Threat Hunting and Fast Forensics in Windows environments for free! (CODE BLUE 2022)

(Windows環境で無償の脅威ハンティングとファストフォレンジック)

2022/10/28

Zach Mathis / Zakku Tanaka（マシス・ザック/田中ザック）

注意 (Warning)

- 30分しか無いのに、スライドが70枚以上もあるので、簡単に大事なところだけ説明します！
  I only have 30 minutes but over 70 slides so I will just cover the most important points.
- トークが終わったら、プレゼン資料をアップロードするので、後でゆっくり読んで下さい。
  I will upload the presentation after the talk so please read it later at your own pace.
- https://github.com/Yamato-Security/Presentations
- @yamatosecurity / @SecurityYamato

流れ (Talk outline)

1. 自己紹介 (Self-Introduction)
2. Windowsイベントログ解析の重要性
   Importance of Windows event log analysis
3. Windowsイベントログ設定の問題
   Problems with the Windows default log settings
4. Windowsイベントログ解析の課題と解決方法
   Challenges with log analysis and the solution
5. より学びたい貢献したいあなたへの参考情報
   Resources for learning more and/or contributing

1. 自己紹介
(Self-Introduction)

自己紹介

- 名前：Zachary John-Isaac Mathis（マシス・ザック/田中ザック）(@yamatosecurity)
- アメリカ生まれ育ちの大和魂
- 10歳から日本語、コンピュータ、セキュリティを独学する
- 2006年に神戸デジタル・ラボ(KDL)に就職し、「Proactive Defense」のセキュリティチームを立ち上げ、様々なセキュリテイサービスを作成する
- 2007年～2010年、情報セキュリティ専門の大学院であるカーネギーメロン大学日本校(CMUJ)の研究員としてティーチング・アシスタント、システム管理、研究等々
- 2012年に大和セキュリティというセキュリティコミュニティを立ち上げ、無料勉強会で数多くのセキュリティスペシャリストを育てる
- 資格：GCIH(インシデント対応)、GCIA(侵入検知アナリスト)、GCFA(フォレンジック調査)、GPEN(ペネトレーションテスト)、GREM(マルウェア解析)、GCED(エンタープライズデフェンダー)、GCWN(Windowsセキュリティ)、GMON(監視)、GWAS(ウェブセキュリティ)、GDAT(APT対策)、GCFR(クラウドDFIR)等々
- 2016年からSANS講師としてインシデント対応とハッキング技術を教える
- 2020年に会社を立ち上げ、セキュリティ教育やセキュリティサービスを提供する

Self-Introduction

- Name：Zachary Mathis (”Zakku Tanaka” in Japan)(@yamatosecurity)
- Born and raised in the US.
- Self-taught Japanese, computers and security from around 10 years old.
- In 2006, I started work at Kobe Digital Labo (KDL), formed the security team ”Proactive Defense” and created a variety of security services.
- From 2007～2010, I was a researcher and helped teach at Carnegie Mellon CyLab Japan (CMUJ) in Kobe.
- In 2012, I started the Yamato Security community to teach (for free) a wide variety of topics on security.
- Certs：GCIH(Incident Handling)、GCIA(Intrusion Analyst)、GCFA(Forensics Analyst)、GPEN(Penetration Tester)、GREM(Malware Analysis)、GCED(Enterprise Defender)、GCWN(Windows Security)、GMON(Monitoring)、GWAS(Web Security)、GDAT(APT Defenses)、GCFR(Cloud DFIR), etc...
- In 2016, I started to teach SANS 504.
- In 2020, I started my own company for security training, etc...

大和セキュリティについて
About Yamato Security

- 2012年から始まる。Started in 2012.
- 最初は、関西のセキュリティコミュニティを盛り上げるために勉強会を開催する。
  Was first free events to build a local security community in Western JP.
- １～２日間の楽しい！スパルタ教育。
  Usually 1～2 days of brutal (but fun!) training.
- 現在は全国で活動している。大抵、300名以上が勉強会に参加する。
  Now I teach all over Japan. Usually 300+ people show up to events.
- 現在は勉強会よりOSSのDFIRツール開発がメイン。
  Nowadays we are focused on developing open-source DFIR tools.
  - EnableWindowsLogSettings, WELA, Hayabusa, Takajo, etc...
- 品質の高い日本製のツールとリソースを海外にも提供できるよう頑張っている。
  We are trying to provide high quality tools and resources with the spirit of Japanese craftsmanship.

2. Windowsイベントログ解析の重要性
(Importance of Windows event log analysis)

Windowsイベントログ解析スキルの重要性
Importance of Windows Event Log Analysis

- どのWindows端末にも入っているので、Windowsのフォレンジック調査の基本となる。
  Event logs are on all Windows machines so they are a core artifact to Windows investigations.

- 事前に正しくログを設定したら、有償のEDR等を導入しなくても詳細な証拠が残る。
  If you properly configure them in the preparation phase, you can collect for free as much detailed evidence as commercial EDR software does.

- ただし、かなり”くせがある”ので、最初はとても分かりにくい。
  However, they are an ”acquired taste” so it takes getting used to.

- インシデント対応の準備段階で、Windowsイベントログを迅速に解析できるように、時間をかけてトレーニングしなければならない。
  I highly recommend spending the time to train yourself in analyzing these logs before an incident happens as it will take a long time to master.

2.Windowsイベントログ設定の問題
(Problems with Windows event logs default settings)

Windowsのデフォルトログ設定の問題(1)
Default log settings challenges(1)

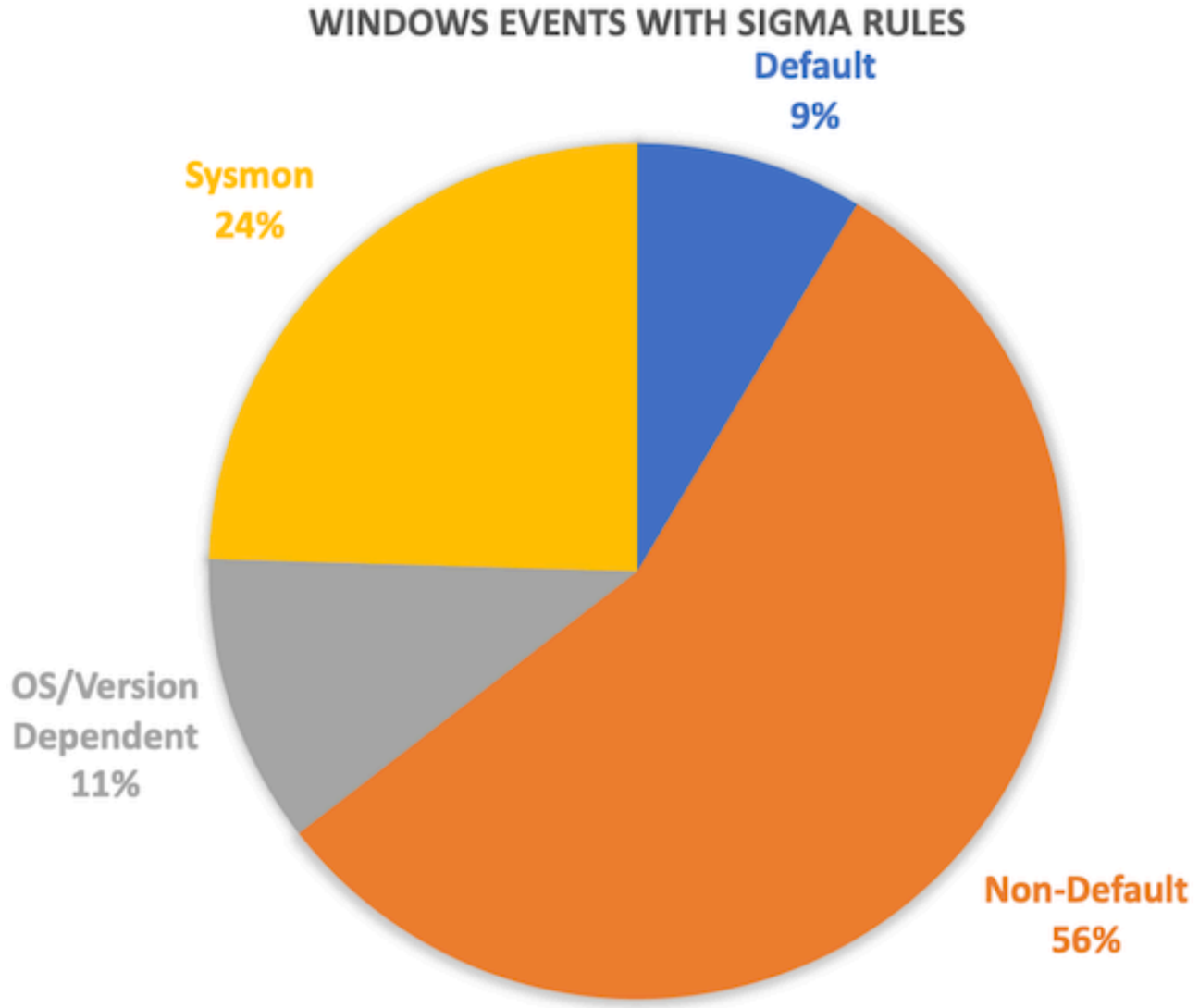
- Windowsログのデフォルト設定は不十分！
  The default settings are insufficient!
- デフォルトでは8割ぐらいの欲しいログが記録されない！
  Around 80% of the logs you want won't get recorded!
- また、約7割以上のログはノイズでDFIR調査に役に立たない！
  Also, usually 70%+ of events are noise and not useful!
- デフォルトのログサイズはたった1～20MBなので、特にDCやサーバのログはすぐに上書きされ、証拠が無くなってしまうことが多い。
  The default log size is a mere 1～20MB so especially in the case of DCs, much evidence will quickly be overwritten.

