2.11 Microsoft Sysinternals – Windows-Prozesse und Systemaktivitäten analysieren

Microsoft Sysinternals ist eine Sammlung spezialisierter Werkzeuge zur Diagnose von Windows-Systemen. Die Programme ermöglichen wesentlich tiefere Einblicke als der Task-Manager oder die üblichen Windows-Bordmittel.

Mit Sysinternals lassen sich unter anderem folgende Fragen beantworten:

- Welcher Prozess verursacht eine hohe CPU- oder Arbeitsspeicherauslastung?
- Welcher Prozess hält eine Datei oder einen Ordner geöffnet?
- Welche DLLs wurden von einem Prozess geladen?
- Welche Datei-, Registry- und Prozesszugriffe führt eine Anwendung aus?
- Welches Programm stellt eine bestimmte Netzwerkverbindung her?
- Welche Programme, Dienste und Aufgaben werden automatisch gestartet?
- Ist eine ausführbare Datei digital signiert?
- Warum startet eine Anwendung nicht?
- Warum dauert die Anmeldung ungewöhnlich lange?
- Welcher Prozess verursacht einen Speicher- oder Handle-Anstieg?
- Wie kann für eine abgestürzte oder nicht reagierende Anwendung ein Speicherabbild erstellt werden?

> **Wichtig:** Sysinternals liefert technische Beobachtungen, aber nicht automatisch die Ursache einer Störung. Ein einzelner ungewöhnlicher Eintrag ist noch kein Beweis für einen Fehler oder Schadsoftware. Entscheidend sind Zusammenhang, zeitlicher Ablauf, Vergleichswerte und reproduzierbares Verhalten.

---

1. Kennzeichnungen und Sicherheitsregeln

Kennzeichnung	Bedeutung
[RO]	Read-only: liest Informationen aus, ohne den Zustand absichtlich zu verändern
[TEST]	Führt einen aktiven Test aus oder erzeugt zusätzliche Systemlast
[PRIV]	Benötigt möglicherweise Administratorrechte
[FILE]	Erzeugt oder verändert eine Datei
[SENS]	Ergebnis kann vertrauliche Daten enthalten

Kennzeichnung	Bedeutung
[CHANGE]	Verändert Einstellungen oder einen Systemzustand
[DISRUPT]	Kann Programme, Verbindungen oder Dienste unterbrechen

Bei der Arbeit mit Sysinternals gelten folgende Grundregeln:

1. Werkzeuge ausschließlich von Microsoft beziehungsweise über die offizielle Sysinternals-Seite beziehen.
2. Vor einer Analyse Zeitpunkt, betroffenen Computer, angemeldeten Benutzer und Fehlerbild dokumentieren.
3. Zuerst nur beobachten und Daten erfassen.
4. Prozesse, Handles, Verbindungen oder Autostarteinträge nicht vorschnell beenden beziehungsweise löschen.
5. Administratorrechte nur verwenden, wenn sie für die Untersuchung erforderlich sind.
6. Speicherabbilder, Process-Monitor-Aufzeichnungen und exportierte Listen als vertrauliche Daten behandeln.
7. VirusTotal-Abfragen nur unter Beachtung der betrieblichen Datenschutz- und Sicherheitsvorgaben verwenden.
8. Änderungen immer mit Rückweg, Sicherung und dokumentiertem Ausgangszustand durchführen.

2. Sysinternals sicher beziehen und starten

Die Werkzeuge können einzeln oder als vollständige Sysinternals Suite heruntergeladen werden.

Offizielle Bezugsquellen:

- Sysinternals-Übersicht: `https://learn.microsoft.com/sysinternals/`
- Sysinternals Suite: `https://learn.microsoft.com/sysinternals/downloads/sysinternals-suite`
- Sysinternals Live: `https://live.sysinternals.com/`

Die Suite eignet sich besonders für einen zentral gepflegten administrativen Werkzeugbestand.

Beispiel für eine lokale Ablage

```
C:\Admin\Sysinternals\
```

Start über Sysinternals Live

```
\\live.sysinternals.com\tools\procexp.exe
```

```
\\live.sysinternals.com\tools\procmon.exe
```

Das direkte Starten über Sysinternals Live kann durch Firewall-, Proxy-, WebDAV-, SMB- oder Sicherheitsrichtlinien verhindert werden. Für reproduzierbare Analysen ist eine lokal bereitgestellte und betrieblich freigegebene Version häufig sinnvoller.

Grundlegende Prüfung einer heruntergeladenen Datei

```
[RO] Get-AuthenticodeSignature "C:\Admin\Sysinternals\procexp.exe"
```

```
[RO] Get-FileHash "C:\Admin\Sysinternals\procexp.exe" -Algorithm SHA256
```

Die Signatur sollte gültig sein und zu Microsoft gehören. Ein Hashwert dient zur eindeutigen Dokumentation einer untersuchten Version, beweist allein aber nicht deren Vertrauenswürdigkeit.

Wichtiger Hinweis zur Lizenzvereinbarung

Viele Sysinternals-Kommandozeilenwerkzeuge unterstützen:

```
-accepteula
```

Damit wird die Lizenzvereinbarung ohne interaktive Rückfrage akzeptiert. Diese Option sollte nur eingesetzt werden, wenn die Lizenzvereinbarung organisatorisch geprüft und akzeptiert wurde.

3. Welches Sysinternals-Werkzeug eignet sich für welches Problem?

Problem oder Fragestellung	Geeignetes Werkzeug	Typische Untersuchung
Hohe CPU-Auslastung	Process Explorer, PsList, ProcDump	Verursachenden Prozess und Threads bestimmen
Ungewöhnlich hoher Speicherverbrauch	Process Explorer, RAMMap, VMMap	Speicherverteilung und Prozesswachstum untersuchen
Datei oder Ordner ist gesperrt	Process Explorer, Handle	Prozess mit geöffnetem Handle ermitteln

