**MITRE ATT&CK Fundamentals (1 day)**

* Understands the MITRE ATT&CK framework, a globally accessible knowledge base, and a cyber adversary behavior model based on real-world observations.
* Is familiar with how the ATT&CK knowledge base documents real-world adversary tactics, techniques, and procedures (TTPs).
* Can visualize the various ways to exploit the understanding of adversary TTPs to address current (operational) and future (strategic) threats.
* Grasps how ATT&CK enables us to produce measurable and trackable answers to the hard questions we face every day as defenders, such as “how does our decision to \_\_\_\_ make us better/worse at defending against threats?”
* Link Video: <https://www.youtube.com/watch?v=1cCt2XZr2ms>

Module 1: Understanding ATT&CK

* Introduction to ATT&CK
  + Là 1 cơ sở tri thức của hành vi của đối thủ
  + Dựa trên quan sát ở thế giới thực
  + Mở miễn phí và có thể truy cập trên toàn cầu
  + Thúc đẩy đóng góp cộng đồng
* Matrices/Platforms
  + Matrix cho ta 1 cái nhìn tổng quát về mqh giữa tactic, technique và sub-tech
  + Mỗi matrix tập trung vào 1 lĩnh vực công nghệ cụ thể (MITRE có 3 matrix: enterprice(doanh nghiệp), mobile và ICS)
  + Các Platforms phổ biến trong ATT&CK bao gồm Windows, macOS, Linux, Cloud, Mobile, và các hệ điều hành nhúng khác.
  + Có những technique là phổ biến trên các matrix khác nhau.
* Tactics (có 14 tactics trong enterprise)(vd truy cập thông tin xác thực [Credential Access](https://attack.mitre.org/tactics/TA0006))
  + Là mục tiêu của đối thủ khi thực hiện tấn công
  + Trả lời câu hỏi “tại sao” khi đối thủ thực hiện 1 hành động hoặc 1 technique
  + List tactic có thể khác nhau giữa những lĩnh vực công nghệ khác nhau
  + 1 tactic được gắn 1 ID và 1 description
* Techniques and Sub-Techniques
  + Technique là cách mà đối thủ đạt được tactic (từ quan điểm của đối thủ chứ k phải là của defender). Trả lời câu hỏi “làm thế nào” mà đối thủ thực hiện được mỗi hành động
  + List technique có thể khác nhau giữa các nền tảng, nhưng có thể phát triển và tiến hóa theo thời gian
  + Có những technique là duy nhất cho 1 tactic, nhưng cũng có những technique đồng thời được sử dụng cho cả 2 tactic
  + Sub-technique mô tả cụ thể hơn về hành vi của đối thủ đươc sử dụng để đạt được mục tiêu. 1 sub-technique chỉ thuộc về 1 technique duy nhất
  + Được thiết kế để giảm các thay đổi đối với technique khi 1 biến thể và nền tảng mới được thêm vào
  + Sub technique thường xuất hiện ở các technique đa nền tảng (platform), biểu thị cách mà technique đó thực hiện trên các nền tảng khác nhau (như việc khai thác trên Windows sẽ khác trên Linux)
  + Vd technique Brute-force -> có 3 sub technique : password guesing(đoán pass của 1 acc, có thể dựa theo thoogn tin thu thập từ kĩ nghệ xã hội), password cracking(sử dụng tool tấn công vào 1 acc, và ban đầu không có thông tin gì để guess) và password spraying(dùng list pass thông dụng cho nhiều acc)
* Mitigations
  + Các cấu hình, tool, quy trình có thể ngăn 1 technique hoạt động hoặc có được kết quả mong muốn của đối thủ
  + Cho phép ta thực hiện 1 hành động như thay đổi chính sách hoặc triển khai 1 tool với mục đích ngăn chặn kẻ thù
  + Mitigation giúp ngăn chặn hành động, detection giúp xác định khi nào hành động đó xảy ra -> sử dụng detection, sau đó dùng mitigation
  + 1 mitigation có thể áp dụng cho nhiều technique
  + Vd ngăn brute-force: -sd xác thực đa yếu tố hay thiết lập chính sách mật khẩu(đăng nhập sai quá 5 lần khóa tài khoản)
* Data Sources and Detections
  + Data source được thu thập bởi sensor hoặc logging system (thông tin thu thập bởi sensor/log)
  + Được sử dụng để thu thập thông tin liên quan đến việc xác định hành động của đối thủ
  + “Là nơi để thu thập dữ liệu”(file, command, driver, named pipe…)
  + Data source cũng bao gồm các data component để xác định rõ hơn data requirement
  + Detection là phân tích cấp cao các quy trình, sensor, data, và detection strategies
  + Rất hữu ích để xác định 1 technique mà đối thủ sử dụng
  + Detections là các quy tắc, nguyên tắc hoặc mô hình mà người dùng và nhà quản trị mạng sử dụng để phát hiện các hoạt động tấn công trong dữ liệu được thu thập từ các Data Sources.
  + “cách diễn giải dữ liệu đã thu thập”
  + Brute-force có datasouce là command, data component là command execution
  + Detect: Giám sát các command hoặc đối số mà có thể sử dụng brute force technique
* Procedure
  + Là triển khai cụ thể mà đối thủ sử dụng cho technique hoặc sub-technique(những APT là ví dụ)
  + Mô tả group hoặc software entity với mô tả ngắn gọn về cách sử dụng technique
* Groups and Software
  + Các group có liên quan đến hoạt động xâm nhập được theo dõi bởi 1 tên chung
  + 1 số nhóm có nhiều tên liên quan đến các hoạt động tương tự (đại khái group là 1 nhóm người hay 1 tổ chức chịu trách nhiệm cho 1 hoặc nhiều cuộc tấn công , có thể được gọi bằng nhiều cái tên khác nhau)
  + Software là tool hoặc mal mà kẻ thù sử dụng trong quá trình xâm nhập
  + 1 số software có nhiều tên
* How ATT&CK Grows and Evolves
  + Update version khoảng 1 năm 2 lần
  + Lấy thu thập đóng góp từ người dùng

