



SANS

Life is a bit easier with What2Log.com

Mick Douglas & Flynn Weeks

February 3, 2021

Mick

- Managing Partner of InfoSec Innovations
- Teach SANS 504 & 555
- IANS Faculty
- @BetterSafetyNet



Flynn



- Intern at InfoSec Innovations
- Senior at University of Maine at Augusta
- @soundsofthetime

Slides are freely available at

<https://InfoSecInnovations.com/talks>





WHAT 2 LOG

W2L Mission Statement

What2Log is a crowd sourced site that teaches you what to log, how they help you, and builds custom scripts.

What2Log is a crowd sourced site that teaches you what to log, how they help you, and builds custom scripts.



DEMO W2L Site

What the site has:

- Suggested logs to track for multiple OSes
- How to use built-in tools for setting and reading logs (LOL for logging)
- W2L:Sawmill (more on this later)
- Blog

Agenda

Why we had to build this.

Who this site is for.

What it is right now.

What we want to do.

We need your help!

Why did we do this?

We had to.

Seriously, nobody has done this.

Many months ago...

Flynn: can you point me to a resource that shows how all OSes log stuff?

Mick: yeah... about that....

Flynn: Wow. How can that not exist? Let's make it!

Mick: Heck yes!

Flynn: it won't be that hard.

(cue ominous music)

Agenda

Why we had to build this.

Who this site is for.

What it is right now.

What we want to do.

We need your help!

This site is for everyone!

Audience	What they get
Auditors & GRC types	Able to give practical fixes
SIEM engineers	Quickly change log settings
Pen testers	Give more meaningful remediations
Forensics folks	Go beyond “next” button on forensics tool
Non-security IT folks	Better understanding possibilities

Agenda

Why we had to build this.

Who this site is for.

What it is right now.

What we want to do.

We need your help!

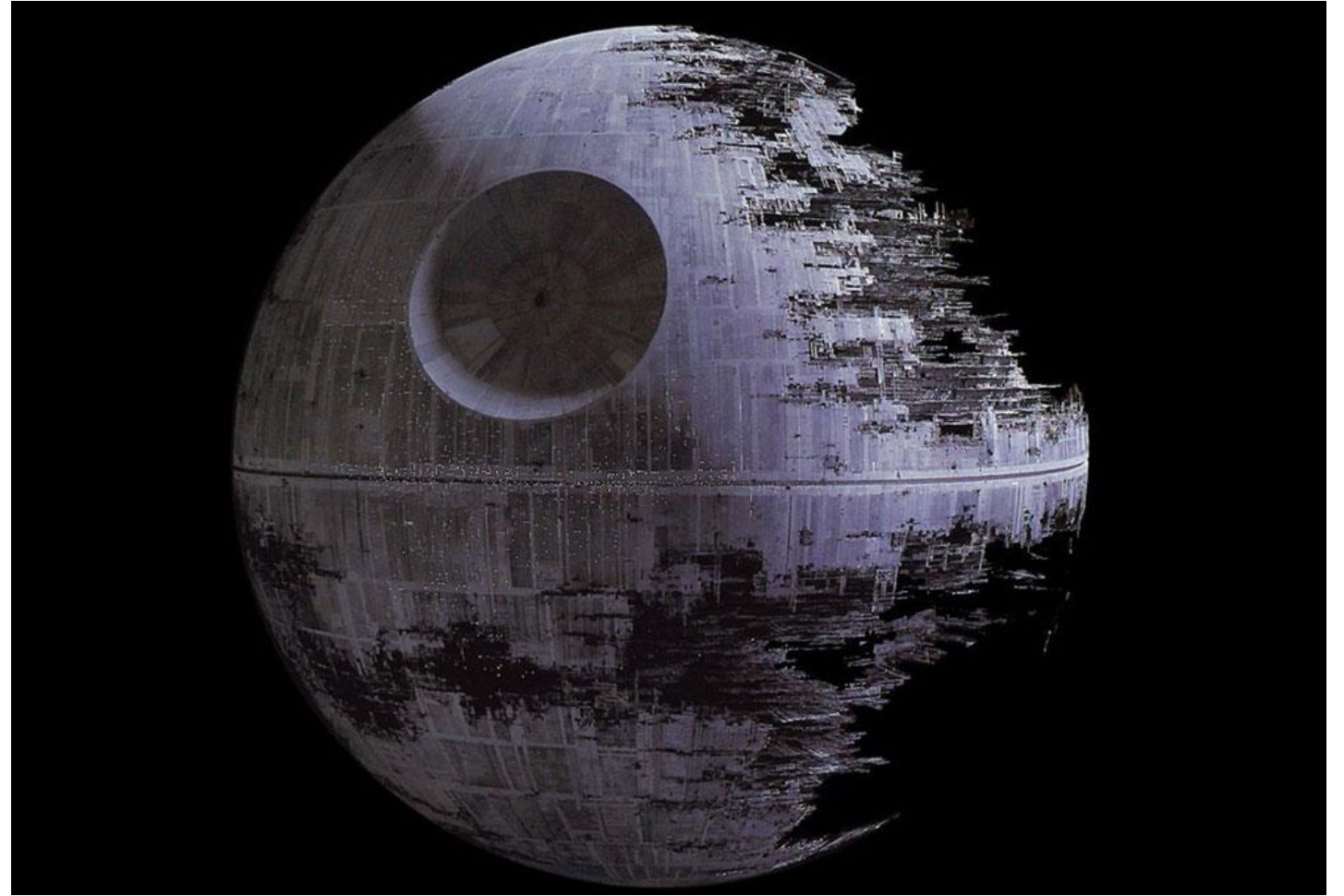
Under construction, yet fully functional.

