FIRST Regional Symposium Asia-Pacific

Sysmon Log Analysis Tool -SysmonSearch-

2018/10/25

Wataru Takahashi (JPCERT/CC)

Self-introduction

Wataru Takahashi

- Incident Response Group at JPCERT/CC
- Malware analysis, Forensics investigation.
- Written up posts on malware analysis and technical findings on this blog and GitHub.
  - https://blogs.jpcert.or.jp/en/
  - https://github.com/JPCERTCC/

The Challenges in Current Incident Response

The attacker intrudes into the network, and infect many hosts and servers with malware.

Many hosts need investigation in incident response.

Take months to investigate the whole incident.

Importance of logging

- Necessity to retain logs on a daily basis:
  - Application log
  - Network communication log
  - System log

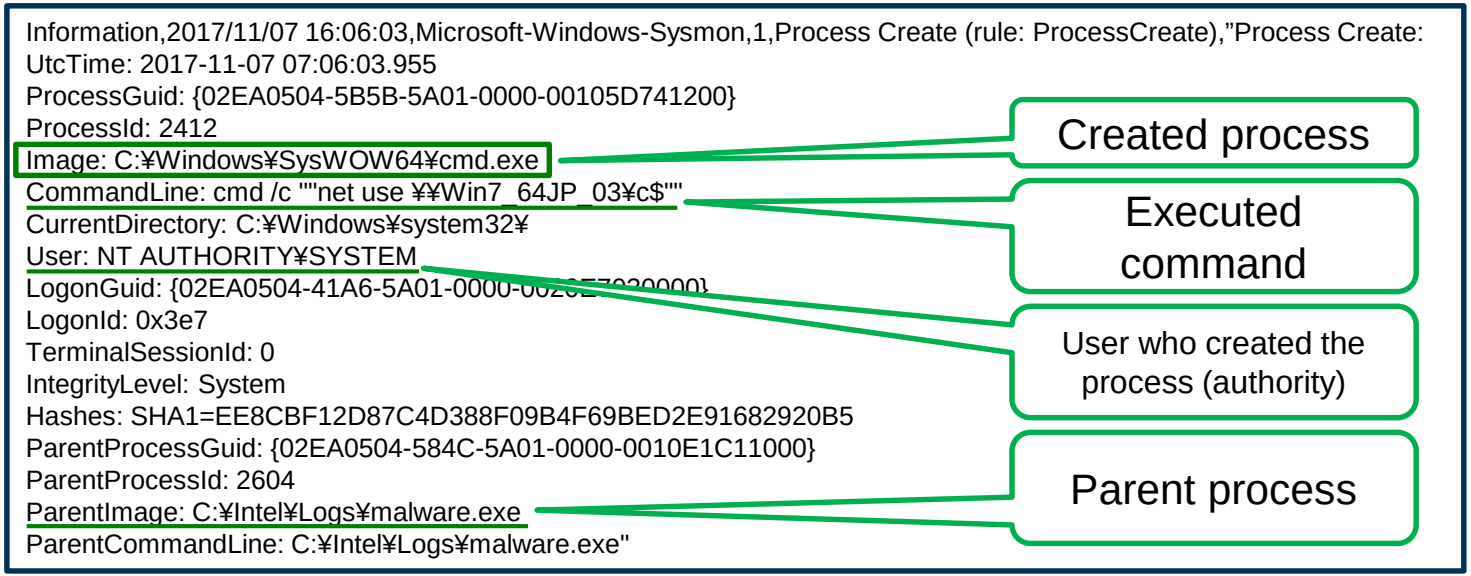
Sysmon
(System Monitor)

Sysmon

- Sysmon is a free tool provided by Microsoft.
- Tool to record various Windows OS operations (applications, registry entries, communication etc.)

Sysmon log

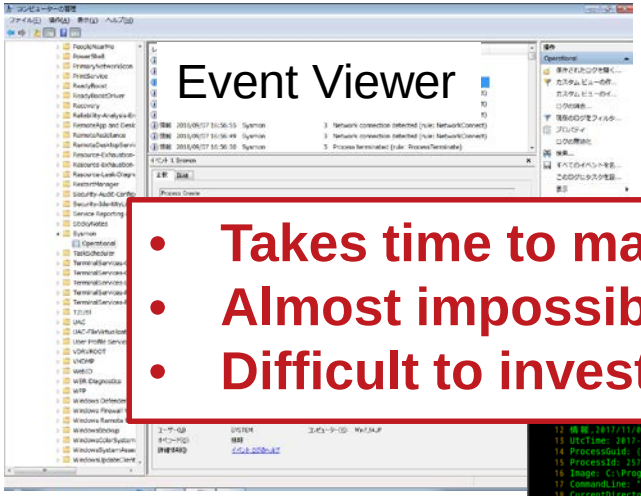
- Example log (Process Create)