Problem oder Fragestellung	Geeignetes Werkzeug	Typische Untersuchung
Anwendung startet nicht	Process Monitor, Autoruns, Sigcheck	Fehlende Dateien, Berechtigungsfehler und Abhängigkeiten suchen
Anwendung stürzt ab	ProcDump, Process Monitor	Speicherabbild und Aktivitäten vor dem Absturz erfassen
Anwendung reagiert nicht	Process Explorer, ProcDump	Threads untersuchen und Hang-Dump erzeugen
Unbekannte Netzwerkverbindung	TCPView, Process Explorer	Verbindung einem Prozess zuordnen
Langsame Windows-Anmeldung	Autoruns, Process Monitor	Anmeldeobjekte, Dienste und Dateizugriffe untersuchen
Verdächtiger Autostart	Autoruns, Sigcheck	Herausgeber, Signatur, Pfad und Startmechanismus prüfen
Unbekannte ausführbare Datei	Sigcheck, Process Explorer	Signatur, Hash, Pfad und laufenden Prozess untersuchen
DLL-Konflikt	Process Explorer, ListDLLs, Process Monitor	Geladene DLL-Versionen und Suchpfade vergleichen
Handle-Leak	Process Explorer, Handle	Entwicklung der Handle-Anzahl beobachten
Speicherverteilung des Systems	RAMMap	Standby-Liste, Dateicache und physische Speichernutzung analysieren
Speicherbelegung eines Prozesses	VMMap	Private, gemeinsam genutzte und zugeordnete Bereiche untersuchen
Dauerhafte Ereigniserfassung	Sysmon	Sicherheitsrelevante Systemereignisse protokollieren
Fernadministration	PsTools	Autorisierte Prozess-, Dienst- und Systemabfragen durchführen

4. Process Explorer – Prozesse genauer untersuchen

Process Explorer ist eine erweiterte Prozessanzeige. Das Werkzeug stellt Prozesse hierarchisch dar und zeigt unter anderem:

- übergeordnete und untergeordnete Prozesse,
- Prozess-ID und Benutzerkonto,
- CPU- und Arbeitsspeicherauslastung,
- gestarteten Programmpfad,
- Kommandozeile,
- digitale Signatur,
- geladene DLLs,

- geöffnete Handles,
- Threads und deren CPU-Auslastung,
- Netzwerk- und Datenträgeraktivitäten.

Sinnvoller Diagnoseablauf

1. Process Explorer möglichst zunächst ohne Administratorrechte starten.
2. Prozessbaum und auffällige Prozesse identifizieren.
3. Bei unvollständiger Sichtbarkeit kontrolliert als Administrator neu starten.
4. Eigenschaften des betroffenen Prozesses öffnen.
5. Pfad, Kommandozeile, Benutzerkonto und übergeordneten Prozess prüfen.
6. CPU-, Speicher-, Datenträger- und Netzwerkentwicklung beobachten.
7. Digitale Signatur kontrollieren.
8. Bei hoher CPU-Auslastung die einzelnen Threads untersuchen.
9. Beobachtungen mit Zeitpunkt und Prozess-ID dokumentieren.

Wichtige Bewertungsfragen

Eigenschaft	Fragestellung
Image Path	Liegt die Datei im erwarteten Programmverzeichnis?
Command Line	Mit welchen Parametern wurde der Prozess gestartet?
Parent Process	Welcher Prozess hat ihn gestartet?
User Name	Unter welchem Benutzer- oder Dienstkonto läuft er?
Verified Signer	Ist die Signatur gültig und passt der Herausgeber?
Start Time	Begann das Problem mit dem Prozessstart?
Threads	Welcher Thread erzeugt die Auslastung?
Handles	Steigt die Anzahl dauerhaft an?
TCP/IP	Baut der Prozess unerwartete Verbindungen auf?

Datei oder DLL suchen

Über die Suchfunktion von Process Explorer kann nach einem Teil des Datei-, Ordner-, Registry- oder DLL-Namens gesucht werden. Dadurch lässt sich beispielsweise ermitteln, welcher Prozess eine Datei geöffnet hält.

```
Find → Find Handle or DLL
```

Wichtige Grenzen

- Ein unbekannter Prozess ist nicht automatisch schädlich.

- Eine fehlende digitale Signatur ist kein Malware-Beweis.
- Eine gültige Signatur beweist nicht, dass ein Programm harmlos ist.
- Das Beenden eines Prozesses kann Datenverlust und Dienstausfälle verursachen.
- Systemprozesse dürfen nicht ohne vorherige Identifikation beendet werden.
- Unterschiedliche Prozesse können denselben Dateinamen verwenden.

Eingreifende Funktionen

Aktion	Risiko
Prozess beenden	[CHANGE][DISRUPT] Ungespeicherte Daten können verloren gehen
Prozessbaum beenden	[CHANGE][DISRUPT] Beendet zusätzlich untergeordnete Prozesse
Prozess anhalten	[CHANGE][DISRUPT] Anwendung oder abhängige Dienste können blockieren
Handle schließen	[CHANGE][DISRUPT] Anwendung kann abstürzen oder Daten beschädigen
Priorität ändern	[CHANGE] Kann Leistungsverhalten und Stabilität beeinflussen

Diese Funktionen gehören nicht zur ersten Diagnosephase.

5. Process Monitor – Datei-, Registry- und Prozesszugriffe verfolgen

Process Monitor, kurz Procmon, zeichnet in Echtzeit folgende Aktivitäten auf:

- Dateisystemzugriffe,
- Registry-Zugriffe,
- Prozess- und Thread-Ereignisse,
- Laden von Abbildern und DLLs,
- Zugriffsresultate,
- Prozess-ID, Benutzer und Aufrufpfad,
- auf Wunsch zugehörige Aufrufstapel.

Process Monitor eignet sich besonders, wenn eine Anwendung:

- nicht startet,
- eine Datei nicht findet,
- keine Konfiguration speichern kann,
- einen Berechtigungsfehler meldet,
- eine falsche DLL lädt,
- auf einen nicht erreichbaren Pfad zugreift,
- beim Start ungewöhnlich lange wartet.

Empfohlener Aufnahmeablauf

1. Fehlerbild und genaue Uhrzeit notieren.
2. Process Monitor starten.
3. Laufende Aufzeichnung zunächst anhalten.
4. Bereits angezeigte Ereignisse leeren.
5. Filter auf den betroffenen Prozess setzen.
6. Aufzeichnung starten.
7. Fehler genau einmal reproduzieren.
8. Aufzeichnung sofort wieder anhalten.
9. Ereignisse unmittelbar vor und nach dem Fehler untersuchen.
10. Originalaufzeichnung im PML-Format sichern.
11. Sensible Daten und Aufbewahrungsregeln beachten.