Module 2: Benefits of Using ATT&CK

* Community Perspective
  + MITRE ATT&CK cung cấp phương pháp tiếp cận dựa vào cộng đồng đối với an ninh mạng. Nó thúc đẩy sự cộng tác và chia sẻ thông tin giữa các chuyên gia, nhà nghiên cứu và tổ chức an ninh mạng. Bằng cách đóng góp và cộng tác trong cộng đồng ATT&CK, các chuyên gia bảo mật có thể cùng nhau nâng cao cơ sở kiến ​​thức, cải thiện thông tin tình báo về mối đe dọa và hiểu rõ hơn về các mối đe dọa mạng mới nổi và hành vi của kẻ thù.
  + Quan điểm cộng đồng cho phép các tổ chức tận dụng chuyên môn và kinh nghiệm tập thể của nhiều bên liên quan để được thông báo về các xu hướng và chiến thuật đe dọa mới nhất được sử dụng bởi các đối thủ. Cách tiếp cận hợp tác này tăng cường khả năng phòng thủ an ninh mạng và tạo điều kiện cho phản ứng chủ động và thích ứng hơn đối với các mối đe dọa đang gia tăng.
* Common Language
  + ATTT&CK thiết lập một ngôn ngữ chung để mô tả và phân loại các hoạt động đe dọa mạng. Nó cung cấp một khuôn khổ và phân loại được tiêu chuẩn hóa để nêu chi tiết các chiến thuật, kỹ thuật và quy trình (TTP) khác nhau được các tác nhân đe dọa sử dụng.
  + Ngôn ngữ chung này giúp tăng cường giao tiếp và hiểu biết giữa các nhóm bảo mật, cho phép phát hiện và ứng phó với mối đe dọa hiệu quả hơn giữa các tổ chức và ngành khác nhau. Việc có một vốn từ vựng dùng chung để mô tả các mối đe dọa trên mạng sẽ tạo điều kiện thuận lợi cho sự cộng tác, trao đổi thông tin và đo điểm chuẩn giữa các chuyên gia bảo mật một cách liền mạch.
  + ATT&CK adversary language là quan trọng đối vs việc chia sẻ nhất quán các các ý tưởng về hành vi của kẻ thù
  + Ngôn ngữ được trừu tượng hóa ở cấp độ hoạt động
  + Cách sử dụng phổ biến là kết nôi quan điểm của kẻ thù vs các biện pháp đối phó phòng thủ
* Quantitative Scorecard
  + Thẻ điểm định lượng là một tính năng có giá trị của ATTT&CK cho phép các tổ chức đánh giá tình trạng và hiệu quả bảo mật của họ. Nó cung cấp một cách tiếp cận có cấu trúc và có thể đo lường được để đánh giá khả năng của một tổ chức trong việc bảo vệ chống lại các mối đe dọa mạng.
  + Bằng cách sắp xếp các khả năng phòng thủ với Chiến thuật và Kỹ thuật của ATT&CK, các nhóm bảo mật có thể đo lường và theo dõi khả năng phát hiện và ngăn chặn của họ đối với các loại tấn công cụ thể. Thẻ điểm giúp các tổ chức xác định các điểm yếu và ưu tiên cải thiện để bảo vệ tốt hơn trước các mối đe dọa phổ biến và có liên quan nhất.
* ATT&CK Navigator
  + Được thiết kế để cung cấp điều hướng và chú thích cơ bản của matrix
  + Trực quan hóa phạm vi phòng thủ, lập kế hoạch cho red/blue team, tần suất của các kĩ thuật phát hiện …
  + Thao tác với các ô trong matrix
  + ATT&CK Navigator là một công cụ tương tác cho phép các nhóm bảo mật trực quan hóa, khám phá và điều hướng cơ sở kiến ​​thức ATT&CK. Nó cung cấp một giao diện thân thiện với người dùng để tìm kiếm và lọc các kỹ thuật, lập bản đồ phạm vi phòng thủ và theo dõi thông tin tình báo về mối đe dọa.
  + Bộ điều hướng hỗ trợ lập kế hoạch và phát triển các chiến lược an ninh mạng hiệu quả bằng cách cho phép các nhà phân tích bảo mật xác định các lỗ hổng trong hệ thống phòng thủ của họ, đánh giá mức độ phù hợp của các kỹ thuật cụ thể với môi trường của họ và thiết kế các biện pháp phát hiện và giảm thiểu có mục tiêu.

Module 3: Operationalizing ATT&CK(vận hành)

