Hunting with Sysmon to Unveil the Evil

Felipe “Pr0teus” Esposito
@pr0teusBR

Rodrigo “Sp0oKeR” Montoro
@spookerlabs

TENCHI
down-to-earth cloud security

About us

Felipe Esposito

@pr0teusbr

Senior Researcher Tenchi Security

Senior Instructor at BlueOps

Rodrigo Montoro

@spookerlabs

Senior Researcher Tenchi Security

Senior Instructor at BlueOps

Motivation

Agenda

- **Sysmon Basics**
- **Sysmon Field Hunter (SFH)**
  - Events analyzed
  - Structure
  - Scoring Library
  - Results
- **SFH & Elastic for the Hunting**

SYSMON

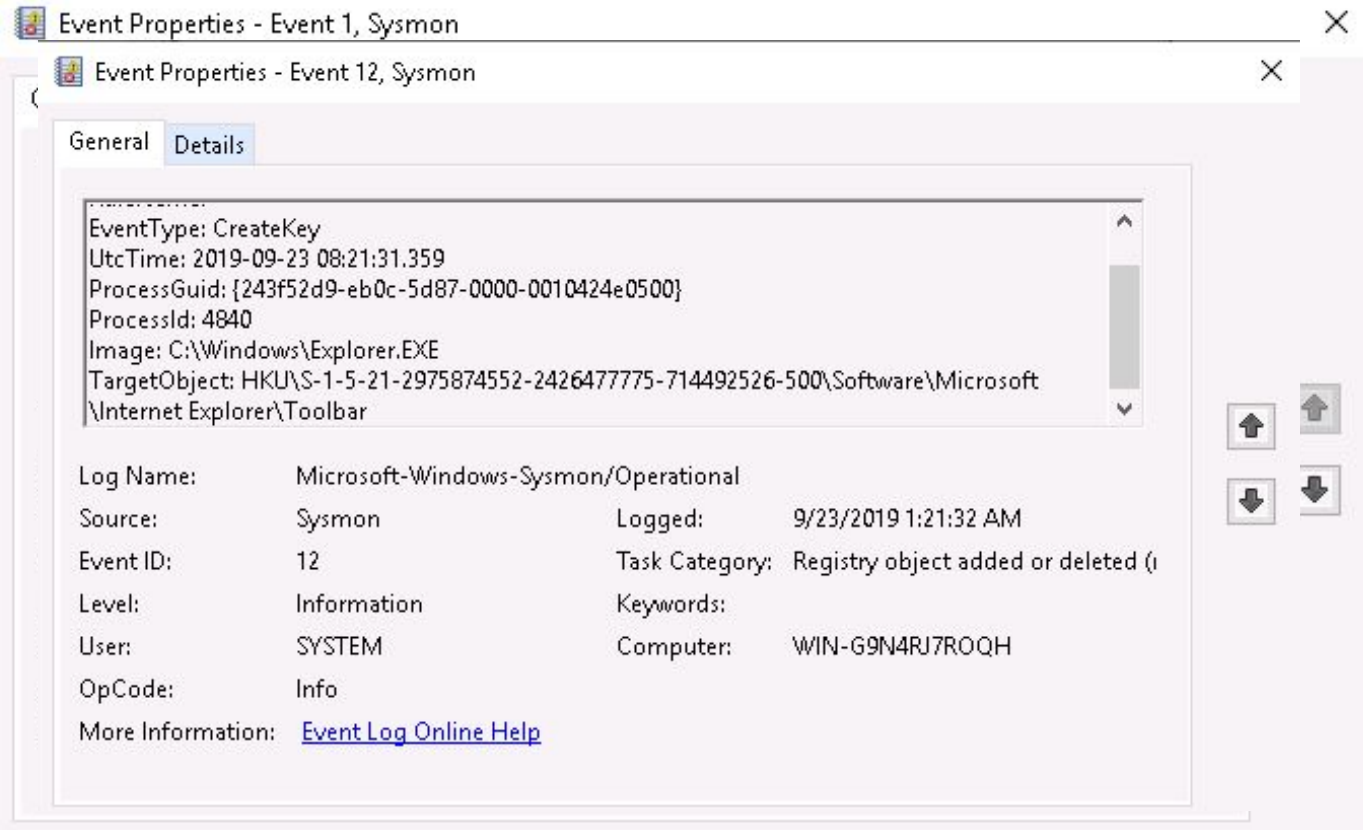
Sysmon

- Launched August of 2014
- Current Version 10.4
- 22 events
- Last update September/2019