Windowsのデフォルトログ設定の問題(2)
Default log settings challenges(2)

- ログオンに失敗、PowerShell実行、プロセス実行等々のログが残らない場合があるので、フォレンジック調査がとても困難になる。
  Failed logons, PowerShell execution, process creation, etc... does not get logged by default, making investigations very difficult.
- GPO（グループポリシーオブジェクト）、Intune、スタートアップスクリプト等で端末のログ設定を改善した上で、マイクロソフトのsysmonツールを導入し、詳細なフォレンジックエビデンスを残すべき。
  You should be enable the proper log audit settings with GPOs, Intune, startup scripts, etc... and install sysmon so that you have the evidence you need for forensics investigations.

DFIR調査に必要なログ

Logs needed for a proper DFIR investigation



- Sigmaの攻撃検知ルールが検知するWindowsイベントを分析した
  I looked up the % of Win events with Sigma detection rules.
- デフォルトでは1～2割のSigmaルールしか使えない
  Only 10～20% of Sigma rules can be used with default settings.
- Windowsログ設定を全部有効にすると75%のSigmaルールが使える
  Enable all Windows log settings to use up to 75% of the rules.
- Sysmonの導入で全ルールが利用可能
  Install Sysmon to use all rules.

Sigmaルールが検知するWindowsイベント

Windows events with sigma rules

Sigma Log Source	Channel and EID	Default Settings	Rules	Percent
process_creation	Microsoft-Windows-Sysmon/Operational 1 or Security 4688	non-default	804	49.36%
security	Security	partial	139	8.53%
ps_script	Microsoft-Windows-PowerShell/Operational 4104	partial	125	7.67%
registry_set	Microsoft-Windows-Sysmon/Operational 13	sysmon	109	6.69%
file_event	Microsoft-Windows-Sysmon/Operational 11	sysmon	96	5.89%
system	System	default	50	3.07%
image_load	Microsoft-Windows-Sysmon/Operational 7	sysmon	39	2.39%
registry_event	Microsoft-Windows-Sysmon/Operational 12/13/14	sysmon	37	2.27%
ps_module	Microsoft-Windows-PowerShell/Operational 4103	non-default	30	1.84%
network_connection	Microsoft-Windows-Sysmon/Operational 3	sysmon	29	1.78%
process_access	Microsoft-Windows-Sysmon/Operational 10	sysmon	25	1.53%
pipe_created	Microsoft-Windows-Sysmon/Operational 17/18	sysmon	14	0.86%
application	Application	default	13	0.80%
dns_query	Microsoft-Windows-Sysmon/Operational 22	sysmon	12	0.74%
ps_classic_start	Windows PowerShell 400	default	10	0.61%
create_remote_thread	Microsoft-Windows-Sysmon/Operational 8	sysmon	10	0.61%

Sigmaルールが検知するSecurityログのイベント
Security log events with sigma rules

EID	Event	Default Settings	Rules	%
4688	Process Creation	No	695	73.70%
4697	Service installed	Yes - Win 10/2016+	20	2.12%
5145	Access attempt to a network share object	No	18	1.91%
4624	Successful logon	Yes	12	1.27%
4656	Object handle request	No	12	1.27%
4663	Access attempt to object	No	12	1.27%
4625	Failed logon	Server OS only	10	1.06%
4776	NTLM Authentication	Success Only - Servers only	6	0.64%
4662	Operation performed on object	Server OS only	6	0.64%
5136	Directory service object was modified	No	6	0.64%
4657	A registry value was modified	No	5	0.53%
5156	Windows Filtering Platform has allowed a connection	No	4	0.42%
4720	User account created	Success only	4	0.42%
4738	User account changed	Success Only	4	0.42%

3.Windowsイベントログ設定の改善
(Improving the Windows event log audit settings)

Windowsのデフォルトログ設定の改善
Improving default settings

- 大和セキュリティによる、DFIRと脅威ハンティングのためのWindowsイベントログ設定の究極ガイド
  Yamato Security's Ultimate Windows Event Log Configuration Guide For DFIR And Threat Hunting
- https://github.com/Yamato-Security/EnableWindowsLogSettings
- (※日本語にも対応しているが、英語の方が最新)
  (Note: I'm trying to update the JP translations as quickly as possible but there is usually a lag. The EN documents have the latest info.)

Kerberos認証サービスのサブカテゴリ設定の例
Example of Kerberos sub-category settings:

Kerberos Authentication Service

> **Note: These events are only generated on domain controllers**

Volume: `High`

Default settings: `Client OS: No Auditing` | `Server OS: Success`

Recommended settings: `Client OS: No Auditing` | `Server OS: Success and Failure`

Notable Sigma rules:

- `(4768) (High) PetitPotam Suspicious Kerberos TGT Request`
- `(4768) (Med) Disabled Users Failing To Authenticate From Source Using Kerberos`
- `(4768) (Med) Invalid Users Failing To Authenticate From Source Using Kerberos`: Username guessing.
- `(4771) (Med) Valid Users Failing to Authenticate From Single Source Using Kerberos`: Password guessing.

各カテゴリのイベントIDの一覧:

List of all the important Event IDs by categories:

Event ID	Description	Sigma Rules	Hayabusa Rules	Level	Notes
4768	Kerberos TGT Request	3	Yes	Info~High	
4771	Kerberos Pre-Auth Failed	1	Not Yet	Info~Med	
4772	Kerberos Authentication Ticket Request Failed	0	No	None	This log is not in use. EID 4768 failure events are used instead.

4.Windowsイベントログ解析の課題と解決方法

(Challenges with event log analysis and the solution)

Windowsイベントログ解析の課題（1）
Windows event log challenges (1)

- ログの内容が分かりにくい！
  The logs are not intuitive!
- 7割以上がノイズ！
  Over 70% is usually noise!
- デフォルトで重要なログは残らない！
  Important logs aren't enabled by default!
- イベントログが300個以上のログで分散されている！
  Logs are separated over 300+ different logs!

Windowsイベントログ解析の課題（2）
Windows event log challenges (2)

- イベントレベルはDFIR観点ではない！
  Event log levels are not ideal for DFIR.
- 小規模のネットワークでも（1GB以下のデータでも）
  イベント数が十数万件以上ある！
  Even in a small network (with less than 1GB of data), there will be hundreds of thousands of events!
- →手動で調査できない！
  →Pure manual analysis is impossible!

解決方法:Fast Forensics解析ツールを利用する！
Solution: Use fast forensics analysis tools!

- Fast Forensicsツールは情報収集だけではない！
  Fast Forensics is NOT just about collection!
- Windows Event Log Fast Forensics解析ツール:
  (Windows event log fast forensics analysis tools)
  1. WELA
  2. Hayabusa
  3. Takajo

1. WELA (Windows Event Log Analyzer) (亦羅)

- 作者(Authors)：Zach Mathis、DustInDark、oginoPmP
- https://github.com/Yamato-Security/WELA
- 言語(Language)：Powershell
- ノイズをなるべく削減しながら、様々なイベント情報を抽出し、ログオンタイムラインを作成する。
  Creates a logon timeline from various event log sources and reduces all of the noise.
- NTLM使用の確認、攻撃検知等も可能。
  Other features: NTLM usage analysis, attack detection, etc...

