AON

Keep the F in DFIR

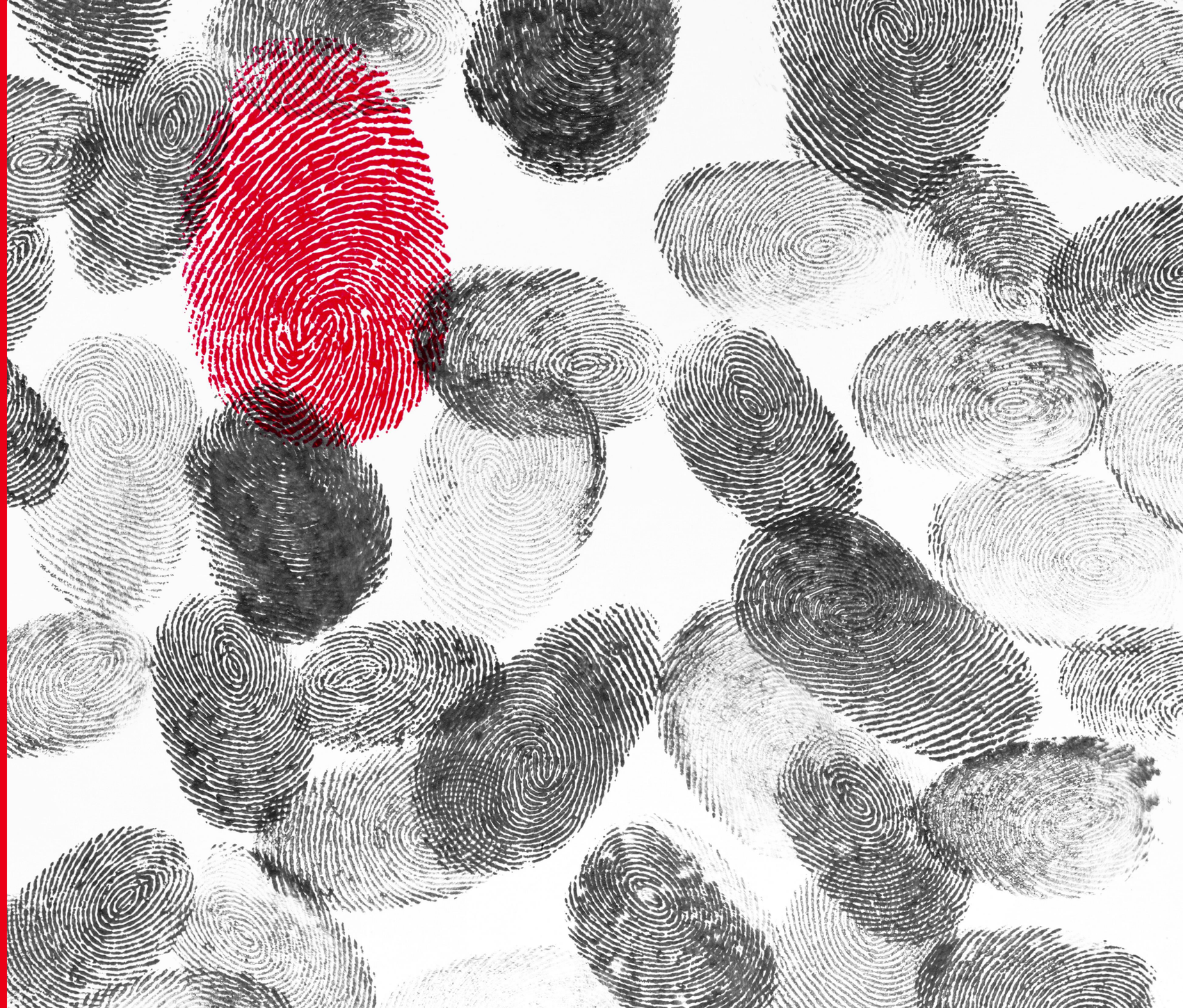
Importance of Digital Forensics in Incident Response

August 27, 2023

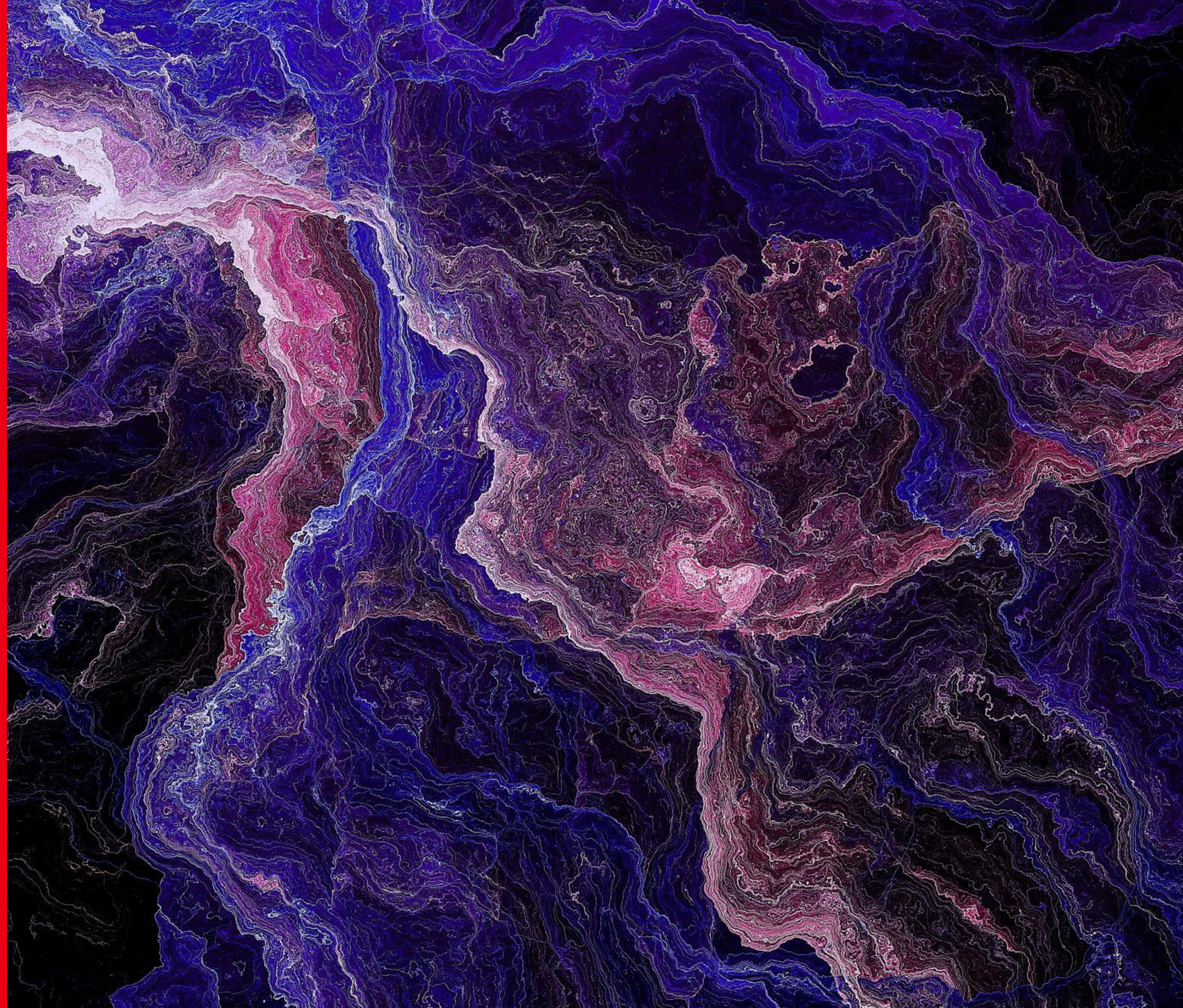
Presented By:

Partha Alwar and Carly Battaile

Stroz Friedberg DFIR Services



Introduction

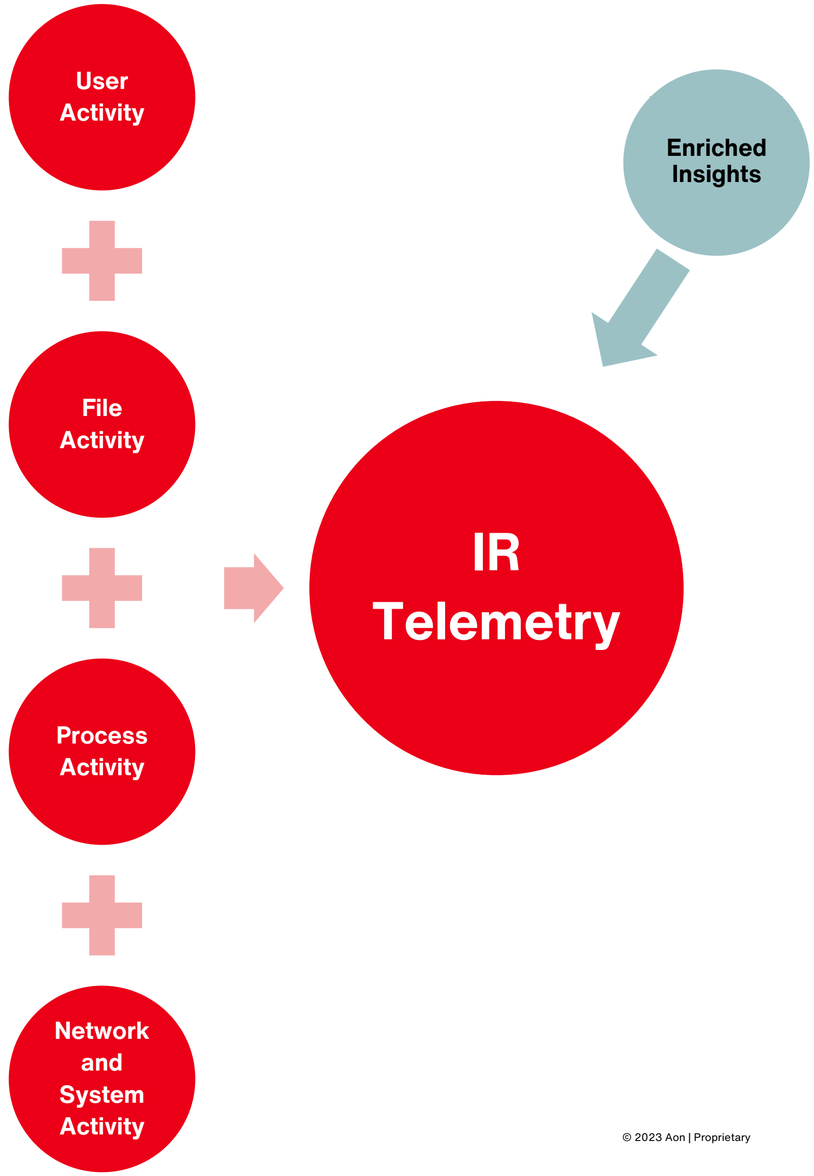


Importance of Visibility in Incident Response

Data is King

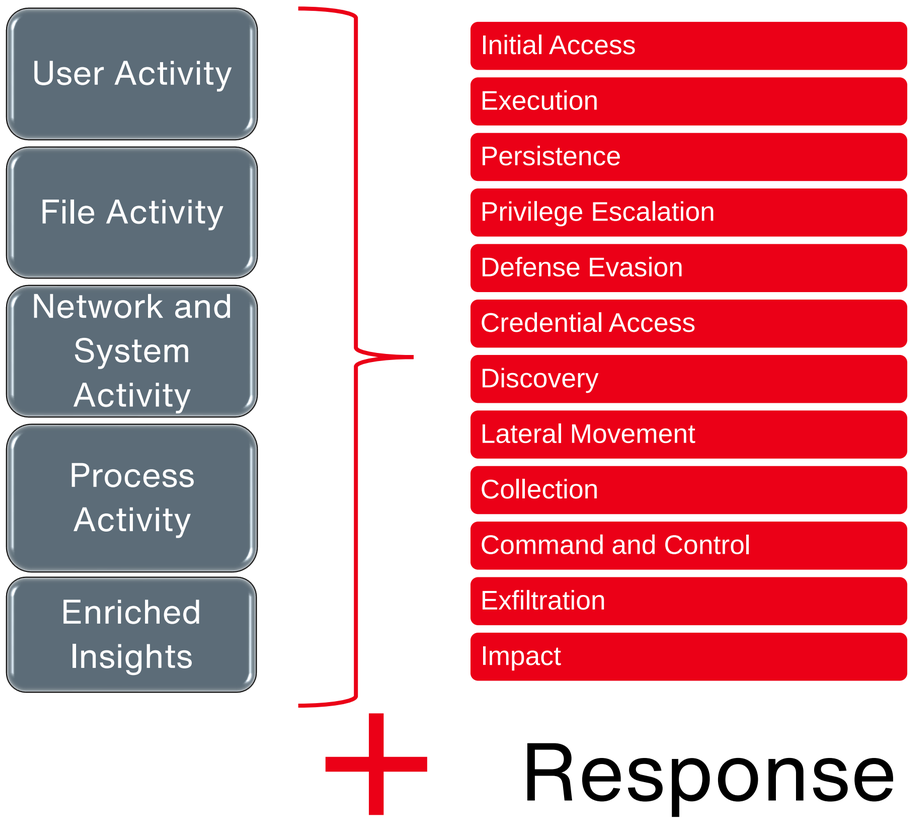
- **Raw Data**
  - **User Activity**: User login, User logoff, User sessions
  - **File Activity**: File creations, File deletions, File modifications, File Hashes
  - **Process Activity**: Process creations, terminations, parent-child spawns
  - **Network and System Activity**: Ingress/Egress traffic, DNS lookups, system-level logging

- **Enriched Insights**
  - MITRE TTP lookups
  - Intelligence lookups
  - IP lookups
  - Command patterns



Enter EDRs!

- **EDR Telemetry is hugely beneficial in IR**
  - Data ∝ Insights
  - ↑ Data → ↑ Insights → ↑ Confidence



EDR is going to solve all our security issues, right?

EDR alerted us to someone trying to dump credentials

Why didn’t the EDR prevent this attack?

We’ve issued a block for known IOCs in our EDR

Sorry, the retention in our EDR is only 14 days.

Without EDRs, we would not have caught this attack this early.

We only have 1 person to man the EDR. Can you train them?

We were able to figure out data exfiltration in our EDRs

EDR is detecting all our legitimate files. So, we disabled blocking.

We got all these alerts in our EDR, but don’t know what they mean. So, we called you.

We installed EDR on only user endpoints and some servers. DCs don’t have EDR installed.

AON

Dark side of ~~the~~ ~~Moon~~ EDRs

- High Signal-to-Noise Ratio
- Non-responsive agents
- OS Compatibility
- Compatibility with evolving technologies
- EDR Configuration
- Threat actor interactive activity
- Data retention

VISIBILITY

AON

Agenda

What to expect from this talk

Current Landscape of EDRs

Where do we stand today with EDRs?

Dark Side of ~~the Moon~~ EDRs

What gaps in visibility do EDRs have?

Forensics to the rescue

How can forensics help fill in the gaps?

AON

EDR Landscape

What is an EDR?

Endpoint Detection and Response

COLLECT: Process activity, network activity, file activity, user activity etc.

ALERT: Based on pre-built rules and known IOCs, notify users on suspicious activity

BLOCK: Based on known IOCs, rules and command patterns, automatically block process activity

INVESTIGATE: Conduit for investigating threats based on data collected by EDR

Common EDRs*

- Carbon Black
- Crowdstrike Falcon
- SentinelOne
- Windows Defender for Endpoints

***Some products are also branded as XDR for “extended detection and response”.**

Usage of EDR

Proactive and Reactive uses

Baselining

- What does normal look like in my network?

Rogue Apps

- Are employees using unauthorized apps or sites?

