

Blue Team Level 1 Certification  
(Standard)

## Introduction to BTL1

✓ Welcome to Blue Team Level 1

4 Topics

✓ Lab and Forum Access

## SECURITY FUNDAMENTALS DOMAIN

✓ Introduction to Security Fundamentals

1 Topic

✓ Soft Skills

7 Topics

✓ Security Controls

5 Topics 1 Quiz

✓ Networking 101

6 Topics 1 Quiz

✓ Management Principles

4 Topics 1 Quiz

## PHISHING ANALYSIS DOMAIN

✓ PA1) Introduction to Emails and Phishing

7 Topics 1 Quiz

✓ PA2) Types of Phishing Emails

10 Topics 2 Quizzes

✓ PA3) Tactics and Techniques Used

12 Topics 2 Quizzes

✓ PA4) Investigating a Phishing Email

8 Topics 2 Quizzes

✓ PA5) Analysing URLs, Attachments, and Artifacts

8 Topics 1 Quiz

○ PA6) Taking Defensive Actions

12 Topics 1 Quiz

○ PA7) Report Writing

7 Topics 1 Quiz

○ PA8) Phishing Response Challenge

3 Topics 1 Quiz

## THREAT INTELLIGENCE DOMAIN

○ TI1) Introduction to Threat Intelligence

7 Topics

○ TI2) Threat Actors &amp; APTs

6 Topics 2 Quizzes

○ TI3) Operational Threat Intelligence

7 Topics 1 Quiz

○ TI4) Tactical Threat Intelligence

7 Topics 1 Quiz

○ TI5) Strategic Threat Intelligence

5 Topics 1 Quiz

○ TI6) Malware and Global Campaigns

6 Topics 1 Quiz

## DIGITAL FORENSICS DOMAIN

○ DF1) Introduction to Digital Forensics

5 Topics

○ DF2) Forensics Fundamentals

10 Topics 5 Quizzes

# Sysmon

Blue Team Level 1 Certification (Standard) &gt; SI2) Logging &gt; Sysmon

IN PROGRESS



Sysmon is a Windows system service and device driver that, once installed on a system, remains resident across system reboots to monitor and log system activity to the Windows event log. It provides detailed information about process creations, network connections, and changes to file creation time. By collecting the events it generates using Windows Event Collection or SIEM agents and subsequently analyzing them. In this way, you can identify malicious or anomalous activity and understand how intruders and malware operate on your network.

## BENEFITS AND CAPABILITIES

- Logs process creation with full command line for both current and parent processes.
- Include a session GUID in each events to allow correlation of events on same logon session.
- Logs loading of drivers or DLLs with their signatures and hashes.
- Optionally logs network connections, including each connection's source process, IP addresses, port numbers, hostnames and port names.
- Detects changes in file creation time to understand when a file was really created. Modification of file create timestamps is a technique commonly used by malware to cover its tracks.
- Rule filtering to include or exclude certain events dynamically.

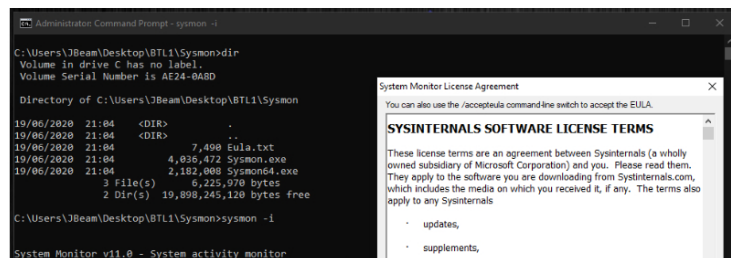
## Windows Event Logs vs Sysmon Logs

Some security professionals believe that Windows event logs are.. well.. terrible, and that Sysmon is a **much** better way to log information on Windows endpoints. Why? Because the formatting is nicer, and there's just a ton more useful information compared to Windows event logs. Black Hills Information Security made a great YouTube video covering the use of Sysmon, and we recommend all students watch it at the following link:

<https://youtu.be/9qsP5h033Qk?t=491>.

## INSTALLING SYSMON

If you want to try out Sysmon on your Windows host or virtual machine, below is a quick guide on how to set it up! First, download Sysmon from the Sysinternals website [here](#). Once you've extracted the folder within the Zip file, open a command prompt as administrator (Windows search bar > CMD > Right-click > Run as Administrator) and move to the location of the executable files. Use the command **sysmon -i** to begin the install, and click Agree when the EULA pops up.



DF3) Digital Evidence Collection

8 Topics 1 Quiz

DF4) Windows Investigations

3 Topics 3 Quizzes

DF5) Linux Investigations

4 Topics 2 Quizzes

DF6) Volatility

3 Topics 1 Quiz

DF7) Autopsy

4 Topics 1 Quiz

SECURITY INFORMATION AND EVENT MANAGEMENT DOMAIN

SI1) Introduction to SIEM

7 Topics 1 Quiz

SI2) Logging

6 Topics 2 Quizzes

Section Introduction, Logging

What is Logging?