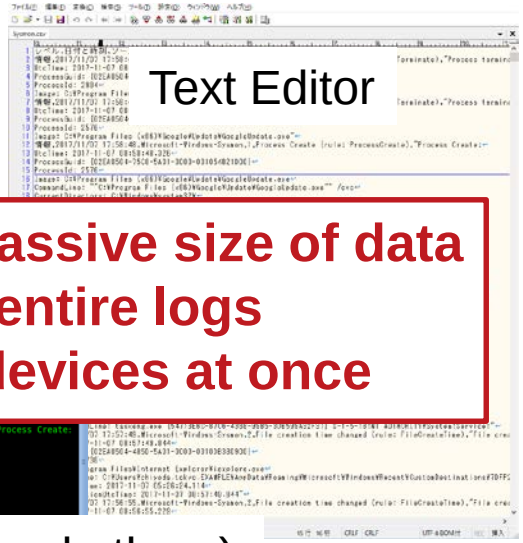


- What you can see from the logs

> "malware.exe" executes cmd /c net use ¥¥Win7_64JP_03¥c$ (network sharing) with SYSTEM privilege.

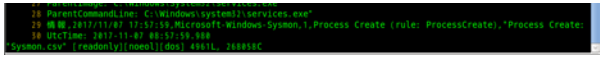
Challenges in Sysmon log analysis





- **Takes time to manually check massive size of data**
- **Almost impossible to grasp the entire logs**
- **Difficult to investigate multiple devices at once**

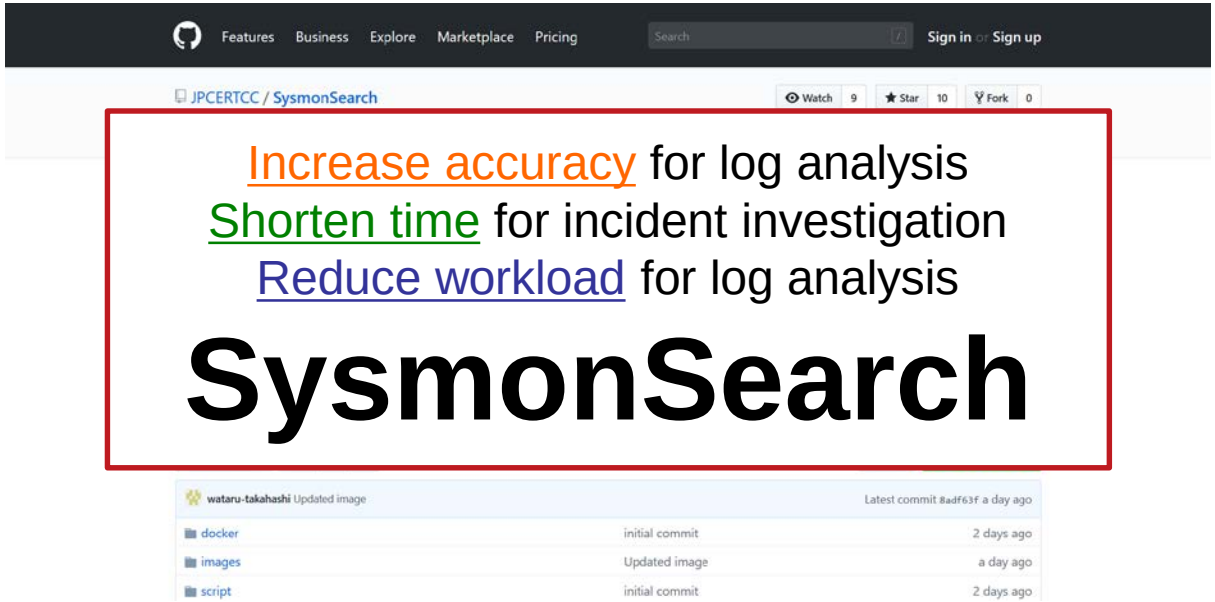
Linux commands (grep, awk and others)



Any ways to do it effectively?

Solution!