Nützliche Standard-Tastenkombinationen

Funktion	Tastenkombination
Aufzeichnung starten oder anhalten	Strg+E
bisher angezeigte Ereignisse löschen	Strg+X
Filterdialog öffnen	Strg+L
Ereignis suchen	Strg+F
Aufnahme speichern	Strg+S

Beispiel für einen Prozessfilter

```
Process Name  is  beispiel.exe  Include
```

Weitere nützliche Filter:

```
Process ID    is       4321         Include
Result        is       ACCESS DENIED Include
Path          contains  \Config\     Include
Operation     is       CreateFile    Include
```

Mehrere `Include`-Filter derselben Eigenschaft wirken typischerweise wie eine ODER-Verknüpfung. Unterschiedliche Eigenschaften grenzen das Ergebnis weiter ein. Der Filter sollte deshalb bewusst aufgebaut und im Filterdialog kontrolliert werden.

Häufige Resultate richtig interpretieren

Resultat	Grundbedeutung	Bewertung
SUCCESS	Operation war erfolgreich	Kein Fehler für diese einzelne Operation
NAME NOT FOUND	Name oder Objekt wurde nicht gefunden	Kann normaler Suchlauf oder tatsächliche Ursache sein
PATH NOT FOUND	Ein Bestandteil des Pfades fehlt	Pfad, Laufwerk, Freigabe oder Konfiguration prüfen
ACCESS DENIED	Zugriff wurde verweigert	Berechtigungen, Integritätsstufe und Sicherheitssoftware prüfen
SHARING VIOLATION	Objekt ist inkompatibel geöffnet	Öffnenden Prozess und Freigabemodus untersuchen
BUFFER OVERFLOW	bereitgestellter Puffer war zunächst zu klein	Häufig Bestandteil einer normalen Größenabfrage
REPARSE	Zugriff wurde über einen Reparse Point umgeleitet	Junction, symbolischen Link oder Cloud-Platzhalter prüfen
END OF FILE	Dateiende wurde erreicht	Kann bei normalen Lesevorgängen auftreten

> NAME NOT FOUND und BUFFER OVERFLOW treten bei normalen Windows-Abläufen sehr häufig auf. Entscheidend ist, ob danach ein erfolgreicher Alternativzugriff erfolgt oder die Anwendung unmittelbar anschließend scheitert.

PML-Dateien

Eine gespeicherte PML-Datei kann enthalten:

- Benutzernamen,
- Dateipfade,
- Registry-Pfade,
- Server- und Freigabenamen,
- Prozessnamen und Kommandozeilen,
- Anwendungs- und Dokumentnamen,
- Hinweise auf interne Infrastruktur.

Daher gilt:

[SENS][FILE] PML-Dateien nur geschützt speichern und kontrolliert weitergeben.

6. Autoruns – Autostarts und Anmeldeverzögerungen untersuchen

Autoruns zeigt zahlreiche Stellen, über die Programme, Dienste, Treiber und Erweiterungen automatisch gestartet werden können.

Dazu gehören unter anderem:

- Benutzeranmeldung,
- Dienste,
- Treiber,
- geplante Aufgaben,
- Explorer-Erweiterungen,
- Winlogon-Komponenten,
- Browser-Erweiterungen,
- WMI-basierte Autostarts,
- Winsock- und Netzwerkkomponenten,
- Druckmonitor-DLLs,
- bekannte DLLs und Image-Hijacks.

Sicherer Diagnoseablauf

1. Autoruns starten und vollständiges Einlesen abwarten.
2. Betroffenen Benutzer und Systemkontext beachten.
3. Eintrag, Pfad, Herausgeber und digitale Signatur prüfen.
4. Vor Veränderungen einen Export oder Screenshot erstellen.
5. Microsoft-Einträge nur ausblenden, um Fremdsoftware übersichtlicher zu prüfen.
6. Bei einem begründeten Verdacht einen Eintrag zunächst deaktivieren.
7. System oder Anmeldung kontrolliert testen.
8. Ergebnis dokumentieren.
9. Eintrag wieder aktivieren, wenn keine Verbesserung eingetreten ist.

Das Entfernen des Häkchens deaktiviert einen Eintrag und ist grundsätzlich leichter rückgängig zu machen als das Löschen.

```
[CHANGE] Deaktivieren: Eintrag abwählen
```

```
[CHANGE][DISRUPT] Löschen: Eintrag dauerhaft entfernen
```

Autostarteinträge sollten während der Fehleranalyse nicht vorschnell gelöscht werden.

Autorunsc – Kommandozeilenversion

Alle Kategorien anzeigen:

```
[RO][PRIV] autorunsc.exe -a * -s
```

Alle Kategorien mit Signaturprüfung und CSV-Ausgabe erfassen:

```
[RO][PRIV][FILE] autorunsc.exe -a * -s -c > C:\Temp\autoruns.csv
```

Microsoft-Einträge ausblenden:

```
[RO][PRIV] autorunsc.exe -a * -m -s
```

Geplante Aufgaben anzeigen:

```
[RO][PRIV] autorunsc.exe -a t -s
```

Dienste und nicht deaktivierte Treiber anzeigen:

```
[RO][PRIV] autorunsc.exe -a s -s
```

Anmeldeeinträge anzeigen:

```
[RO] autorunsc.exe -a l -s
```

WMI-Autostarts anzeigen:

```
[RO][PRIV] autorunsc.exe -a m -s
```

Wichtige Kategorien

Option	Kategorie
`-a *`	Alle Kategorien
`-a b`	Boot-Execute-Einträge
`-a d`	AppInit-DLLs
`-a e`	Explorer-Erweiterungen
`-a h`	Image Hijacks
`-a i`	Internet-Explorer-Erweiterungen

Option	Kategorie
`-a k`	Known DLLs
`-a l`	Anmeldeeinträge
`-a m`	WMI-Einträge
`-a n`	Winsock- und Netzwerkprovider
`-a p`	Druckmonitor-DLLs
`-a r`	LSA-Sicherheitsprovider
`-a s`	Dienste und nicht deaktivierte Treiber
`-a t`	Geplante Aufgaben
`-a w`	Winlogon-Einträge

VirusTotal-Hinweis

Die Autoruns- und Autorunsc-Integration kann Hashwerte an VirusTotal übermitteln. Abhängig von den gewählten Optionen können unbekannte Dateien auch hochgeladen werden.

[SENS] Keine VirusTotal-Abfrage ohne betriebliche Freigabe durchführen.