OS tools

Lists several major
Operating Systems

Logging levels

Gives sample code to
find log entries



Agenda

Why we had to build this.

Who this site is for.

What it is right now.

What we want to do.

We need your help!

Next steps

- How to enable logs from the command line
- Mac OS logs (will be released soon!)
- Other Linux distributions (Red Hat... others?)
- Additional Windows logs
- Application logs (web servers first... then what?)
- Firewall logs
- Different formats (Spreadsheet, JSON, Github)

Next Steps: Logging Frameworks

- NIST SP 800-53 & SP 800-171
- JPCERT/CC Guidance
- NSA Cyber Event Forwarding Guidance
- HIPAA Compliance
- PCI DSS Compliance

Next Steps: Potential log enrichments & field removal

- Log field breakdown
- Suggested Enrichments
- Fields you *might* be able to remove*
* ALWAYS consult compliance/legal first!!

Agenda

Why we had to build this.

Who this site is for.

What it is right now.

What we want to do.

We need your help!

W2L Mission Statement

What2Log is a **crowd sourced** site that teaches you what to log, how they help you, and builds custom scripts.

Get involved, please!

Twitter- @What2Log
Reddit- r/What2Log

Thanks for the ideas so far!

- ZenRandom for the HIPAA coverage suggestions
- Adam Gaydosh for PCI coverage suggestions
- Cyber_00011011 for the NSA Cyber Event Forwarding Guidance suggestion

W2L Mission Statement

What2Log is a crowd sourced site that **teaches you what to log**, how they help you, and builds custom scripts.

Not all logs are equal

Signal to noise ratio

Sizing limitations

“Half life of usefulness”

