Wie Sie Ihre Windows-Umgebung für die Forensik vorbereiten: Ein praktischer Leitfaden

Windows Event Log Size

Heben Sie die Dateigrössen der Logdateien an, um eine Überschreibung von wichtigen Daten zu verhindern.

```
Pfad: Computer
Configuration\Policies\Administrative
Templates\Windows Components\Event Log
Service\Application\
Pfad: Computer
Configuration\Policies\Administrative
Templates\Windows Components\Event Log
Service\Security\
Pfad: Computer
Configuration\Policies\Administrative
Templates\Windows Components\Event Log
Service\Setup\
Pfad: Computer
Configuration\Policies\Administrative
Templates\Windows Components\Event Log
Service\System\
Einzustellen: Application, Setup and System:
>=100 MB, Security: >=2 GB
```

Windows Event forwarding

Senden Sie Logdateien an einen zentralen Logserver weiter, um diese dort zu speichern und Korrelationen zu erkennen.

```
Pfad: Computer
Configuration\Policies\Administrative
Templates\Windows Components\Event
Forwarding\
Einzustellen: Die URL des Windows Collector
```

PowerShell Auditing

Erweitern Sie die Aufnahme Ihrer Logdateien, um die ausgeführten PowerShell Kommandos, Scripts und Konsolensitzung aufzunehmen.

Module Logging
Aufzeichnen vom Output eines Moduls.

```
Pfad: Administrative Templates\Windows
Components\Windows PowerShell
Einzustellen: Enable
```

Script Block Logging
Aufzeichnen von ausgeführten Scripts.

```
Pfad: Administrative Templates\Windows
Components\Windows PowerShell
Einzustellen: Enable
```

Transcription
Aufzeichnen von PowerShell Sessions.

```
Pfad: Administrative Templates\Windows
Components\Windows PowerShell
Einzustellen: Enable
```

Prefetch Files

Stellen Sie sicher, dass auf Client und Server Prefetch Dateien geschrieben werden, um Metadaten über die Ausführung von Programmen sicherzustellen.

```
Pfad: KEY_LOCAL_MACHINE\SYSTEM\
CurrentControlSet\Control\Session
Manager\Memory Management\PrefetchParameters
REG_DWORD "EnablePrefetcher" auf 3 setzen
Einzustellen: 3 auf Client und Server
```

Command Line Process Auditing

Erweitern Sie die Aufnahme, um die Logdateien von «*Process tracking*» zusätzlich mit dem ausgeführten Kommandozeilenbefehl zu erweitern.

```
Pfad: Computer Configuration\Administrative
Templates\System\Audit Process Creation
Einzustellen: Enable
Abhängikeit: «Process tracking» muss
aktiviert sein
```

Basic security audit policies

Erweitern Sie die Aufnahme Ihrer Logdateien, um mehr Beweismittel zu generieren.

Account logon events
Aufzeichnung von An- und Abmeldung von Benutzer, die an einem anderen System stattfindet.

```
Pfad: Computer Configuration\Windows
Settings\Security Settings\Local
Policies\Audit Policy
Einzustellen: Success and Failure
```

Account management
Aufzeichnung von Benutzerverwaltung.

```
Pfad: Computer Configuration\Windows
Settings\Security Settings\Local
Policies\Audit Policy
Einzustellen: Success auf Domänenkontroller
und Memberserver
```

Logon events
Aufzeichnung von An- und Abmeldung von Benutzer am eigenen System.

```
Pfad: Computer Configuration\Windows
Settings\Security Settings\Local
Policies\Audit Policy
Einzustellen: Success and Failure
```

Object Access
Aufzeichnung von Zugriff auf Objekte wie Dateien, Ordner, Registryschlüssel, Drucker, etc.

```
Pfad: Computer Configuration\Windows
Settings\Security Settings\Local
Policies\Audit Policy
Einzustellen: Success
```

Policy change
Aufzeichnung von Änderungen an Richtlinien.

```
Pfad: Computer Configuration\Windows
Settings\Security Settings\Local
Policies\Audit Policy
Einzustellen: Success auf Domänenkontroller
und Memberserver.
```

Privilege use
Aufzeichnung von Ausübung von Benutzerrechten.

```
Pfad: Computer Configuration\Windows
Settings\Security Settings\Local
Policies\Audit Policy
Einzustellen: Success
```

Process tracking
Aufzeichnung von detaillierten Informationen über die Erstellung und Beendung von Prozessen.

```
Pfad: Computer Configuration\Windows
Settings\Security Settings\Local
Policies\Audit Policy
Einzustellen: Success
```