Syslog

Windows Event Logs

Lab) Event Log Analysis

Sysmon

Other Logs

Activity) End of Section Review, Logging

SI3) Aggregation

2 Topics 1 Quiz

SI4) Correlation

6 Topics 1 Quiz

SI5) Using Splunk

5 Topics 2 Quizzes

INCIDENT RESPONSE DOMAIN

IR1) Introduction to Incident Response

8 Topics 1 Quiz

IR2) Preparation Phase

10 Topics 2 Quizzes

IR3) Detection and Analysis Phase

7 Topics 4 Quizzes

IR4) Containment, Eradication, and Recovery Phase

5 Topics 1 Quiz

IR5) Lessons Learned and Reporting

7 Topics

IR6) MITRE ATT&CK

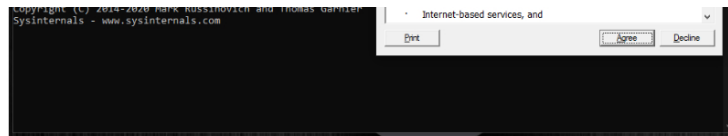
13 Topics 2 Quizzes

BTL1 EXAM

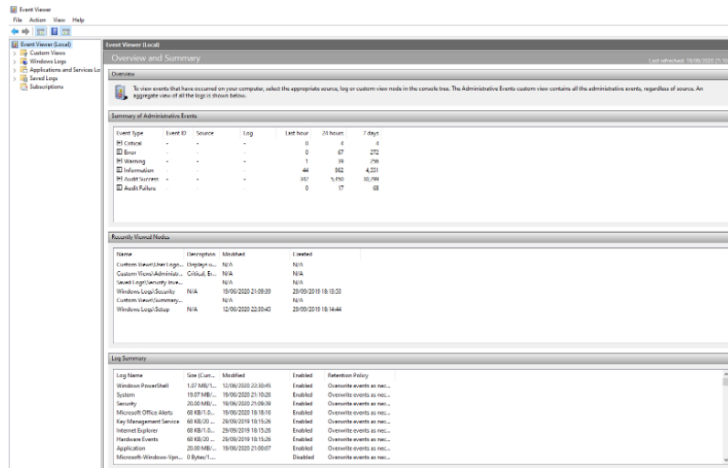
Exam Preparation

Using RDP and SSH

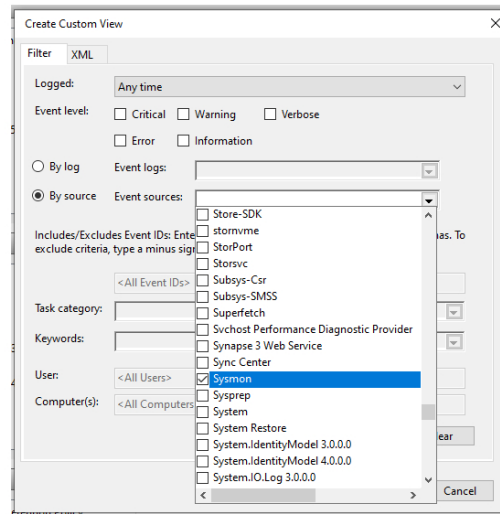
How to Start Your Exam



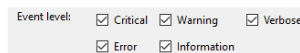
Now Sysmon is installed! Easy right? Now we want to look at Sysmon logs alongside Windows Event Logs in the tool Event Viewer. Press the Windows start button, search for "Event Viewer" and open the application.



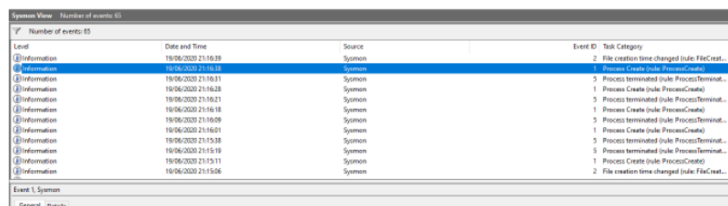
To actually see Sysmon logs, we need to create a Custom View - something we covered in the previous lesson. Click "Create Custom View" on the right-hand side, and copy what we've done in the below screenshot.



We also want to tick all of the Event Level options to ensure we can see all Sysmon logs.



Name the View whatever you want - we've decided to go for the simple name "Sysmon View", and click OK. We can now see Syslog logs, and boy do they contain a lot of information!



```
Process Create
PathName
InitTime 2020-06-19 20:16:38.121
ProcessId 4828d8e8-1630-59d3-25d1-000000000000
ProcessName
Image C:\Windows\System32\SearchHost.exe
Reference 7264
Description Microsoft Windows Search Host
Product Windows Search
Company Microsoft Corporation
OriginalFileName SearchHost.exe
CommandLine C:\Windows\system32\SearchHost.exe -S 760 764 712 832 768
CurrentDirectory C:\Windows\system32
User NT AUTHORITY\SYSTEM
LogonGuid {4283d8e8-1630-59d3-25d1-000000000000}
LogonId 0x127
TerminalSessionId
IntegrityLevel Medium
Hashes SHA1:A4ADCC8CA1A0AC8AA5C6B08CE0F31B26FAF4
PowerHashName {4828d8e8-1630-59d3-25d1-000000000000}
PowerProcessName 1084
ParentImage C:\Windows\System32\SearchHost.exe
ParentCommandLine C:\Windows\system32\SearchHost.exe /Embedding

Log Name: Microsoft Windows-System/Operational
Source: System
Logon: 18/06/2020 21:16:38
Event ID: 1 Task Category: Process Create (aka ProcessCreate)
Level: Information Keywords:
User: SYSTEM Computer: DESKTOP-VAG05VQ
OpCode: Info
```

In an organization, we could then feed this into our SIEM to provide additional detailed logs from Windows endpoints, working alongside Windows Event Logs! The problem with Sysmon is that it's very broad, and can generate a lot of noise, something we don't want to fill our SIEM up with. To combat this, we can use Sysmon configuration files, that work to reduce logs that aren't really necessary, allowing us to focus on the logs that we really need to monitor.

An example of a Sysmon configuration file can be found here – <https://github.com/SwiftOnSecurity/sysmon-config>. Take a look! The file has lots of comments and explanations, meaning it can also act as a tutorial on the important logs for monitoring.

[< Previous Topic](#)
[Mark Complete ✓](#)
[Next Topic >](#)