Insbesondere darf eine Upload-Funktion nicht für vertrauliche, proprietäre oder personenbezogene Dateien verwendet werden. Eine VirusTotal-Erkennung ist außerdem nur ein Hinweis und kein abschließender Malware-Beweis.

7. TCPView und Tcpvcon – Netzwerkverbindungen Prozessen zuordnen

TCPView zeigt TCP- und UDP-Endpunkte einschließlich:

- lokalem Endpunkt,
- entferntem Endpunkt,
- Verbindungsstatus,
- Prozessname,
- Prozess-ID,
- zugehörigem Dienst.

Damit lässt sich beispielsweise feststellen, welches Programm eine Verbindung zu einer bestimmten IP-Adresse aufgebaut hat oder welcher Prozess auf einem lokalen Port lauscht.

Typischer Untersuchungsablauf

1. TCPView starten.

2. Nach Prozess, Port oder Zieladresse suchen.
3. Namensauflösung bei Bedarf deaktivieren, damit nur tatsächliche IP-Adressen erscheinen.
4. Prozess-ID und Programmpfad mit Process Explorer abgleichen.
5. Zieladresse, Port, Prozesskontext und Verbindungszeitpunkt dokumentieren.
6. Erst danach bewerten, ob die Verbindung erwartet ist.

Tcpvcon – Kommandozeilenversion

Aktive TCP-Verbindungen anzeigen:

```
[RO] tcpvcon.exe
```

Alle TCP- und UDP-Endpunkte anzeigen:

```
[RO] tcpvcon.exe -a
```

Namensauflösung deaktivieren:

```
[RO] tcpvcon.exe -a -n
```

CSV-Ausgabe erzeugen:

```
[RO][FILE] tcpvcon.exe -a -n -c > C:\Temp\tcp-endpoints.csv
```

Bestimmten Prozess untersuchen:

```
[RO] tcpvcon.exe -a -n beispiel.exe
```

Bestimmte PID untersuchen:

```
[RO] tcpvcon.exe -a -n 4321
```

Option	Bedeutung
-a	Alle Endpunkte anzeigen
-c	CSV-Ausgabe erzeugen
-n	Adressen nicht in Namen auflösen

Option	Bedeutung
Prozessname oder PID	Ausgabe auf einen Prozess begrenzen

TCPView kann eine bestehende TCP-Verbindung schließen:

```
[CHANGE][DISRUPT] Close Connection
```

Dadurch wird nur die konkrete Verbindung unterbrochen. Der Prozess kann anschließend erneut eine Verbindung herstellen. Diese Funktion ersetzt weder eine Firewall-Regel noch das Beenden oder Konfigurieren des verursachenden Programms.

8. Handle – Dateisperren und offene Objekte ermitteln

Handle zeigt geöffnete Handles eines Prozesses an. Damit kann insbesondere festgestellt werden, welches Programm eine Datei oder einen Ordner geöffnet hält.

Handle benötigt laut Microsoft Administratorrechte.

Nach einem Teil eines Dateinamens suchen:

```
[RO][PRIV] handle.exe bericht.xlsx
```

Nach einem Pfadbestandteil suchen:

```
[RO][PRIV] handle.exe C:\Daten\Projekt
```

Handles eines bestimmten Prozesses anzeigen:

```
[RO][PRIV] handle.exe -p explorer
```

Handles einer bestimmten PID anzeigen:

```
[RO][PRIV] handle.exe -p 4321
```

Besitzenden Benutzer anzeigen:

```
[RO][PRIV] handle.exe -u bericht.xlsx
```

Anzahl der verschiedenen Handle-Typen anzeigen:

```
[RO][PRIV] handle.exe -s
```

Alle Arten von Handles anzeigen:

```
[RO][PRIV] handle.exe -a -p 4321
```

Beispielausgabe sinngemäß interpretieren

```
beispiel.exe pid: 4321
  7C: File  C:\Daten\Projekt\bericht.xlsx
```

Feld	Bedeutung
`beispiel.exe`	Prozessname
`4321`	Prozess-ID
`7C`	Handle-Wert in hexadezimaler Schreibweise
`File`	Objekttyp
Pfad	geöffnetes Objekt

Handle kann ein einzelnes Handle zwangsweise schließen:

```
[CHANGE][DISRUPT][PRIV] handle.exe -c 7C -p 4321
```

> Das erzwungene Schließen eines Handles kann Anwendungen zum Absturz bringen, Daten beschädigen oder das System destabilisieren. Diese Funktion ist kein regulärer erster Lösungsweg. Besser ist es, das verantwortliche Programm geordnet zu schließen oder den zugehörigen Dienst kontrolliert zu beenden.

Die Option `-y` unterdrückt die Sicherheitsabfrage beim Schließen und sollte bei einer manuellen Fehleranalyse nicht eingesetzt werden.

9. Sigcheck – Signaturen, Versionen und Hashwerte prüfen

Sigcheck zeigt unter anderem:

- Dateiversion,
- Zeitstempel,
- digitale Signatur,
- Zertifikatskette,
- Hashwerte,
- optional den VirusTotal-Status.

Erweiterte Dateiinformationen anzeigen:

```
[RO] sigcheck.exe -nobanner -a "C:\Programme\Beispiel\beispiel.exe"
```

Hashwerte anzeigen:

```
[RO] sigcheck.exe -nobanner -h "C:\Programme\Beispiel\beispiel.exe"
```

Signatur und Zertifikatskette anzeigen:

```
[RO] sigcheck.exe -nobanner -i "C:\Programme\Beispiel\beispiel.exe"
```

Kombinierte Prüfung:

```
[RO] sigcheck.exe -nobanner -a -h -i "C:\Programme\Beispiel\beispiel.exe"
```

Nicht signierte ausführbare Dateien in `System32` suchen:

```
[RO][PRIV] sigcheck.exe -nobanner -u -e C:\Windows\System32
```

Unterordner rekursiv untersuchen:

```
[RO][PRIV] sigcheck.exe -nobanner -u -e -s C:\Windows\System32
```

Option	Bedeutung
`-a`	Erweiterte Versionsinformationen anzeigen
`-e`	Nur ausführbare Images untersuchen
`-h`	Hashwerte anzeigen