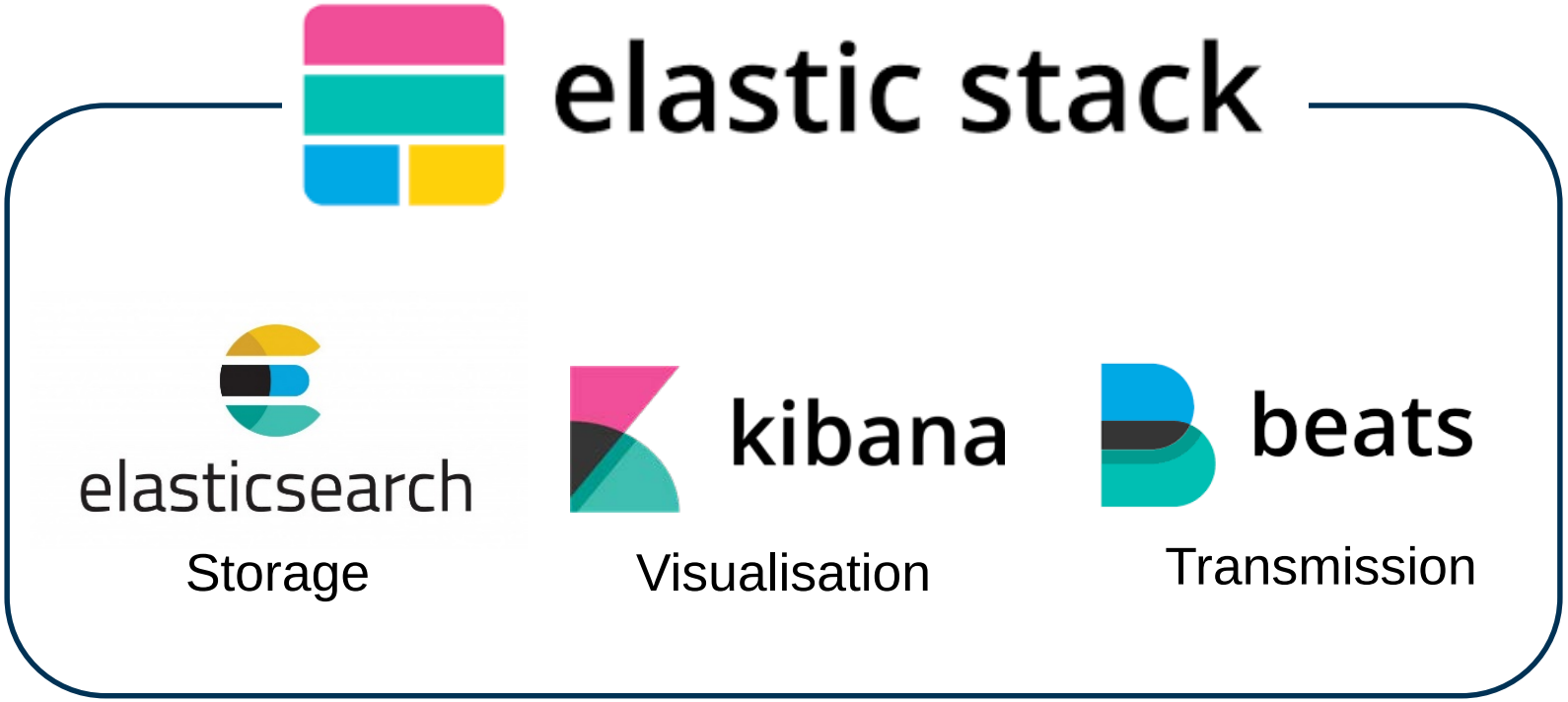
JPCERT/CC developed a tool to support sysmon log analysis