- Justin Henderson

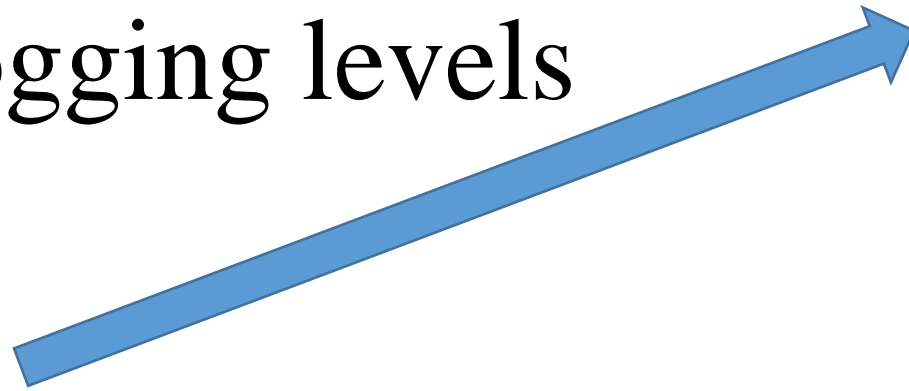


Suggested logging levels

Minimum	-
User Logon	
Failed User Login	
User Logoff	
Account Created	
Account Deleted	
Account Changed	
Software Installed	
Group Creation	
Group Change	
Member Added to Group	
Member Removed from Group	
Ideal	-
Group Deletion	
Service Installed	
Software Updated	
Software Uninstalled	
Extreme	-
WiFi Connection	
WiFi Disconnection	
Application Opened	
Application Closed	

Suggested logging levels

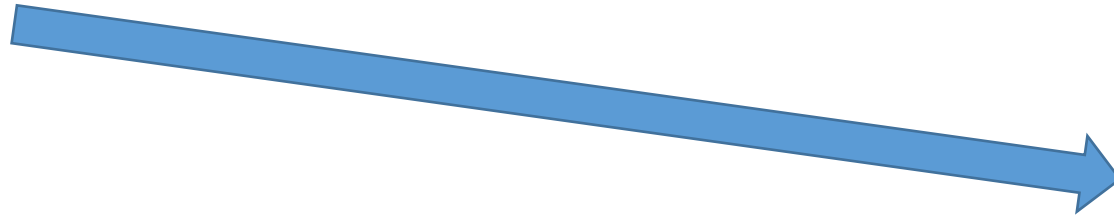
Minimum:



Minimum	-
User Logon	
Failed User Login	
User Logoff	
Account Created	
Account Deleted	
Account Changed	
Software Installed	
Group Creation	
Group Change	
Member Added to Group	
Member Removed from Group	
Ideal	-
Group Deletion	
Service Installed	
Software Updated	
Software Uninstalled	
Extreme	-
WiFi Connection	
WiFi Disconnection	
Application Opened	
Application Closed	

Suggested logging levels

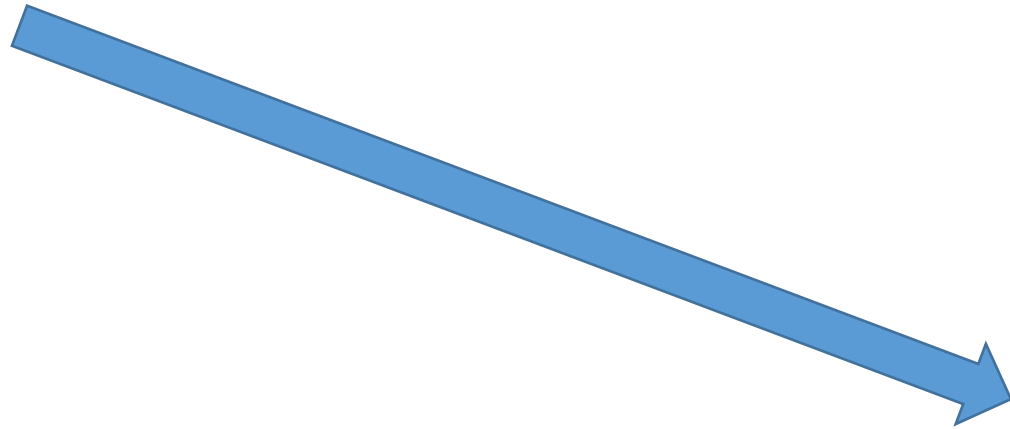
Ideal:



Minimum	-
User Logon	
Failed User Login	
User Logoff	
Account Created	
Account Deleted	
Account Changed	
Software Installed	
Group Creation	
Group Change	
Member Added to Group	
Member Removed from Group	
Ideal	-
Group Deletion	
Service Installed	
Software Updated	
Software Uninstalled	
Extreme	-
WiFi Connection	
WiFi Disconnection	
Application Opened	
Application Closed	

Suggested logging levels

Extreme:



Minimum	-
User Logon	
Failed User Login	
User Logoff	
Account Created	
Account Deleted	
Account Changed	
Software Installed	
Group Creation	
Group Change	
Member Added to Group	
Member Removed from Group	
Ideal	-
Group Deletion	
Service Installed	
Software Updated	
Software Uninstalled	
Extreme	-
WiFi Connection	
WiFi Disconnection	
Application Opened	
Application Closed	

W2L Mission Statement

What2Log is a crowd sourced site that teaches you what to log, **how they help you**, and builds custom scripts.

Let Logs help you

- Early Signs of Attack
- Breadcrumbs in wake of an attack
- General health check

What is in each entry:

Log name

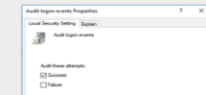
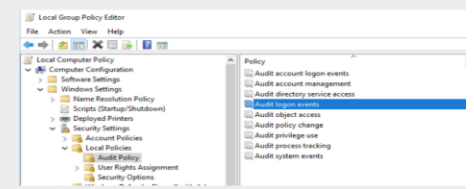


User Logon
Windows 10 Professional

A users log in will likely be the first sign of an attack and can indicate suspicious behavior. It can also give an analyst a starting time to create a timeline of events. This log is required in the HIPAA and PCI DSS regulations and is recommended by the NSA Event Forwarding Guidance and JPCERT.

```
Powershell wevtutil qe Security "/q:*(System [(EventID=4624)])" /f:6447 /a:1
```

does not log this by default. To enable logging of this activity, launch the Group Policy Editor. From here, expand the Windows settings folder and open the Security Settings tab. Finally, expand the Local Policies & Audit Policy header.



In order to turn on login auditing, double click "Audit logon events". Clicking the Success box will allow for the auditing of all successful login attempts.

not require login auditing be turned on and is done by default. To view this log in the Event Viewer, open the event viewer and navigate to the Windows Logs heading and then the Security Tab. From here, select arch for the value 4624 , or filter the log for the ID 4624.

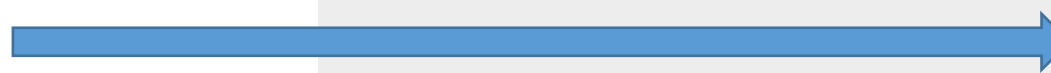
Event 4624: Microsoft Windows security auditing	
General	
Details	
Subject	Security ID: SYSTEM Account Name: Name of Computer Account Domain: NT AUTHORITY Logon ID: 0x0
Logon Information:	
Logon Type	5
Initial Logon	No
Extended Logon	No
Impersonation Level: Impersonation	
User Logon:	
Security ID	SYSTEM
Account Name	SYSTEM
Account Domain	NT AUTHORITY
Logon ID	0x0
Initial Logon	No
Extended Logon	No
Impersonation Level	Impersonation
Logon GUID	{00000000-0000-0000-0000-000000000000}
Process Information:	
Log Name	Security
Source	Microsoft Windows security
Event ID	4624
Level	Informational
User	N/A
OpCode	0x0
More Information	Event Log Online Help

```
wevtutil qe Security "/q:*(System [(EventID=4624)])" /f:6447 /a:1
```

To view this log in the command line (via powershell or command prompt), enter the command `wevtutil qe Security "/q:*(System [(EventID=4624)])"`. This will show all instances of the event ID 4624, which is the logon log ID.