Sysmon Capabilities

- Process creation
- DNS queries
- Network Connections
- Registry modifications
- File creation
- WMI Events
- Very flexible configuration file

Sysmon



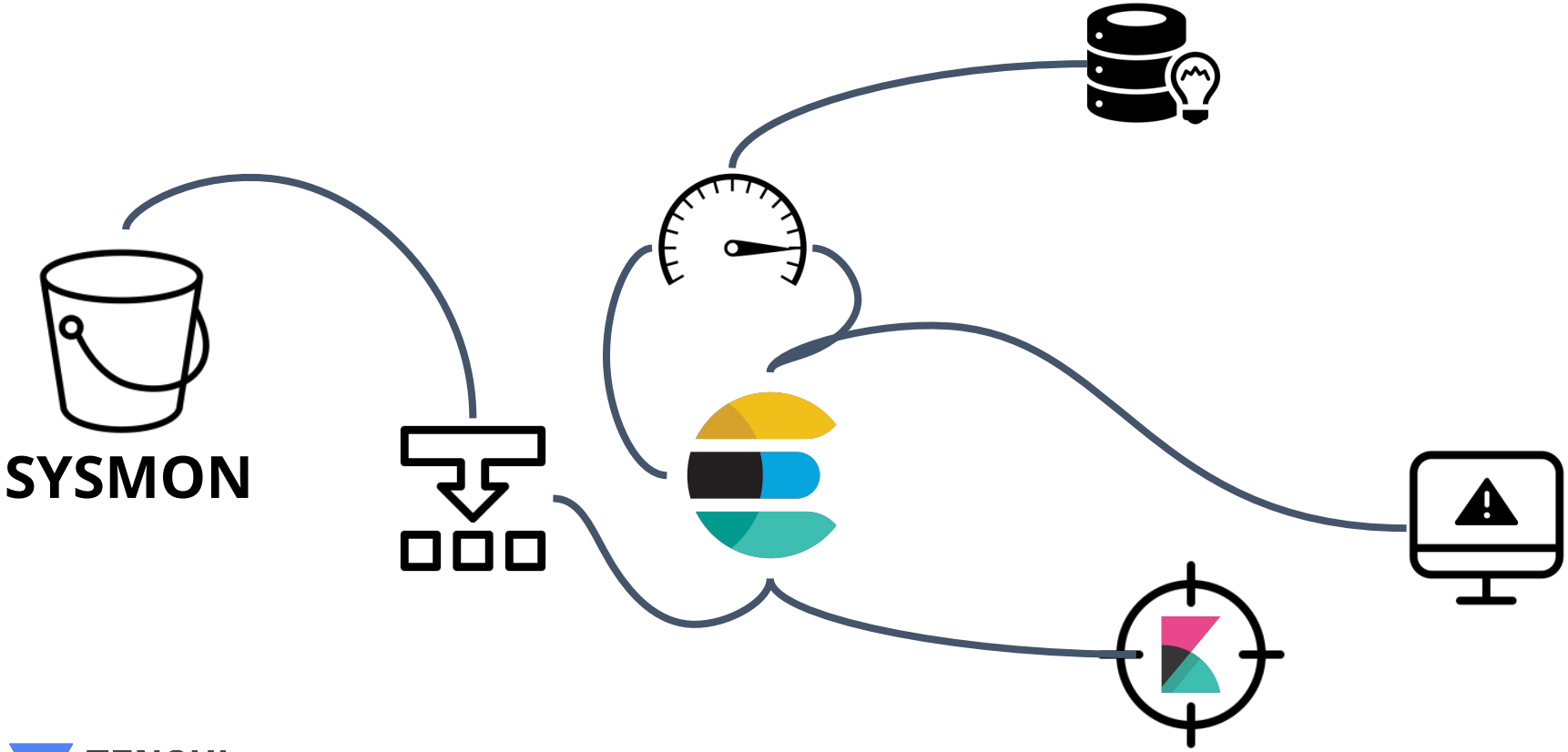
Sysmon Field Hunter (SFH)

TENCHI
down-to-earth cloud security

What is SFH ?