Fast Forensicsログオンタイムライン(1)
Fast Forensics Logon Timeline(1)

- Windowsの横展開の痕跡が以下のログに残る:
  (These event IDs are often used for tracking lateral movement):
  4624: ログオンに成功 (Logon success)
  4634,4647: ログオフ (Logoff)
  4672: 管理者ログオン(Admin Logon)

Fast Forensicsログオンタイムライン(2)
Fast Forensics Logon Timeline(2)

・本来のログオンイベント解析の問題:
Traditional challenges with logon timeline analysis:

1. バックグラウンドでシステムアカウントのログオンイベントが頻繁に生成されるので、ノイズが非常に多い。
   System accounts will also logon and logoff in the background creating a lot of noise.
2. ログオン時間を計算するのに手動で計算する必要があった。
   Calculating the logon time was a manual process.
3. 管理者権限でログオンすると、２つのイベントが記録されるので、手動の関連付けは手間がかかる。
   Two logons happen with local admin accounts making correlating them more tedious.

WELA Usage (1)

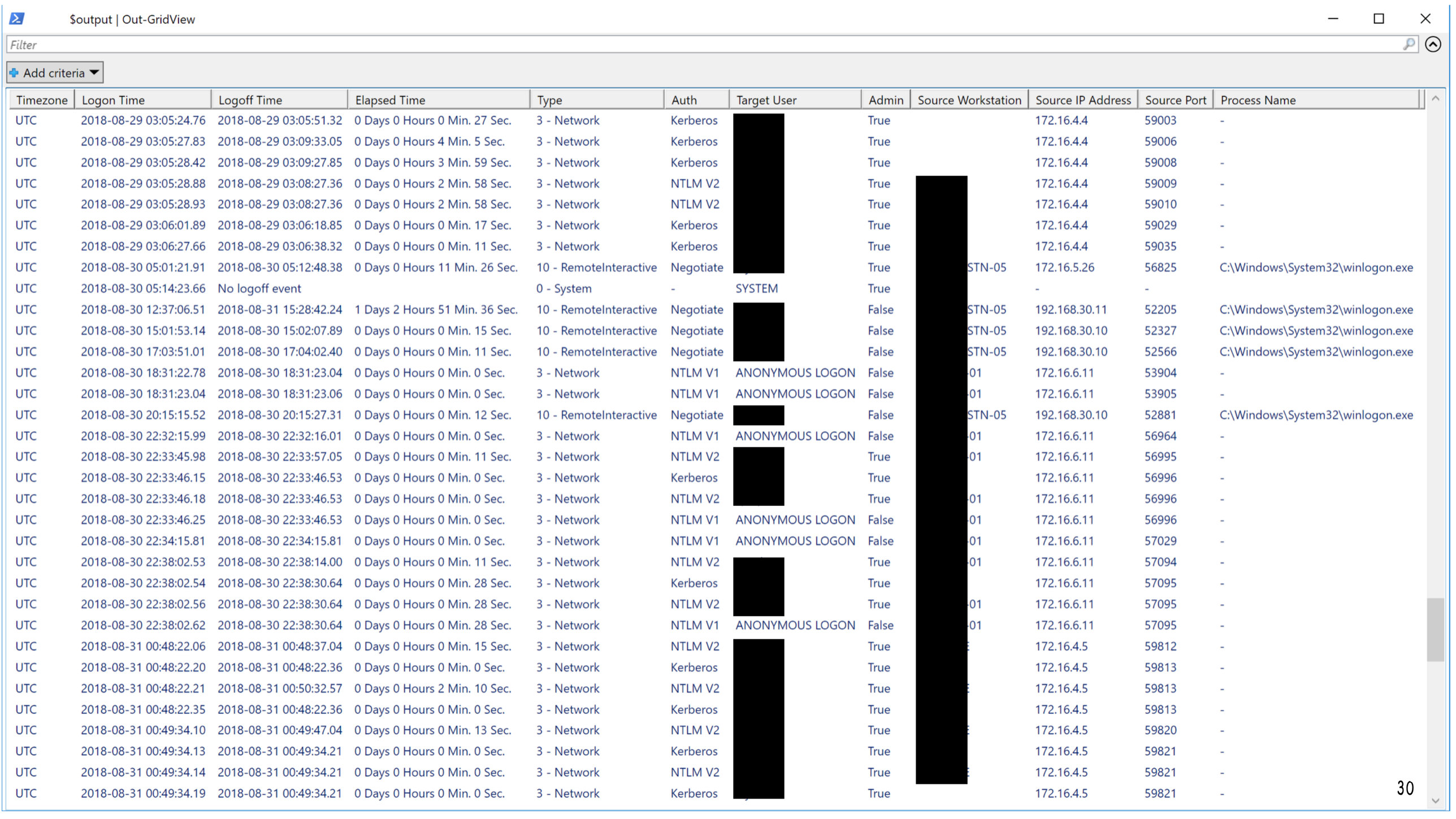
- PowerShellを開く。
  Open PowerShell。
- ライブ調査する場合は、管理者として開く。
  If you are doing live analysis, you need to run PowerShell with a local Administrator account.
- **WELA.ps1**でヘルプ画面が出力される。
  Run **WELA.ps1** to display the help menu.

WELA Usage (2)

- ライブ調査時のタイムライン作成:
  Generate Logon Timeline with Live Analysis：
  WELA.ps1 -LiveAnalysis $true -LogonTimeline $true -OutputGUI $true
- イベントIDの集計 (Event ID Metrics)：
  WELA.ps1 -LiveAnalysis $true -EventIDStatistics $true
- **-Japanese $true**で日本語で出力される。(Japanese output)
- **-SaveOutput file.txt**で結果を保存できる。(Save to file)

WELA Usage (3)

- オフライン解析(Offline Analysis)：
  WELA.ps1 -LogFile ..\evidence\Cobalt-Strike-Security.evtx -LogonTimeline $true -OutputGUI $true
- ローカル時間で表示されるが、**-UTC $true**を追加するとUTC時間で出力できる。
  Default is local time but can change to UTC with **-UTC $true**
- バグやまだ実装していないことがあるので、ソースコードをチェックして下さい！
  Please check the source code to see what is going on under the hood!



