

TABLE CHART Columns

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

TimeGenerated [Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna]	Source	EventLog	Computer	EventCategory	EventLevel	EventLevelName	UserName	Message
EventLevelName	Information							
UserName	NT AUTHORITY\SYSTEM							
ParameterXml	<Param> technique_id=T1089,technique_name=Disabling Security Tools,phase_name=Defense Evasion</Param><Param> 2019-07-28 18:17:05.776</Param><Param> {883D9709-E6A1-5D3D-0000-0010C4220601}</Param><Param> 10036</Param><Param> C:\ProgramData\Microsoft\Windows Defender\Platform							
EventData	<DataItem type="System.XmlData" time="2019-07-28T18:17:05.8171196+00:00" sourceHealthServiceId="26F39B2F-1B0F-13F3-1032-BCE61BE3A88F"><EventData xmlns="http://schemas.microsoft.com/win/2004/08/events/event"><Data Name="RuleName">technique_id=T1089,technique_na							
EventID	1							
RenderedDescription	Process Create: RuleName: technique_id=T1089,technique_name=Disabling Security Tools,phase_name=Defense Evasion UtcTime: 2019-07-28 18:17:05.776 ProcessGuid: {883D9709-E6A1-5D3D-0000-0010C4220601} ProcessId: 10036 Image: C:\ProgramData\Microsoft\Windows Defender\Platform							
MG	00000000-0000-0000-0000-000000000001							
ManagementGroupName	AOI-3351a890-c19e-45c7-ad84-6ad12fb580ff							
Type	Event							
_ResourceId	/subscriptions/86ddb844-4026-4cd2-903a-b5c8ffdaeb80/resourcegroups/sentinel-attack/providers/microsoft.compute/virtualmachines/test-vm-2							
2019-07-28T20:17:06.023	Microsoft-Windows-Sysmon	Microsoft-Windows-Sysmon/Operational	test-vm-2	1	4	Information	NT AUTHORITY\SYSTEM	
2019-07-28T20:17:06.112	Microsoft-Windows-Sysmon	Microsoft-Windows-Sysmon/Operational	test-vm-2	1	4	Information	NT AUTHORITY\SYSTEM	

... a parser is provided by Microsoft, but does not map to a datamodel

Other observations

Overview of additional observations made while experimenting

Additionally we identified the following two ATT&CK-specific gaps:

- No available dashboards leveraging ATT&CK
- No ATT&CK-based threat hunting notebooks

Other observations:

- Limited documentation
- Some features are (for the moment) hidden, like automated playbook execution and case grouping
- Advanced hunting features require some advanced skills (Python, Jupyter and data science modules)
- Inability to bulk import detection rules, it's a highly manual process
- IAM controls not available (yet), anybody added to the workspace can access everything
- Cannot drill down from dashboards

The solution

Do it yourself!

An overview of the repository – found @ <https://github.com/BlueTeamToolkit/sentinel-attack> - PRs welcome!

Branch: defcon

New pull request

Create new file

Upload files

Find File

Clone or download

This branch is 45 commits ahead, 12 commits behind master.

Pull request


Compare

netevert Update README.md

Latest commit 798b689 35 minutes ago

dashboards	Add files via upload	6 days ago
detections	Update T1216_Signed_Script_Proxy_Execution.txt	4 days ago
docs	minor fix	12 days ago
guides	Update Sysmon-onboarding-quickstart.md	11 days ago
hunting	added 20 detections	2 months ago
lab	Update install-utilities.ps1	4 days ago
parsers	Update Sysmon-OSSEM.txt	6 days ago
.gitignore	added lab and guides	12 days ago
README.md	Update README.md	35 minutes ago
sysmonconfig.xml	Update sysmonconfig.xml	4 days ago