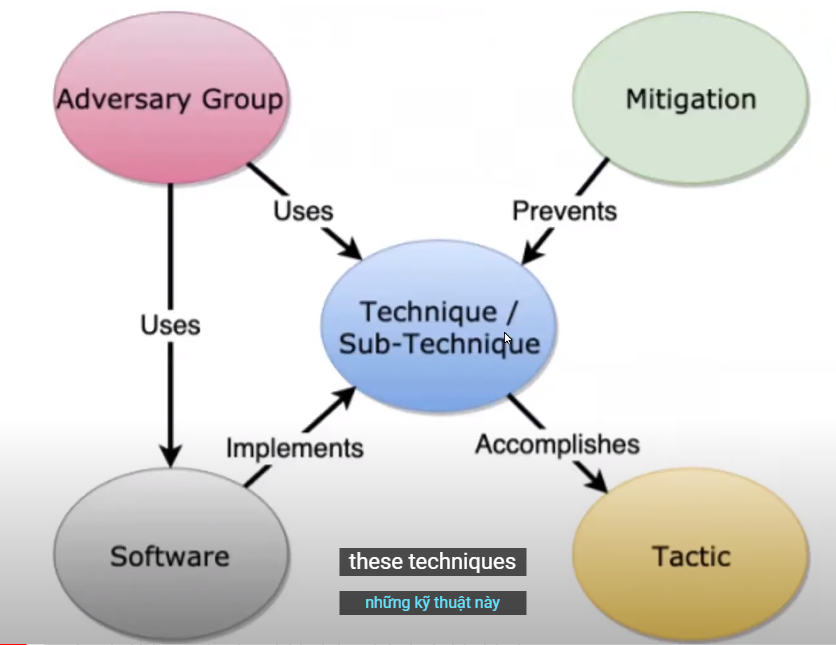
* Cyber Threat Intelligence
  + CTI (Cyber Threat Intelligence) là tất cả về việc hiểu rõ những gì mà các đối thủ thực hiện.
  + Là điều quan trọng để cải thiện việc ra quyết định cũng như định hình hoạt động(phong thủ trước mối đe dọa)
  + Cyber threat intelligence – Thông tin mối đe dọa an ninh mạng (CTI) là một lĩnh vực của an ninh mạng tập trung vào việc thu thập và phân tích thông tin về các cuộc tấn công hiện tại và tiềm năng đe dọa sự an toàn của một tổ chức hoặc tài sản của tổ chức. Lợi ích của thông tin mối đe dọa là đó là một biện pháp bảo mật chủ động, ngăn chặn vi phạm dữ liệu và tiết kiệm cho bạn chi phí tài chính để dọn dẹp sau khi xảy ra sự cố. Mục đích của nó là cung cấp cho các công ty một sự hiểu biết sâu sắc về các mối đe dọa gây rủi ro lớn nhất cho cơ sở hạ tầng của họ và cho biết những gì họ có thể làm để bảo vệ doanh nghiệp.
  + CTI có thể là 1 đoạn code, 1 bài report, hay 1 bài viết blog… từ những nguồn khác nhau mà các nhà phân tích trích xuất được cti đó có liên quan đến technique nào, và tổng hợp được tất cả technique được sử dụng
* Detection and Analysis
  + Phần này tập trung vào tầm quan trọng của khả năng phát hiện và phân tích hiệu quả. Đội ngũ an ninh học cách phát triển và triển khai các quy tắc phát hiện, sử dụng các công cụ phân tích hành vi, và phân tích các bản ghi log bảo mật để xác định và phản ứng với các mối đe dọa tiềm ẩn.
* Threat Emulation(Mô phỏng Mối đe dọa)
  + Red team sẽ băt chước 1 threat đã biết -> quan sát và đánh giá khả năng phòng thủ của chúng ta từ quan điểm của đối thủ
  + Mô phỏng mối đe dọa liên quan đến việc giả lập các kịch bản tấn công thực tế để kiểm tra khả năng phòng thủ của tổ chức. Bằng việc thực hiện các bài tập mô phỏng mối đe dọa, các tổ chức có thể đánh giá tình trạng bảo mật của mình, xác định điểm yếu và nâng cao sẵn sàng phản ứng sự cố.
* Assessment and Engineering (Đánh giá và Kỹ thuật)
  + Phần này nhấn mạnh tầm quan trọng của việc đánh giá liên tục và kỹ thuật hóa các biện pháp phòng thủ. Bằng cách đánh giá và tối ưu hóa các điều khiển bảo mật, các tổ chức có thể duy trì tính linh hoạt và khả năng chống lại các mối đe dọa tiến triển.
* Putting it all Together into Threat-Informed Defense (Tổng hợp thành Phòng thủ dựa trên Mối đe dọa)

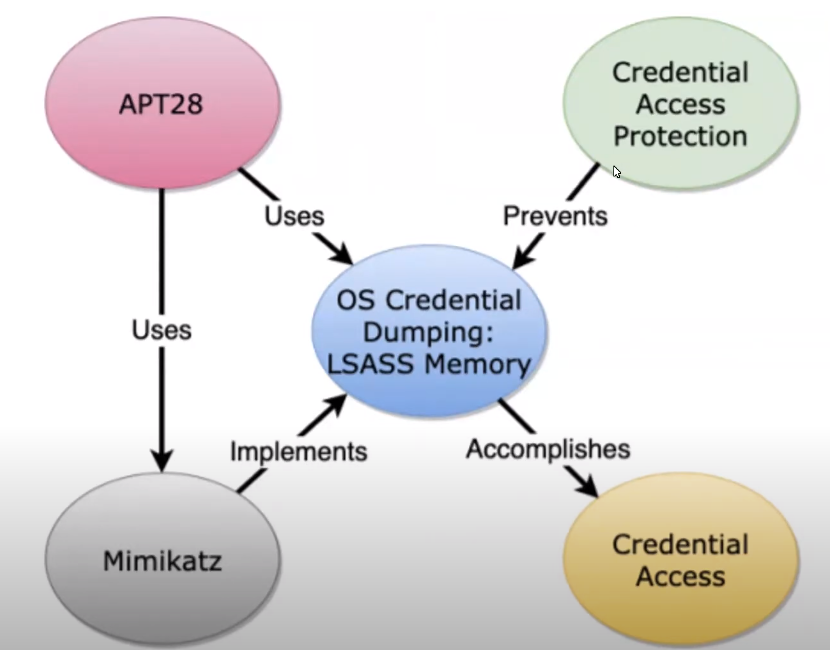
Trong phần này, người tham gia học cách kết hợp tất cả các khái niệm đã bàn trong khóa học để xây dựng một chiến lược phòng thủ toàn diện dựa trên mối đe dọa. Bằng cách sử dụng kiến thức thu thập từ Cyber Threat Intelligence, phát hiện và phân tích, mô phỏng mối đe dọa, và đánh giá bảo mật, các tổ chức có thể xây dựng một hệ thống bảo mật vững chắc đối phó với các mối đe dọa mạng.

* Course Summary

#### 1 số phần nhỏ

* Tactics luôn “tĩnh”, nhưng technique và sub-technique luôn luôn có những cái mới hoặc chi tiết mới
* Mô hình của 1 cuộc tấn công





**Sysmon Log Basic (2 days)**

* This course covers the fundamentals of Microsoft Sysinternals Sysmon, from basic use of the command line to deployment considerations and understanding how each event type works.
* This course is designed for the defender who is just getting started with using the Sysinternals Sysmon tool for collecting information to aid in the hunt and detection of abuse of Windows environments.
* Link video: <https://www.youtube.com/watch?v=kESndPO5Fig&list=PLk-dPXV5k8SG26OTeiiF3EIEoK4ignai7>

**Day 1**

Sysmon là bộ công cụ của Microsoft dùng để kiểm tra những hoạt động của Windows: process, network, file… và đưa vào windows event log.