Timezone	Logon Time	Logoff Time	Elapsed Time	Type	Auth	Target User	Admin	Source Workstation	Source IP Address	Source Port	Process Name
UTC	2018-08-29 03:05:24.76	2018-08-29 03:05:51.32	0 Days 0 Hours 0 Min. 27 Sec.	3 - Network	Kerberos	[redacted]	True		172.16.4.4	59003	-
UTC	2018-08-29 03:05:27.83	2018-08-29 03:09:33.05	0 Days 0 Hours 4 Min. 5 Sec.	3 - Network	Kerberos		True		172.16.4.4	59006	-
UTC	2018-08-29 03:05:28.42	2018-08-29 03:09:27.85	0 Days 0 Hours 3 Min. 59 Sec.	3 - Network	Kerberos		True		172.16.4.4	59008	-
UTC	2018-08-29 03:05:28.88	2018-08-29 03:08:27.36	0 Days 0 Hours 2 Min. 58 Sec.	3 - Network	NTLM V2		True	[redacted]	172.16.4.4	59009	-
UTC	2018-08-29 03:05:28.93	2018-08-29 03:08:27.36	0 Days 0 Hours 2 Min. 58 Sec.	3 - Network	NTLM V2		True		172.16.4.4	59010	-
UTC	2018-08-29 03:06:01.89	2018-08-29 03:06:18.85	0 Days 0 Hours 0 Min. 17 Sec.	3 - Network	Kerberos		True		172.16.4.4	59029	-
UTC	2018-08-29 03:06:27.66	2018-08-29 03:06:38.32	0 Days 0 Hours 0 Min. 11 Sec.	3 - Network	Kerberos		True		172.16.4.4	59035	-
UTC	2018-08-30 05:01:21.91	2018-08-30 05:12:48.38	0 Days 0 Hours 11 Min. 26 Sec.	10 - RemoteInteractive	Negotiate		True	STN-05	172.16.5.26	56825	C:\Windows\System32\winlogon.exe
UTC	2018-08-30 05:14:23.66	No logoff event		0 - System	-	SYSTEM	True		-	-	
UTC	2018-08-30 12:37:06.51	2018-08-31 15:28:42.24	1 Days 2 Hours 51 Min. 36 Sec.	10 - RemoteInteractive	Negotiate	[redacted]	False	STN-05	192.168.30.11	52205	C:\Windows\System32\winlogon.exe
UTC	2018-08-30 15:01:53.14	2018-08-30 15:02:07.89	0 Days 0 Hours 0 Min. 15 Sec.	10 - RemoteInteractive	Negotiate		False	STN-05	192.168.30.10	52327	C:\Windows\System32\winlogon.exe
UTC	2018-08-30 17:03:51.01	2018-08-30 17:04:02.40	0 Days 0 Hours 0 Min. 11 Sec.	10 - RemoteInteractive	Negotiate		False	STN-05	192.168.30.10	52566	C:\Windows\System32\winlogon.exe
UTC	2018-08-30 18:31:22.78	2018-08-30 18:31:23.04	0 Days 0 Hours 0 Min. 0 Sec.	3 - Network	NTLM V1	ANONYMOUS LOGON	False	01	172.16.6.11	53904	-
UTC	2018-08-30 18:31:23.04	2018-08-30 18:31:23.06	0 Days 0 Hours 0 Min. 0 Sec.	3 - Network	NTLM V1	ANONYMOUS LOGON	False	01	172.16.6.11	53905	-
UTC	2018-08-30 20:15:15.52	2018-08-30 20:15:27.31	0 Days 0 Hours 0 Min. 12 Sec.	10 - RemoteInteractive	Negotiate	[redacted]	False	STN-05	192.168.30.10	52881	C:\Windows\System32\winlogon.exe
UTC	2018-08-30 22:32:15.99	2018-08-30 22:32:16.01	0 Days 0 Hours 0 Min. 0 Sec.	3 - Network	NTLM V1	ANONYMOUS LOGON	False	01	172.16.6.11	56964	-
UTC	2018-08-30 22:33:45.98	2018-08-30 22:33:57.05	0 Days 0 Hours 0 Min. 11 Sec.	3 - Network	NTLM V2		True	01	172.16.6.11	56995	-
UTC	2018-08-30 22:33:46.15	2018-08-30 22:33:46.53	0 Days 0 Hours 0 Min. 0 Sec.	3 - Network	Kerberos		True		172.16.6.11	56996	-
UTC	2018-08-30 22:33:46.18	2018-08-30 22:33:46.53	0 Days 0 Hours 0 Min. 0 Sec.	3 - Network	NTLM V2		True	01	172.16.6.11	56996	-
UTC	2018-08-30 22:33:46.25	2018-08-30 22:33:46.53	0 Days 0 Hours 0 Min. 0 Sec.	3 - Network	NTLM V1	ANONYMOUS LOGON	False	01	172.16.6.11	56996	-
UTC	2018-08-30 22:34:15.81	2018-08-30 22:34:15.81	0 Days 0 Hours 0 Min. 0 Sec.	3 - Network	NTLM V1	ANONYMOUS LOGON	False	01	172.16.6.11	57029	-
UTC	2018-08-30 22:38:02.53	2018-08-30 22:38:14.00	0 Days 0 Hours 0 Min. 11 Sec.	3 - Network	NTLM V2		True	01	172.16.6.11	57094	-
UTC	2018-08-30 22:38:02.54	2018-08-30 22:38:30.64	0 Days 0 Hours 0 Min. 28 Sec.	3 - Network	Kerberos		True		172.16.6.11	57095	-
UTC	2018-08-30 22:38:02.56	2018-08-30 22:38:30.64	0 Days 0 Hours 0 Min. 28 Sec.	3 - Network	NTLM V2		True	01	172.16.6.11	57095	-
UTC	2018-08-30 22:38:02.62	2018-08-30 22:38:30.64	0 Days 0 Hours 0 Min. 28 Sec.	3 - Network	NTLM V1	ANONYMOUS LOGON	False	01	172.16.6.11	57095	-
UTC	2018-08-31 00:48:22.06	2018-08-31 00:48:37.04	0 Days 0 Hours 0 Min. 15 Sec.	3 - Network	NTLM V2		True		172.16.4.5	59812	-
UTC	2018-08-31 00:48:22.20	2018-08-31 00:48:22.36	0 Days 0 Hours 0 Min. 0 Sec.	3 - Network	Kerberos		True		172.16.4.5	59813	-
UTC	2018-08-31 00:48:22.21	2018-08-31 00:50:32.57	0 Days 0 Hours 2 Min. 10 Sec.	3 - Network	NTLM V2		True		172.16.4.5	59813	-
UTC	2018-08-31 00:48:22.35	2018-08-31 00:48:22.36	0 Days 0 Hours 0 Min. 0 Sec.	3 - Network	Kerberos		True		172.16.4.5	59813	-
UTC	2018-08-31 00:49:34.10	2018-08-31 00:49:47.04	0 Days 0 Hours 0 Min. 13 Sec.	3 - Network	NTLM V2		True		172.16.4.5	59820	-
UTC	2018-08-31 00:49:34.13	2018-08-31 00:49:34.21	0 Days 0 Hours 0 Min. 0 Sec.	3 - Network	Kerberos		True		172.16.4.5	59821	-
UTC	2018-08-31 00:49:34.14	2018-08-31 00:49:34.21	0 Days 0 Hours 0 Min. 0 Sec.	3 - Network	NTLM V2		True		172.16.4.5	59821	-
UTC	2018-08-31 00:49:34.19	2018-08-31 00:49:34.21	0 Days 0 Hours 0 Min. 0 Sec.	3 - Network	Kerberos		True		172.16.4.5	59821	-

```
Processing time: 0 hours 0 minutes 3 seconds.
--------------------
# Successful_Logons:

User             Type 0 Type 2 Type 3 Type 4 Type 5 Type 7 Type 8 Type 9 Type 10 Type 11 Type 12 Type 13 Unknown
----             ------ ------ ------ ------ ------ ------ ------ ------ ------- ------- ------- ------- -------
SYSTEM                3      0      0      0    283      0      0      0       0       0       0       0       0
UMFD-0                0      3      0      0      0      0      0      0       0       0       0       0       0
UMFD-1                0      3      0      0      0      0      0      0       0       0       0       0       0
NETWORK SERVICE       0      0      0      0      3      0      0      0       0       0       0       0       0
DWM-1                 0      6      0      0      0      0      0      0       0       0       0       0       0
LOCAL SERVICE         0      0      0      0      3      0      0      0       0       0       0       0       0
ANONYMOUS LOGON       0      0      3      0      0      0      0      0       0       0       0       0       0
Sec504                0     10      0      0      0      0      0      0       0       0       0       0       0


# BadUser_Failed_Logons:
No events of this event type.

# BadPassword_Failed_Logons:

User    Type 0 Type 2 Type 3 Type 4 Type 5 Type 7 Type 8 Type 9 Type 10 Type 11 Type 12 Type 13 Unknown
----    ------ ------ ------ ------ ------ ------ ------ ------ ------- ------- ------- ------- -------
Sec504       0      1      0      0      0      0      0      0       0       0       0       0       0
```

```
8001 (Outbound NTLM Authentication) Log Analysis:
Outgoing NTLM authentication to servers:
ldap/[redacted]0
ldap/[redacted].jp
cifs/[redacted].jp

Outgoing NTLM authentication with usernames:
[redacted]dc
[redacted]admin

8002 (Inbound NTLM  Authentication) Log Analysis:
Inbound NTLM authentication with usernames :
ISMG-[redacted]$


8004 (NTLM  Authentication to DC) Log Analysis:
Summary:
------------
8001 Events: 1065
8002 Events: 46
8004 Events: 0
```

- NTLMログ解析
  NTLM usage anlaysis
- NTLMはSMBv1ほど危険なプロトコル！
  NTLM can be as dangerous as SMBv1!
- どうしても必要な場合はポリシーで除外できるので、NTLMを無くそう！
  Use this to discover your NTLM usage and disable if you can. You can always set exceptions when needed!