README.md



maintained

yes

last commit

july

PRs

welcome

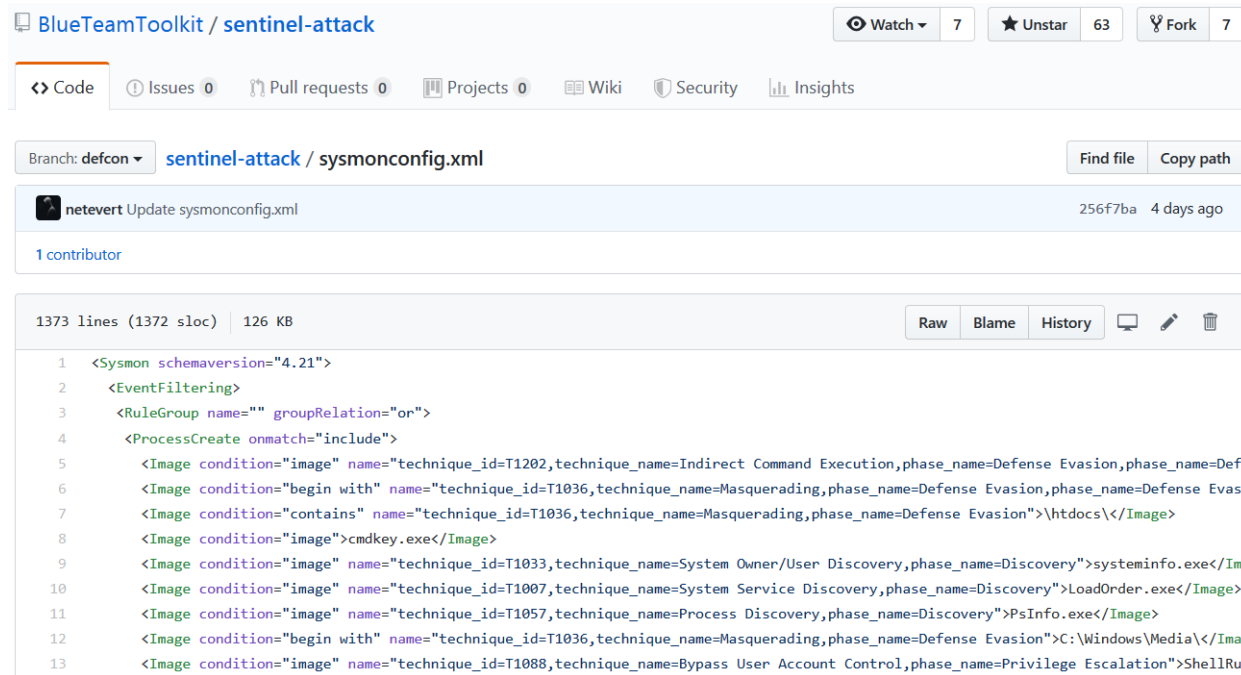
2019

DEF CON 27

Sysmon configuration

Sysmon can be configured to monitor for specific ATT&CK techniques

An XML configuration file is provided to configure Sysmon to collect specific ATT&CK technique data



The screenshot shows the GitHub interface for the `BlueTeamToolkit / sentinel-attack` repository. The file `sysmonconfig.xml` is selected, showing its commit history and content. The file is 1373 lines (1372 sloc) and 126 KB. The commit was made by `netever` 4 days ago. The XML content is as follows:

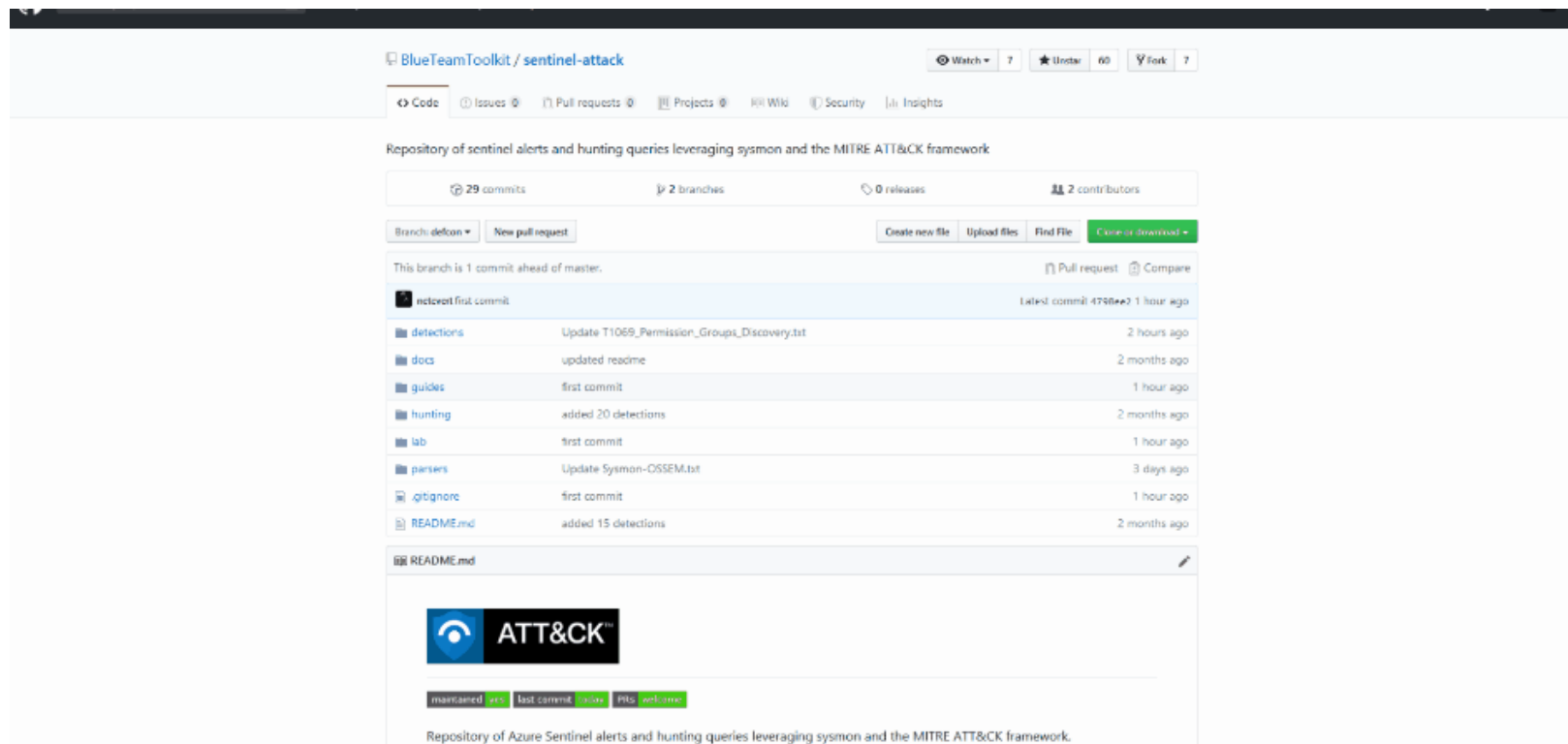
```
1 <Sysmon schemaversion="4.21">
2   <EventFiltering>
3     <RuleGroup name="" groupRelation="or">
4       <ProcessCreate onmatch="include">
5         <Image condition="image" name="technique_id=T1202,technique_name=Indirect Command Execution,phase_name=Defense Evasion,phase_name=Def
6         <Image condition="begin with" name="technique_id=T1036,technique_name=Masquerading,phase_name=Defense Evasion,phase_name=Defense Evas
7         <Image condition="contains" name="technique_id=T1036,technique_name=Masquerading,phase_name=Defense Evasion">\htdocs</Image>
8         <Image condition="image">cmdkey.exe</Image>
9         <Image condition="image" name="technique_id=T1033,technique_name=System Owner/User Discovery,phase_name=Discovery">systeminfo.exe</Im
10        <Image condition="image" name="technique_id=T1007,technique_name=System Service Discovery,phase_name=Discovery">LoadOrder.exe</Image>
11        <Image condition="image" name="technique_id=T1057,technique_name=Process Discovery,phase_name=Discovery">PsInfo.exe</Image>
12        <Image condition="begin with" name="technique_id=T1036,technique_name=Masquerading,phase_name=Defense Evasion">C:\Windows\Media\</Ima
13        <Image condition="image" name="technique_id=T1088,technique_name=Bypass User Account Control,phase_name=Privilege Escalation">ShellRu
```

The configuration file is easily installed with the command: “sysmon -c sysmonconfig.xml”

Sysmon parsing in Sentinel

How to parse Sysmon logs in Sentinel

Sentinel-ATT&CK provides a dedicated parser that maps log fields against the OSSEM log standard, found @ <https://github.com/Cyb3rWard0g/OSSEM>



Using Kusto to execute precise hunts

- The repository provides 120 Kusto detection/hunting queries covering 156 ATT&CK techniques
- The combination of ATT&CK, Sysmon and the parser makes it possible to execute very clear and legible hunting queries ... taking you from this:

Run Time range: Last 7 days Save Copy Export + New alert rule Pin to dashboard

```
Event
where EventID == 1
extend d=parse_xml(EventData)
where d.DataItem.EventData.Data[10]["#text"] contains "shellrunas"
```

Completed. Showing results from the last 7 days.