Sysmon thường được dùng để audit những hành vi bất thường của ứng dụng (process, thread, connection, file, command, sign ,dns…)

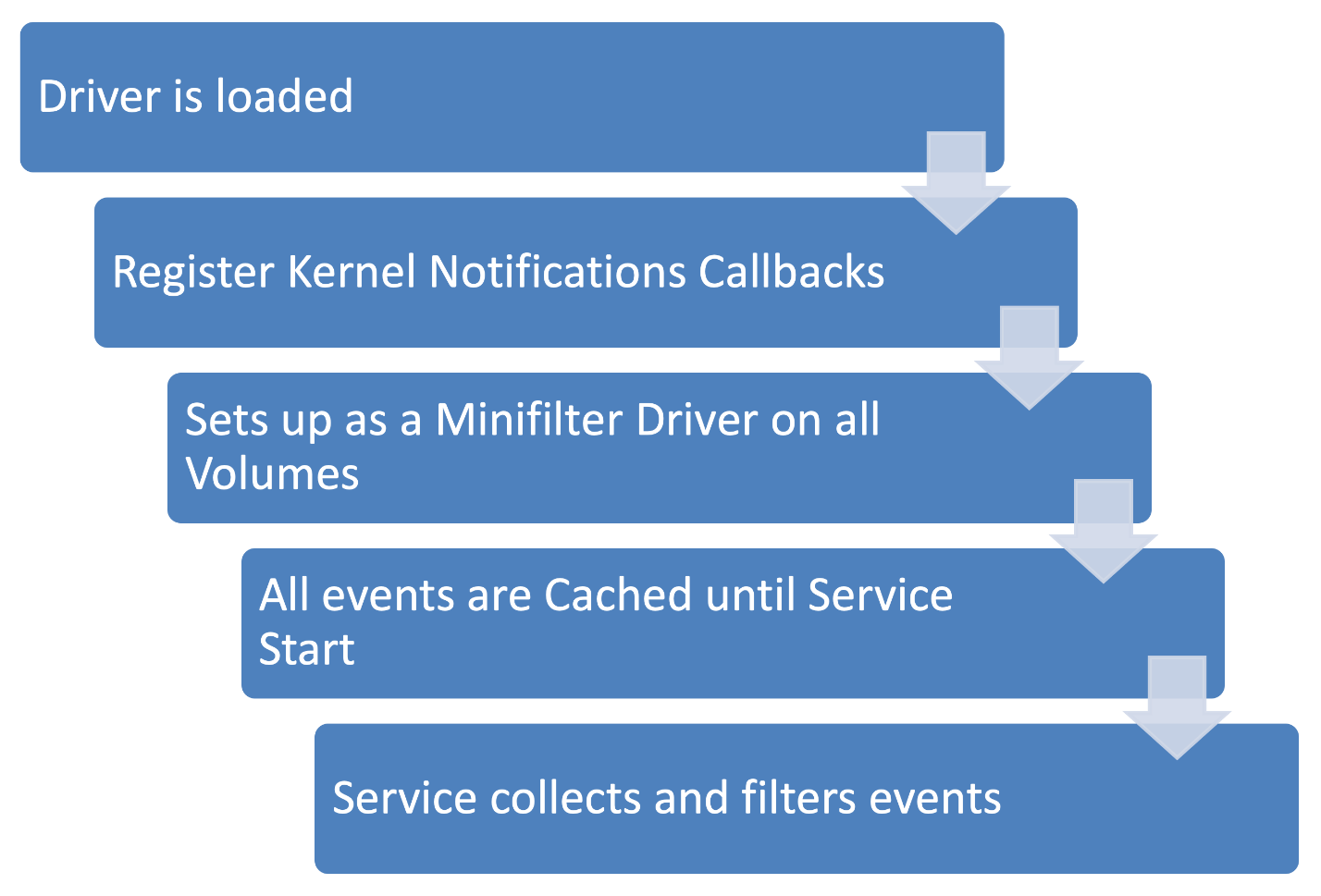
* The Sysmon Driver – This overview of the core of Sysmon will discuss how this component captures the information that is then stored in the Windows event log. (SysmonDrv.sys)

<https://github.com/trustedsec/SysmonCommunityGuide\>

<https://rootdse.org/posts/understanding-sysmon-events>

driver sẽ kết nối với Windows API và tận dụng tính năng Theo dõi sự kiện cho Windows (event tracing for window) (ETW) để thu thập thông tin về các hành động mà driver muốn theo dõi.

ETW là theo dõi cấp kernel giúp trace và log event do các ứng dụng ở chế độ người dùng và driver ở chế độ kernel đưa ra để giám sát các ứng dụng và hành vi của chúng



* Installation and Configuration – We will understand the basic installation of Sysmon and the command line parameters used. Additionally, we will take a look at some best practice recommendations and cover how to author XML configuration files.

**Day 2**

* Event Types – We will look at the different event types generated by Sysmon and best practices for working with each one. The following event types will be covered:

<https://github.com/olafhartong/sysmon-modular>

#### Sysmon Events

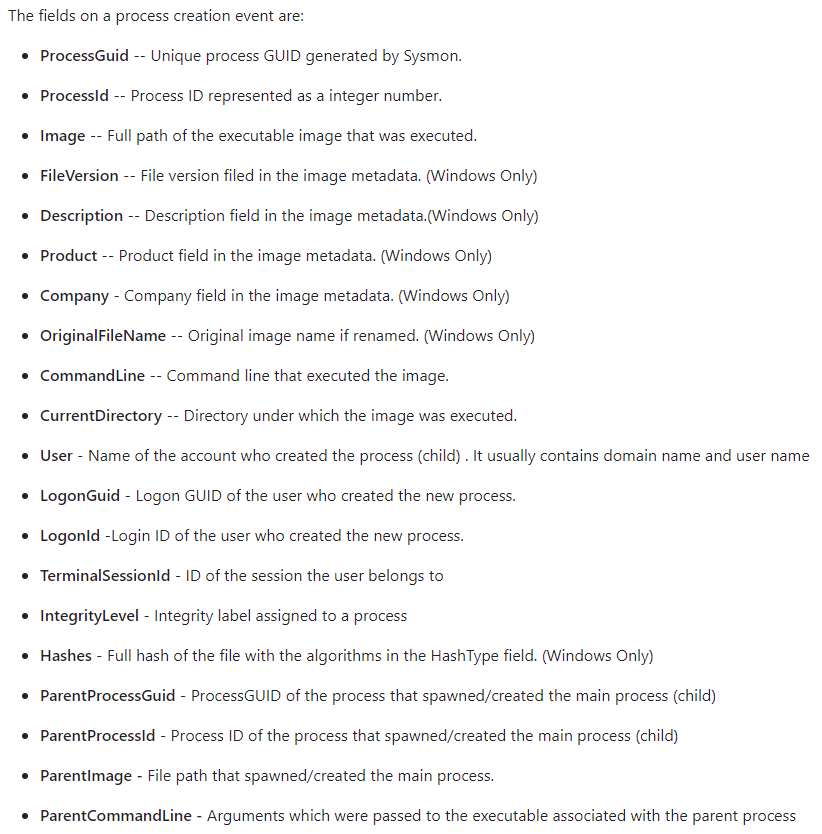
Trong Sysmon, khái niệm "Image" đề cập đến các tệp thực thi (executables) hoặc tiến trình (processes) trên hệ thống Windows. Image được sử dụng để đại diện cho các ứng dụng, tệp thực thi và tiến trình mà Sysmon theo dõi và ghi lại thông tin liên quan.

##### Process Events

* Trong Window, process event được ghi lại qua ObjRegisterCallbacks ở kernel level bằng cách sử dụng driver của nó và chứa một ProcessGuid và LogonGuid duy nhất, được tạo một cách xác định, tương ứng với process intance và LSA (Local Security Authority) logon session của chúng.
* ProcessGuid và LoginGuid giúp theo dõi process và user riêng lẻ dễ dàng hơn nhiều. ProcessGuid attribute được sử dụng trong tất cả các event được liên kết với quy trình của nó và, không giống như ProcessID, sẽ không được host system sử dụng lại sau này. Tương tự, LogonGuid attribute được gán cho login session của một người dùng cụ thể và sẽ không được sử dụng lại sau này như LoginID.
* ProcessGUID được tạo bởi Sysmon khi Sysmon ghi sự kiện. Sysmon theo dõi GUID cho đến khi process exit.
* ProcessGUID được tạo:
  + Windows: ProcessGUID = Timestamp + ProcessID + MachineGUID
  + Linux: ProcessGUID = Timestamp + ProcessID + giá trị hex của /etc/machine-id
* ProcessGUID được tham chiếu trong một số event dưới các tên khác nhau: Parent, Source, Target + ProcessGUID (ex: ParentProcessGUID)
* Chỉ có 2 Event Type không tham chiếu đến ProcessGUID và các tên dẫn xuất của nó:
  + WMI events
  + Kernel Driver Load
* Tất cả các process được liên kết với một logon session duy nhất có thể được ánh xạ bằng trường LogonGuid. Trường này được tạo bằng cách sử dụng các giá trị tương tự như ProcessGuid với ngoại lệ là thay vì dùng ProcessID, thì ta sử dụng giá trị hex của Logon Session trong Window hay giá trị của LogonID trong Linux để tạo mã định danh duy nhất khớp với tất cả các hành động được thực hiện.
  + Window: Timestamp + *giá trị hex của Logon Session* + MachineGUID
  + Linux: Timestamp + *LogonID* + giá trị hex của /etc/machine-id
* Khi người dùng đăng nhập vào phiên bản Windows hiện đại (Windows 2016/10), họ sẽ được chỉ định 2 Logon ID nếu:
  + Người dùng là thành viên của local Administrator Group.
  + UAC (Kiểm soát truy cập người dùng) được bật.
* Các sessionnày sẽ được liên kết bằng Linked Login ID trong Window Event ID 4624 (Successful Logon) khiến việc logging event này trở nên quan trọng.

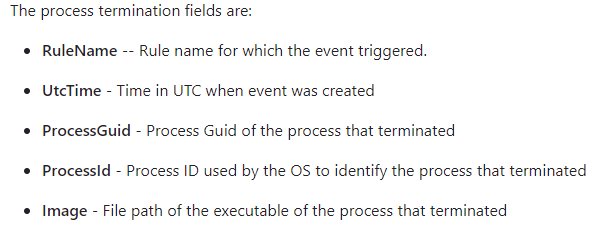
###### Process Creation \*

* Để tạo 1 process mới, chương trình cần register với kernel. Mỗi khi như vậy sysmon lại log EventID 1
* Trên Windows Sysmon sẽ tạo ProcessGuid và LogonGuid với thông tin mà nó thu được và nó sẽ hash process main image. Command line của process sẽ được parse và logged vào eventlog.