Option	Bedeutung
`-i`	Zertifikatskette und Katalog anzeigen
`-s`	Unterverzeichnisse rekursiv durchsuchen
`-u`	Ohne VirusTotal nur nicht signierte Dateien anzeigen
`-c`	CSV-Ausgabe
`-ct`	Tabulatorgetrennte Ausgabe
`-nobanner`	Startbanner ausblenden
`-accepteula`	Lizenzvereinbarung ohne Dialog akzeptieren

Bewertung einer Signatur

Ergebnis	Aussage
Gültige Signatur	Datei wurde signiert und seit der Signierung nicht entsprechend verändert
Ungültige Signatur	Signaturprüfung ist fehlgeschlagen
Keine Signatur	Datei besitzt keine auswertbare digitale Signatur
Bekannter Herausgeber	Herausgeber ergibt sich aus dem Zertifikat
Unbekannter Herausgeber	Vertrauenskette oder Signatur fehlt beziehungsweise ist nicht vertrauenswürdig

Eine gültige Signatur bedeutet nicht automatisch, dass die Datei sicher oder erwünscht ist. Eine nicht signierte Datei ist umgekehrt nicht automatisch Schadsoftware.

VirusTotal-Optionen

```
-v
```

fragt den VirusTotal-Status anhand des Dateihashs ab.

```
-vs
```

kann Dateien, die VirusTotal noch nicht kennt, zur Analyse hochladen.

```
[SENS] `-vs` niemals ohne ausdrückliche Datenschutz- und Sicherheitsfreigabe verwenden.
```

10. PsList und weitere PsTools – Prozesse und Dienste per Kommandozeile prüfen

Die PsTools enthalten verschiedene Kommandozeilenwerkzeuge für lokale und entfernte Windows-Systeme.

Werkzeug	Aufgabe	Risiko
PsList	Prozessinformationen anzeigen	[RO]
PsService	Dienste abfragen und verwalten	Abfrage [RO], Änderungen [CHANGE][DISRUPT]
PsLoggedOn	angemeldete Benutzer anzeigen	[RO][SENS]
PsInfo	Systeminformationen anzeigen	[RO]
PsKill	Prozesse beenden	[CHANGE][DISRUPT]
PsExec	Prozesse lokal oder remote starten	[PRIV][CHANGE][DISRUPT]
PsShutdown	Computer herunterfahren oder neu starten	[PRIV][CHANGE][DISRUPT]

Lokale Prozesse anzeigen:

```
[RO] pslist.exe
```

Prozessbaum anzeigen:

```
[RO] pslist.exe -t
```

Detaillierte Speicherinformationen anzeigen:

```
[RO] pslist.exe -m
```

Bestimmte PID untersuchen:

```
[RO] pslist.exe 4321
```

Entfernten Computer abfragen:

```
[RO][PRIV] pslist.exe \\PC-023
```

Remote-Abfragen dürfen ausschließlich auf autorisierten Systemen erfolgen. Windows-Firewall, administrative Freigaben, Namensauflösung, Dienststeuerung und Berechtigungen können den Zugriff beeinflussen.

Umgang mit Zugangsdaten

PsTools können bei manchen Werkzeugen Benutzername und Kennwort als Parameter entgegennehmen. Kennwörter sollten nicht direkt in Befehlszeilen eingetragen werden, da sie beispielsweise in:

- Befehlsverläufen,
- Prozesslisten,
- Skripten,
- Protokollen,
- Bildschirmaufzeichnungen

sichtbar werden können.

Wenn möglich, sollte ein bereits autorisierter administrativer Kontext oder eine betrieblich freigegebene Lösung zur privilegierten Administration verwendet werden.

Besonders eingreifende Werkzeuge

```
[CHANGE][DISRUPT] pskill.exe 4321
```

beendet einen Prozess.

```
[PRIV][CHANGE][DISRUPT] psexec.exe \\PC-023 Programm.exe
```

startet einen Prozess auf einem entfernten Computer.

Diese Befehle sind keine reinen Diagnosebefehle. Vor ihrer Verwendung müssen Zielsystem, Prozess, Auswirkung, Berechtigung und Rückweg eindeutig geklärt sein.

11. ProcDump – Speicherabbilder bei Abstürzen, Hängern und Lastspitzen erstellen

ProcDump kann Speicherabbilder eines Prozesses manuell oder beim Eintreten bestimmter Bedingungen erzeugen.

Typische Auslöser sind:

- hohe CPU-Auslastung,

- nicht reagierendes Programmfenster,
- unbehandelte Ausnahme,
- Prozessende,
- bestimmter Speicherverbrauch,
- bestimmter Leistungsindikator.

Vollständiges Speicherabbild einer PID erzeugen

```
[TEST][PRIV][FILE][SENS] procdump.exe -ma 4321 C:\Dumps
```

Speicherabbild bei nicht reagierendem Fenster

```
[TEST][PRIV][FILE][SENS] procdump.exe -ma -h beispiel.exe C:\Dumps
```

Bis zu drei Speicherabbilder bei erhöhter CPU-Auslastung

```
[TEST][PRIV][FILE][SENS] procdump.exe -ma -n 3 -s 5 -c 80 beispiel.exe C:\Dumps
```

Der Befehl reagiert, wenn der Prozess die angegebene CPU-Schwelle für die festgelegte Anzahl aufeinanderfolgender Sekunden überschreitet.

Speicherabbild bei einer unbehandelten Ausnahme

```
[TEST][PRIV][FILE][SENS] procdump.exe -ma -e beispiel.exe C:\Dumps
```

Auf einen noch nicht gestarteten Prozess warten

```
[TEST][PRIV][FILE][SENS] procdump.exe -ma -e -w beispiel.exe C:\Dumps
```

Option	Bedeutung
`-ma`	vollständiges Speicherabbild
`-mm`	Mini-Dump; Standard
`-n 3`	maximal drei Abbilder erzeugen
`-s 5`	Bedingung muss fünf Sekunden bestehen
`-c 80`	CPU-Schwelle von 80 Prozent
`-h`	bei einem nicht reagierenden Fenster auslösen
`-e`	bei unbehandelter Ausnahme auslösen

Option	Bedeutung
`-e 1`	zusätzlich bei First-Chance-Ausnahmen auslösen
`-w`	auf den Start des Prozesses warten
`-t`	beim Beenden des Prozesses auslösen
`-o`	vorhandene Zieldatei überschreiben

Warum Speicherabbilder besonders geschützt werden müssen

Ein Speicherabbild kann unter anderem enthalten:

- Kennwörter oder Kennwortfragmente,
- Sitzungstoken,
- personenbezogene Daten,
- Inhalte geöffneter Dokumente,
- kryptografische Schlüssel,
- Verbindungszeichenfolgen,
- interne Servernamen,
- Anwendungsdaten.

```
[SENS][FILE] Speicherabbilder verschlüsselt ablegen, Zugriff begrenzen und nach der Analyse kontrolliert löschen.
```

Vollständige Abbilder können groß sein und während der Erstellung zusätzliche CPU-, Arbeitsspeicher- und Datenträgerlast verursachen. Auf produktiven Systemen sind Speicherplatz und mögliche Unterbrechungen vorab zu prüfen.