Threat Hunts

- Proactive hunts to identify new and evolving threats

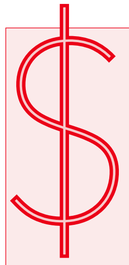
Incident Response

- Active response to an incident

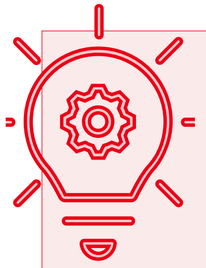
AON

Considerations

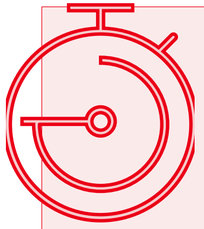
What is the difference between these tools?



Cost

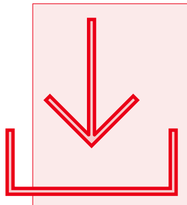


Features



Historical Lookback

Queryability



Data Retention

OS Compatibility

Handling EDR Data

What are the considerations for managing EDR data?

Configuration

- What rules should we enable?
- What exemptions should we enable?
- Who should have access?

Volume

- How do we search through this data?
- Is threat hunting part of our process or do we rely on alerting?

Retention

- How long is the data retained?
- Can we pay for increased retention?
- Can we detect events fast enough to respond within the retention period?

Centralization

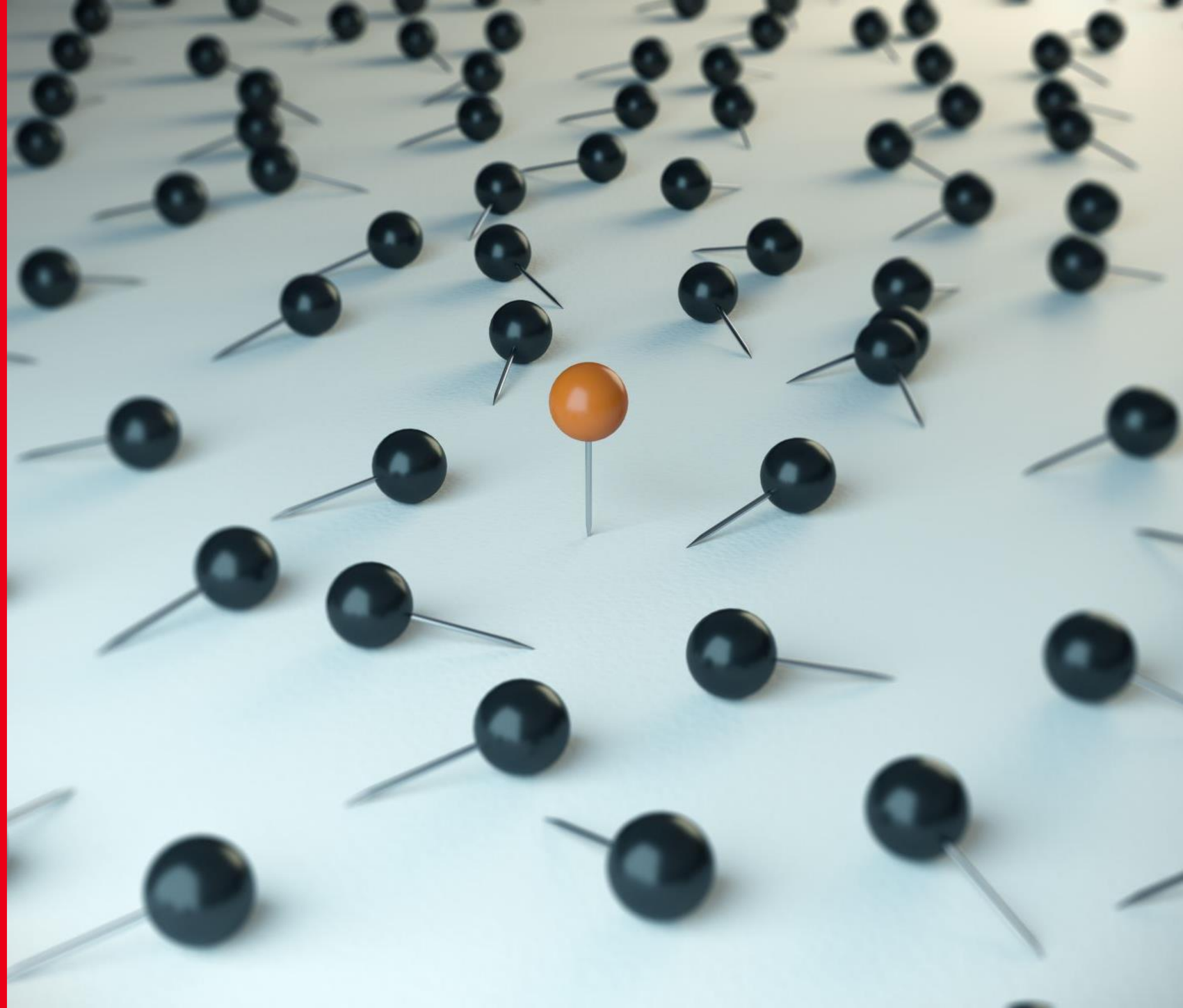
- Do we send EDR data to a SIEM?
- Is this EDR compatible with our SIEM platform?
- How much storage do we need?
- Can we query all this data?

AON

AON

Challenges with EDRs

- Scope of Deployment
- Human factors
- Threat actor interaction



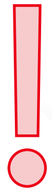
Deployment

How do you deploy agents across the network?

Some organizations may not deploy EDR to every system on the network. Exceptions may include...

Critical Systems

Temporary Systems



Downtime Considerations

Package Management Issues

Unsupported OS/ Appliances

Unresponsive Sensors

Staffing and Management

A team's response can limit an EDR's effectiveness

Trust in tooling

- "EDR will catch everything"
- Overreliance on alerts
- Never checking console or low-severity alerts

Large volume of data

- Teams may not be able to effectively investigate
- Querying speed and narrowing down data

Misconfiguration

- Allowing broad folders via allow list/exclusion
- Configure to alert only and not block
- Not enabling MFA
- Enabling bypass mode

If that wasn’t enough....

Threat actors can make things worse

Threat Actor Interference

How will bad actors try to defeat EDR?

Abuse of Exclusions

- Placing malware in paths that are commonly allowed

Safe Mode

- EDR may not run in safe mode

We have a blog about this! →

Uninstall EDRs

- Utilize vulnerable kernel drivers to terminate security tools

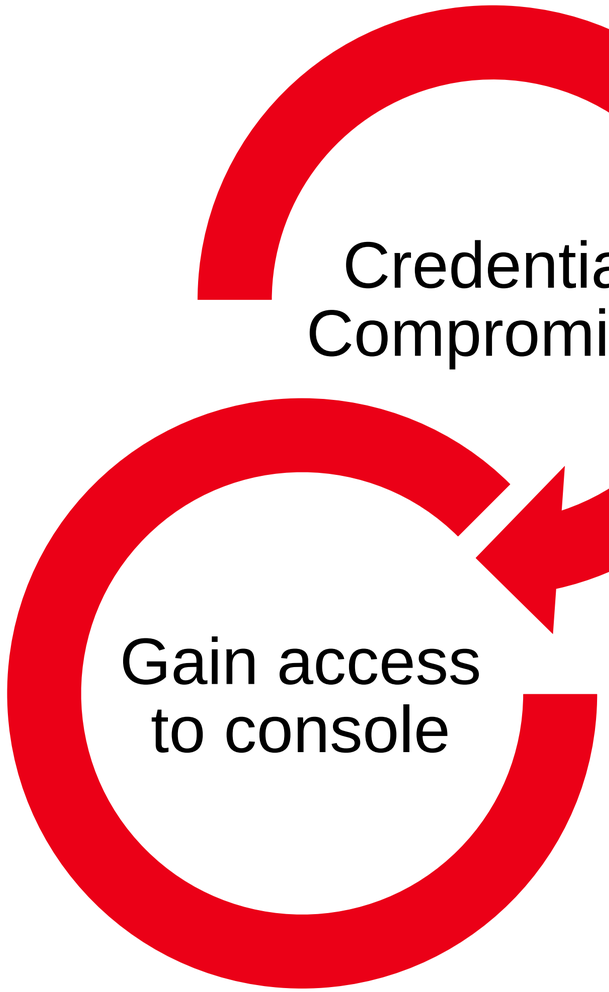
Console Access

- Lots of opportunity for further actions…

AON

Compromised EDR Console

Yikes



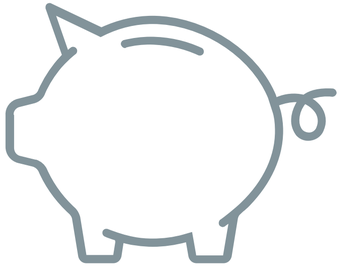
- Email compromise -> Password reset
- Password manager compromise
- Web credential theft

- Policy reconnaissance
- Modifying policies
- Limited shell functionality
- Push out malware/tooling

How does this look in real-life?