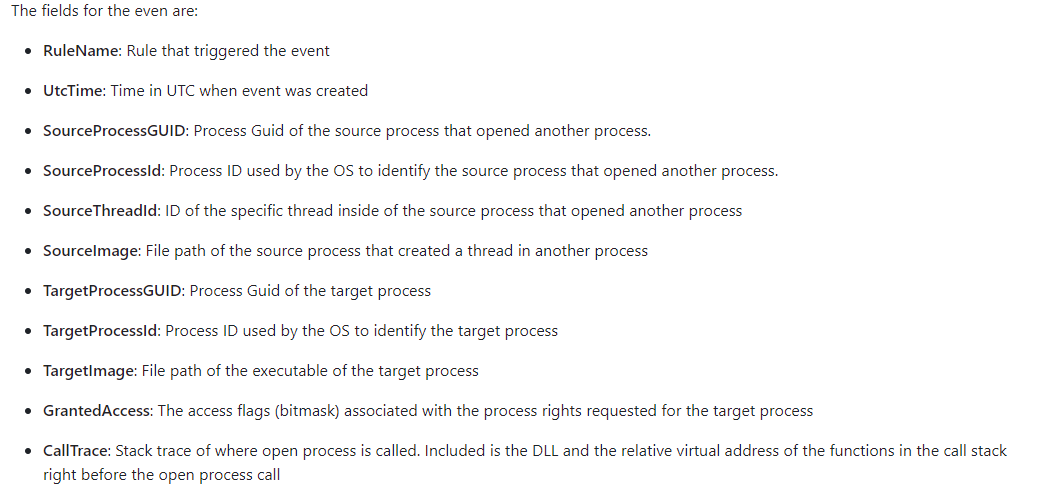
###### Process Termination \*

* Khi event Process Termination xảy ra, Sysmon sẽ ghi lại EventID 5
* Bằng cách log process termination events giúp tính toán thời gian 1 process hoạt động (chỉ cần trù đi cái móc thời gian process được tạo).
* Process termination cũng sẽ liên quan đến shutdown and start event khi mà 1 process bị attacker làm cho terminate



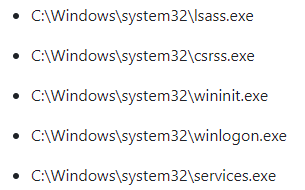
###### Process Access \*

* Khi 1 process mở 1 process khác -> Sysmon log EventID 10
* Kỹ thuật này đã được sử dụng để truy cập thông tin đăng nhập, key và data trong process memory.
* Tác vụ này cũng phổ biến đối với các quy trình lành tính truy vấn thông tin trên một quy trình khác, chẳng hạn như Trình quản lý tác vụ, tasklist.exe và các quy trình khác, điều này yêu cầu một đường cơ sở được thiết lập và lọc ra ở cấp SIEM có tính đến các yếu tố khác như đường dẫn đầy đủ của hình ảnh, quy trình gốc và tài khoản được sử dụng để ngăn chặn bất kỳ quy trình trong danh sách trắng nào được sử dụng làm dàn dựng cho các cuộc tấn công.

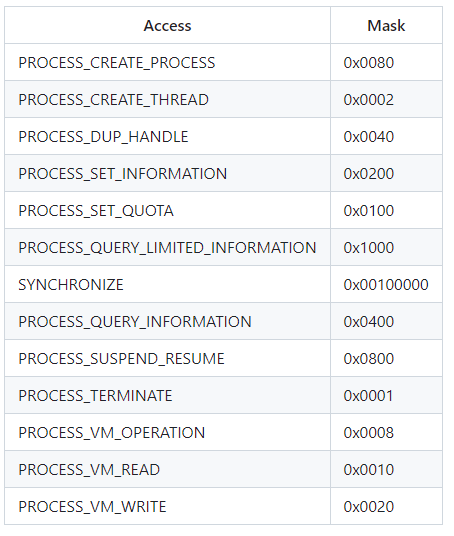


* Sysmon tạo event này bằng cách sử dụng ObRegisterCallbacks tận dụng driver của nó. 2 main filtering field được khuyến nghị là:
  + **TargetImage:** đường dẫn của tệp thực thi đang được truy cập bởi 1 process khác

Tối thiểu phải có những critical process sau:



* + **GrantedAccess:** là 1 access flag mà biểu thị yêu cầu quyền cho target process

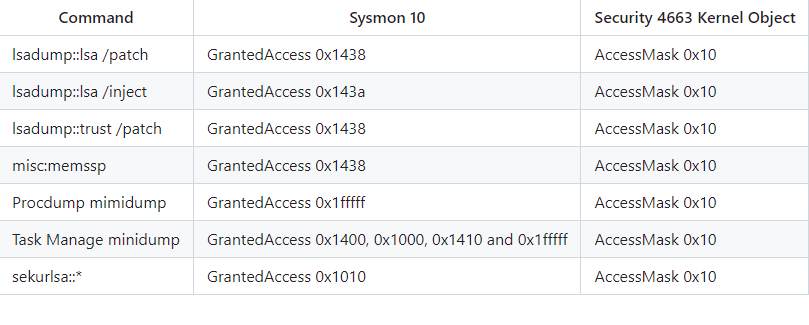


Ví dụ flag là 0x0030 -> PROCESS\_VM\_READ + PROCESS\_VM\_WRITE

Ví dụ:

|  |
| --- |
| <Rule groupRelation="and">  <TargetImage name="technique\_id=T1003,technique\_name=Credential Dumping" condition="is">C:\Windows\system32\lsass.exe</TargetImage>  <GrantedAccess>0x1FFFFF</GrantedAccess>  </Rule> |

