

SECURITY MONITORING MIT BORDMITTELN

Defense um € 0 Softwarekosten

ASSUME BREACH



PROBLEME DER VERTEIDIGER



Teilweise völliger Blindflug



Zu viel Information



Gleichzeitig zu wenig Information



Ressourcenmangel – Zeit/Geld

ASYMMETRISCH

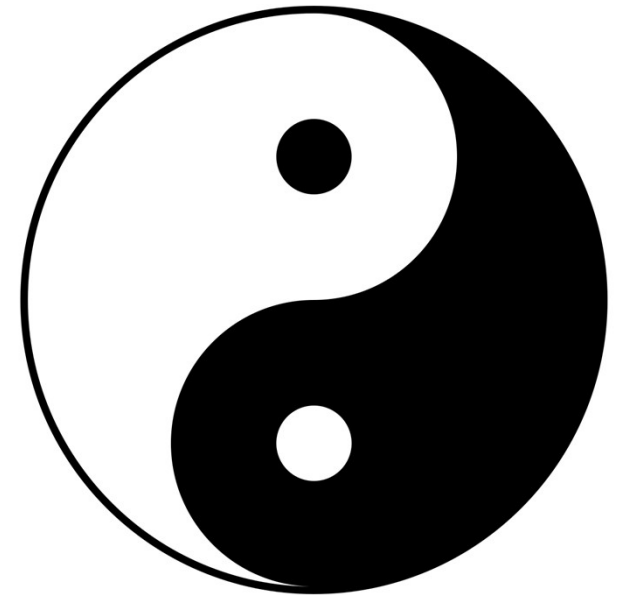
+Angreifer

+Muss nur eine Schwachstelle erfolgreich nutzen

+Verteidiger

+Muss immer alles im Griff haben

+Erwischen -> Gegenmaßnahmen



SYSINTERNALS SYSMON (SYSTEM MONITOR)