Recurring Ransomware

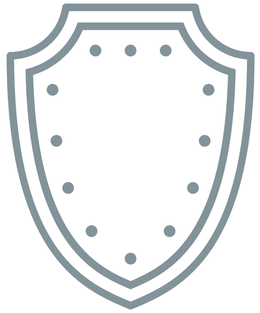
Background



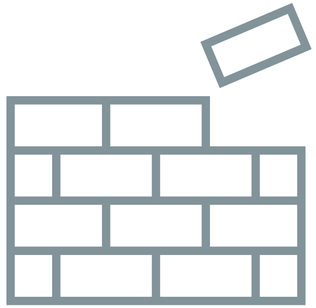
Healthy security budget

Third party manages part of environment

Experienced ransomware in the first half of the year



Deployed top-tier EDR after RW incident



Continued to experience large-scale intrusions in the second half of the year

Recurring Ransomware

Critical system deployment

Common disk-level encryption attack pattern exhibited:

No EDR on ESXI server

+

Individual hosts had EDR, but hypervisor did not

+

Threat actor gained access to ESXi

=

Encrypted VMDKs

Recurring Ransomware

Environment managed by third party

Third-party management of systems may be necessary

- **More machines than staffing allows**
- **Team focused on operations, not security**

In this case, this introduced many issues:

Separate tooling

Internal team didn't have insight into these systems

Requests for data or changes took time, went through regular ticketing process

Recurring Ransomware

Threat actor access to EDR

User had write access to EDR → Threat actor gained user's credentials → MFA not set up on account

↓

Threat actor accessed console → Threat actor removed policy blocking malware → If not immediately caught, threat actor could have done more...

Conduct recon

Push out malware

And more...

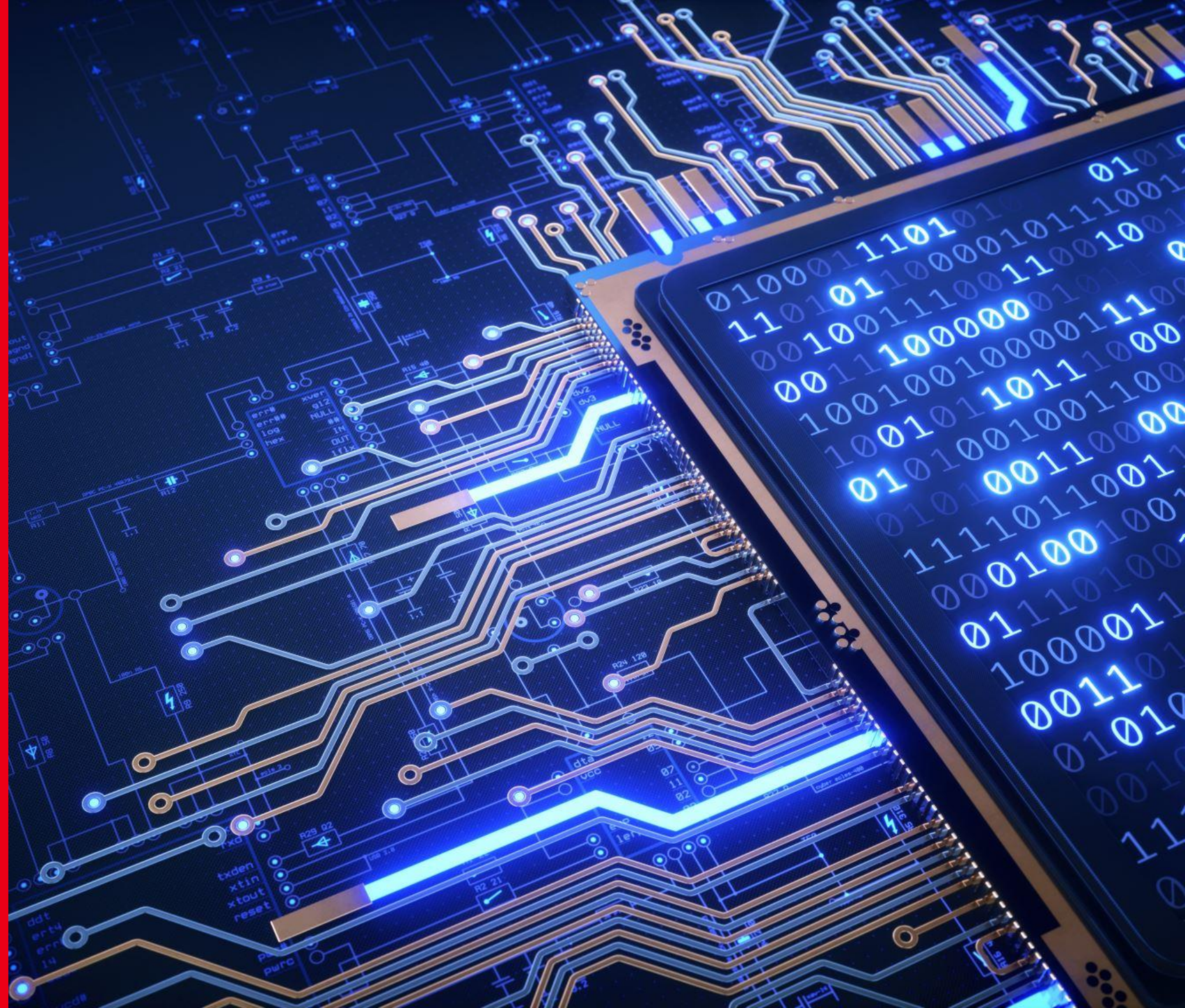
Enforce MFA on your EDR console.

Keep your list of users with EDR access to a minimum.

Your EDR console is one of the places you REALLY don't want your threat actors to be!

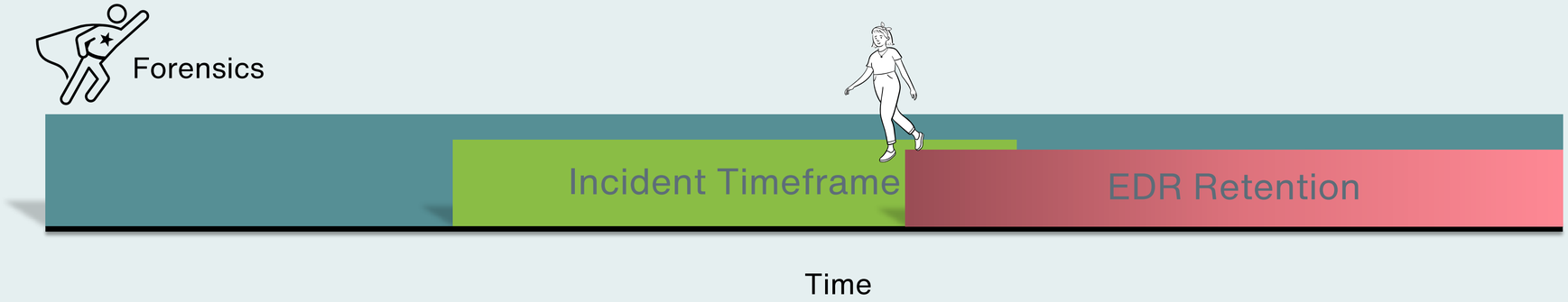
AON

Importance of Forensics in IR



You’re in the middle of an IR

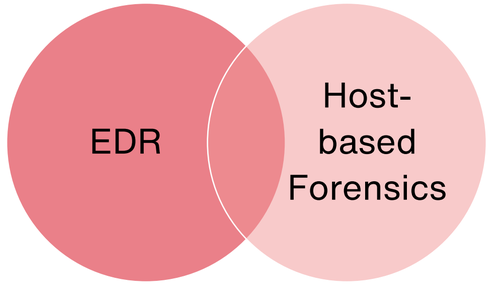
You have an awesome EDR, but you realize that there are gaps