TABLE CHART Columns ▾ Display time (UTC+02:00) ▾

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

	TimeGenerated [Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna] ▾	d	Source	EventLog
ParameterXml	<Param>technique_id=T1088,technique_name=Bypass User Account Control,phase_name=Privilege Escalation</Param><Param>2019-07-28 13:40:13.323</Param><Param>(883D9709-A5B0)			
EventData	<DataItem type="System.XmlData" times="2019-07-28T13:40:13.3712726+00:00" sourceHealthServiceId="26F39B2F-1B0F-13F3-1032-BCE61BE3A88F"><EventData xmlns="http://schemas.microsoft.com/win/2004/10/xmlns">			
EventID	1			
RenderedDescription	Process Create: RuleName: technique_id=T1088,technique_name=Bypass User Account Control,phase_name=Privilege Escalation UtcTime: 2019-07-28 13:40:13.323 ProcessGuid: (883D9709-A5B0)			
MG	00000000-0000-0000-0000-000000000001			
ManagementGroupName	AOI-3351a890-c19e-45c7-ad84-6ad12fb580ff			
Type	Event			
_ResourceId	/subscriptions/86ddb844-8426-4cd2-903a-b5c8ffaeb80/resourcegroups/sentinel-attack/providers/microsoft.compute/virtualmachines/test-vm-2			
▼ d	[{"DataItem":{"@type":"System.XmlData","@time":"2019-07-28T13:40:13.3712726Z","@sourceHealthServiceId":"26f39b2f-1b0f-13f3-1032-bce61be3a88f","EventData":{"@xmlns":"http://schemas.microsoft.com/win/2004/10/xmlns":			
▶ DataItem	{"@type":"System.XmlData","@time":"2019-07-28T13:40:13.3712726Z","@sourceHealthServiceId":"26f39b2f-1b0f-13f3-1032-bce61be3a88f","EventData":{"@xmlns":"http://schemas.microsoft.com/win/2004/10/xmlns":			

< 2019-07-26T11:45:55.430 [{"DataItem":{"@type":"System.XmlData","@time":"2019-07-26T09:45:55... Microsoft-Windows-Sysmon Microsoft-Windows-Sysmon/Operational

Kusto karate

Using Kusto to execute precise hunts

... to this:

The screenshot shows the Microsoft Defender Security Center Kusto query interface. At the top, there is a 'Run' button and a 'Time range: Last 7 days' filter. The query entered is 'Sysmon | where process_commandline contains "shellrunas"'. The interface shows the query has completed, displaying results from the last 7 days. The results are shown in a table view with 2 records. The table has columns for TimeGenerated, Source, EventID, Computer, Username, RenderedDescription, and event_creation_time. The first record shows a process_id of 3372, process_path of C:\Users\plankton\Desktop\ShellRunas.exe, file_version of 1.01, file_description of Run as different user, file_product of Sysinternals ShellRunAs, file_company of Sysinternals - www.sysinternals.com, process_commandline of ShellRunas, file_directory of "C:\Users\plankton\Desktop\ShellRunas.exe" cmd, user_name of C:\Users\plankton\Desktop\, user_logon_guid of test-vm-2\plankton, user_logon_id of {883d9709-9ca3-5d3d-0000-0020c78b4900}, and user_session_id of 0x498bc7.

Run Time range: Last 7 days Save Copy Export + New alert rule Pin to dashboard

Sysmon
| where process_commandline contains "shellrunas"

Completed. Showing results from the last 7 days. 00:00:00.643 2 records

TABLE CHART Columns Display time (UTC+02:00)

