

# DFIR -

## Digital Forensics & Incident Response

TEMS SECURITY SERVICES



**Work smarter  
Not harder**



# whoami



## Michael Meixner, CISSP

- Certified IT-Witness
- Managing Director of Computerforensic & more since 2013
- Managing Director of Tems Security Services since 2022
- Penetration Tester (White Hat)
- Threat Hunting Services
- Incident Response Services
- Computerforensic Services
- eDiscovery Expert
- IT-Security Strategy Consulting Services
- Lector for IT-Security (Technikum Vienna)

# My comparison in Incident Response





# Before and during IR

- **Before:**
  - Documentation (network, segments, server list, software list).
  - SIEM (would be helpful)
- **During IR:**
  - Keep calm
  - Get an overview
  - Disconnect Internet
  - Isolate IT Systems as best as possible
  - AD Check (Do I still have access?)
  - Storage check (Do I still have access and am I missing disks?)
  - Virtualization (Do I still have access and am I missing servers?)



# Standards for IR

## **NIST Incident Response Steps**

- Step #1: Preparation
- Step #2: Detection and Analysis
- Step #3: Containment, Eradication and Recovery
- Step #4: Post-Incident Activity

## **SANS Incident Response Steps**

- Step #1: Preparation
- Step #2: Identification
- Step #3: Containment
- Step #4: Eradication
- Step #5: Recovery
- Step #6: Lessons Learned





# From the field



- **Stay calm and professional**  
(Job is done in case of IR by the Hacker Team. Mostly the Hacker is already disconnected)
- **Designated document writer**
  - Collect and record all events, track activities
- **Define communication channel to the IR Team**  
(phone, messages, documents)
- **Define IR Leader**
  - Shutdown Remote Access
  - Check Backup System Status
  - Check File Server Status
  - Check ERP System Status
  - Check AV-Server Status
  - Export AD with last password changes
- **At least two IR-Teams**
  - Team 1: Check if the hacker is still in the network and collect IOC's, preserve evidence, find the initial vector
  - Team 2: Check and document damage, check running systems, check backup
- **Big questions to discuss with IT-Team and IR-Team:**
  - Should AD be reinstalled from scratch?
  - How long was the hacker in the system/network?
  - What was the initial vector?
  - Communication with the MGMT



*IOC = indicator of compromise , ERP = Enterprise resource planning, AD = Active Directory, AV = Anti Virus*



# From the field



- Everyone from the IR should have reading access to at least the following IOC at any time and (IR - Message of the Day):
  - Affected systems (*confirmed*)
  - Files of Interest (*confirmed*)
  - Accessed and taken data (*confirmed*)
  - Significant attacker activities (*confirmed*)
  - Verified and proven IOC (*confirmed*)
  - Compromised accounts (*confirmed*)
  - *Lateral movement map (confirmed)*









## Useful artifacts

Running Processes	Running Services	Executable Hashes	Installed Applications	Local and Domain Users	Listening Ports and Associated Services
Domain Name System (DNS) Resolution Settings and Static Routes	Established and Recent Network Connections	Run Key and other AutoRun Persistence	Scheduled tasks and cron jobs	Artifacts of past execution (e.g., Prefetch and Shimcache)	Event logs
Group policy and WMI artifacts	Anti-Virus detections	Binaries in temporary storage locations	Remote access credentials	Network connection telemetry (e.g., netflow, firewall permits)	DNS traffic and activity
Remote access activity including Remote Desktop Protocol (RDP, SSH)	virtual private network (VPN)	virtual network computing (VNC) and other remote access tools	Uniform Resource Identifier (URI) strings, and proxy enforcement actions	Web Traffic (HTTP/HTTPS)	User agent strings

<https://Any.run>

<https://VirusTotal.com>

X-Ways

Memory Dump

<https://hybrid-analysis.com>

Security Onion

Cuckoo

CYLR

EvtxECmd.exe

dtSerach

## Set of Tools for IR

Notepad++

Excel

<https://otx.alienvault.com>

Wireshark

NetFlow

volatility

WinWord

<https://gchq.github.io/CyberChef/>

Elastic Stack

NUIX

EnCase

Axiom (IEF)