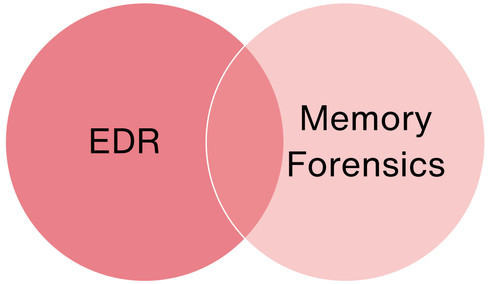
How can forensics help?

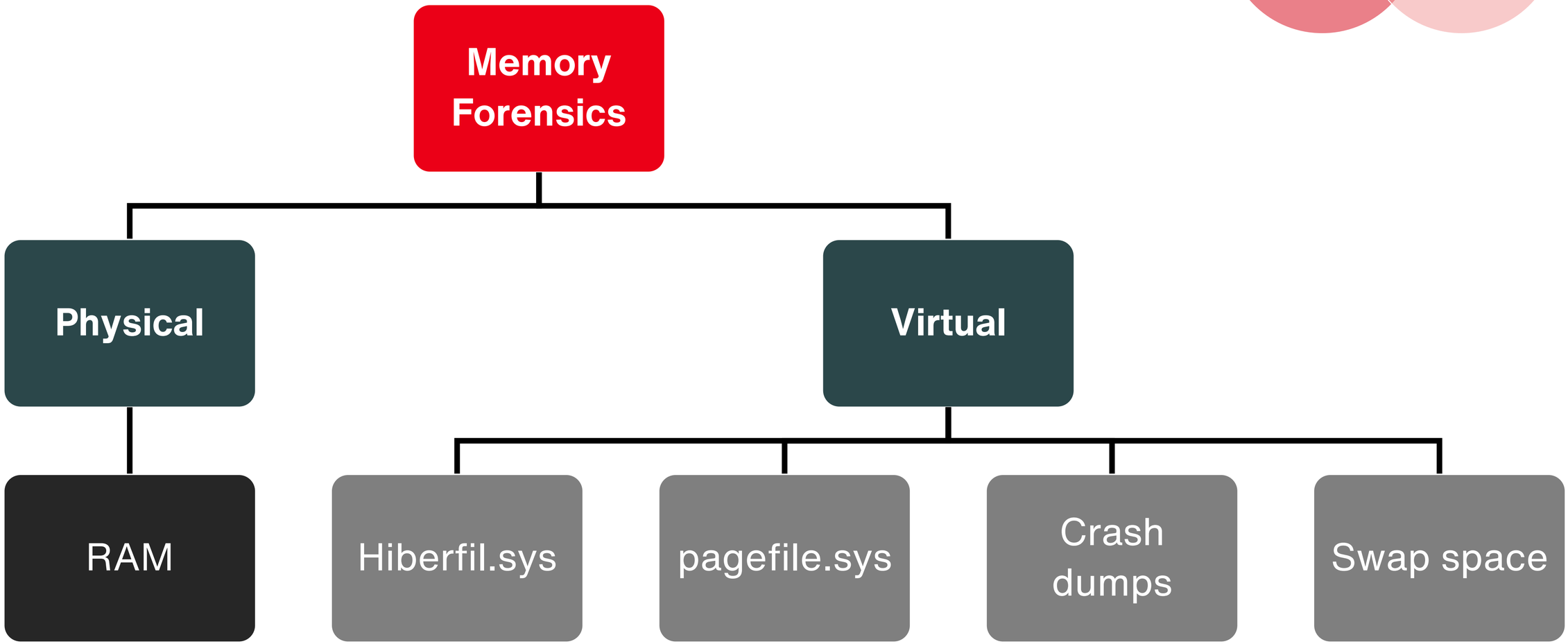
Dead-box forensics + Live Forensics

Process Activity	▪ Process creations, hash values, timestamps, dependencies, user information
File Activity	▪ File MACBs, File deletions, File recovery, File Owners, Folder Interactions, File Permissions
Network and System Activity	▪ Incoming/outgoing connections, DNS activity, USB activity, Remoting activity
User Activity	▪ User creations, account deletions, user login/logoff