What is in each entry:

Applicable OS

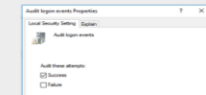
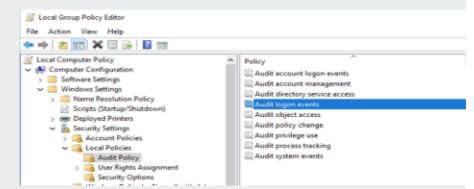


User Logon
Windows 10 Professional

A users log in will likely be the first sign of an attack and can indicate suspicious behavior. It can also give an analyst a starting time to create a timeline of events. This log is required in the HIPAA and PCI DSS regulations and is recommended by the NSA Event Forwarding Guidance and JPCERT.

```
Powershell wevtutil qe Security "/q:*[System [(EventID=4624)]]" /f:6447 /a:1
```

does not log this by default. To enable logging of this activity, launch the Group Policy Editor. From here, expand the Windows settings folder and open the Security Settings tab. Finally, expand the Local Policies and Audit Policy header.



In order to turn on login auditing, double click "Audit logon events". Clicking the Success box will allow for the auditing of all successful login attempts.

not require login auditing be turned on and is done by default. To view this log in the Event Viewer, open the event viewer and navigate to the Windows Logs heading and then the Security Tab. From here, select arch for the value 4624 , or filter the log for the ID 4624.



```
wevtutil qe Security "/q:*[System [(EventID=4624)]]" /f:6447 /a:1
```

To view this log in the command line (via powershell or command prompt, enter the command `wevtutil qe Security "/q:*[System [(EventID=4624)]]"` This will show all instances of the event ID 4624 , which is the logon ID.

What is in each entry:

Why you want this (including frameworks)

User Logon
Windows 10 Professional

A users log in will likely be the first sign of an attack and can indicate suspicious behavior. It can also give an analyst a starting time to create a timeline of events. This log is required in the HIPAA and PCI DSS regulations and is recommended by the NSA Event Forwarding Guidance and JPCERT.

PowerShell: `wevtutil qe Security "/q:*[System [(EventID=4624)]]" /f:6444 /v:1`

Local Group Policy Editor: Local Computer Policy > Security Settings > Local Policies > Audit Policy > Audit logon events

not require login auditing be turned on and is done by default. To view this log in the Event Viewer, open the event viewer and navigate to the Windows Logs heading and then the Security Tab. From here, select arch for the value 4624 , or filter the log for the ID 4624.

not require login auditing be turned on and is done by default. To view this log in the Event Viewer, open the event viewer and navigate to the Windows Logs heading and then the Security Tab. From here, select arch for the value 4624 , or filter the log for the ID 4624.

```
wevtutil qe Security "/q:*[System [(EventID=4624)]]" /f:6444 /v:1
```

Log Name	Source	Event ID	Category	Level	Task Category	Source	Source GUID
Security	Microsoft Windows security	4624	Login	Information	Logon	Local Security	{595961bc-878a-4d1e-8c92-8d4c7a894b7c}