p0f

Regripper

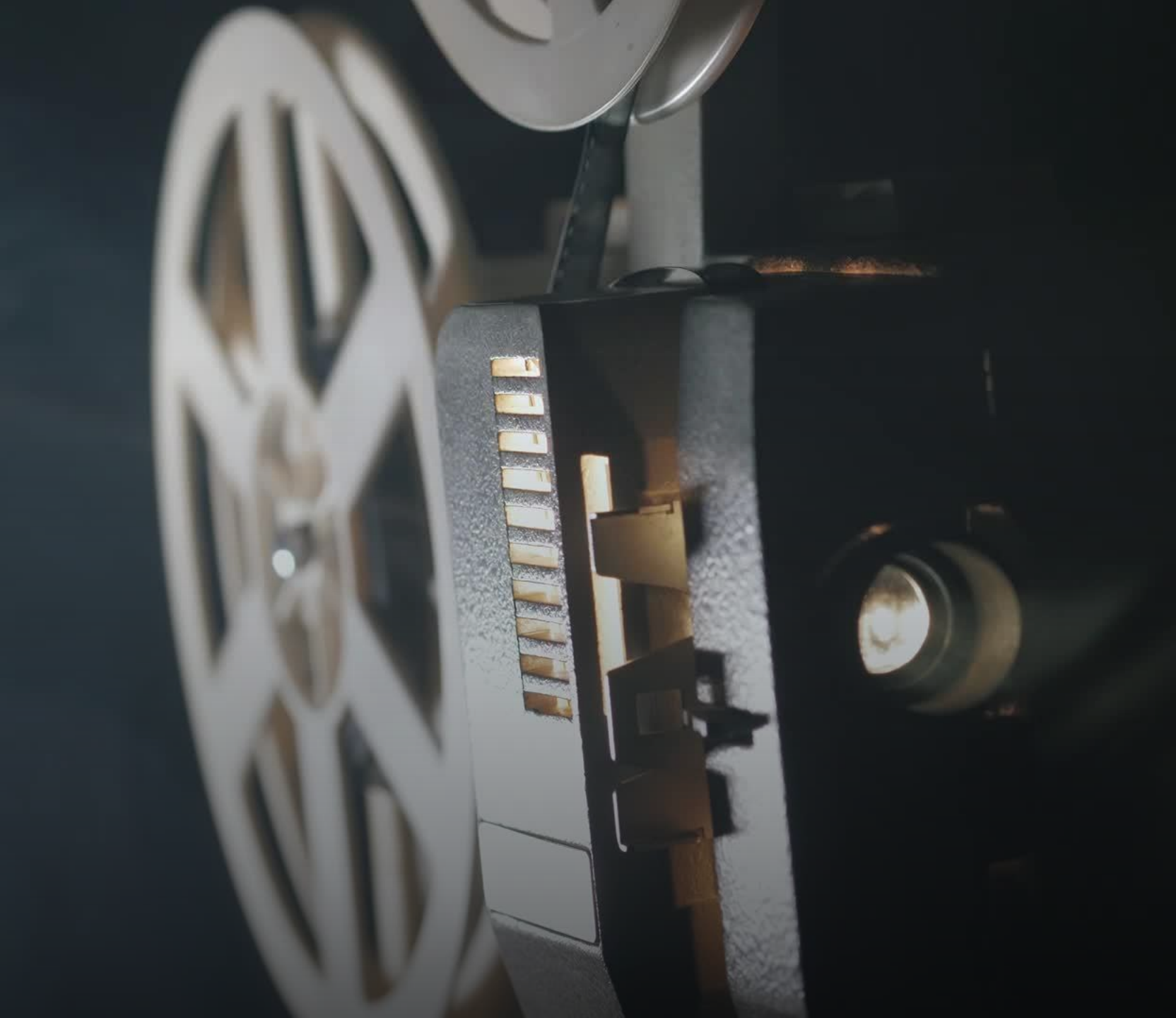
---

**HINT: Keep it simple and use only tools which you have known before**

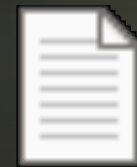
*Internet resource*

Commercial Software





From an investigation in Summer 2022 I found on a victim's machine the following script



Hacker-Script.txt

# How to make it harder for the attacker

*State of the art administration*

Protect Backup  
Solution

Proper Client  
Patch  
Management

Recurring change  
of service account  
password



# Past Incidents



# Cases

---

- Big Austrian Company > 5000 Employees
- Big Austrian Company > 1000 Employees
- Small Company 50 – 100 Employees
- Small Company < 20 Employees

**7 out of 12**

**5 out of 12**

**4 out of 12**

**4 out of 12**





# Rules of the game



- The hacker needs **only one vulnerability or misconfiguration** and the hacker has access to a company network.
- A company can catch the hacker **only through command or lateral movement** within the network, and we are able to detect the hacker.

**Training and knowledge are the key factor for success**

Know  
your  
limit


Work smarter  
Not harder



Source: Internet


Get in contact with us

Philip Berger  
Managing Director

 +43(664) 343 8644

 [Philip.berger@tems-security.at](mailto:Philip.berger@tems-security.at)

Michael Meixner, CISSP  
Managing Director

 +43(664) 1453328

 [Michael.meixner@tems-security.at](mailto:Michael.meixner@tems-security.at)