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

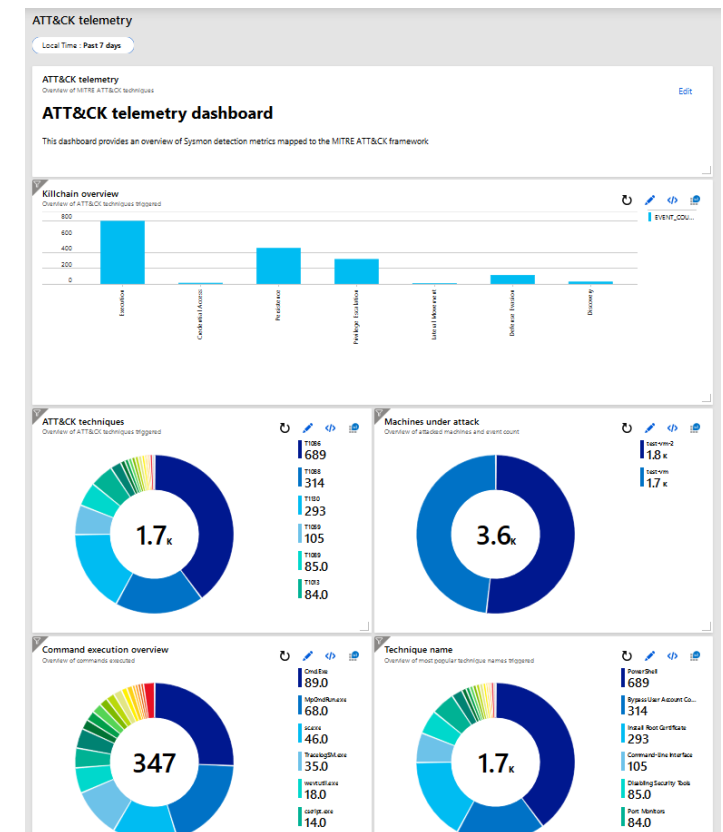
TimeGenerated [Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna]	Source	EventID	Computer	Username	RenderedDescription	event_creation_time
process_id	3372					
process_path	C:\Users\plankton\Desktop\ShellRunas.exe					
file_version	1.01					
file_description	Run as different user					
file_product	Sysinternals ShellRunAs					
file_company	Sysinternals - www.sysinternals.com					
process_commandline	ShellRunas					
file_directory	"C:\Users\plankton\Desktop\ShellRunas.exe" cmd					
user_name	C:\Users\plankton\Desktop\					
user_logon_guid	test-vm-2\plankton					
user_logon_id	{883d9709-9ca3-5d3d-0000-0020c78b4900}					
user_session_id	0x498bc7					

Threat hunting dashboard

Providing ATT&CK telemetry across the network

The repository also provides an ATT&CK-based, threat hunting dashboard, that has the following features:

- Easily importable through a JSON file
- Provides ATT&CK data overviews over different timespans
- Shows the number of techniques executed mapped to the killchain
- Provides an overview of machines affected
- Shows the top ATT&CK techniques and commands executed
- Provides a time chart of ATT&CK techniques executed over time