- Analysis based mostly in an unique event
- Flexible scoring system
- Hunting tool
- Alert Fatigue helper
- **Not a silver bullet**

SFH flow structure



Events Coverage (1st phase)

- Process Creation
  - Event ID 1
- Registry Events
  - Event ID 12
  - Event ID 13
  - Event ID 14

Future Events Coverage (2nd phase)

- Network Connection
  - Event ID 3
- File Create
  - Event ID 11
- WMI Events
  - Event ID 19
  - Event ID 20
  - Event ID 21

SYSMON

SFH in the Shell

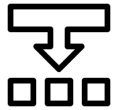
```
[root@elastic sysmonfieldhunter]# python sfh.py -h
usage: sfh.py [-h] -i INDEX -t TIMEFRAME -s SIZE -q QUERY -e EVENTID -m MODE
              [-db DATABASES] [-summary SUMMARY] [-save] [--tag TAG]

Sysmon Field Hunter - BlueOps Labs

optional arguments:
  -h, --help            show this help message and exit
  -i INDEX, --index INDEX
                        Index name
  -t TIMEFRAME, --timeframe TIMEFRAME
                        Timeframe
  -s SIZE, --size SIZE  Number max events response
  -q QUERY, --query QUERY
                        query filter
  -e EVENTID, --eventid EVENTID
                        Sysmon EventID
  -m MODE, --mode MODE  low / medium / high / paranoid
  -db DATABASES, --databases DATABASES
                        directory with db files (default db/)
  -summary SUMMARY, --summary SUMMARY
                        Just show general stats
  -save, --save         Save results to Elasticsearch
  --tag TAG             Add a TAG
```

Event ID 1: Process Creation


```
"event": {
  "action": "Process Create (rule: ProcessCreate)",
  "created": "2019-10-06T16:32:00.384Z",
  "module": "sysmon",
  "category": "process",
  "type": "process_start",
  "kind": "event",
  "code": 1
},
"process": {
  "args": [
    "C:\\Windows\\system32\\PING.EXE",
    "uol.com.br"
  ],
  "working_directory": "C:\\Users\\Administrator\\",
  "parent": {
    "args": [
      "C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe"
    ],
    "name": "powershell.exe",
    "entity_id": "{52c960fe-e171-5d99-0000-001096321300}",
    "pid": 3448,
    "executable": "C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe"
  },
  "name": "PING.EXE",
  "entity_id": "{52c960fe-16fe-5d9a-0000-0010943f4f00}",
  "pid": 3356,
  "executable": "C:\\Windows\\System32\\PING.EXE"
},
"user": {
  "domain": "WIN-KBJR7N0PMAA",
  "name": "Administrator"
},
```


TENCHI
down-to-earth cloud security

Event ID 12 13 14: Registry Events




```
    "process": {
      "entity_id": "{52c960fe-b9ca-5d9a-0000-00100b508000}",
      "pid": 4396,
      "executable": "C:\\Windows\\system32\\reg.exe",
      "name": "reg.exe"
    },
```

```
    "channel": "Microsoft-Windows-Sysmon/Operational",
    "record_id": 1602,
    "opcode": "Info",
    "event_id": 13,
    "provider_name": "Microsoft-Windows-Sysmon",
    "event_data": {
      "EventType": "SetValue",
      "TargetObject": "HKLM\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\osk.exe\\Debugger",
      "Details": "C:\\windows\\system32\\cmd.exe"
    },
    "provider_guid": "{5770385f-c22a-43e0-bf4c-06f5698ffbd9}",
    "task": "Registry value set (rule: RegistryEvent)"
  },
  "event": {
    "created": "2019-10-07T04:06:36.566Z",
    "kind": "event",
    "code": 13,
    "action": "Registry value set (rule: RegistryEvent)",
    "module": "sysmon"
  }
```