https://github.com/JPCERTCC/SysmonSearch

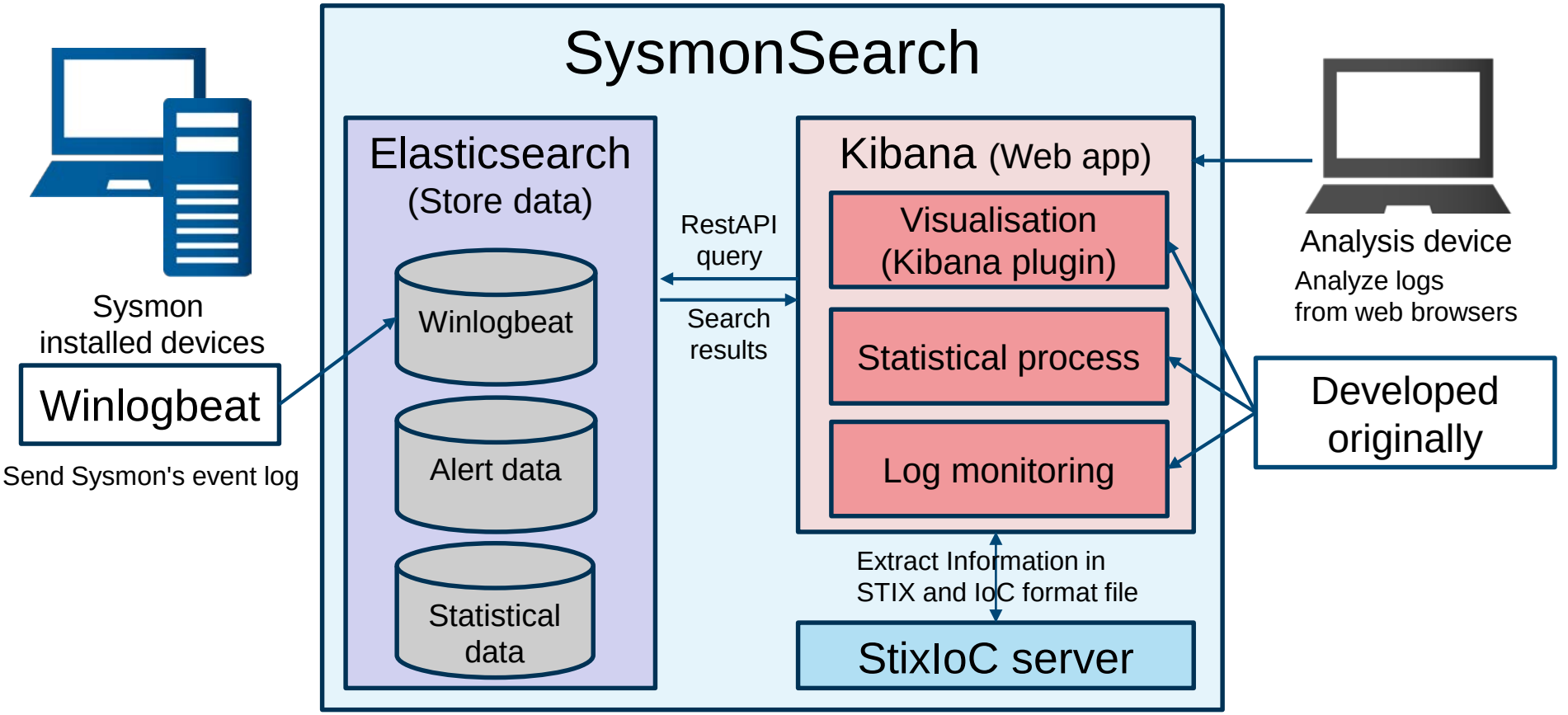
SysmonSearch

SysmonSearch overview



Powering Data Search, Log Analysis, Analytics | Elastic
https://www.elastic.co/products

System overview



SysmonSearch functions

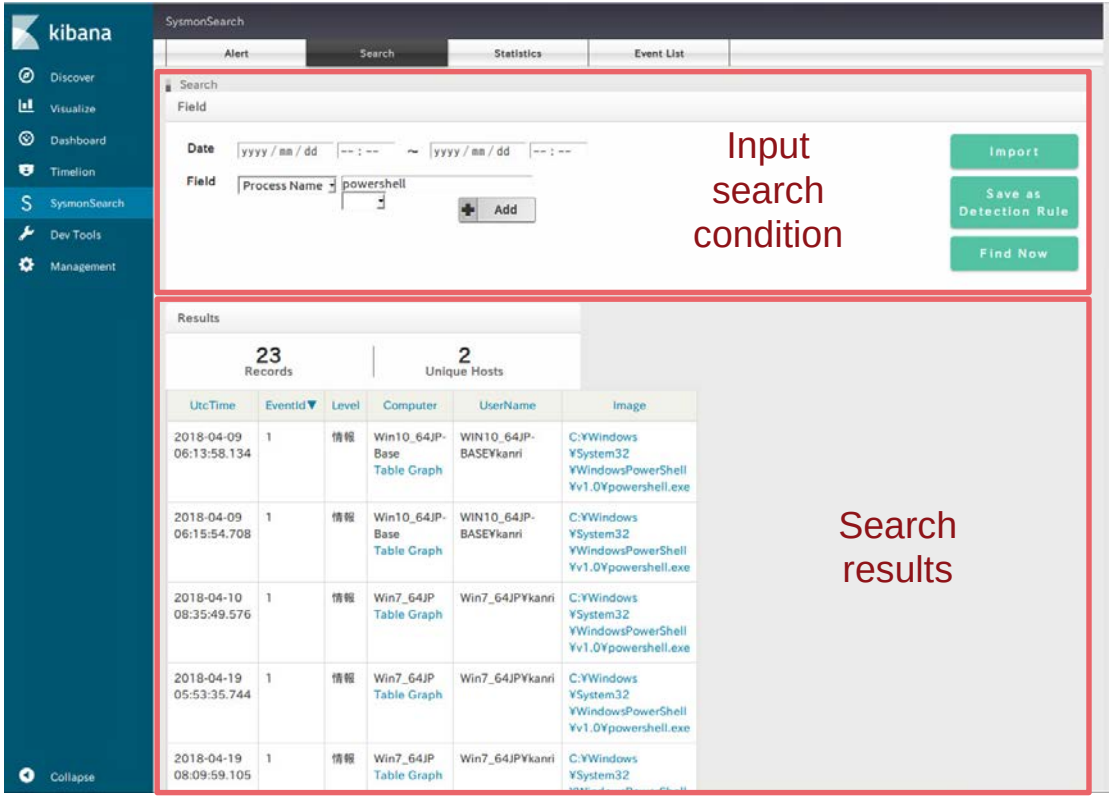
Search
By hash value,
host names etc.