2. Hayabusa(隼) (Peregrine Falcon)

- Released: 2021/12/25。Latest stable version: 1.7.2
- HP: https://github.com/Yamato-Security/hayabusa
- WindowsイベントログのFast Forensicsタイムライン作成＆脅威ハンティングツール。
  A Windows event log fast forensics timeline generator and threat hunting tool.
- 開発者(Developers):
  - Akira Nishikawa (@nishikawaakira)
  - DustInDark (@hitenkoku)
  - James Takai / hachiyone(@hach1yon)
  - ItiB (@itiB_S144)
  - Kazuminn (@k47_um1n)
  - Garigariganzy (@garigariganzy31)
  - Fukusuke Takahashi (@fukuseket)
  - Yusuke Matsui (@apt773)(AD Hacking Group Leader)

Hayabusaの特徴
Hayabusa attributes

- Rustで開発しているので:
  Developed in Rust:
  - 高速！(Very fast!)
  - 安全！(Memory safe!)
  - Windows, Linux, macOS, その他に対応！
    Supports Windows, Linux, macOS, etc...
  - スタンドアロンで実行可能！
    Executable is standalone!
- ルールはSigmaのYAMLルールなので、書きやすい！
  Rules are Sigma YAML files so easy to write!

Hayabusa

- 様々な端末の300個以上のWindowsイベントログをスキャンし、重要なログや攻撃の痕跡だけを抽出し、一個のCSVまたはJSON/Lタイムラインを作成する。
  Scans the 300+ Windows event logs, detects attacks, possible attacks and important events and saves the results to CSV or JSON/L for easy analysis.
- CSVの解析ツール: Excel, Timeline Explorer, Elastic Stack(ELK), Timesketch (Import the CSV into one of these.)
- JSON/Lはjqで解析や情報抽出が可能。(Analyze JSON with jq)
- 約8割のノイズ削減! (Reduces noise by about 80%!)

データ削減 (Data reduction)

- 大半の不要のイベントを無視するだけではなく、抽出するイベントのデータも省略する
  Not only does Hayabusa ignore the majority of unneeded events, it also abbreviates the amount of data in events to the bare minimum.
- ファイルサイズがかなり小さくなるだけではなく、全データが一台のモニターに収まるので、解析が楽で速くなる。
  Not only does the file size get reduced to a fraction, but all of the data can fit on one screen, so analysis becomes easier and faster.

EID 4624 Example

An account was successfully logged on.

Subject:
- Security ID: SYSTEM
- Account Name: SEC504STUDENT$
- Account Domain: SEC504
- Logon ID: 0x3E7

Logon Information:
- Logon Type: 5
- Restricted Admin Mode: -
- Virtual Account: No
- Elevated Token: Yes

Impersonation Level: Impersonation

New Logon:
- Security ID: SYSTEM
- Account Name: SYSTEM
- Account Domain: NT AUTHORITY
- Logon ID: 0x3E7
- Linked Logon ID: 0x0
- Network Account Name: -
- Network Account Domain: -
- Logon GUID: {00000000-0000-0000-0000-000000000000}

Process Information:
- Process ID: 0x290
- Process Name: C:\Windows\System32\services.exe

Network Information:
- Workstation Name: -
- Source Network Address: -
- Source Port: -

Detailed Authentication Information:
- Logon Process: Advapi
- Authentication Package: Negotiate
- Transited Services: -
- Package Name (NTLM only): -
- Key Length: 0

This event is generated when a logon session is created. It is generated on the computer that was accessed.

The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.

The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network).

The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on.

The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases.

The impersonation level field indicates the extent to which a process in the logon session can impersonate.

The authentication information fields provide detailed information about this specific logon request.
- Logon GUID is a unique identifier that can be used to correlate this event with a KDC event.
- Transited services indicate which intermediate services have participated in this logon request.
- Package name indicates which sub-protocol was used among the NTLM protocols.
- Key length indicates the length of the generated session key. This will be 0 if no session key was requested.

2170 Bytes

591B

User: IEUser ¦
Comp: IE10WIN7 ¦
IP-Addr: 127.0.0.1 ¦
LID: 0x17125

69B

and/or

AuthenticationPackageName: Negotiate ¦ IpAddress: 127.0.0.1 ¦ IpPort: 0 ¦ KeyLength: 0 ¦ LmPackageName: - ¦ LogonGuid: 00000000-0000-0000-0000-000000000000 ¦ LogonProcessName: User32 ¦ LogonType: 2 ¦ ProcessId: 0x17c ¦ ProcessName: C:\Windows\System32\winlogon.exe ¦ SubjectDomainName: WORKGROUP ¦ SubjectLogonId: 0x3e7 ¦ SubjectUserName: IE10WIN7$ ¦ SubjectUserSid: S-1-5-18 ¦ TargetDomainName: IE10WIN7 ¦ TargetLogonId: 0x17125 ¦ TargetUserName: IEUser ¦ TargetUserSid: S-1-5-21-3463664321-2923530833-3546627382-1000 ¦ TransmittedServices: - ¦ WorkstationName: IE10WIN7

省略 (Abbreviations)

- `DvrFmwk` : `Microsoft-Windows-DriverFrameworks-UserMode/Operational`
- `Exchange` : `MSExchange Management`
- `Firewall` : `Microsoft-Windows-Windows Firewall With Advanced Security/Firewall`
  - `Recon` : Reconnaissance
  - `ResDev` : Resource Development
  - `InitAccess` : Initial Access
  - `Exec` : Execution
  - `Persis` : Persistence
  - `PrivEsc` : Privilege Escalation
  - `Evas` : Defense Evasion
  - `CredAccess` : Credential Access
  - `Disc` : Discovery
  - `LatMov` : Lateral Movement
  - `Collect` : Collection
  - `C2` : Command and Control
  - `Exfil` : Exfiltration
  - `Impact` : Impact

- `Perm` -> Permament
- `Pkg` -> Package
- `Priv` -> Privilege
- `Proc` -> Process
- `PID` -> Process ID
- `PGUID` -> Process GUID (Global Unique ID)
- `Ver` -> Version

Hayabusaの検知ルール
Hayabusa's detection rules

- Hayabusa rules: 141
- Sigma rules: 3011
- 毎日Sigmaコミュニティに更新される！
  Updated daily by the Sigma community!

Sigma

- HP: https://github.com/SigmaHQ/sigma
- OSSで提供されているYAML形式の検知ルール。
  Open source YAML based detection rules.
- ログベースIoCの基準。
  Default standard for log-based IoCs.
- Windowsイベントログ以外にLinux、macOS、クラウド、ネットワーク、ウェブ、プロキシ等々の検知ルールもある。
  Besides Windows rules, there are rules for linux, macOS, cloud, network, web, proxies, etc...
- Sigmaルールから多くのSIEM等のクエリに変換できる！
  You can convert sigma rules into any other SIEM query format!

Sigmaコンバータが対応しているバックエンド
Backends supported by Sigma

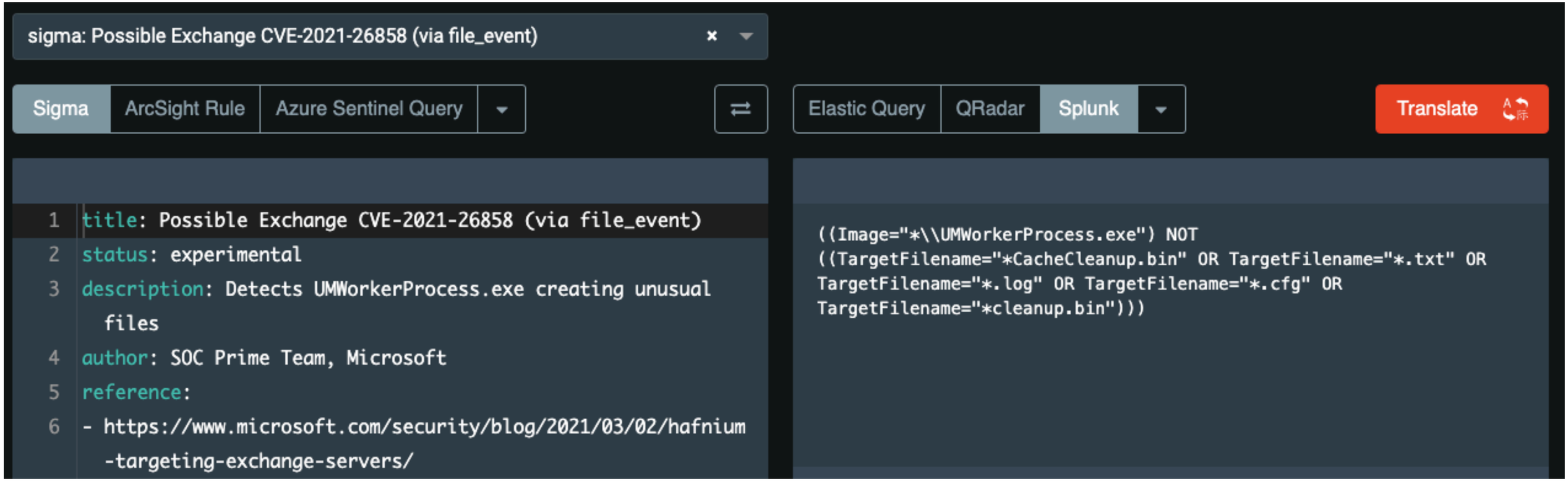
- sumologic-cse-rule, splunkxml, dnif, athena, qradar, netwitness-epl, arcsight, splunk, streamalert, ala-rule, grep, fireeye-helix, logpoint, elastalert-dsl, ee-outliers, kibana, fortisiem, hayabusa, humio, sumologic, es-rule, es-eql, hawk, datadog-logs, sysmon, graylog, carbonblack, mdatp, crowdstrike, splunk, fieldlist, qualys, devo, arcsight-esm, powershell, limacharlie, opensearch-monitor, sentinel-rule, sql, csharp, stix, es-qs, elastalert, lacework, xpack-watcher, logiq, ala, uberagent, sumologic-cse, hedera, kibana-ndjson, es-dsl, hayabusa, netwitness, es-rule-eql, es-qs-lr, chronicle, sqlite

```yaml
title: Possible Exchange CVE-2021-26858 (via file_event)
status: experimental
description: Detects UMWorkerProcess.exe creating unusual files
author: SOC Prime Team, Microsoft
reference:
- https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26858
tags:
- attack.initial_access
- attack.t1190
logsource:
    category: file_event
    product: windows
detection:
    selection:
        Image:
        - '*\UMWorkerProcess.exe'
    filter:
        TargetFilename|endswith:
        - CacheCleanup.bin
        - .txt
        - .log
        - .cfg
        - cleanup.bin
    condition: selection and not filter
falsepositives:
- unknown
level: medium
```