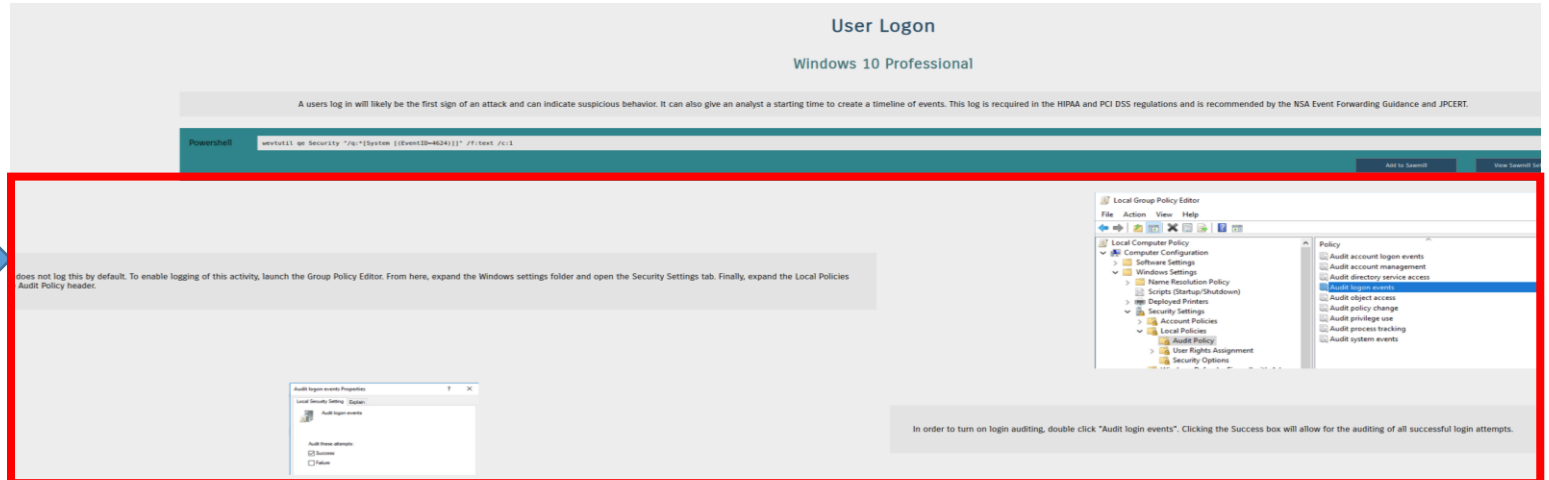
Event 4624, Microsoft Windows security auditing

Field	Value
Subject	Security ID: SYSTEM Account Name: Name of Computer Logon ID: 0x00000000
Logon Information	Logon Type: 5 Initial Logon: No Extended Logon: No
Impersonation Level	Impersonation
Process Information	Process ID: SYSTEM Process Name: SYSTEM Logon ID: 0x00000000 Initial Logon ID: 0x00000000 Network Account Name: \\.\r\n Logon GUID: 00000000-0000-0000-0000-000000000000

To view this log in the command line (via powershell or command prompt), enter the command `wevtutil qe Security "/q:*[System [(EventID=4624)]]"`. This will show all instances of the event ID 4624 , which is the logon ID.

What is in each entry:

How to enable GUI



User Logon
Windows 10 Professional

A users log in will likely be the first sign of an attack and can indicate suspicious behavior. It can also give an analyst a starting time to create a timeline of events. This log is required in the HIPAA and PCI DSS regulations and is recommended by the NSA Event Forwarding Guidance and JPCERT.

does not log this by default. To enable logging of this activity, launch the Group Policy Editor. From here, expand the Windows settings folder and open the Security Settings tab. Finally, expand the Local Policies Audit Policy header.

In order to turn on login auditing, double click "Audit logon events". Clicking the Success box will allow for the auditing of all successful login attempts.

not require login auditing to be turned on and is done by default. To view this log in the Event Viewer, open the event viewer and navigate to the Windows Logs heading and then the Security Tab. From here, select arch for the value 4624 , or filter the log for the ID 4624.

```
wevtutil qe Security "/q:*[System [(EventID=4624)]]" /f:6447 /a:1
```

Field	Value
Subject	Security ID: SYSTEM Account Name: Admin of Computer Logon ID: 0x00000000
Logon Information	Logon Type: 5 Remote Access Mode: No Extended Logon: No
Impersonation Level	Impersonation
Process Information	Process Name: Security Owner: Microsoft Windows security Event ID: 4624 Level: Informational User: N/A OpCode: 0x0

```
wevtutil qe Security "/q:*[System [(EventID=4624)]]" /f:6447 /a:1
```

```
Log Name: Security  
Source: Microsoft Windows security  
Event ID: 4624  
Level: Informational  
User: N/A  
OpCode: 0x0
```

What is in each entry:

Sample log & how to view (GUI & CLI)



User Logon
Windows 10 Professional

A users log in will likely be the first sign of an attack and can indicate suspicious behavior. It can also give an analyst a starting time to create a timeline of events. This log is required in the HIPAA and PCI DSS regulations and is recommended by the NSA Event Forwarding Guidance and JPCERT.

```
PowerShell wevtutil qe Security "/q:*[System [(EventID=4624)]]" /f:6447 /a:1
```

Local Group Policy Editor

Local Security Policy

Audit logon events Properties

In order to turn on login auditing, double click "Audit logon events". Clicking the Success box will allow for the auditing of all successful login attempts.