Monitor
Based on rules

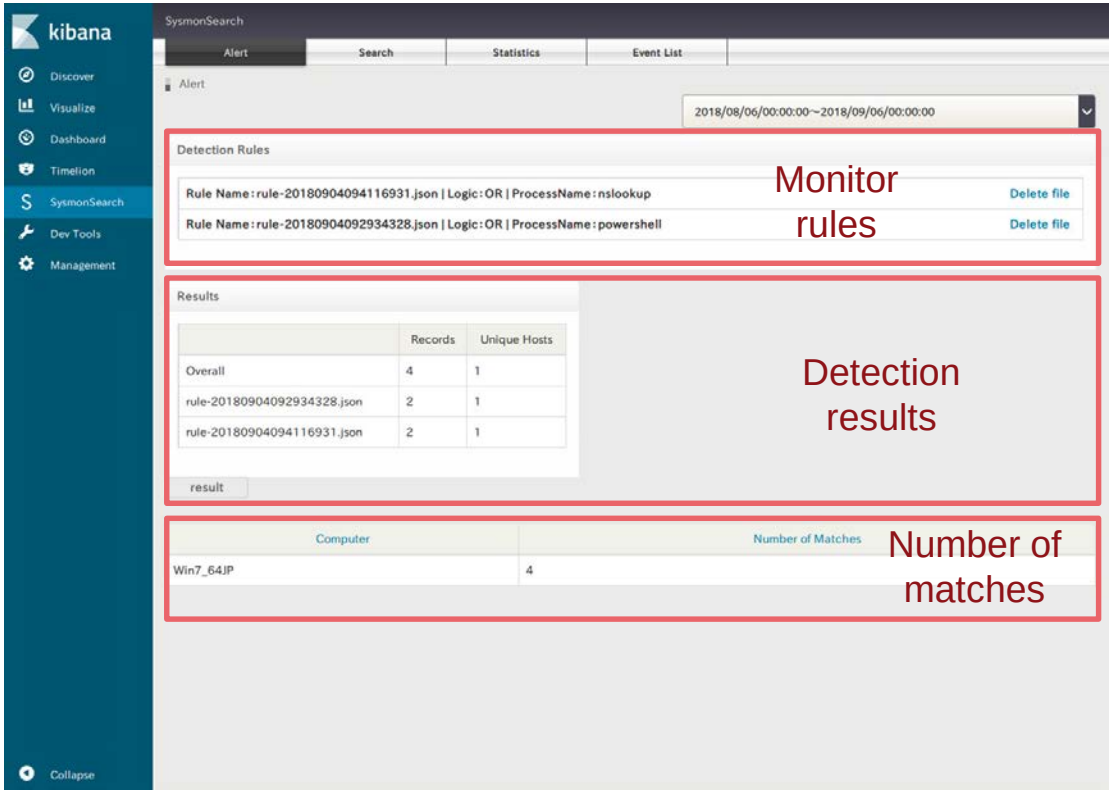
Visualise
In simple graphics

Create statistics
In regular basis

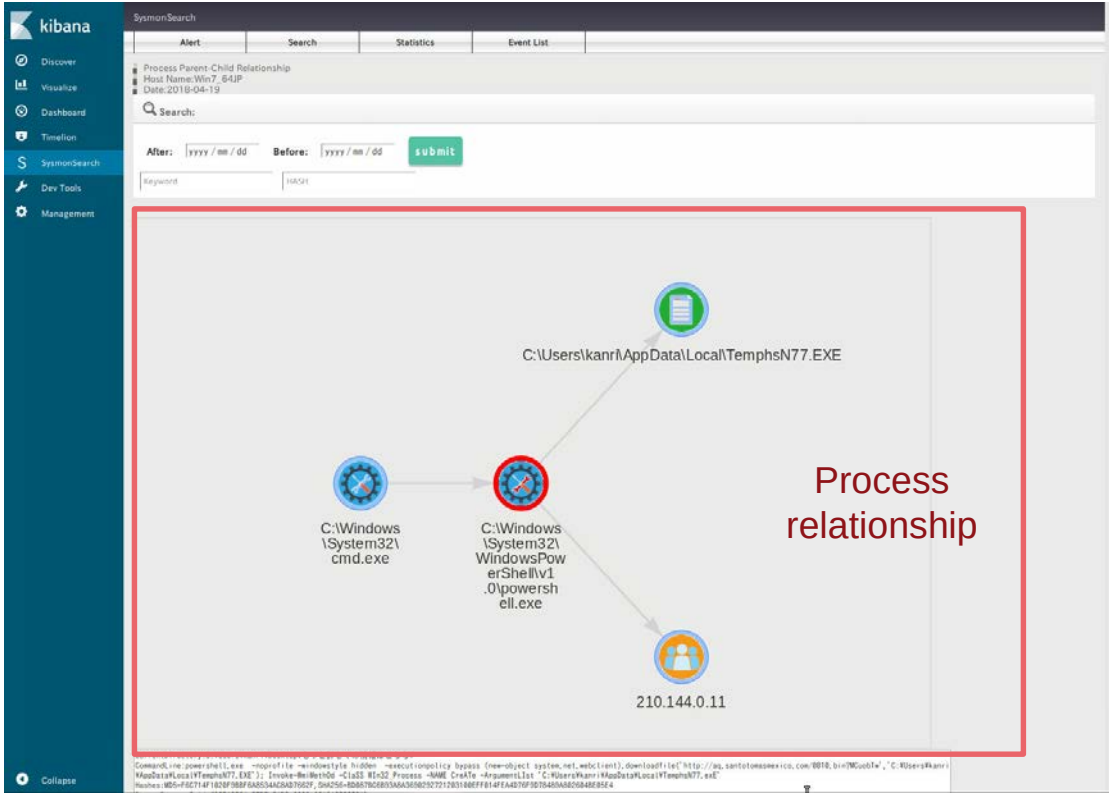
Search



Monitor