Sigmaルールの変換サイト

Sigma rule conversion test site

- https://uncoder.io/



Hayabusa Rules

- 殆どはSigmaルールのサブセット（互換性があるので、同じように他のSIEMクエリに変換できる。）
  Almost all are a subset of sigma. (They are compatible so can be converted like sigma rules as well.)
- Sigmaルールにない機能もある(detailsやequalsfieldのフィールド)
  There are some extensions (details, equalsfield, etc...)
- 詳細(Details):
  https://github.com/Yamato-Security/hayabusa-rules

SigmaとHayabusaルールの違い (Rule differences)

Sigma

```yaml
logsource:
    category: process_access
    product: windows
detection:
    selection:
        TargetImage|endswith: '\WINDOWS\System32\svchost.exe'
        GrantedAccess: '0x1F3FFF'
        CallTrace|contains: 'UNKNOWN'
    condition: selection
```

Converted Hayabusa Rule

```yaml
detection:
    SELECTION_1:
        EventID: 10
    SELECTION_2:
        Channel: Microsoft-Windows-Sysmon/Operational
    SELECTION_3:
        TargetImage: '*\WINDOWS\System32\svchost.exe'
    SELECTION_4:
        GrantedAccess: '0x1F3FFF'
    SELECTION_5:
        CallTrace: '*UNKNOWN*'
    condition: (SELECTION_1 and SELECTION_2 and SELECTION_3 and SELECTION_4 and SELECTION_5)
```

Simple Hayabusa Rule

- ”Hidden User Account Created!”

```yaml
logsource:
    product: windows
    service: security
detection:
    selection:
        Channel: Security
        EventID: 4720
        TargetUserName|endswith: "$"
    condition: selection
```

← Sigmaとの互換性のためにlogsourceを定義している。
(To keep compatibility with Sigma, we define the logsource even in Hayabusa rules.)

FP(False Positive)がある場合はfilterする

Define ”filter” conditions to exclude FPs

- ”Local User Account Created”

```
logsource:
    product: windows
    service: security
detection:
    selection:
        Channel: Security
        EventID: 4720
    filter:
        TargetUserName|endswith: "$" #Filter out machine/computer accounts
    condition: selection and not filter
```

よく使うオプション(Common Options)

- -h, --help : ヘルプメニュー (Help)
- -u, --update-rules : ルール更新 (Rule Updates)
- -d, --directory : ディレクトリスキャン (Dir. Scan)
- -f, --filepath : ファイルスキャン (File Scan)
- -o, --output : CSVに保存する (CSV Output)
- -U, --UTC : UTC時間を使う (Use UTC)
- -m, --min-level low : アラートだけ出力 (Just alerts)
- -l, --live-analysis : Windows端末でのライブ調査 (Live)

出力プロファイル(Output Profiles)

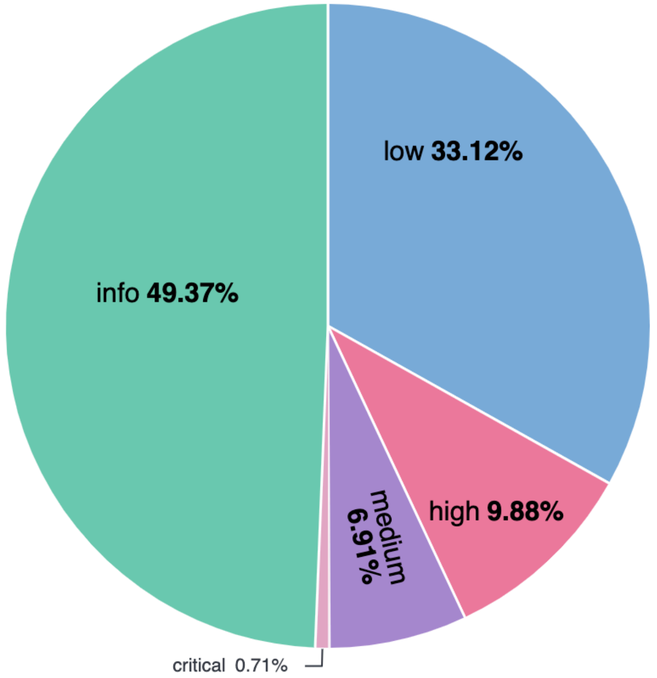
- -P, --profile <profile>で出力する情報をカスタマイズできる。
  What you want to output is completely customizable.
  Default is the ”standard” profile。
- 現在の用意されたプロファイル(Built-in profiles):
  minimal, standard, verbose, all-field-info, all-field-info-verbose, super-verbose, timesketch-minimal, timesketch
- --list-profilesオプションでプロファイルの内容確認する。
  Check the built-in profiles with this option.
- ./config/profiles.yamlでプロファイルをカスタマイズ。
  You can configure your own output profile in this config file.

プロファイルの比較(Profile Comparisons)

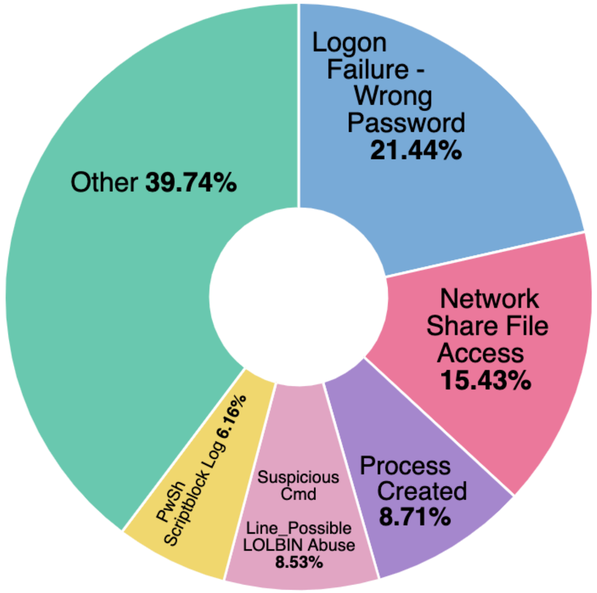
Profile	Processing Time	Output Filesize
minimal	16 minutes 18 seconds	690 MB
standard	16 minutes 23 seconds	710 MB
verbose	17 minutes	990 MB
timesketch-minimal	17 minutes	1015 MB
all-field-info-verbose	16 minutes 50 seconds	1.6 GB
super-verbose	17 minutes 12 seconds	2.1 GB