ProcDump kann außerdem als systemweiter Postmortem-Debugger registriert werden. Da dies die Systemkonfiguration verändert, gehört eine solche Registrierung nicht in die normale spontane Diagnose:

```
[PRIV][CHANGE] procdump.exe -ma -i C:\Dumps
```

Rücknahme:

```
[PRIV][CHANGE] procdump.exe -u
```

12. RAMMap und VMMap – Arbeitsspeicher genauer analysieren

RAMMap

RAMMap untersucht die Verwendung des physischen Arbeitsspeichers des gesamten Windows-Systems.

Wichtige Ansichten:

Ansicht	Aussage
Use Counts	Speichernutzung nach Verwendungsart
Processes	physische Speichernutzung nach Prozess
Priority Summary	Speicher nach Priorität
Physical Pages	einzelne physische Speicherseiten
Physical Ranges	physische Speicherbereiche
File Summary	im RAM befindliche Dateidaten
File Details	einzelne Dateien und Speicherseiten

RAMMap hilft bei Fragen wie:

- Warum wird sehr viel physischer Speicher verwendet?
- Wie groß ist der Dateicache?
- Welche Dateien befinden sich in der Standby-Liste?
- Wie viel Speicher wird durch Treiber oder Kernelstrukturen verwendet?
- Entspricht der hohe Speicherverbrauch tatsächlich einem einzelnen Prozess?

VMMap

VMMap untersucht den virtuellen und physischen Speicher eines einzelnen Prozesses.

VMMap zeigt unter anderem:

- privaten Speicher,
- gemeinsam genutzten Speicher,
- Images und DLLs,
- zugeordnete Dateien,
- Heap-Bereiche,
- Thread-Stacks,
- reservierte und zugesicherte Speicherbereiche.

VMMap ist besonders nützlich, wenn der Speicherverbrauch eines bestimmten Prozesses über längere Zeit zunimmt.

Beobachtung statt Momentaufnahme

Bei einem vermuteten Speicherproblem sollten mehrere Messpunkte dokumentiert werden:

Zeitpunkt	Private Bytes	Working Set	Commit	Handles	Threads
Start	...	...	...	...	...
nach 15 Minuten	...	...	...	...	...
nach Reproduktion	...	...	...	...	...
nach 60 Minuten	...	...	...	...	...

Ein hoher Wert allein beweist kein Speicherleck. Entscheidend ist, ob die Nutzung unter vergleichbaren Bedingungen dauerhaft wächst und nicht wieder freigegeben wird.

RAMMap enthält Funktionen zum Leeren bestimmter Speicherlisten. Diese verändern den Systemzustand und können Messergebnisse verfälschen:

```
[CHANGE][DISRUPT] „Empty“-Funktionen nicht während der ursprünglichen Beweissicherung verwenden.
```

13. ListDLLs – geladene DLLs eines Prozesses anzeigen

ListDLLs zeigt die von Prozessen geladenen DLLs an. Das Werkzeug kann helfen, wenn:

- eine falsche DLL-Version vermutet wird,
- eine Anwendung eine DLL aus einem unerwarteten Verzeichnis lädt,
- 32-Bit- und 64-Bit-Komponenten verwechselt werden,
- mehrere Versionen einer Bibliothek vorhanden sind,
- ein Programm nach einem Update nicht mehr startet.

DLLs eines bestimmten Prozesses anzeigen:

```
[RO] listdlls.exe beispiel.exe
```

DLLs einer bestimmten PID anzeigen:

```
[RO] listdlls.exe 4321
```

Nach Prozessen suchen, die eine bestimmte DLL geladen haben:

```
[RO] listdlls.exe beispiel.dll
```

Versionsinformationen anzeigen:

```
[RO] listdlls.exe -v beispiel.exe
```

Nicht signierte DLLs hervorheben beziehungsweise anzeigen:

```
[RO] listdlls.exe -u beispiel.exe
```

Bei der Bewertung sind mindestens folgende Punkte zu prüfen:

- vollständiger DLL-Pfad,
- Dateiversion,
- Produktversion,
- Architektur,
- digitaler Herausgeber,
- Änderungszeitpunkt,
- Übereinstimmung mit einer funktionierenden Referenzinstallation.

Eine DLL mit ungewöhnlichem Pfad ist ein Prüfhinweis, aber noch kein Beweis für Manipulation.

14. Sysmon – dauerhafte sicherheitsrelevante Ereigniserfassung

Sysmon installiert einen Windows-Systemdienst und einen Treiber. Anschließend protokolliert es abhängig von der Konfiguration detaillierte Systemereignisse, beispielsweise:

- Prozessstarts,
- Netzwerkverbindungen,
- Dateiänderungen,
- Treiber- und DLL-Ladevorgänge,
- Registry-Aktivitäten,
- DNS-Abfragen,
- Prozesszugriffe,
- WMI-Aktivitäten.

Die Ereignisse befinden sich üblicherweise unter:

```
Anwendungs- und Dienstprotokolle
└─ Microsoft
   └─ Windows
      └─ Sysmon
```

```
    └─ Operational
```

Sysmon ist kein spontanes Read-only-Diagnosewerkzeug. Installation und Konfiguration verändern das System dauerhaft:

```
[PRIV][CHANGE] sysmon64.exe -accepteula -i config.xml
```

Aktuelle Konfiguration anzeigen:

```
[RO][PRIV] sysmon64.exe -c
```

Konfiguration aktualisieren:

```
[PRIV][CHANGE] sysmon64.exe -c config.xml
```

Sysmon deinstallieren:

```
[PRIV][CHANGE][DISRUPT] sysmon64.exe -u
```

Vor einer Einführung müssen geklärt werden:

- Welche Ereignisse werden benötigt?
- Welche Daten dürfen protokolliert werden?
- Wie hoch ist das erwartete Datenvolumen?
- Wie lange werden Protokolle aufbewahrt?
- Wer darf darauf zugreifen?
- Werden Ereignisse an ein SIEM weitergeleitet?
- Wie wird die Konfiguration getestet und versioniert?
- Welche Datenschutz- und Betriebsratsvorgaben gelten?