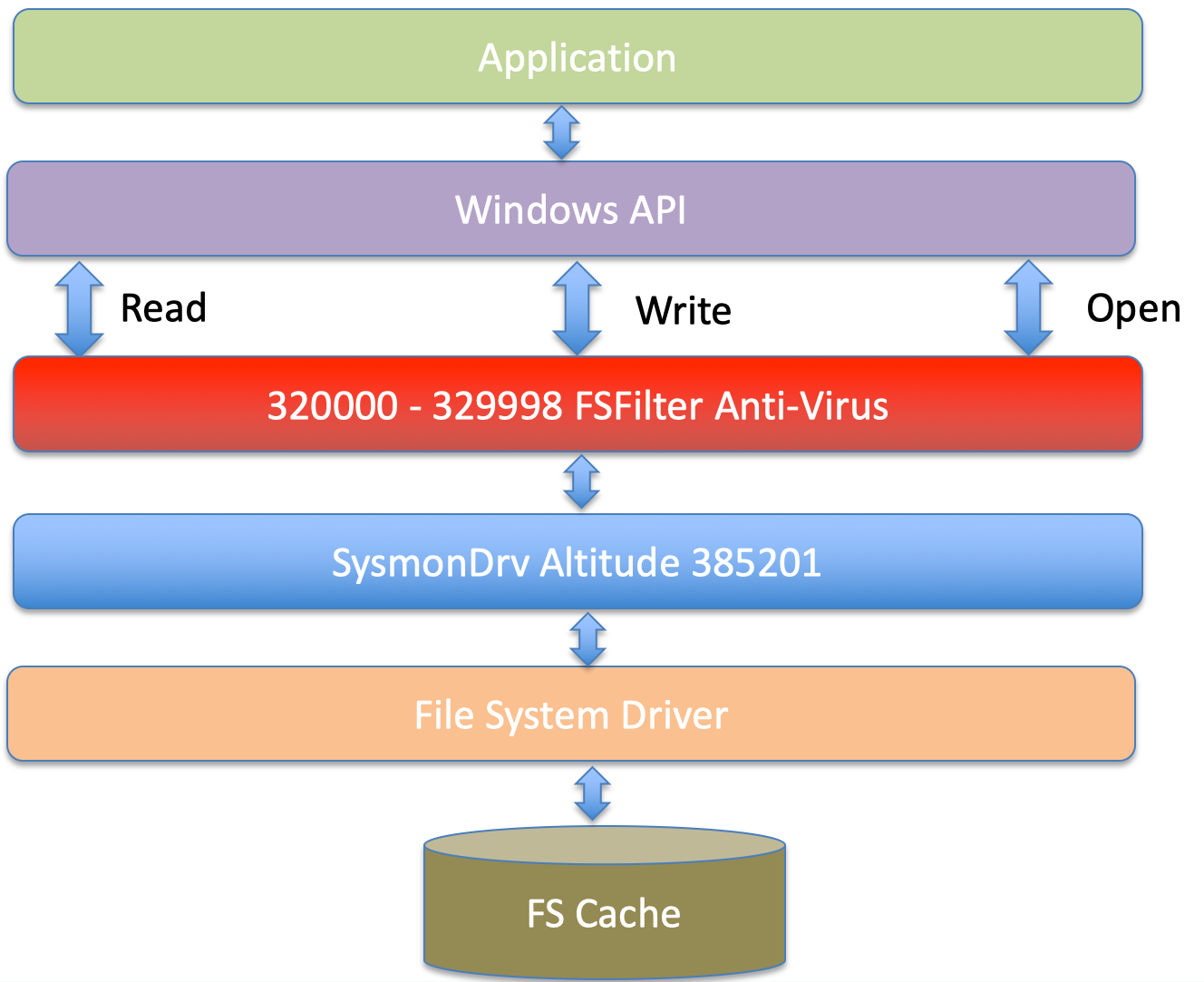
* Sysmon sẽ so sánh bitmask được cấp ở grantedaccess trong rule với bitmask được tìm thấy trong event -> chỉ khi khớp hoàn toàn thì mới lấy (ex: 0x1412: nếu event là 0x1410 hay 0x0040 thì không lấy, chỉ lấy duy nhất 0x1412)



##### File Events

###### File Create \*

* Thông qua filter driver, sysmon có thể log việc tọa tệp và thông tin về process nào tạo file bằng EventID 11. Điều này giúp cho defender:
  + Drop các file được sử dụng để thực thi sau này (PowerShell, Office Apps, certutil.exe)
  + Sửa cấu hình hệ thống (Scheduled Tasks, WMI)
  + Phát hiện các hành vi độc hại mà tạo các tệp temp hay log file(.Net compile and run, DotNet2JS)
* AV minifilters load trước sysmon(do altitude number thấp hơn sysmon), nên nếu AV hoặc EDR minifilter driver phát hiện được malicious file và chặn không cho nó ghi vào disk thì sysmon sẽ không ghi log nữa



* Trường quan trọng nhất là **TargetFilename**

|  |
| --- |
| <Rule groupRelation="or">  <TargetFilename name="technique\_id=T1170,technique\_name=Mshta" condition="end with">.hta</TargetFilename>  </Rule> |

###### File Create Time Change\*

* EventID 2 dành cho kĩ thuật sửa timestamp của 1 file (the modify, access, create, and change times)
* Điều này được thực hiện thường xuyên để bắt chước các tệp nằm trong cùng một thư mục nhằm ẩn các tệp đã bị xóa hoặc tệp đã truy cập để tránh bị phát hiện tình cờ.
* 1 số app sửa đổi timestamp trong hoạt động bt của chúng -> 1 cách giảm thiểu là loại những app mà thường thay đổi file creation times như các executable, Chrome, OneDrive…
* Tối thiểu directory User phải được theo dõi

###### File Stream Creation Hash \*

* Sysmon sẽ log EventID 15 để tạo Alternate Data Streams (ADS).
* Alternate Data Streams (ADS) là 1 file attribute chỉ có thể tìm thấy trên NTFS file system.

##### Named Pipes –

* A named pipe is a named, one-way or duplex pipe for communication (giao tiếp) between the pipe server and one or more pipe clients.
* Malware thường sử dụng named pipe để giao tiếp giữa các process
* Sysmon will generate a events
  + EventID 17 when a named pipe server is created
  + EventID 18 when a client connects to a named piper server.
* Đối vs named pipe thì có 2 cách tiếp cận
  + Include tất cả event và loại trừ các pipe không nguy hại đã biết -> bao quát tất cả nhưng yêu cấu bảo trì nhiều hơn
  + Chỉ include những pipe nguy hại đã biết -> nhắm vào mục tiêu tốt hơn, nhưng dễ bỏ sót những cái không biết
* Attacker thường tránh những pipe đã biết để tránh phá vỡ hoạt động bt của hệ thống

##### Driver Loading \*

* EventID 6
* Driver thường bị attacker sử dụng để install rootkit hoặc để chạy các tool ở kernel (vd mimikatz)
* Cách làm ổn nhất là filter dựa theo 2 field **Signature** và **SignatureStatus** và loại trừ những drver đã biết, Nguyên nhân là do có nhiều attacker ăn cắp các certificate đã được thu hồi. Bằng cách check **SignatureStatus** là *valid* thì có thể xác định được nó có hợp lệ hay không.