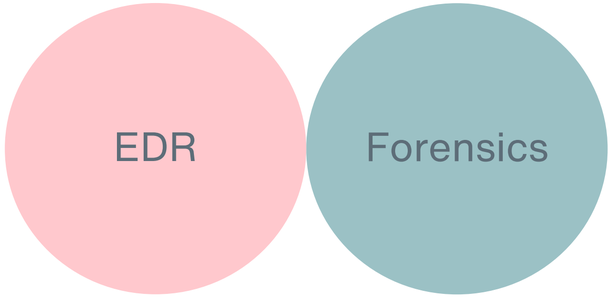
Memory Forensics

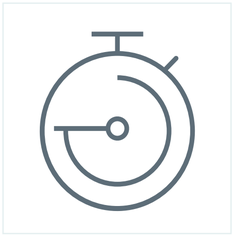




The Forensic Differentiator

Forensics over EDRs



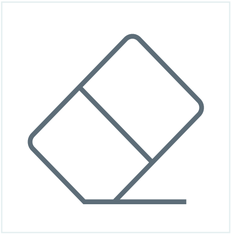


Historical activity

- Data from forensic artifacts typically go back years

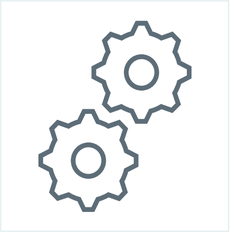
Interactive activity

- File/Folder Browsing



File recovery

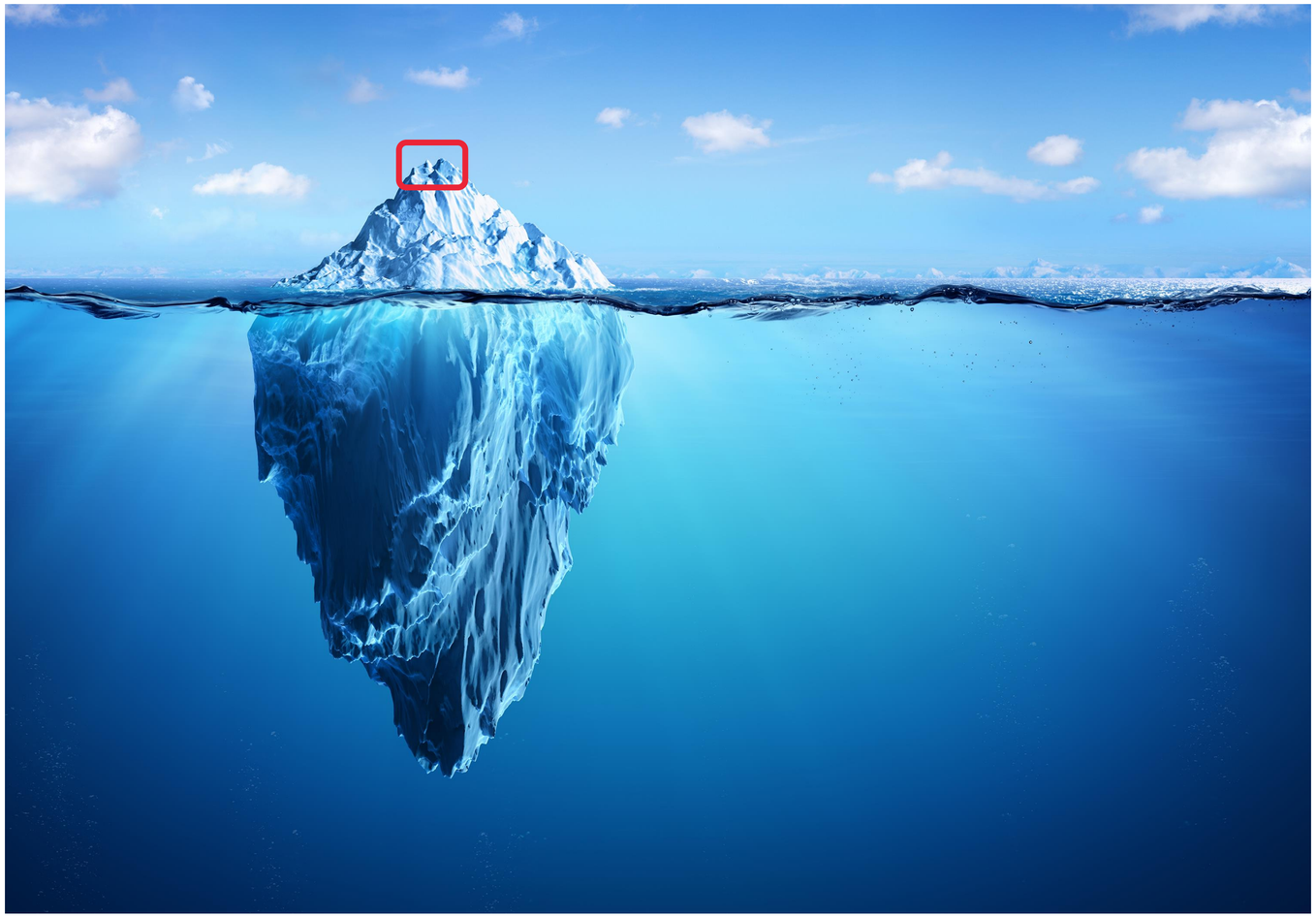
- Recovery of deleted files



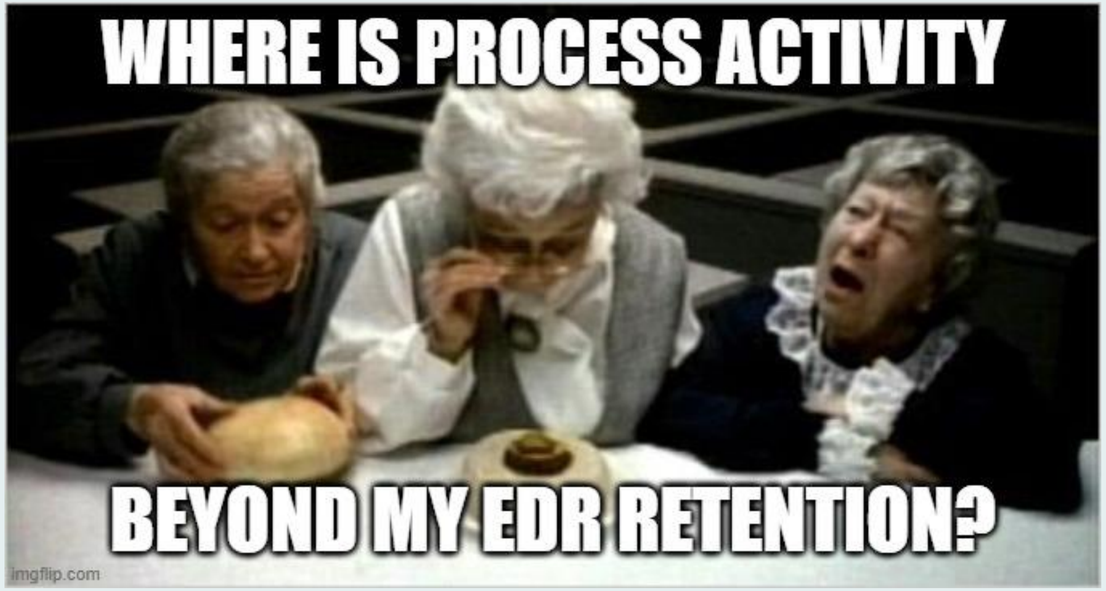
Application-specific activity

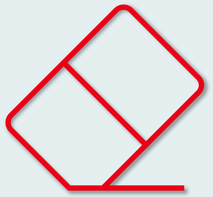
- Recovery of application settings
- E.g: What's the public fingerprint of an SSH connection?

Digital Forensics is vast!



Process Activity





Erasure of data due to retention

Non-responsive sensors

Execution from inside a VM

AON

Process Execution

Artifacts with ***Years*** of Retention

What artifact?	What does it track?	How does it help in IR?
Amcache	• **Execution time** • Full Path • File **Metadata** (Publisher, Company, Product, Size, etc.) • MAC timestamps, **SHA-1 hash**	• Program executions across several years • Great artifact for gathering additional IOCs • Metadata can reveal renamed binaries
Prefetch	• **Full path** • Number of executions • Timestamp of execution • **Files/volumes accessed** by application	• Program executions across several years • Execution count • Files used by executing application
Syscache	• SHA-1 hash • **Parent File** SHA-1 hash • MFT/Journal details • Owner	• Program executions across several years • Parent-child relationships

AON

There’s so much more...

Shimcache

LNK Files

SRUM

User Assist

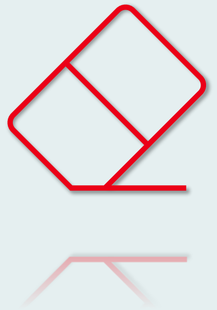
MRU

Jumplists

Windows event logs

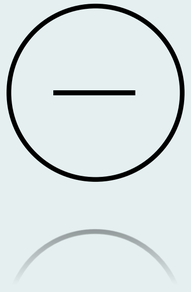
WMI CIM

File/Folder Activity



File deletion by the threat actor

Non-responsive sensors



Removal of EDR software

File MACB and Deletion Activity

$MFT, $UsnJrnl:$J, $I30 and VSS

Where?	What does it track?	How does it help in IR?
$MFT	Full path, size**,** MACB timestamps**, Owner, Permissions**	• Does this file exist on disk? If yes, when was it created? And, who owns it?
$UsnJrnl:$J	**Type of file modifications**, Timestamp of operation, Full path	• Did this file exist at some point on disk? • If yes, when was it created, deleted/modified?
$I30	Full path of **deleted file**, size, all associated MACB timestamps	• Did a file exist in this directory at some point?
Volume Shadow Copies	Stores **backups** of files	• File recovery • Log recovery

AON

Interactive Activity

What if we want to track file/folder interaction by the threat actor?