Sysmon bewertet Ereignisse nicht selbst als gutartig oder bösartig. Die Qualität der Ergebnisse hängt wesentlich von der Konfiguration und der anschließenden Auswertung ab.

15. Praxisfall – hohe CPU-Auslastung untersuchen

Ziel: Verursachenden Prozess und möglichst den auslösenden Thread bestimmen.

1. Uhrzeit und wahrgenommene Auswirkung dokumentieren.
2. Mit Task-Manager oder Process Explorer den Prozess bestimmen.

3. CPU-Verlauf über einen angemessenen Zeitraum beobachten.
4. Prozesspfad, Benutzer, Kommandozeile und übergeordneten Prozess prüfen.
5. In Process Explorer die Prozesseigenschaften öffnen.
6. Unter `Threads` nach CPU-Auslastung sortieren.
7. Auffälligen Thread und zugehöriges Modul dokumentieren.
8. Ereignisanzeige und Anwendungsprotokolle zum selben Zeitpunkt prüfen.
9. Bei reproduzierbaren Lastspitzen kontrolliert ProcDump einsetzen.
10. Speicherabbild an Hersteller oder Entwicklung zur Analyse übergeben.

Nicht vorschnell tun:

- Prozess sofort beenden,
- Priorität ohne Begründung verändern,
- Sicherheitssoftware deaktivieren,
- wiederholt vollständige Dumps ohne Speicherplatzkontrolle erzeugen.

16. Praxisfall – Datei oder Ordner lässt sich nicht ändern, löschen oder umbenennen

Typische Meldungen

- Datei wird von einem anderen Prozess verwendet.
- Zugriff verweigert.
- Freigabeverletzung.
- Ordner kann nicht gelöscht werden.

Diagnoseablauf

1. Vollständigen Pfad dokumentieren.
2. Berechtigungen und Besitzverhältnisse prüfen.
3. Mit Process Explorer nach Dateiname oder Pfad suchen.
4. Alternativ Handle verwenden:

```
[RO][PRIV] handle.exe "C:\Daten\Projekt\bericht.xlsx"
```

5. Prozessname, PID, Benutzerkonto und Zweck identifizieren.
6. Prüfen, ob der Prozess regulär geschlossen werden kann.
7. Bei einem Dienst den zuständigen Dienst bestimmen.
8. Anwendung oder Dienst kontrolliert schließen.
9. Dateioperation erneut testen.
10. Ergebnis dokumentieren.

Ein Handle sollte nicht zwangsweise geschlossen werden, solange ein geordnetes Beenden des verantwortlichen Programms möglich ist.

17. Praxisfall – Anwendung startet nicht

Diagnoseablauf

1. Exakte Fehlermeldung und Uhrzeit dokumentieren.
2. Anwendungspfad und Version prüfen.
3. Digitale Signatur der Programmdatei prüfen:

```
[RO] sigcheck.exe -nobanner -a -h -i "C:\Programme\Beispiel\beispiel.exe"
```

4. Ereignisanzeige und anwendungseigene Protokolle prüfen.
5. Process Monitor vorbereiten.
6. Filter auf den Prozessnamen setzen.
7. Aufnahme starten und Anwendung einmal starten.
8. Aufnahme sofort stoppen.
9. Letzte Zugriffe vor dem Prozessende untersuchen.
10. Besonders auf folgende Resultate achten:

```
ACCESS DENIED
PATH NOT FOUND
NAME NOT FOUND
SHARING VIOLATION
BAD IMAGE
```

11. Geladene DLLs und deren Pfade prüfen.
12. Vergleich mit einem funktionierenden Referenzsystem durchführen.
13. Erst nach belegter Ursache Berechtigung, Pfad, Konfiguration oder Installation ändern.

Viele `NAME NOT FOUND`-Ereignisse sind Teil eines normalen Suchvorgangs. Relevant ist häufig der letzte nicht erfolgreich ersetzte Zugriff unmittelbar vor dem Abbruch.

18. Praxisfall – unbekannte Netzwerkverbindung untersuchen

1. Lokale und entfernte Adresse dokumentieren.
2. Port, Protokoll und Verbindungsstatus erfassen.
3. Prozess-ID mit TCPView oder Tcpvcon bestimmen:

```
[RO] tcpvcon.exe -a -n
```

4. Prozess-ID in Process Explorer untersuchen.

5. Dateipfad, Kommandozeile, Benutzer und übergeordneten Prozess prüfen.
6. Signatur und Hash der ausführbaren Datei erfassen.
7. DNS-Auflösung und Zielsystem kontrollieren.
8. Prüfen, ob die Verbindung zur Funktion der Anwendung passt.
9. Firewall-, Proxy- und Sicherheitsprotokolle zum selben Zeitpunkt vergleichen.
10. Bei tatsächlichem Verdacht das Incident-Response-Verfahren des Unternehmens anwenden.

Eine unbekannte externe IP-Adresse kann beispielsweise zu einem CDN, Cloudanbieter, Update-Dienst oder Sicherheitsdienst gehören. Eine Eigentümerabfrage allein beweist daher weder Zweck noch Vertrauenswürdigkeit der Verbindung.