Scoring Library - Event ID 1

- admin access
- whitelist process
- creator company
- cli regex
- work hours
- cli byte count
- (entropy + score)*
- token
- directory path*
- common commands*
- parent versus process*
- host risk*
- command hash*
- entropy

Scoring Library - Event ID 12, 13, 14

- work Hour
- whitelist process
- blacklist registry
- event Type
- targetobject
- entropy

Scoring samples (1 / 5)

```
id:      Pu8XgW0BL6gH7RcNEonr
timestamp:       2019-07-19T15:11:17.243Z
eventid:         1
Parent Process:  C:\Windows\System32\cmd.exe
Process Name:    C:\Windows\System32\reg.exe
Whitelist:       2.2
User:    IEUser
score_user:      5
company:         Microsoft Corporation
score_company:   -0.9
token:   -1.3
commandline:     reg  save HKLM\sam sam
entropy:         3.48171457299
score_size:      -0.4
msghour:         Work Hour Time
result: SUSPICIOUS
score:   2.9
```

TENCHI
down-to-earth cloud security

Scoring samples (2 / 5)

```
id:      Mu8XgW0BL6gH7RcNEonr
timestamp:       2019-07-19T15:09:40.973Z
eventid:         1
Parent Process:  C:\Windows\System32\svchost.exe
Process Name:    C:\Windows\System32\consent.exe
Whitelist:       -2
User:    SYSTEM
score_user:      3
company:         Microsoft Corporation
score_company:   -0.9
token:   0.8
commandline:     consent.exe 4516 288 0000023C0CA1FA70
entropy:         4.09698689377
score_size:      -0.4
msghour:         Work Hour Time
result: REGULAR
score:   -1.2
```

TENCHI
down-to-earth cloud security

Scoring samples (3 / 5)

```
id:      Fu8XgW0BL6gH7RcNEonr
timestamp:       2019-07-19T14:57:15.776Z
eventid:         1
Parent Process:  C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Process Name:    C:\Windows\System32\mavinject.exe
Whitelist:       2.2
User:    IEUser
score_user:      5
company:         Microsoft Corporation
score_company:   -0.9
token:   -1.3
commandline:     "C:\Windows\system32\mavinject.exe" 3912 /INJECTRUNNING C:\AtomicRedTeam\atomics\T1055\src\
x64\T1055.dll
entropy:         5.10632716065
score_size:      0.2
msghour:         Work Hour Time
result: SUSPICIOUS
score:   3.5
```

Scoring samples (4 / 5)

```
id:     gO8XgW0BL6gH7RcNEYcY
timestamp:      2019-07-19T14:48:41.050Z
eventid:        1
Parent Process: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Process Name:   C:\Windows\System32\cmd.exe
Whitelist:      2.2
User:   IEUser
score_user:     5
company:        Microsoft Corporation
score_company:  -0.9
token:  -1.3
commandline:    "C:\Windows\system32\cmd.exe" /c "cmd.exe /c " net use \\Target\C$ P@ssw0rd1 /u:DOMAIN\Admi
nistrator
entropy:        4.850693816
score_size:     -0.4
msghour:        Work Hour Time
result: MALICIOUS
score:  10.9
```

Scoring samples (5 / 5)

