



# SIGMA & PAYAMPARDAZ RULES

# سیگما چیست؟

- ما قوانین سیگما را برای تشخیص ترافیک شبکه داریم، برای شناسایی فایل‌های مشکوک، از قوانین سیگما را برای جستجو/تطابق الگو از طریق داده‌های گزارش استفاده می‌کنیم.
- سیگما یک فرمت امضای عمومی و باز است که به تحلیلگران اجازه می‌دهد تا جستجوها را روی داده‌های گزارش به روشی ساده بنویسند و توصیف کنند.
- این قوانین را می‌توان تبدیل کرد و در بسیاری از سیستم‌های مدیریت لاگ یا SIEM اعمال کرد.
- نوشتن قوانین سیگما آسان است و از فرمت YAML پیروی می‌کند که برای جا دادن فیلدهای سفارشی کاملاً انعطاف پذیر است.

# ساختار قوانین سیگما

Sections	Attributes	Value (Example)	Remark
Metadata	title	Installation of Malicious Service	Mandatory
	id	2cfe636e-317a-4bee-9f2c-1066d9f54d1a	Optional
	status	stable	
	author	Blusapphire, SOC	
	date	2017/03/27	
	modified	2021/07/06	
	description	Detects known malicious service installs that only appear in cases of lateral movement, credential dumping, and other suspicious activities.	
	references	- <a href="https://awakesecurity.com/blog/threat-hunting-for-paexec/">https://awakesecurity.com/blog/threat-hunting-for-paexec/</a> - <a href="https://blog.f-secure.com/wp-content/uploads/2019/10/CosmicDuke.pdf">https://blog.f-secure.com/wp-content/uploads/2019/10/CosmicDuke.pdf</a>	
	tags	- attack.t1035 - attack.t1050	
	falsepositives	- Penetration testing	
	level	critical	
Logsource	logsource		Mandatory
	category		Optional
	product	windows	
	service	system	
	definition		
Detection	detection	selection: EventID: 7045 malsvc_paexec: ServiceFileName contains: '\PAExec' malsvc_wannacry: ServiceName: 'mssecsvc2.0' malsvc_persistence: ServiceFileName contains: 'net user'	Mandatory
	condition	selection and (malsvc_paexec or malsvc_wannacry or malsvc_persistence)	

# نمونه ای از قانون سیگما

```
title: Potential OGNL Injection Exploitation In JVM Based Application
id: 4d0af518-828e-4a04-a751-a7d03f3046ad
status: experimental
description: |
  Detects potential OGNL Injection exploitation, which may lead to RCE.
  OGNL is an expression language that is supported in many JVM based systems.
  OGNL Injection is the reason for some high profile RCE's such as Apache Struts (CVE-2017-5638) and Con
references:
  - https://www.wix.engineering/post/threat-and-vulnerability-hunting-with-application-server-error-logs
author: Moti Harmats
date: 2023/02/11
tags:
  - attack.initial_access
  - attack.t1190
  - cve.2017.5638
  - cve.2022.26134
logsource:
  category: application
  product: jvm
  definition: 'Requirements: application error logs must be collected (with LOG_LEVEL=ERROR and above)'
detection:
  keywords:
    - 'org.apache.commons.ognl.OgnlException'
    - 'ExpressionSyntaxException'
  condition: keywords
falsepositives:
  - Application bugs
level: high
```

# نمونه ای از قوانین پیامپرداز

## Payam pardaz rules

Rule.....	2
@id .....	2
@owner .....	2
@kbid .....	2
@enable .....	2
@ver .....	2
@file_name .....	2
filter_list .....	2
filter .....	2
action .....	2
alert .....	2
prerequisite .....	2
consequence .....	2
regulation .....	2
sequence .....	2