19. Häufige Fehlinterpretationen vermeiden

Beobachtung	Falscher Schluss	Richtige Einordnung
Prozess ist unbekannt	Prozess ist Schadsoftware	Pfad, Signatur, Herausgeber, Parent und Funktion prüfen
Datei ist nicht signiert	Datei ist schädlich	Signatur ist nur ein Bewertungskriterium
Datei ist signiert	Datei ist sicher	Auch signierte Software kann unerwünscht oder verwundbar sein
Procmon zeigt `NAME NOT FOUND`	Ursache wurde gefunden	Suchvorgänge erzeugen diesen Status regelmäßig
Procmon zeigt `BUFFER OVERFLOW`	Speicherüberlauf der Anwendung	Häufig normale Ermittlung der benötigten Puffergröße
Viele TCP-Verbindungen	System ist kompromittiert	Browser, Cloud- und Kommunikationsprogramme erzeugen viele Verbindungen
Hoher RAM-Verbrauch	Arbeitsspeicher ist defekt	Cache, Commit, Working Set und Speichertypen getrennt prüfen
Hohe Handle-Anzahl	Sicheres Handle-Leak	Verlauf und Referenzwerte beobachten
VirusTotal meldet nichts	Datei ist garantiert sicher	Fehlende Erkennungen sind keine Sicherheitsgarantie
Autoruns-Eintrag ist unbekannt	Eintrag muss gelöscht werden	Zweck, Pfad und Herausgeber zunächst ermitteln
Prozess lässt sich beenden	Problem ist gelöst	Ursache kann weiterbestehen und erneut auftreten

20. Empfohlener Sysinternals-Diagnoseablauf

Phase	Vorgehen	Geeignete Werkzeuge
1. Störung aufnehmen	Fehler, Zeitpunkt und Auswirkung dokumentieren	Ticket, Screenshot, Ereignisanzeige
2. Prozess bestimmen	Prozessname, PID und Benutzer ermitteln	Process Explorer, PsList
3. Herkunft prüfen	Pfad, Parent, Kommandozeile und Signatur prüfen	Process Explorer, Sigcheck
4. Aktivität beobachten	Datei-, Registry-, Prozess- und Netzwerkzugriffe erfassen	Process Monitor, TCPView
5. Ressourcen untersuchen	CPU, Handles und Speicherentwicklung prüfen	Process Explorer, Handle, RAMMap, VMMap
6. Autostart prüfen	Startmechanismen und Anmeldeobjekte untersuchen	Autoruns
7. Fehler reproduzieren	Gefilterte, zeitlich begrenzte Aufnahme erstellen	Process Monitor
8. Beweise sichern	PML, CSV, Screenshots oder Dump geschützt speichern	Procmon, Autorunsc, ProcDump
9. Hypothese testen	Nur eine kontrollierte Änderung durchführen	abhängig von Ursache
10. Ergebnis bestätigen	Ausgangsfehler erneut testen und Nebenwirkungen prüfen	gleiche Messmethode
11. Dokumentieren	Ursache, Änderung, Ergebnis und Rückweg festhalten	BookStack, Ticketsystem

Merksatz

> Erst beobachten, dann zuordnen, anschließend vergleichen und erst danach verändern.

21. Kompakte Befehlsübersicht

Aufgabe	Befehl	Kennzeichnung
Signatur mit PowerShell prüfen	`Get-AuthenticodeSignature "C:\Pfad\Datei.exe"`	[RO]
SHA-256-Hash berechnen	`Get-FileHash "C:\Pfad\Datei.exe" -Algorithm SHA256`	[RO]
Alle Autostarts anzeigen	`autorunsc.exe -a * -s`	[RO][PRIV]

Aufgabe	Befehl	Kennzeichnung
Autostarts als CSV speichern	`autorunsc.exe -a * -s -c > C:\Temp\autoruns.csv`	[RO][PRIV][FILE]
Alle Netzwerkendpunkte anzeigen	`tcpvcon.exe -a -n`	[RO]
Endpunkte als CSV speichern	`tcpvcon.exe -a -n -c > C:\Temp\tcp.csv`	[RO][FILE]
Dateiinhaber suchen	`handle.exe bericht.xlsx`	[RO][PRIV]
Handles eines Prozesses anzeigen	`handle.exe -p 4321`	[RO][PRIV]
Dateisignatur und Hash prüfen	`sigcheck.exe -nobanner -a -h -i Datei.exe`	[RO]
Nicht signierte System32-Dateien suchen	`sigcheck.exe -nobanner -u -e C:\Windows\System32`	[RO][PRIV]
Prozessliste anzeigen	`pslist.exe`	[RO]
Prozessbaum anzeigen	`pslist.exe -t`	[RO]
DLLs eines Prozesses anzeigen	`listdlls.exe 4321`	[RO]
vollständiges Prozessabbild erzeugen	`procdump.exe -ma 4321 C:\Dumps`	[TEST][PRIV][FILE][SENS]
Dump bei nicht reagierendem Fenster	`procdump.exe -ma -h beispiel.exe C:\Dumps`	[TEST][PRIV][FILE][SENS]
Sysmon-Konfiguration anzeigen	`sysmon64.exe -c`	[RO][PRIV]
Handle zwangsweise schließen	`handle.exe -c 7C -p 4321`	[PRIV][CHANGE][DISRUPT]
Prozess zwangsweise beenden	`pskill.exe 4321`	[CHANGE][DISRUPT]

22. Dokumentationsvorlage für eine Sysinternals-Analyse

Ticketnummer:

Analysedatum:

Administrator:

Betroffener Computer:

Betriebssystem:

Angemeldeter Benutzer:

Fehlerbeginn:

Fehlerbeschreibung:

Auswirkung:

Betroffener Prozess:

Prozess-ID:

Programmdatei:

Dateiversion:

Benutzerkonto:

Übergeordneter Prozess:

Kommandozeile:

Digitale Signatur:

SHA-256:

Verwendete Sysinternals-Werkzeuge:

Werkzeugversionen:

Verwendete Filter:

Aufnahmezeitraum:

Beobachtungen:

-

-

-

Ermittelte Auffälligkeiten:

-

-

-

Arbeitshypothese:

Beleg für die Hypothese:

Durchgeführter Test:

Testergebnis:

Durchgeführte Änderung:

Rückweg:

Abschlussprüfung:

Erzeugte Dateien:

- PML:

- CSV:

- Speicherabbild:

- Screenshots:

Speicherort:

Zugriffsberechtigung:

Lösch- oder Aufbewahrungsfrist:

23. Offizielle Quellen und weiterführende Dokumentation

- Microsoft Sysinternals – Übersicht
- Sysinternals Suite
- Process Explorer
- Process Monitor
- Autoruns und Autorunsc
- TCPView und Tcpvcon
- Handle
- Sigcheck
- PsTools
- PsList
- ProcDump
- RAMMap
- VMMap
- ListDLLs
- Sysmon

> Da Microsoft die Sysinternals-Werkzeuge regelmäßig aktualisiert, sollte vor dem produktiven Einsatz immer die aktuelle offizielle Dokumentation der verwendeten Version geprüft werden.