Event 4624, Microsoft Windows security auditing

General Details

Subject	Security ID	Process Name	Name of Computer
	SYSTEM	System	NAME-OF-COMPUTER
	SYSTEM	System	NAME-OF-COMPUTER

Logon Information

Logon Type	Logon Process	Process ID
5	System	0x00000000

Process Information

Process Name	Process ID	Process Name	Process ID
System	0x00000000	System	0x00000000

To view this log in the command line (via powershell or command prompt, enter the command `wevtutil qe Security "/q:*[System [(EventID=4624)]]"` This will show all instances of the event ID 4624, which is the logon log ID.

```
wevtutil qe Security "/q:*[System [(EventID=4624)]]" /f:6447 /a:1
```

```
Log Name: Security
Source: Microsoft Windows security auditing
Event ID: 4624
Level: Informational
User: N/A
OpSource: Computer
OpSourcePath: Name of Computer
Category: Logon
Task Category: Logon
Event Type: Audit Success
Date and Time: 5/3/2020 10:01:00 AM
```

```
Log Name: Security
Source: Microsoft Windows security auditing
Event ID: 4624
Level: Informational
User: N/A
OpSource: Computer
OpSourcePath: Name of Computer
Category: Logon
Task Category: Logon
Event Type: Audit Success
Date and Time: 5/3/2020 10:01:00 AM
```

W2L Mission Statement

What2Log is a crowd sourced site that teaches you what to log, how they help you, and **builds custom scripts.**

Why copy and paste from each entry? We bundle it up for you!

Generate a script to make any needed config changes.



DEMO
W2L:Sawmill

Weekly dive into logs and logging systems

Updates about What2Log
(including new versions & features)

Thanks!

YOU!

SANS Defensive Operations Team

**Mick: Thanks to Flynn for asking such great questions...
and driving to answers!**

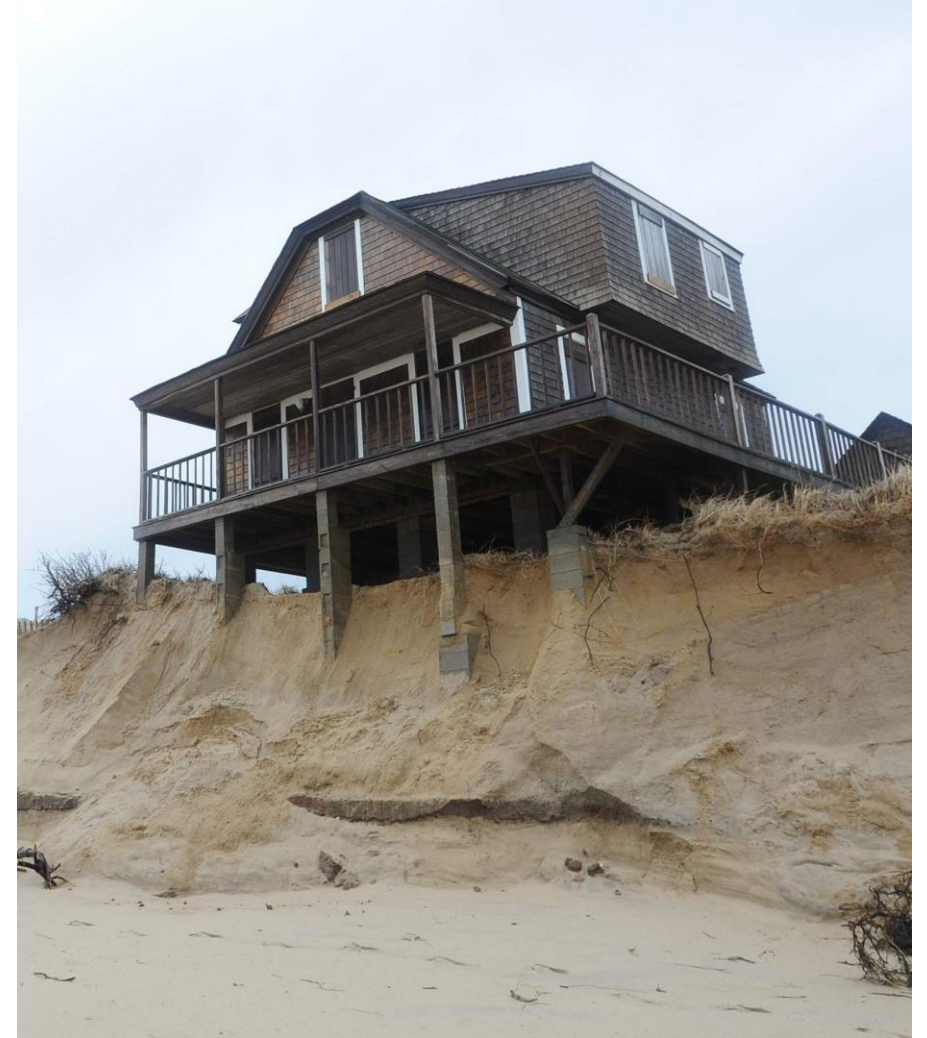
**Flynn: Thanks to Mick for giving me this opportunity and
supporting this project totally.**