Visualise

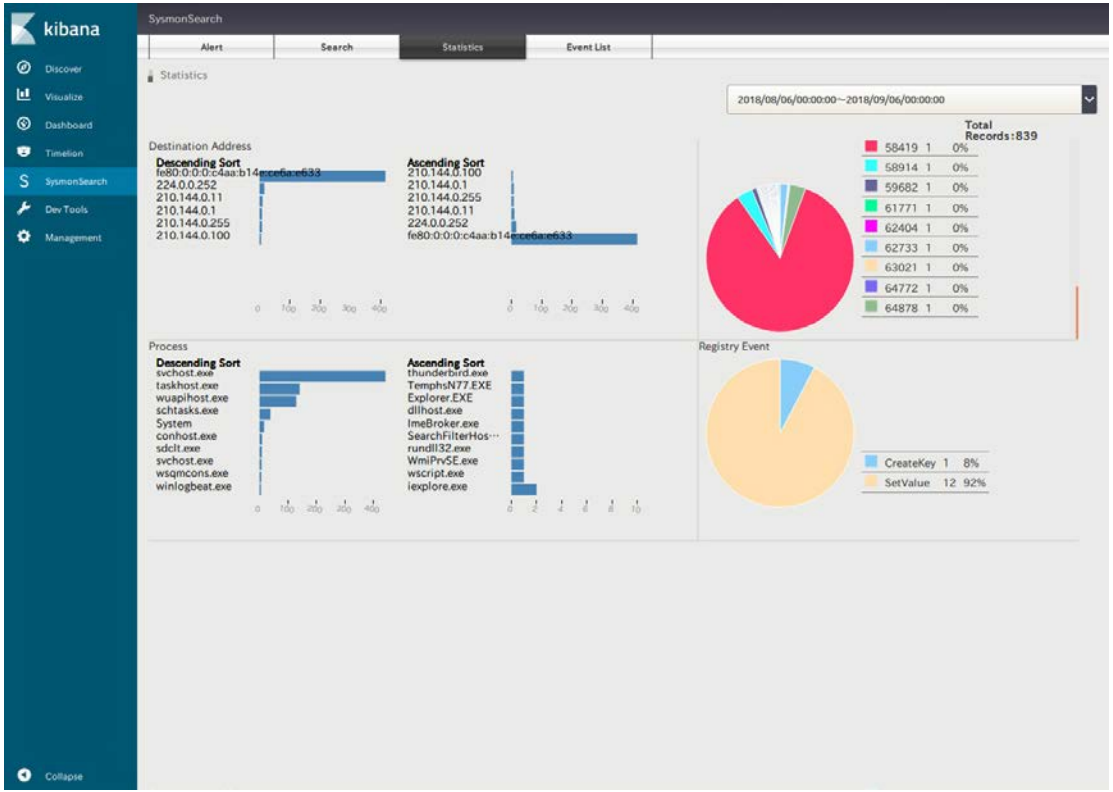


Corresponding icons to IDs

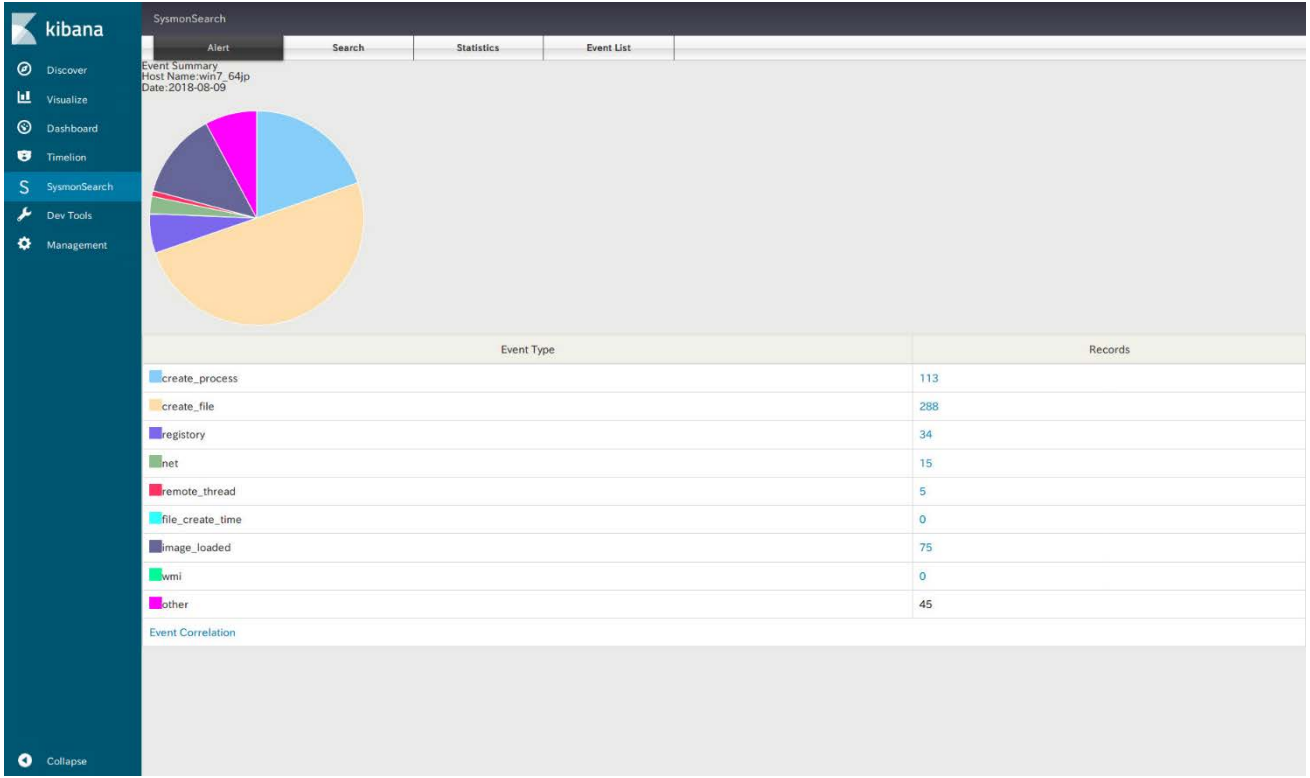
Event ID	Event	Icon
1	Process Create	
2	File creation time changed	
3	Network Connection Detected	
7	Image loaded	
8	CreateRemoteThread	

Event ID	Event	Icon
11	FileCreate	
12 13 14	RegistryEvent (CreateKey)	
12 13 14	RegistryEvent (values)	
19 20 21	WmiEvent	