File/Folder Interaction

Shellbags

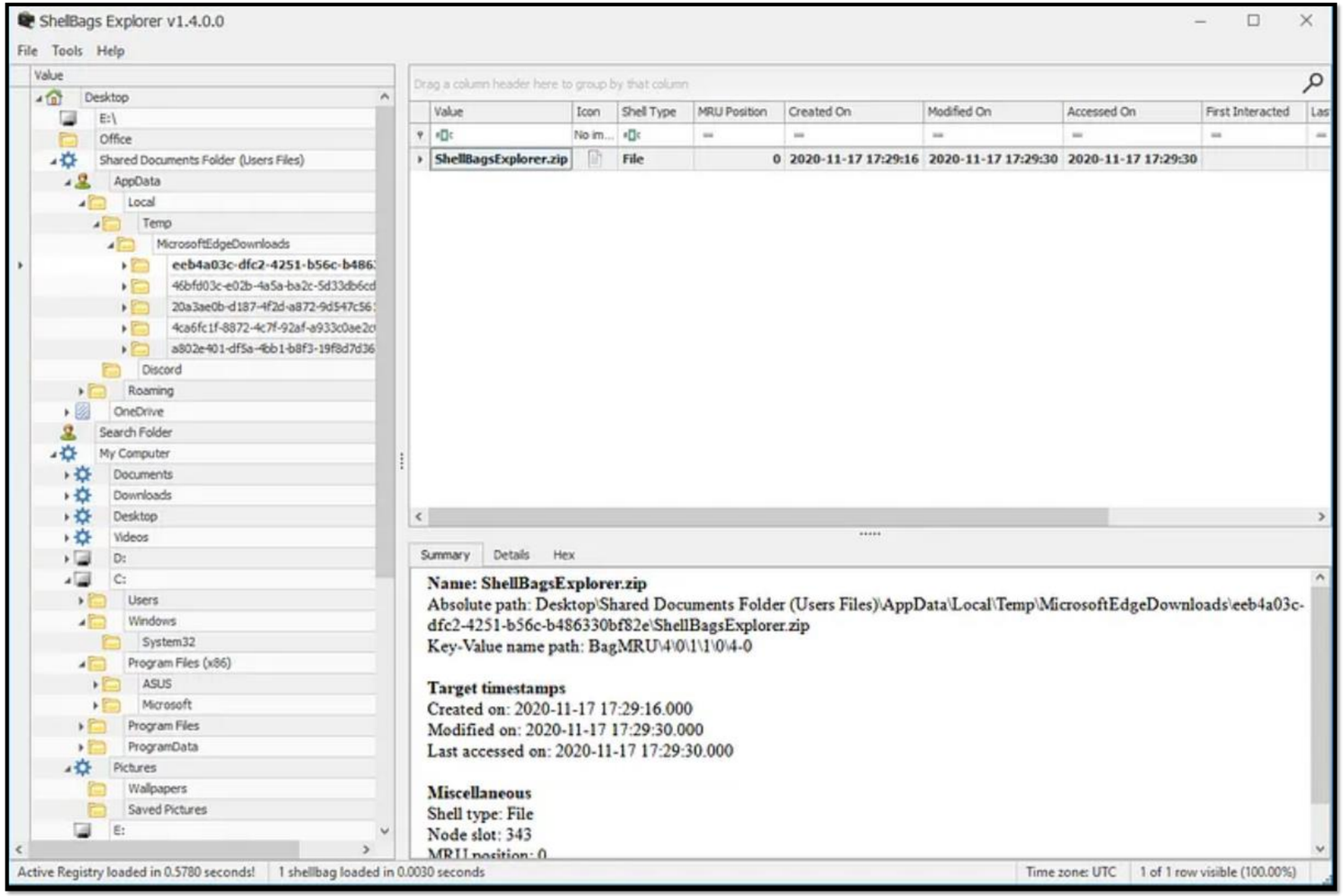
Registry objects – track display of folders on a Windows system

- NTUSER.DAT and UsrClass.DAT

Information that can be recovered:

- Full path
- User
- Timestamps of interaction

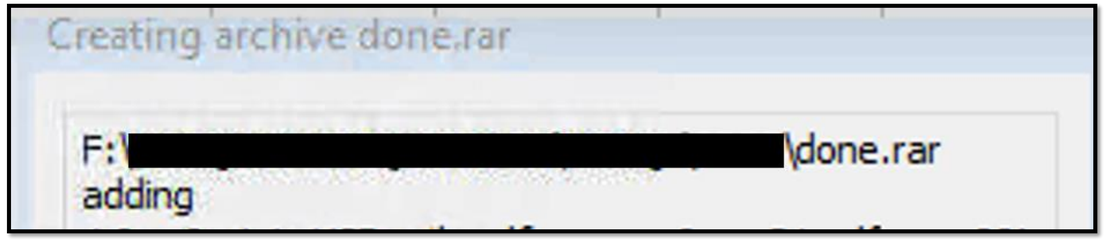
Viewing Shellbags

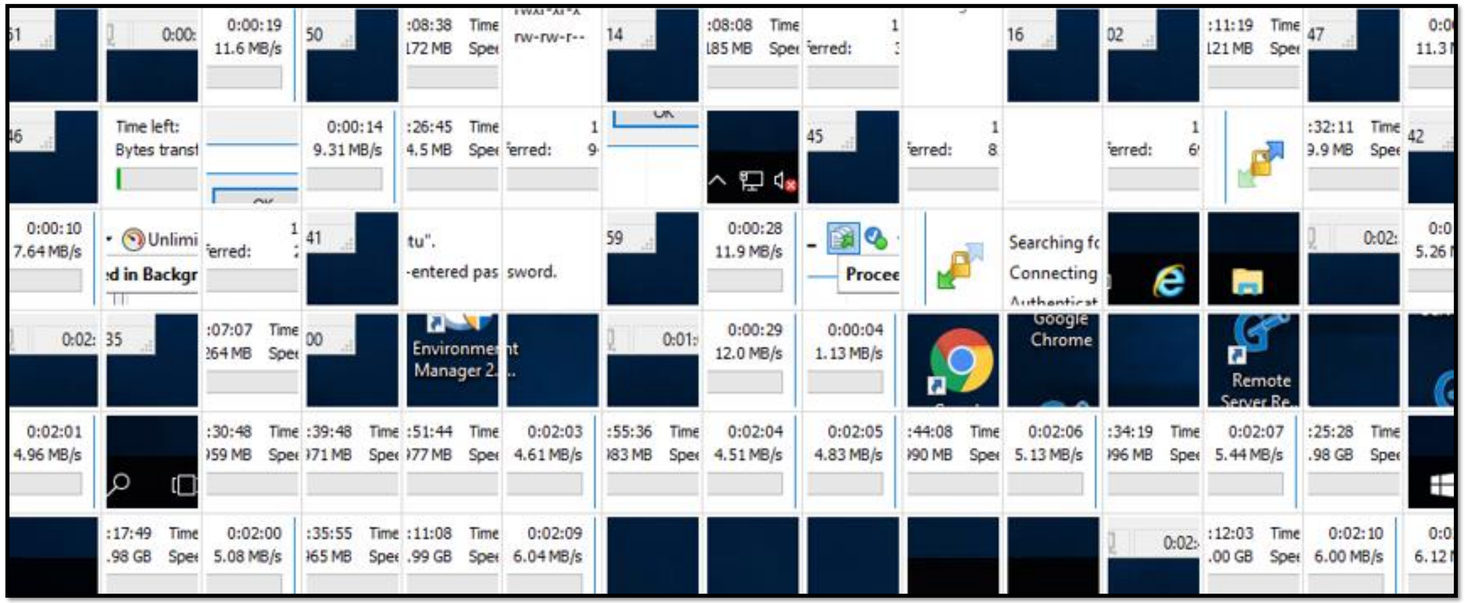


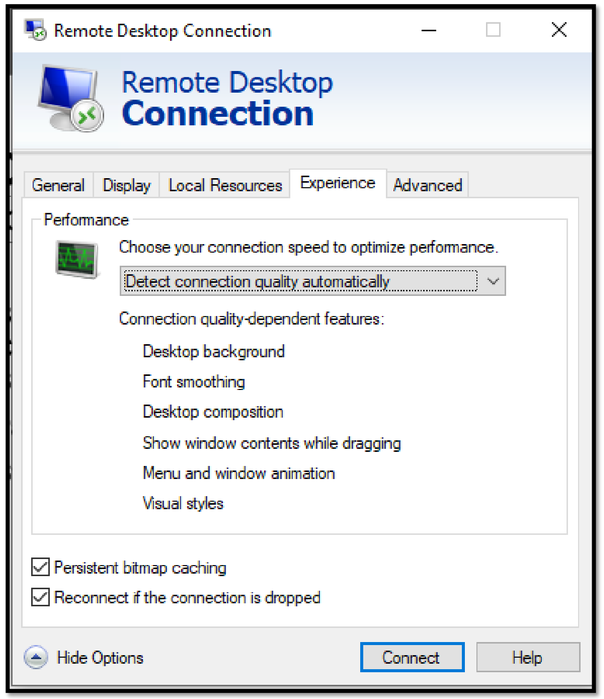
Source: ShellBags Explorer by Zimmerman | ericzimmerman.github.io