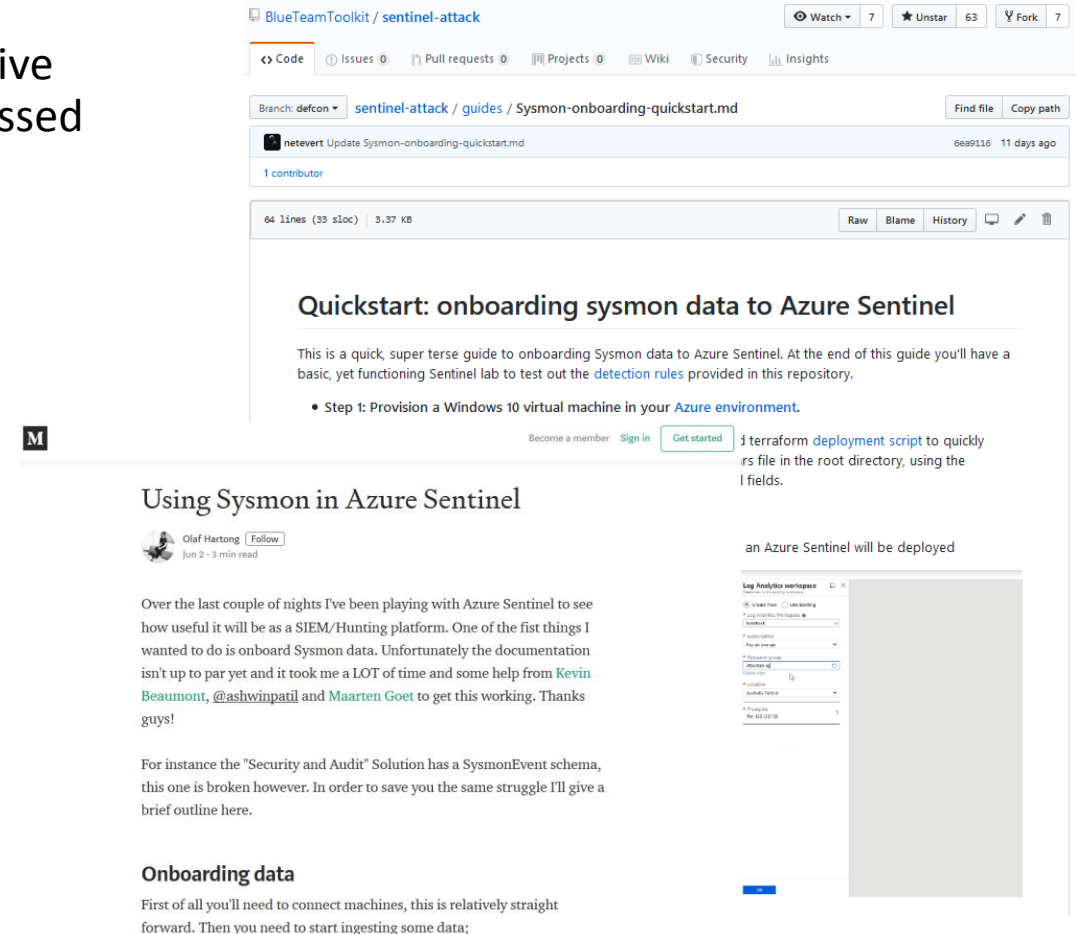
Guidance

You're not left alone

More importantly sentinel-ATT&CK provides comprehensive guidance on how to install and leverage all features discussed

... and we plan to add more!

... we also write on Medium!



The image is a composite of two screenshots. The top screenshot shows a GitHub repository for 'BlueTeamToolkit / sentinel-attack'. It displays the file 'sentinel-attack / guides / Sysmon-onboarding-quickstart.md' with a commit by 'netervert' from 11 days ago. The file content is a 'Quickstart: onboarding sysmon data to Azure Sentinel' guide, which includes a step to provision a Windows 10 virtual machine. The bottom screenshot shows a Medium article titled 'Using Sysmon in Azure Sentinel' by Olaf Hartong. The article discusses the challenges of onboarding Sysmon data to Azure Sentinel and provides a brief outline of the process. It mentions that the 'Security and Audit' solution has a SysmonEvent schema, but it is broken, and the author will provide a brief outline to help others avoid the same struggle.

BlueTeamToolkit / sentinel-attack

Watch 7 Unstar 63 Fork 7

Code Issues 0 Pull requests 0 Projects 0 Wiki Security Insights

Branch: defcon sentinel-attack / guides / Sysmon-onboarding-quickstart.md Find file Copy path

netervert Update Sysmon-onboarding-quickstart.md 6e99116 11 days ago

1 contributor

64 lines (33 sloc) 3.37 KB Raw Blame History

Quickstart: onboarding sysmon data to Azure Sentinel

This is a quick, super terse guide to onboarding Sysmon data to Azure Sentinel. At the end of this guide you'll have a basic, yet functioning Sentinel lab to test out the [detection rules](#) provided in this repository.

- Step 1: Provision a Windows 10 virtual machine in your [Azure environment](#).

Become a member Sign in Get started

1 terraform [deployment script](#) to quickly rs file in the root directory, using the l fields.

Using Sysmon in Azure Sentinel

Olaf Hartong Follow Jun 2 · 3 min read

Over the last couple of nights I've been playing with Azure Sentinel to see how useful it will be as a SIEM/Hunting platform. One of the first things I wanted to do is onboard Sysmon data. Unfortunately the documentation isn't up to par yet and it took me a LOT of time and some help from [Kevin Beaumont](#), [@ashwinpatil](#) and [Maarten Goet](#) to get this working. Thanks guys!

For instance the "Security and Audit" Solution has a SysmonEvent schema, this one is broken however. In order to save you the same struggle I'll give a brief outline here.

Onboarding data

First of all you'll need to connect machines, this is relatively straight forward. Then you need to start ingesting some data;

an Azure Sentinel will be deployed

Log Analytics workspace

Create New Existing

Log Analytics Workspace

Subscription

Pay as you go

Resource group

Location

Availability

Region

SKU

Let's see it!

A lightning look at the platform

We'll showcase a live instance of Sentinel ATT&CK deployed on our Azure lab to

- Walk through the repository and dashboard
- Walk through the threat hunting Jupyter notebook

Q&A

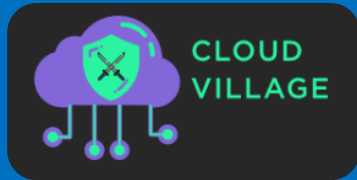
Some questions to get started:

- Who has used Sentinel and what is their opinion of the platform?
- Who uses Sysmon as a process monitoring solution in their network and what is their opinion of the tool?
- What are some of the response activities that could be performed with Sentinel on compromised virtual machines, especially considering the in-built SOAR capabilities of the platform?

IT'S OVER!

Thank you all for your attention, come talk to us!

Thank you



for this amazing opportunity!