Time	Computername	Eventid	Level	Alert	Details
2021-05-22 05:43:18.227 +09:00	fs01.offsec.lan	4648	informational	Explicit Logon	Source User: FS01$: Targ
2021-05-22 05:43:22.562 +09:00	fs01.offsec.lan	4625	low	Logon Failure - Wrong Password	User: admmig@offsec.lan :
2021-05-22 05:43:49.345 +09:00	fs01.offsec.lan	4625	low	Logon Failure - Wrong Password	User: admmig@offsec.lan :
2021-05-22 05:43:50.131 +09:00	fs01.offsec.lan	4625	low	Logon Failure - Wrong Password	User: admmig@offsec.lan :
2021-05-22 05:43:50.607 +09:00	fs01.offsec.lan	4625	low	Logon Failure - Wrong Password	User: admmig@offsec.lan :
2021-05-22 05:43:50.866 +09:00	fs01.offsec.lan	4625	low	Logon Failure - Wrong Password	User: admmig@offsec.lan :
2021-05-23 06:56:57.685 +09:00	fs01.offsec.lan	1102	high	Security log was cleared	User: admmig
2021-05-23 06:57:11.842 +09:00	fs01.offsec.lan	4688	high	Relevant Anti-Virus Event	
2021-05-23 06:57:11.842 +09:00	fs01.offsec.lan	4688	critical	Mimikatz Use	
2021-05-26 22:02:27.149 +09:00	mssql01.offsec.lan	4624	informational	Logon Type 3 - Network	User: admmig : Workstatio
2021-05-26 22:02:27.155 +09:00	mssql01.offsec.lan	5145	medium	DCERPC SMB Spoolss Named Pipe	
2021-05-26 22:02:27.155 +09:00	mssql01.offsec.lan	5145	critical	CVE-2021-1675 Print Spooler Exploitation IPC Access	
2021-05-26 22:02:29.726 +09:00	mssql01.offsec.lan	4624	informational	Logon Type 3 - Network	User: admmig : Workstatio
2021-05-26 22:02:29.734 +09:00	mssql01.offsec.lan	5145	medium	DCERPC SMB Spoolss Named Pipe	
2021-05-26 22:02:29.734 +09:00	mssql01.offsec.lan	5145	critical	CVE-2021-1675 Print Spooler Exploitation IPC Access	
2021-05-26 22:02:34.373 +09:00	mssql01.offsec.lan	4624	informational	Logon Type 3 - Network	User: admmig : Workstatio
2021-05-26 22:02:34.375 +09:00	mssql01.offsec.lan	5145	medium	DCERPC SMB Spoolss Named Pipe	
2021-05-26 22:02:34.379 +09:00	mssql01.offsec.lan	4624	informational	Logon Type 3 - Network	User: admmig : Workstatio
2021-05-26 22:02:34.379 +09:00	mssql01.offsec.lan	4624	informational	Logon Type 3 - Network	User: admmig : Workstatio
2021-05-26 22:02:34.380 +09:00	mssql01.offsec.lan	4624	informational	Logon Type 3 - Network	User: admmig : Workstatio
2021-05-27 05:24:46.570 +09:00	rootdc1.offsec.lan	4768	medium	Possible AS-REP Roasting	Possible AS-REP Roasting
2021-05-27 05:24:46.570 +09:00	rootdc1.offsec.lan	4768	informational	Kerberos TGT was requested	User: admin-test : Servic
2021-06-01 23:06:34.542 +09:00	fs01.offsec.lan	4720	medium	Local user account created	User: WADGUtilityAccount :
2021-06-01 23:08:21.225 +09:00	fs01.offsec.lan	4720	medium	Local user account created	User: elie : SID:S-1-5-21
2021-06-03 21:17:56.988 +09:00	fs01.offsec.lan	1102	high	Security log was cleared	User: admmig
2021-06-03 21:18:12.941 +09:00	fs01.offsec.lan	4672	informational	Admin Logon	User: admmig : LogonID: 0
2021-06-03 21:18:12.942 +09:00	fs01.offsec.lan	4624	informational	Logon Type 3 - Network	User: admmig : Workstatio
2021-06-04 03:34:12.672 +09:00	fs01.offsec.lan	4104	high	Windows Firewall Profile Disabled	
2021-06-04 04:17:44.873 +09:00	fs01.offsec.lan	1102	high	Security log was cleared	User: admmig

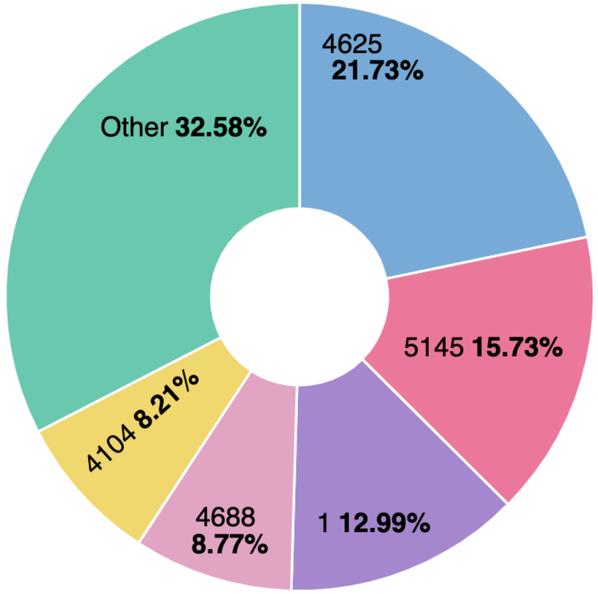
Risk Level



Detection Rule



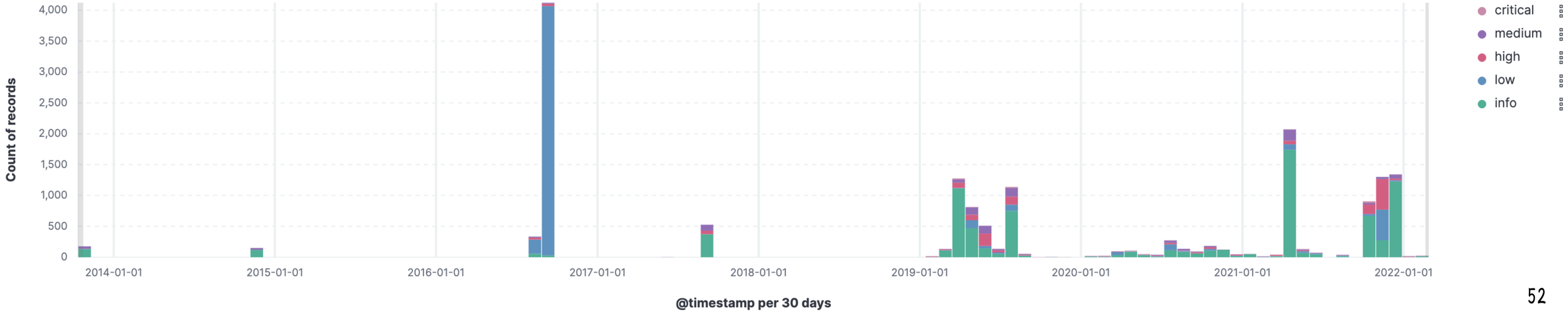
Event ID



Computer Names

Top values of Compı	Count of records
DESKTOP-M5SN04R	3,561
fs03vuln.offsec.lan	2,307
FS03.offsec.lan	2,057
MSEDGEWIN10	2,039
PC01.example.corp	1,274
IEWIN7	1,087
IE10Win7	955
SEC511	526
win10-02.offsec.lan	482
srvdefender01.offse...	480
Other	1,854

Risk Over Time



New feature in 1.7.0!

- HTML Results Summary(DustInDark & Akira Nishikawa)

- スキャンが終わった時点、いつ、どの端末、何があったかは大体想像できる。

  As soon as the scan finishes, you have a good picture of when the incident happened, what hosts were compromised and what techniques were used.

Results Summary

- Saved alerts and events: 128,428
- Total events analyzed: 720,572
- Data reduction: 592,144 events (82.18%)
- Dates with most total detections:
  - critical: 2022-08-06 (33)
  - high: 2022-08-05 (1,045)
  - medium: 2022-08-06 (7,178)
  - low: 2022-08-06 (85,066)
  - informational: 2022-08-06 (127,768)

Computers with most unique critical detections:

- ACC-10.corp.net (2)
- ACC-02.corp.net (2)
- ACC-07.corp.net (2)
- ACC-01.corp.net (2)
- ACC-04.corp.net (2)

Computers with most unique high detections:

- ACC-07.corp.net (43)
- ACC-10.corp.net (41)
- ACC-01.corp.net (39)
- ACC-04.corp.net (39)

Top critical alerts:

- CobaltStrike Named Pipe (28)
- CobaltStrike Service Installations in Registry (5)

Top high alerts:

- Suspicious Svchost Process (511)
- Suspicious Eventlog Clear or Configuration Using Wevtutil (223)
- Suspicious Encoded PowerShell Command Line (178)
- Use Short Name Path in Image (123)
- NetNTLM Downgrade Attack (96)
- Suspicious PowerShell Encoded Command Patterns (90)
- Rundll32 Execution Without DLL File (70)
- Accessing WinAPI in PowerShell (60)

Sigmaルールの毎晩更新

Sigma rules are updated daily!