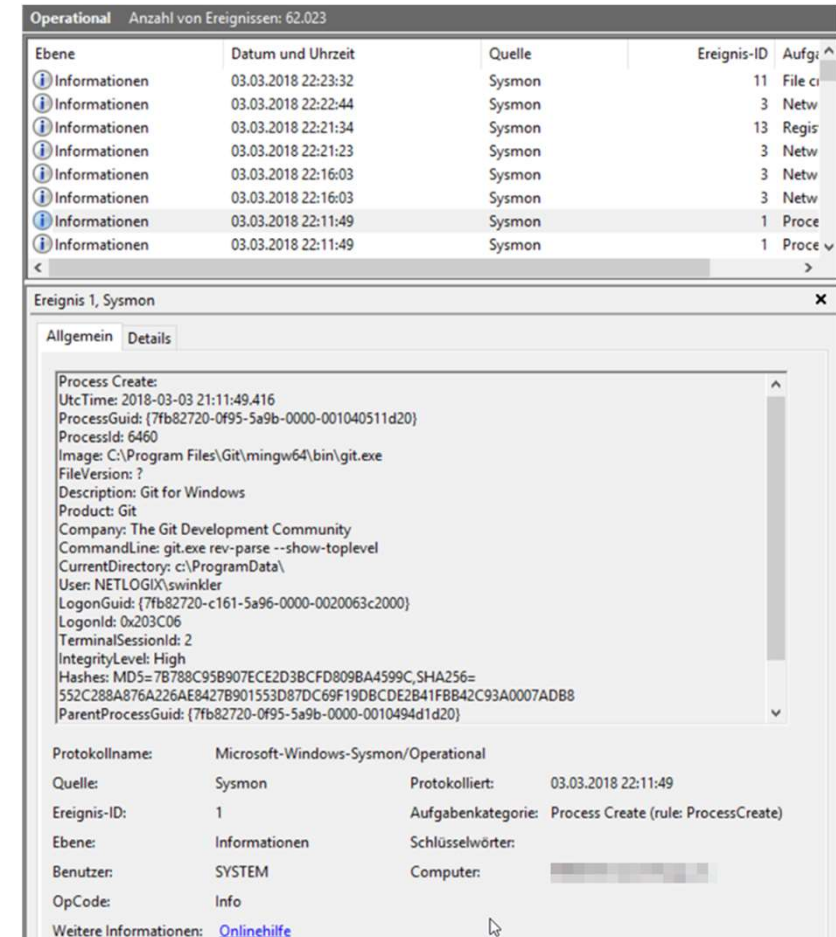


+ Monitoring Utility

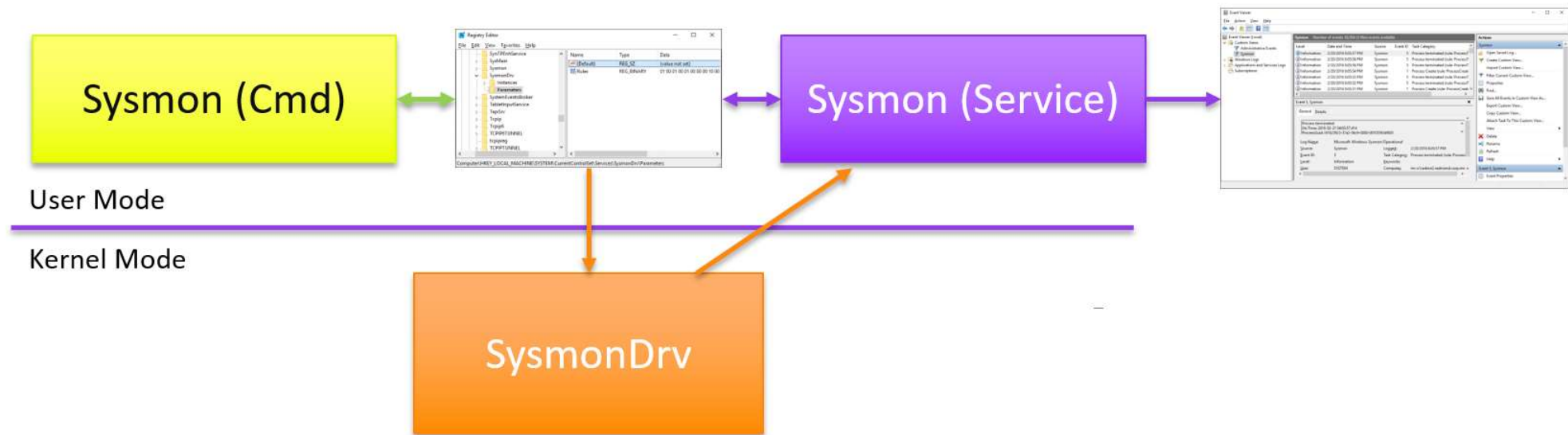
- + Schreibt in Windows Eventlog
- + Ermöglicht Erkennung von Anomalien
- + Für Microsoft Corporate Network geschrieben

+ Kostenloser Download

- + <https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon>



SYSMON ARCHITEKTUR



SYSMON EVENT ID'S

Category	Event ID
Process Create	1
File Creation Time Changed	2
Network Connection	3
Sysmon Service State Change	4
Process Terminated	5
Driver Loaded	6
Image Loaded	7
CreateRemoteThread	8
RawAccessRead	9

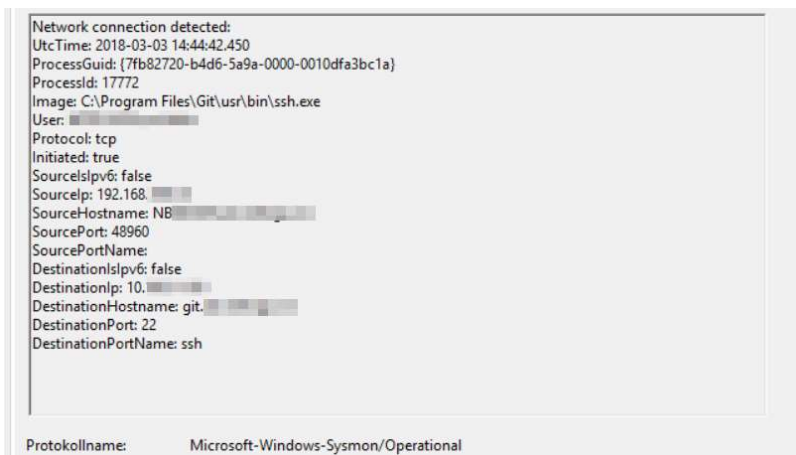
Category	Event ID
Process Access	10
File Create	11
Registry Object CreateDelete	12
Registry Value Create	13
Registry Object Rename	14
File Create Stream Hash	15
Sysmon Configuration Changed	16
Pipe Created	17
Pipe Connected	18
Error	255