In closing

IT and Security has a bad foundation

It's 2021.

This should have been solved in the '60s

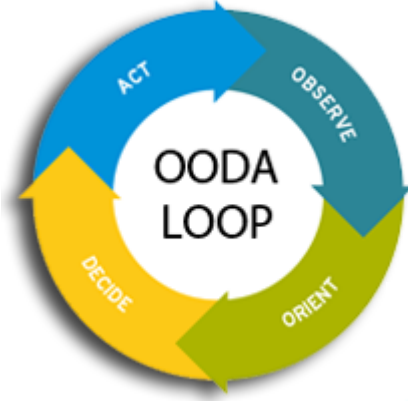


Fun with fundamentals

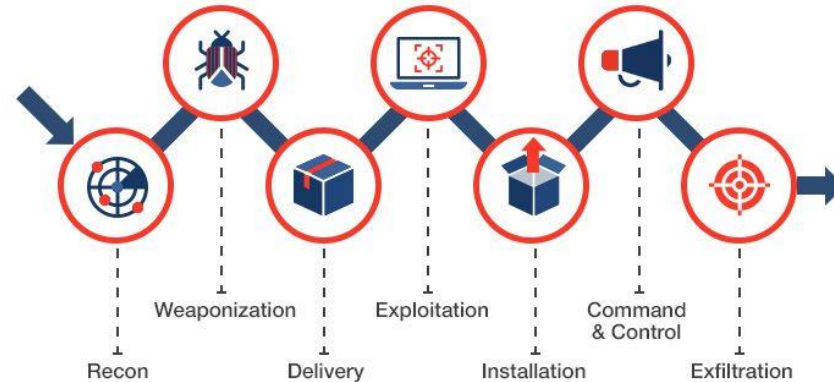
- Logs are the building blocks to your story and without the building blocks, you have no story
- Exciting to get to the bottom of what happened
- Paint the whole picture of an event
- Get the right answers

It's not the tooling... it's how we're thinking of the problems.

OODA loops



Cyber Kill Chain™



MITRE's CWE and ATT&CK



We need help...

- What frameworks should be covered?
- What other OSEs are needed?
- What application logs would you want to see?
- What can we do with this site to be more helpful/usable for you?

What stories do you want to tell?

Reach out!

Twitter

@What2Log

@bettersafetynet

@soundsofthetime

Reddit

r/What2Log

This is an InfoSec Innovations Project



INFOSEC INNOVATIONS

Better Information Security through:
Science, Creativity, and Caring.