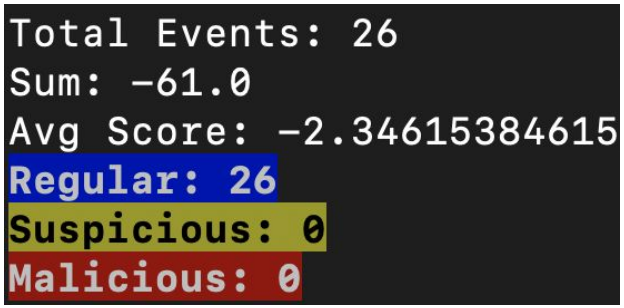
```
id:      LrVIWW0BOU6Q8auzWsfK
timestamp:       2019-09-22T12:02:50.450Z
eventid:         1
Parent Process:  C:\Windows\System32\cmd.exe
Process Name:    C:\Windows\System32\NETSTAT.EXE
Whitelist:       2.2
User:    Administrator
score_user:      3
company:         Microsoft Corporation
score_company:   -0.9
token:   -1.3
commandline:     netstat  -an
entropy:         2.68872187554
score_size:      -0.4
msghour:         Work Hour Time
result: REGULAR
score:   0.9
```

```
id:      TO8AZG0BL6gH7RcNSjx8
timestamp:       2019-09-24T10:59:39.735Z
eventid:         1
Parent Process:  C:\Windows\System32\cmd.exe
Process Name:    C:\Windows\System32\NETSTAT.EXE
Whitelist:       2.2
User:    BlueOps
score_user:      5
company:         Microsoft Corporation
score_company:   -0.9
token:   1.9
commandline:     netstat  -an
entropy:         2.68872187554
score_size:      -0.4
msghour:         Work Hour Time
result: MALICIOUS
score:   6.1
```