Create statistics

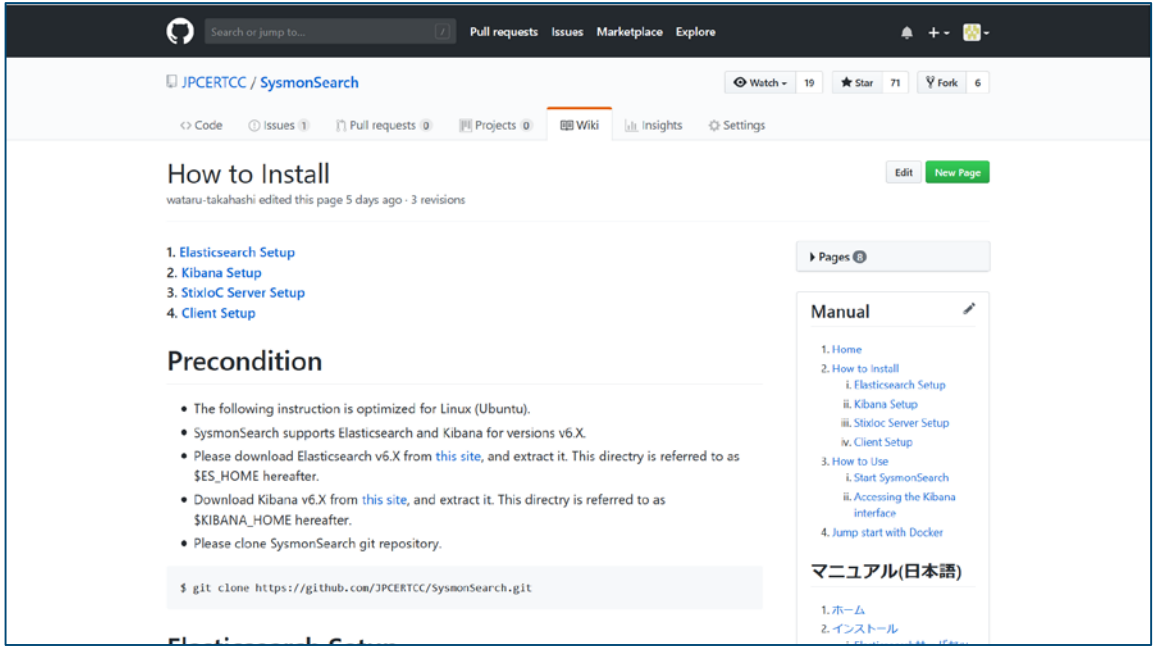


Create statistics



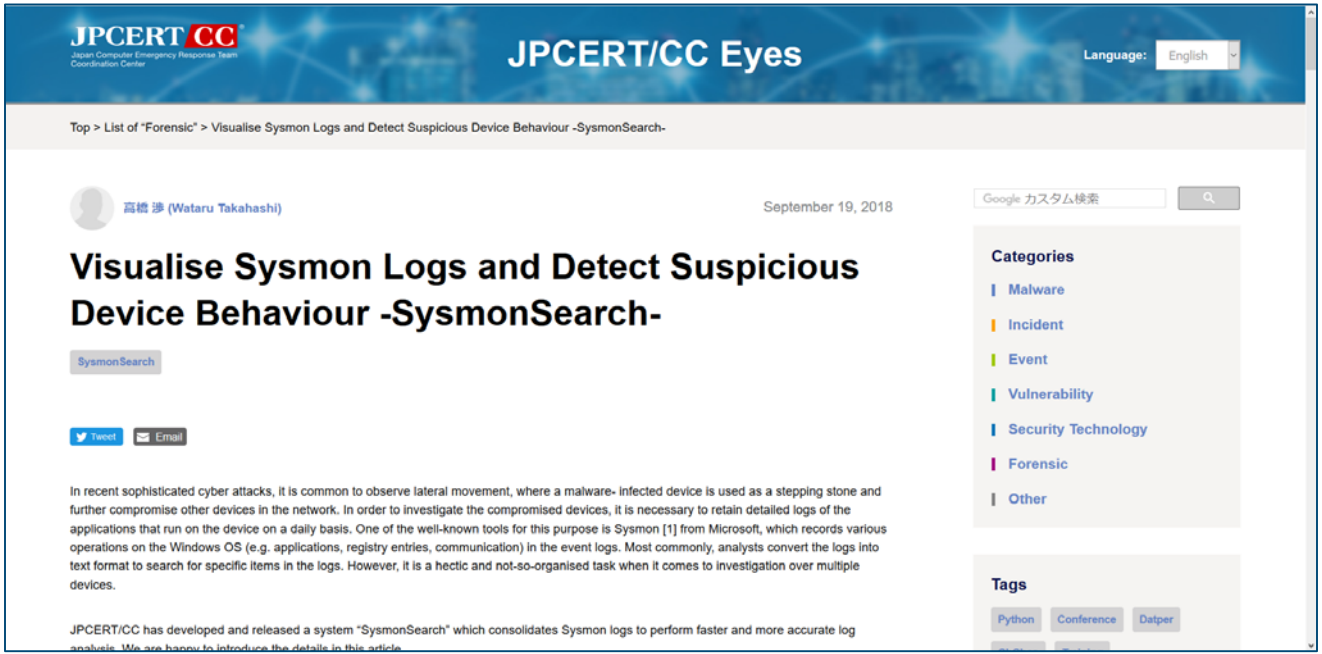
How to Install

- SysmonSearch wiki
  - https://github.com/JPCERTCC/SysmonSearch/wiki



JPCERT/CC Blog

- JPCERT/CC Blog
  - https://blogs.jpcert.or.jp/en/2018/09/visualise-sysmon-logs-and-detect-suspicious-device-behaviour--sysmonsearch.html



Future Works

- Extended functions
  - Import Sysmon logs
  - Raise alert upon detection

Note

- Sysmon log output configuration
  - Besides installing the tool, you will need to change Sysmon configurations to record logs

- Network events recorded in Sysmon
  - Under proxy environment
    - Recorded destination IP address will be set to the proxy
    - Investigation required in line with the proxy server logs

Takeaway

- SysmonSearch can be used for investigation of device operations and log monitoring in peacetime based on rules
  - Investigate suspicious operation by visualising Sysmon logs
  - Detect suspicious operations based on rules

Thank you!!

Please give us feedback.
e-mail: ir-info@jpcert.or.jp