##### Registry Actions –

* Sysmon có khả năng giám sát ba hành động chính đối với Registry
  + EventID 12 - Registry object added or deleted
  + EventID 13 - Registry value set
  + EventID 14 - Registry object renamed
* Windows Registry là nguồn thu thập thông tin, lưu trữ lâu dài và kiểm soát cấu hình cho những kẻ tấn công kể từ khi nó được giới thiệu rộng rãi hơn trong Windows NT 4.0/Windows 95.

##### Image Loading \*

* EventID 7: log khi 1 image được load bởi 1 process
* Có thể gây ra mức sử dụng CPU cao
* Event này được nhắm mục tiêu tốt nhất bằng cách theo dõi các library hoặc combination cụ thể được sử dụng bởi những kẻ tấn công.

##### Network Connections \*

* Sysmon will log EventID 3 for all TCP and UDP network connections
* 1 số field quan trọng được ghi lại như: source and destination host names, IP addresses and port numbers

##### Create Remote Thread \*

* EventID 8 : khi 1 process tạo 1 thread trong 1 process khác bằng cách sử dụng hàm *CreateRemoteThread*
* Technique này được sử dụng bởi malware để inject code và giấu code ở trong 1 process khác
* The event indicates the source and target process. Nó cung cấp thông tin về mã sẽ được chạy trong thread mới: StartAddress, StartModule and StartFunction.

##### Raw Access Read \*

* Sysmon sẽ ghi nhật ký EventID 9 cho bất kỳ process nào đang cố đọc trực tiếp từ thiết bị lưu trữ bằng cách bỏ qua mọi hạn chế hệ thống tệp có thể áp đặt lên process đó
* Là 1 cách thực hiện lỗ hổng Path Travelsal: xài [\\.\](file:///\\.\)

##### DNS Query –

* EventID 22 : được log mỗi khi 1 process thực hiện 1 DNS query, bất kể nó có thành công hay thất bại, được được lưu vào bộ nhớ cache hay không
* Khi thực hiện event nên loại trừ các domain đã biết như Microsoft domains, Windows update, browser update domains
* Event này hữu ích để phát hiện các process tìm kiếm domain độc hại

##### WMI Events \*

**Windows Event Log (2 days)**

**Day 1**

* What’s Windows Event Logs?

<https://www.solarwinds.com/resources/it-glossary/windows-event-log>

<https://sec.vnpt.vn/2022/03/windows-event-logs-1/>

Windows Event Logs gồm những event liên quan đến software, hardware, OS, security. Service Windows Event Log chịu trách nhiệm quản lý các event, event log; nó thu thập các event từ nhiều nguồn khác nhau và lưu trữ tập chung tại một thư mục. Các event này có thể giúp người điều tra biết được chuyện gì đã xảy ra trên hệ thống, chúng xảy ra vào thời gian nào, tham chiếu đến người dùng cụ thể liên quan đến những hành vi đó hay các thông tin của các hệ thống, tài nguyên truy cập từ xa.

* Understand Windows Event Logs basic as:
  + Where are Windows Event Logs located?
    - Ban đầu, ở những phiên bản hệ điều hành cũ (trước Windows Vista) event log sẽ được lưu trữ tập chung tại systemroot%\System32\config ở định dạng nhị phân và với phần mở rộng đuôi .evt.
    - Nhưng bắt đầu từ Win server 2008 và Windwos Vista thì đã có sự thay đổi về định dạng log và vị trí lưu trữ của chúng. Event log được chuyển sang định dạng XML và với phần mở rộng .evtx và chúng được lưu trữ tại %systemroot%\System32\winevt\logs.
  + Format log
    - Lưu trong window vs exension evtx. Khi mở cũng có hỗ trợ xem event ở định dạng xml
    - Các thành phần của 1 log: log name, event id, event date/time, source…
  + Event Types (trường level trong 1 log)

Windows events are further divided into five different types:

* + - Information: cho biết 1 app hay 1 service đang hoạt động bt. vd: 1 app được cài đặt thành công
    - Warning: cho biết 1 vấn đề tiềm ẩn có thể gây hại trong tương lai. vd dung lượng ổ đĩa thấp
    - Error: Mô tả một vấn đề nghiêm trọng khi hệ thống không thể hoạt động bình thường. vd: 1 app gặp lỗi và đóng đột ngột hay hệ điều hành ngừng phản hồi
    - Critical:
    - Success Audit: audit success và audit failure chỉ dành cho sercurity log. Vd : đăng nhập tài khoản thành công, 1 file được truy cập thành công bởi 1 user
    - Failure Audit: vd: 1 user dăng nhập k thành công bởi vì nhập sai pass
  + Log Types

Có 5 log type: application, security, system, setup và forwarded event

* + - System log: chứa những event liên quan đến system và các thành phần của nó, chẳng hạn như lỗi dịch vụ không thể khởi động trong quá trình khởi động.
    - Application log: Ghi lại những sự kiện sinh ra bởi ứng dụng. Ví dụ: Lỗi khi khởi động ứng dụng.
    - Security log: chứa các sự kiện liên quan đến sự an toàn của hệ thống. vd: đăng nhập không thành công và hợp lệ, xóa tệp, v.v.
    - Setup log: chứa các sự kiện xảy ra trong quá trình cài đặt hệ điều hành Windows.
    - Forwarded log: Chứa các event log được chuyển tiếp từ các máy tính khác trong cùng mạng.
* Link: <https://learn.microsoft.com/>

Day 2

* Learn more some types of Log
  + Security Log
  + Application Log
  + System Log
  + Custom Log: CMD, PowerShell, Task Scheduler….
* 1 số Windows Log Event ID
  + 4688 - A new process has been created (tương đương với event id 1 hoặc 10 trên sysmon)
  + 4689 - A process has exited (tương đương với event id 5 trên sysmon)
  + 4673 - A privileged service was called
  + 4674 - An operation was attempted on a privileged object
  + 4720 - A user account was created.
  + 4726 - A user account was deleted.
  + 4738 - A user account was changed.