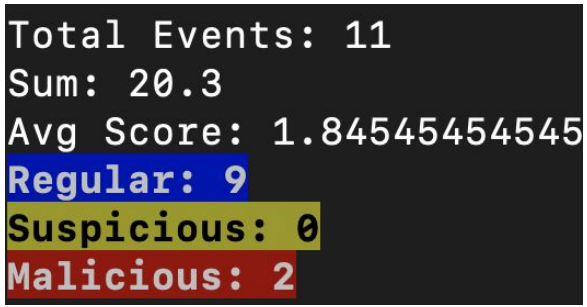
TENCHI
down-to-earth cloud security

Hunting Analysis samples stats

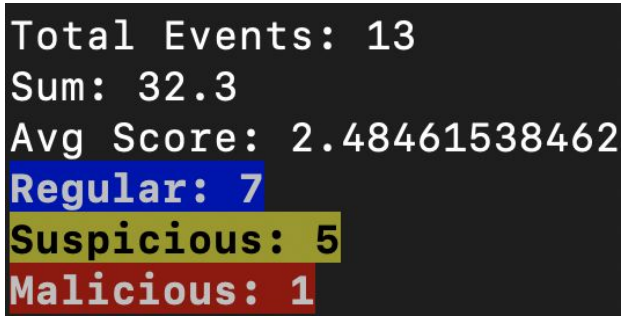
ping



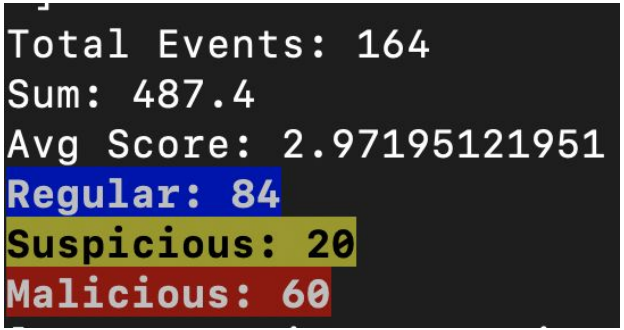
wmic



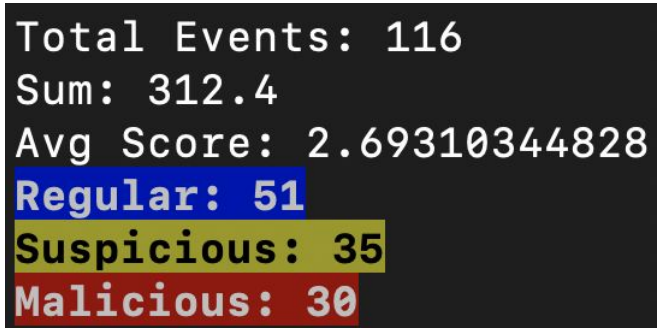
reg.exe



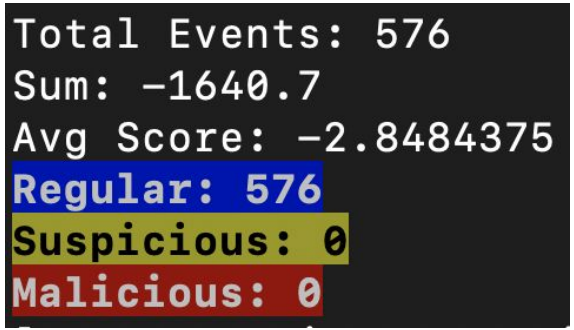
cmd.exe



powershell



conhost



TENCHI
down-to-earth cloud security

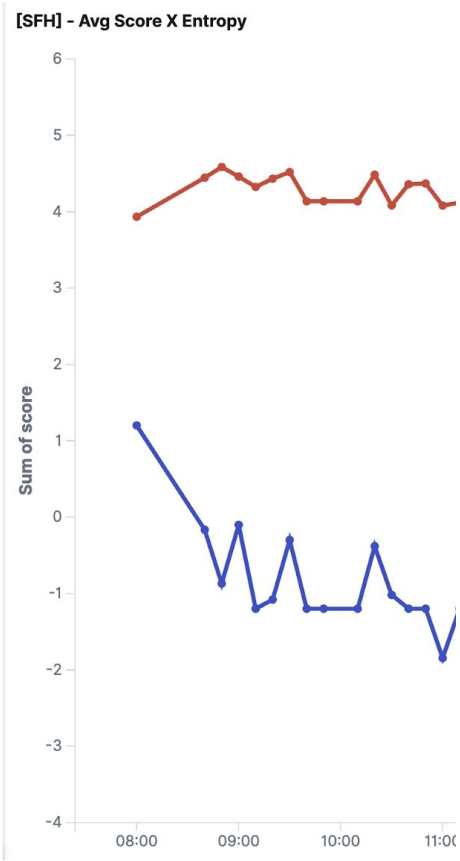
SFH & Elastic for the Hunting

TENCHI
down-to-earth cloud security

Event saved

t	Parent Process	C:\Windows\explorer.exe
t	Process Name	C:\Windows\System32\WindowsPowerShell\v1.0\powershell_ise.exe
t	User	tryme
#	Whitelist	2.2
t	_id	qvDVpG0BL6gH7RcN-o9M
t	_index	test-index
#	_score	1
t	_type	sysmon
t	commandline	C:\Windows\System32\WindowsPowerShell\v1.0\powershell_ise.exe
t	company	Microsoft Corporation
#	entropy	4.456
#	eventid	1
t	id	t_DKpG0BL6gH7RcNMX4Q
t	msghour	Outside Work Hour Window
t	result	MALICIOUS
#	score	6.1
#	score_company	-0.9
#	score_size	-0.4
#	score_user	5
t	tag	SANS
🕒	timestamp	Oct 6, 2019 @ 22:56:10.879

Views

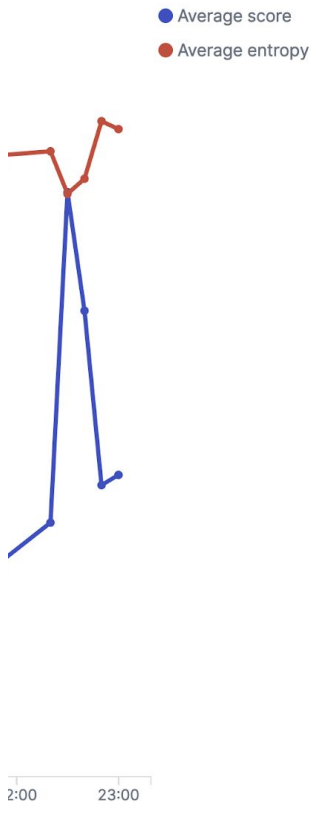


[SFH] - Top 10 Companies

company.keyword: Descending	Count
Microsoft Corporation	582
Sysinternals - www.sysinternals.com	9
?	4
Chocolatey Software, Inc.	2
Mozilla Corporation	1
Mozilla Foundation	1

[SFH] - Top 10 Username

User.keyword: Descending	Count
Administrator	212
SYSTEM	191
NETWORK SERVICE	88
tryme	85
LOCAL SERVICE	17
DWM-4	2
UMFD-4	2
DWM-3	1
UMFD-3	1