Neu in Sysmon 7 – WMI Events

WmiEventFilter activity detected	19
WmiEventConsumer activity detected	20
WmiEventConsumerToFilter activity detected	21

BEISPIEL – NETWORK EVENTS

- + TCP und UDP
- + DNS und Port – Namensauflösung
- + Protokollierung bei Verbindungsaufbau
- + Enthält Image (powershell.exe, ...)



Network Connection Detected	
UtcTime	DestinationIsIpv6
ProcessGuid	DestinationIp
ProcessId	DestinationHostName
Image	DestinationPort
User	DestinationPortName
Protocol	
Initiated	
SourceIsIpv6	
SourceIp	
SourceHostName	
SourcePort	
SourcePortName	

SYSMON KONFIGURATION

+ Konfiguration via XML-File

+ Granulare Filter

install: `sysmon -i -accepteula c:\SysmonConfig.xml`
update: `sysmon -c c:\SysmonConfig.xml`

```
<!--SYSMON EVENT ID 1 : PROCESS CREATION [ProcessCreate]-->
<!--COMMENT: All process launched will be included, except for what matches a rule below. It's best to be as specific as possible, to
avoid user-mode executables imitating other process names to avoid logging, or if malware drops files in an existing directory.
Ultimately, you must weigh CPU time checking many detailed rules, against the risk of malware exploiting the blindness created.
Beware of Masquerading, where attackers imitate the names and paths of legitimate tools. Ideally, you'd use both file path and
code signatures to validate, but Sysmon does not support that. Look into Windows Device Guard for whitelisting support. -->

<!--DATA: UtcTime, ProcessGuid, ProcessID, Image, FileVersion, Description, Product, Company, CommandLine, CurrentDirectory, User, LogonGuid, LogonId,
<ProcessCreate onmatch="exclude">
  <!--SECTION: Microsoft Windows-->
  <CommandLine condition="begin with">C:\Windows\system32\DllHost.exe /Processid</CommandLine> <!--Microsoft:Windows-->
  <CommandLine condition="is">C:\Windows\system32\SearchIndexer.exe /Embedding</CommandLine> <!--Microsoft:Windows: Search Indexer-->
  <Image condition="is">C:\Windows\system32\CompatTelRunner.exe</Image> <!--Microsoft:Windows: Customer Experience Improvement-->
  <Image condition="is">C:\Windows\system32\audiodg.exe</Image> <!--Microsoft:Windows: Launched constantly-->
  <Image condition="is">C:\Windows\system32\conhost.exe</Image> <!--Microsoft:Windows: Command line interface host process-->
  <Image condition="is">C:\Windows\system32\musNotification.exe</Image> <!--Microsoft:Windows: Update pop-ups-->
```

DEMO TIME



SYSMON-CONFIG



The screenshot shows the GitHub repository page for `SwiftOnSecurity/sysmon-config`. The browser address bar displays the URL `https://github.com/SwiftOnSecurity/sysmon-config`. The repository page includes a navigation bar with links for Features, Business, Explore, Marketplace, and Pricing, along with a search bar and "Sign in" or "Sign up" buttons. The repository name is `SwiftOnSecurity / sysmon-config`, with 187 watches, 1,066 stars, and 249 forks. The "Code" tab is selected, showing 10 issues, 6 pull requests, 0 projects, and insights. A "Join GitHub today" banner is present, stating that GitHub is home to over 20 million developers. Below the banner, the repository description is "Sysmon configuration file template with default high-quality event tracing". A list of tags includes `sysmon`, `threatintel`, `threat-hunting`, `sysinternals`, `windows`, `netsec`, `monitoring`, and `logging`. The repository statistics show 114 commits, 1 branch, 0 releases, and 8 contributors. The "Branch: master" dropdown is set to "master", and a "New pull request" button is visible. The "Find file" button is highlighted, and a "Clone or download" button is also present. The file list shows the following files and their commit history:

File	Commit	Time
<code>.gitignore</code>	Edit .gitignore	2 months ago
<code>README.md</code>	Update README.md	a year ago
<code>sysmonconfig-export.xml</code>	64: New monitoring	a month ago

CHOCOLATEY

+ Paketmanager

+ *apt-get/yum/dnf/pacman* für Windows

+ Powershell

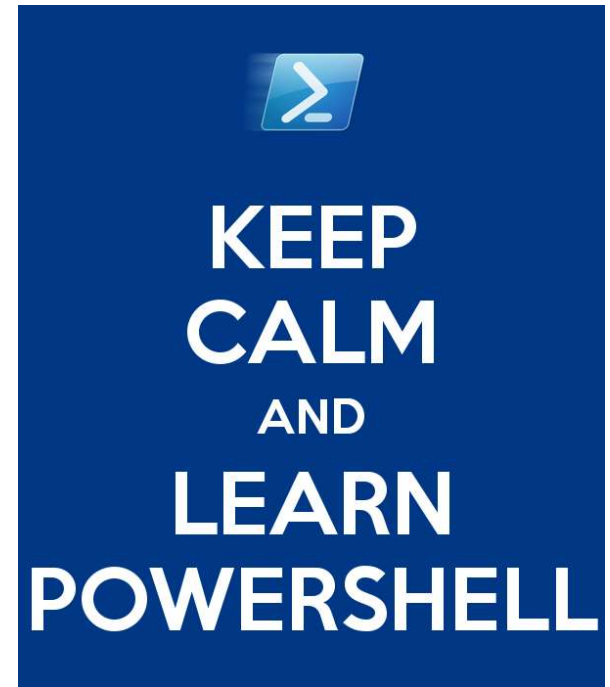
+ <https://chocolatey.org/>



POWERSHELL REPORTING



- +Nach interessanten Logeinträgen suchen
- +Daten verdichten
- +Report erstellen
- +Als Mail versenden



HTML REPORT

← → ↻ GitHub, Inc. [US] | https://github.com/RamblingCookieMonster/PSHTMLTable

Formidable SCOM Alert

Wed 1/29/2014 8:03 AM

SCOM@ [REDACTED]

New SCOM Alert: C on [REDACTED] 320 low (0.48 GB)

To [REDACTED] Engineering; [REDACTED] Operations Center; [REDACTED] Storage [REDACTED]

Property	Value
Computer Name	[REDACTED] 320 [REDACTED] Web App
Alert Name	Logical Disk Free Space is low
Alert Description	The disk C: on computer [REDACTED] 320, [REDACTED] is running out of disk space.
Monitoring Object	C:
Path	[REDACTED] 320, [REDACTED]
vcServerClass	Prod
vcServerContact	[REDACTED]
Free Space on C: (GB)	0.48
Total Space on C: (GB)	11.99
C:\windows\temp (GB)	0.51
C:\Windows\system32\LogFiles (GB)	3.27

Troubleshooting suggestions:

- Check common folders listed in the table (e.g. \temp) for unnecessary files
- Investigate disk space use; for example, Run `\\[REDACTED] 320\Tools\SpaceSniffer.exe scan '\\[REDACTED] 320\C$'`
- If space cannot be cleared up, escalate with appropriate engineer for server-specific analysis and potential drive expansion

LOGS ZENTRALISIEREN

+ Windows Event Forwarding (Windows Bordmittel)

+ <https://aka.ms/WEF>

+ Open Source

+ <https://cyberwardog.blogspot.co.at/2017/03/building-sysmon-dashboard-with-elk-stack.html>

+ Kommerzielles SIEM

+ z.B. Made in Austria: <https://www.iqsol.biz/produkte/logapp/>

LINKS

- + <https://github.com/anlx-sw/sysmon-report>
- + <https://github.com/MHaggis/sysmon-dfir>
- + <https://github.com/SwiftOnSecurity/sysmon-config>



Danke!

Fragen?



ANTARES
NETLOGIX
www.netlogix.at