@id  
 @owner  
 @kbid  
 @enable  
 @ver  
 @file\_name  
 filter\_list

filter

*This is a list that contains several dictionaries with the following structure*

@id

@name

@occurrence second time

@weight

@timeout second time

source

ip

@location first time

@reference\_id second time

@reference\_type second time

port

target

ip

@location first time

@reference\_id second time

@reference\_type second time

port

flag\_list second time

flag

event\_list

event

@sensor\_type

@class\_type optional

tag

*This is a list that contains several dictionaries with the following structure*

@meaning

#text

# سلسله مراتب قوانین پیامپرداز

action

alert

*@priority*  
*@category* optional  
*message*  
*source*

ip

*@reference\_id*  
*@reference\_type*

*target*

ip

*@reference\_id*  
*@reference\_type*

prerequisite

*predicate*

This is a list that contains several dictionaries with the following structure

*@type*

Param

This is a list that contains several dictionaries with the following structure

*@reference\_type*

consequence

*predicate*

This is a list that contains several dictionaries with the following structure

*@timeout* optional

*@type*

Param

This is a list that contains several dictionaries with the following structure

*@reference\_type*

regulation

sequence

*filter*

This is a list that contains several dictionaries with the following structure

*@id*

Group

This is a list that contains several dictionaries with the following structure

*@id*

Filter recursive

# سلسله مراتب قوانین پیامپرداز

# Roadmap

بررسی کلی قوانین سیگما  
و شرکت پیامپرداز

1

ساخت مپ میان قوانین

3

تبدیل فایل json به فایل  
xsd

5

تبدیل فایل aml به  
فایل json

2

ساخت convertor  
Json \_ Json

4

اعتبارسنجی به وسیله  
فایل xmd

6



- ▼ ravin\_correlation\_rules\_git
  - ▼ documentoin
    - 🔗 hierarchy\_in\_payam\_rules.pdf
    - > persian-doc
  - ▼ files
    - 📄 correlation\_rules.json
    - 📄 correlation\_rules.xml
    - 📄 correlation\_rules.xsd
    - > samples
  - ▼ payam\_rules
    - > all\_rules
    - > parts\_of\_payam\_rules
    - > parts\_of\_payam\_rules\_unique
    - > sample\_payam
  - ▼ sigma\_rules
    - > json\_files\_sigma\_rules
    - > sample\_sigma
    - > unique\_json\_files\_sigma\_rules
    - > unique\_yaml\_files\_sigma\_rules
    - > yaml\_files\_sigma\_rules

- 📄 analysis.json
- 📄 author.json
- 📄 date.json
- 📄 description.json
- 📄 detection.json
- 📄 falsepositives.json
- 📄 fields.json
- 📄 id.json
- 📄 level.json
- 📄 logsource.json
- 📄 modified.json
- 📄 references.json
- 📄 related.json
- 📄 status.json
- 📄 tag.json
- 📄 tags.json
- 📄 title.json

- ▼ parts\_of\_payam\_rules
  - 📄 @enable.json
  - 📄 @file\_name.json
  - 📄 @id.json
  - 📄 @kbid.json
  - 📄 @owner.json
  - 📄 @ver.json
  - ▼ action
    - 📄 alert.json
    - 📄 consequence.json
    - 📄 prerequisite.json
    - 📄 action.json
  - ▼ filter
    - 📄 @id.json
    - 📄 filter\_list.json
    - regulation
    - 📄 regulation.json

Sections	Attributes
Metadata	title
	id
	status
	author
	date
	modified
	description
	references
	tags
	falsepositives
Logsource	level
	logsource
	category
	product
	service
Detection	definition
	detection
	condition

Rule	
@id	
@owner	
@kbid	
@enable	
@ver	
@file_name	
filter_list	filter
This is a list that contains several dictionaries with the following attributes:	
@id	
@name	
@occurrence	second time
@weight	
@timeout	second time
source	
ip	
@location	first time
@reference_id	second time
@reference_type	second time
port	
target	
ip	
@location	first time
@reference_id	second time
@reference_type	second time
port	
flag_list	second time
flag	
event_list	
event	
@sensor_type	
@class_type	optional
tag	
This is a list that contains several dictionaries with the following attributes:	
@meaning	

action	
alert	
@priority	
@category	optional
message	
source	
ip	
@reference_id	
@reference_type	
target	
ip	
@reference_id	
@reference_type	
prerequisite	
predicate	
This is a list that contains several dictionaries with the following attributes:	
@type	
Param	
This is a list that contains several dictionaries with the following attributes:	
@reference_type	
consequence	
predicate	
This is a list that contains several dictionaries with the following attributes:	
@timeout	optional
@type	
Param	
This is a list that contains several dictionaries with the following attributes:	
@reference_type	
regulation	
sequence	
filter	
This is a list that contains several dictionaries with the following attributes:	
@id	
Group	
This is a list that contains several dictionaries with the following attributes:	
@id	
Filter	recursive

ممنون از توجهتون