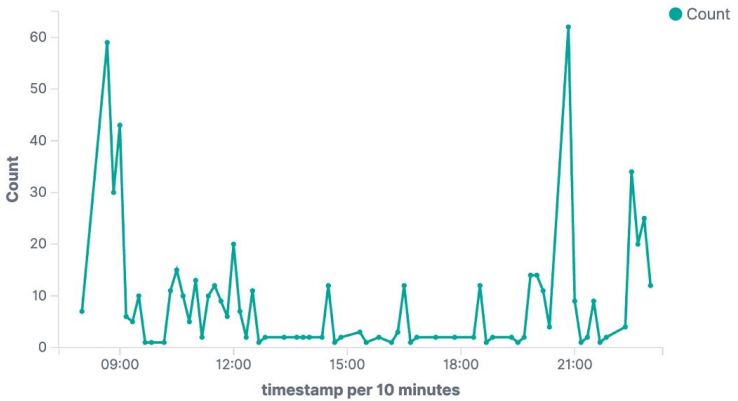


Dashboard

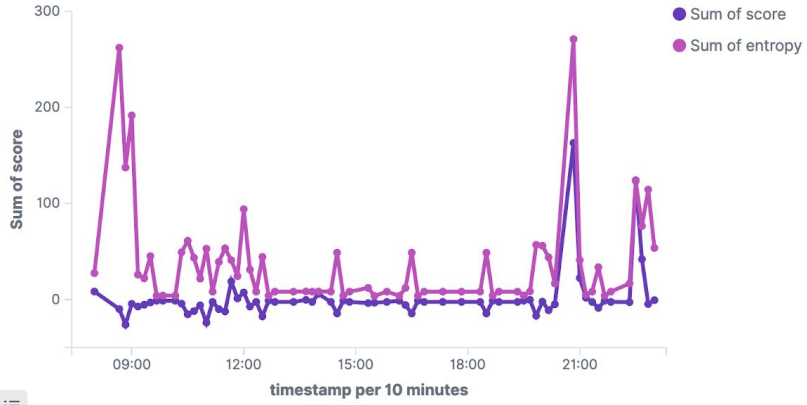
[SFH] - General Results

471	66	62
REGULAR - Count	SUSPICIOUS - Count	MALICIOUS - Count

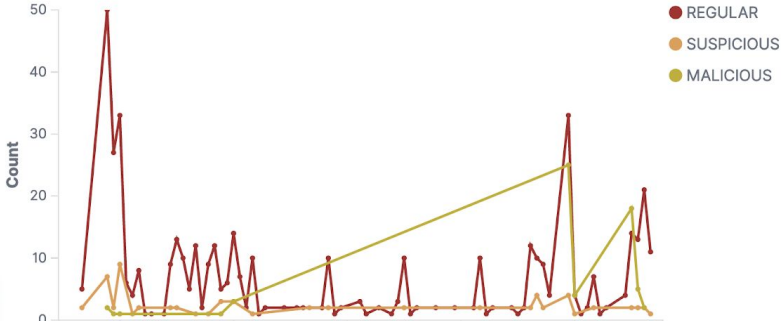
[SFH] - Total Events



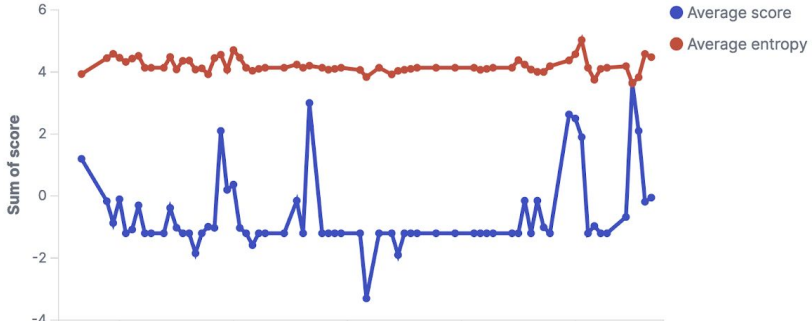
[SFH] - Sum Score X Entropy



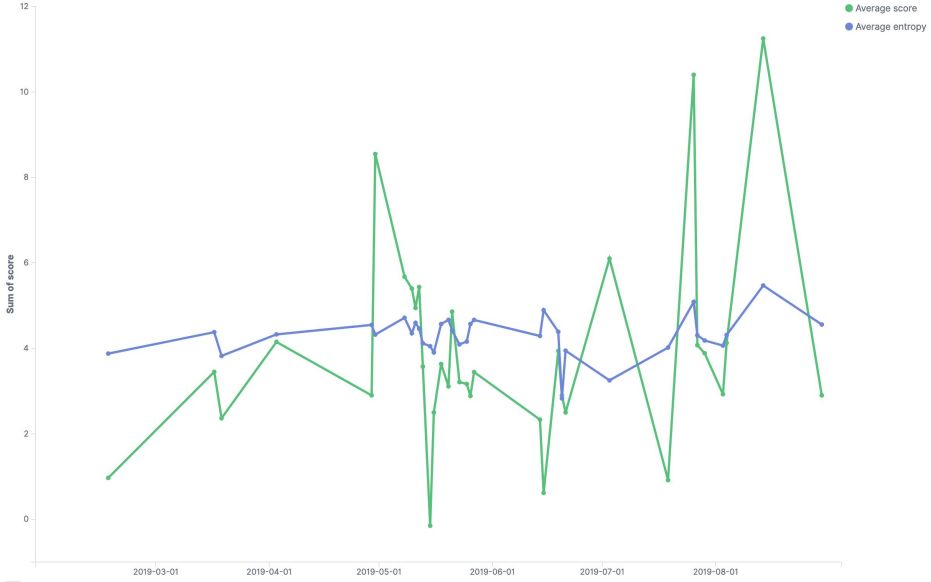
[SFH] - Events Result Timeline



[SFH] - Avg Score X Entropy



Different Behaviors (normal versus malicious)



Thanks Samir @SBousseaden for providing EVTX samples repo https://github.com/sbousseaden/EVTX-ATTACK-SAMPLES

TENCHI
down-to-earth cloud security

Types of possible hunting

- **Results**
- **AvgScores (entropy, score result)**
- **Keywords search**
- **Spikes and Views correlation**

Reduce alerts to analyze

```
Total Events: 4409