- Special thanks to:
  itiB (@itiB_S144)
  James Takai / hachiyone (@hach1yon)
- **hayabusa.exe -u**で簡単にルール更新できる！
  Updating to the latest and greatest rules is as easy as typing **-u** !

脅威ハンティングの注意点(1)

Points to keep in mind about threat hunting(1)

- 誤検知(FP)が出る！(出るようにしている！)
  You will get FPs (False Positives)! (This is by design!)
- 必要以上に誤検知があれば、チューニングすべきだが、ある程度誤検知が出るようにスキャンしなければ未知の攻撃を検出できない。
  Of course if you are getting too many FPs for your environment you will need to tune, fix rules, etc...however, if you are not scanning with generic enough rules that produce some false positives you will most likely not be able to detect unknown attacks.

脅威ハンティングの注意点(2)

Points to keep in mind about threat hunting(2)

- 手動で専門家が確認する必要がある。
  A specialist will have to manually confirm the results.
- 例: 管理者アカウントの作成。管理者が意図的に作ったのか、攻撃者が作ったのか手動で確認する必要がある。
  Simple example: an administrator account creation. Was it created intentionally or did an attacker create it?

セキュリティ監視 V.S.	脅威ハンティング
リアルタイム	インシデントを検出するのにかかる時間は、スキャンの頻度に依存する
検知ルールはその時点の性能に依存する（回避されたら、ずっと気づかない）	検知ルールの性能が段々上がるので、新しいIoCで過去のインシデントに気づく可能性がある
アラートが多過ぎると、SOCアナリストが困るので、出過ぎないようにチューニングされている（デメリット：高度な攻撃や未知の攻撃手法を検知できない可能性が上がる）	徹底的に調査するのになるべく多くの検知ルールを使う。誤検知も沢山でるが、高度な攻撃や未知の攻撃手法を検知する可能性が上がる

Security Monitoring	v.s.	Threat Hunting
Real-time		The time to discover an incident will depend on the frequency of your threat hunting scans.
Detection is limited to your rules at that point in time. (If the rules are bypassed, then you won't be able to discover the attack later.)		Detection rules get better over time so you will be able to discover past incidents with new IoCs.
If there are too many alerts, the SOC analysts will be overloaded so often generic rules are avoided. (Demerit: chances of detecting advanced or unknown attacks decrease.)		In order to do thorough hunts, many generic rules are often used. (Merit: chances of detecting advanced or unknown attacks rise.)

脅威ハンティングのアドバイス(1)
Threat hunting advice(1)

- まず、一つのアラートを深堀りしない！
  At first, don't deep dive into any single alert! (Avoid rabbit holes!)
- アラートレベルの順番にcriticalからlowまで一通り確認して、状況の全体を把握する。
  Take a quick look through all of the alerts in order from critical to low to get a grasp of things.
- Pivotキーワードリストを作成していく。(ログオンID、マルウェアのファイル名、不審なIPアドレスやホスト名、不審なユーザ名等々。)
  Create a pivot keyword list. (Logon IDs, malware filenames, suspicious processes, IP addresses, hostnames, etc...)
- その後、Pivotキーワードを検索したら、他の証拠も出てくるはず。
  Later search on those pivot keywords and more evidence should come up.

脅威ハンティングのアドバイス(2)
Threat hunting advice(2)

- ノイズをなるべくフィルタする！
  Filter noise as much as possible!
- (Excelではなく) Timeline Explorer、Timesketch, Elastic Stack等を使いこなす！
  Use Timeline Explorer, Timesketch, Elastic Stack (not Excel!)
- ルールロジックが理想でない場合(誤検知の場合)は、私に連絡頂ければ、ルールを直して、上流のSigmaレポジトリにPRを出す！
  If you find a rule that does not have ideal logic (you are getting FPs), please inform the upstream sigma repository or tell me and I will try to fix it and send a PR to the sigma repository.

Hayabusaの開発予定の機能
Hayabusa Planned Features

- 各端末で定期的にスキャンして、結果をSIEMに送信する
  Periodically scan endpoints and send the results to a SIEM.

- Windowsイベントログ以外のスキャン(Sysmon for Linux、クラウドログ等々)
  Support for other log sources besides Windows event logs. (Sysmon for Linux, Cloud logs, etc...)

3. Takajo（鷹匠）(Falconer)

- First official release today!: 1.0.0
- HP: https://github.com/Yamato-Security/takajo
- Hayabusa結果の解析ツール (Hayabusa results analyzer)
- Core Developer: DustInDark (@hitenkoku)
- Tool design, coding, etc...: Zach Mathis (@yamatosecurity)
- Nimでの開発 (Developed in Nim)
  - 見た目はPythonのような簡単なスクリプト言語
    Looks like an easy script language like Python
  - C/C++/Javascriptにコンパイルできる！
    But compiles to C/C++/Javascript!
  - 高速！安全！（のはず）
    Fast! Safe! (at least should be)

Takajoの機能 (Features)

- **undetected-evtx**
  - 検知できないサンプルevtxファイルの一覧表示
    List up all of the sample evtx files that aren't detected.
  - 現在は約100個 (There are about 100 at the moment.)
  - 検知できるようにSigmaルールを書こう！
    Let's write sigma rules to detect all the things!
    (Submit to the upstream sigma repo so everyone can benefit.)
- **unused-rules**
  - 使用されていないルールの一覧表示
    List up all of the unused rules.
  - 現在は数百個 (There are hundreds at the moment.)
  - ルールの検証できるようにサンプルevtxファイルを作ろう！
    Let's create as many sample evtx files as possible to verify rules.

Takajoの開発予定の機能 (Planned Features)

- **logon-timeline**
  - WELAのようなログオンタイムライン作成
    Create a logon timeline like WELA does.
- **malicious-process-trees**
  - 悪意のあるプロセスのプロセスツリー図で親子関係の可視化
    Visualize the parent-child relationship of malicious processes with process trees, etc...
- **behavior-analysis**
  - 機械学習を使った行動解析(横展開等々)
    Behavior analysis via ML (Lateral movement, etc...)

5.より学びたい貢献したい
あなたへの参考情報
(Resources for learning more and/or contributing)

ディテクションエンジニアリングについて
About Detection Engineering

- The Bicycle of the Forensic Analyst
  https://cyb3rops.medium.com/the-bicycle-of-the-forensic-analyst-6dc83fb6fb34
- About Detection Engineering
  https://cyb3rops.medium.com/about-detection-engineering-44d39e0755f0
- Capturing Detection Ideas to Improve Their Impact
  https://cyb3rops.medium.com/capturing-detection-ideas-to-improve-their-impact-311cf4e1c7a8

大和セキュリティへの貢献
Contributing to the community

- Hayabusa development (Rust)
- Takajo development (Nim)
- WELA development (PowerShell)
- ドキュメンテーションの和訳 (Documentation localization)
- Hayabusaの検証とルールチューニング (Hayabusa testing & tuning)
- Sigma/Hayabusa rule development (Detection Engineering)
  (https://github.com/Yamato-Security/hayabusa-sample-evtxで検知できないevtxが沢山！) (Many evtx logs are still undetectable!)
- 新しい攻撃手法の検証とサンプルevtxファイル作成
  Create new sample evtx files based on new attacks.
- AD Hacking WGへの参加（隔週の火曜日20時から情報共有）

大和セキュリティへの参加

Joining Yamato Security

- 大和セキュリティslackへ自由に参加して、何でもお聞き下さい。
- https://yamatosecurity.connpass.com/
- Join this slack channel, ask me anything!

Open Sourceツール開発をおすすめ！

I recommend creating some OSS tool!

- コミュニティに貢献するだけではなく、自分のためにもなる！
- It won’t just help out the community but will surely be very beneficial to yourself as well!

ご清聴、

ありがとうございました！

Thank you for listening!