Sum: -1791.4
Avg Score: -0.406305284645
Regular: 3457
Suspicious: 792
Malicious: 160
```

Suspicious + Malicious

Removes 79%

Malicious

Removes 96%

TENCHI
down-to-earth cloud security

Hunting Video Demonstration

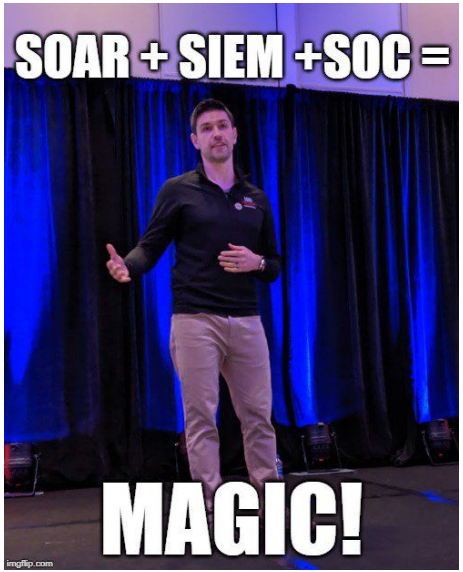
TENCHI
down-to-earth cloud security

Future

- Add more score vectors
- Integration with THE HELK Project
- Correlate between other sysmon events
- Analyze evtx files directly
- Create DB files based on hunting needs
- Export to others SIEM / Products

Conclusions

- Understand your endpoints behavior
- Create and test different DB’s
- Keep testing your endpoint security
- Hunting needs tuning, there is no magic



Thank you!

Felipe Esposito
@pr0teusBR
fesposito@tenchisecurity.com

Rodrigo Montoro
@spookerlabs
rmontoro@tenchisecurity.com