RDP Bitmap Cache Stitching

- **Bitmap cache files found under C:\Users*\AppData\Local\Microsoft\Terminal Server Client\Cache***
- **Parser: https://github.com/ANSSI-FR/bmc-tools**
- **Stitcher: https://github.com/BSI-Bund/RdpCacheStitcher**

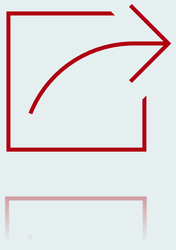






Network and System Activity

Logs overwritten due to retention



Logs not forwarded

Critical system without EDR

SUM Database/Unified Access Log

- In 2021, KPMG discovered a new Windows forensic artifact named UAL (User Access Log) present on Windows servers 2012 and up
  - https://advisory.kpmg.us/blog/2021/digital-forensics-incident-response.html
- UAL logs stored under \Windows\System32\LogFiles\SUM
- Tracks user requests, local software products, Hyper-V stats and IP-Hostname maps
- Helpful in reviewing ingress activity, SMB activity etc. in incident response cases.
- Data retention typically goes back **years**.

RoleGuid	RoleDescription	AuthenticatedUserName	TotalAccesses	InsertDate	LastAccess	IpAddress	ClientName	TenantId	SourceFile
10a9226f-50ee-49d8-a393-9a501d47ce04	File Server	corporate\administrator	1722	2021-01-01 00:00:19	2021-10-25 17:03:43	172.16.119.46		00000000-00	Current.mdb
10a9226f-50ee-49d8-a393-9a501d47ce04	File Server	corporate\user1	2052	2021-01-01 00:00:20	2021-10-15 18:46:54	172.16.119.13		00000000-00	Current.mdb
10a9226f-50ee-49d8-a393-9a501d47ce04	File Server	corporate\user2	12037	2021-01-01 00:00:34	2021-10-31 22:46:26	192.168.1.235		00000000-00	Current.mdb

Tracking RDP Egress

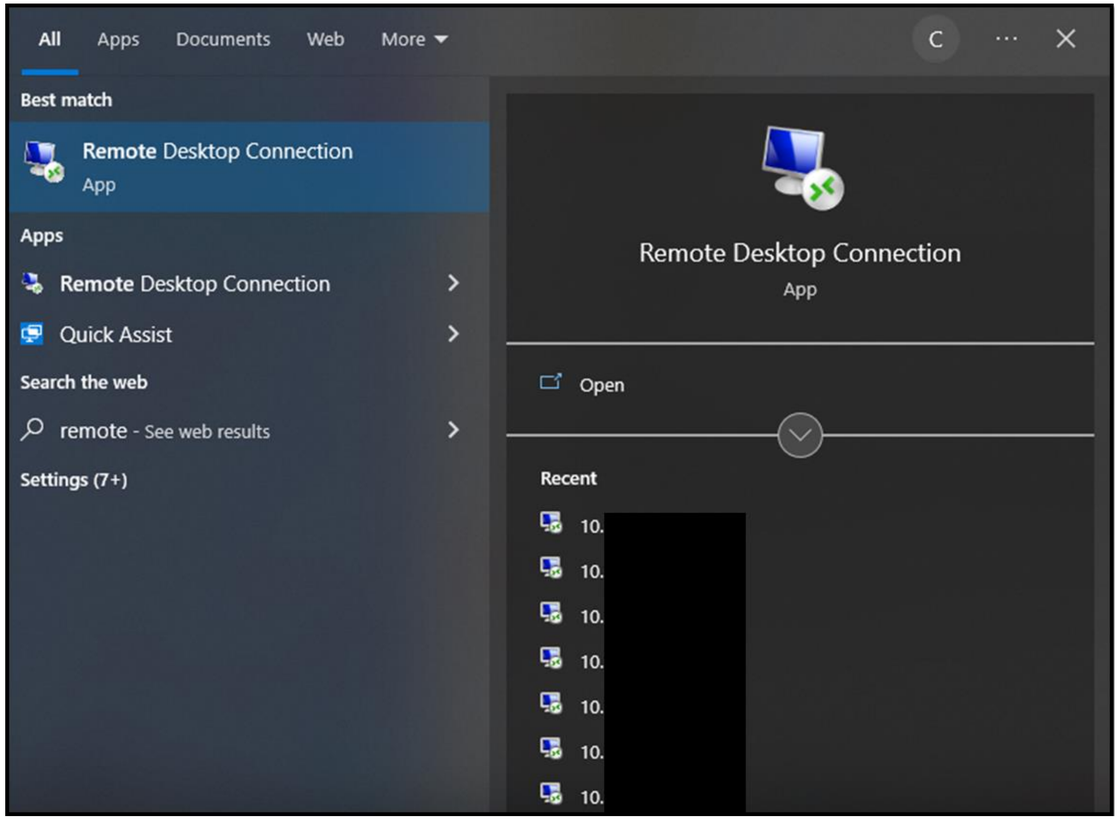
Jumplists and RDP MRU

RDP MRU

- Where?
  - NTUSER.DAT\Software\Microsoft\Terminal Server Client\Default
- Tracks
  - IP/Hostname, Last Modified Time and the user that initiated the connection

Jumplists

- Where?
  - C:\Users*\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations
  - C:\Users*\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations
- Tracks
  - Application, User, Command Flags and Timestamp



Bytes in/Bytes out
SRUM

- **Introduced in Windows 8, SRUM is part of DPS (Diagnostic Policy Service)**
- **Tracks stats on network usage, application resource usage, push notifications and energy usage**
- **SRUM is stored as an ESE DB on disk**

- **Tables:**
  - Application Resource Usage
  - Network Connectivity
  - Network Usage
  - Push Notification Data

  - The SID of the user who launched the process
  - CPU cycle time
  - Context switches
  - Bytes read/written
  - Number of read/write operations
  - Number of flushes

- **SRUM does not track IP addresses!**

The Power of Windows Event Logs

Why Are Event Logs Important in IR?

Security: 4624

Step 1: User connected to the machine

Step 2: User downloads and opens a malicious document

OAlerts: 300

PowerShell: 4104/600
Security: 5156

Step 3: PowerShell command launched to download malware

Step 4: Malware runs

Applocker: 8003/8005

Security: 4688

System: 7045
Schtasks: 102,201

Step 5: Establishes Persistence

In a Few Minutes, You Can Find Out

Security: 4624	Time of login and the username
OAlerts: 300	Name of the malicious document and which program it was E.g.: Word/Excel
PowerShell: 4104/600 Security: 5156	4104/600 - PowerShell command that was executed that reaches out to C2 5156 – Outbound IP address and port of C2
Applocker: 8003/8005 Security: 4688	8003/8005 – Name of executable that was downloaded and executed along with the hash value
System: 7045 Schtasks: 102,201	7045 – Malicious service creation 102/201 – Identify scheduled task creation/deletion and maybe additional copies of malware

AON

Event IDs of interest

Security: 4624, 4625, 4634, 4672, 4688, 4689, 4674, 4648, 5140, 1102, 5145, 4656, 4663, 4697, 4732, 4776, 4724, 4720, 4722, 4738, 4797, 4798,4799, 5156
AppLocker: 8002, 8005
Office Alerts: 300
System: 7045, 7036, 7030, 104, 1014
PowerShell/Operational: 4104, 4100
Powershell: 600
Scheduled Tasks: 201,106,141,140
Sysmon: 1, 3, 19, 20
WMI: 5861
RDP Remote:1149
RDP Local: 21,22,23,24,25
BITS: 3,4,59,60
Shellcore: 9705,9707,62170
RDPClient ActiveX: 1024, 1025, 1026, 1029
Defender: 5007, 1116, 1117

AON

AON

Case Study

Background

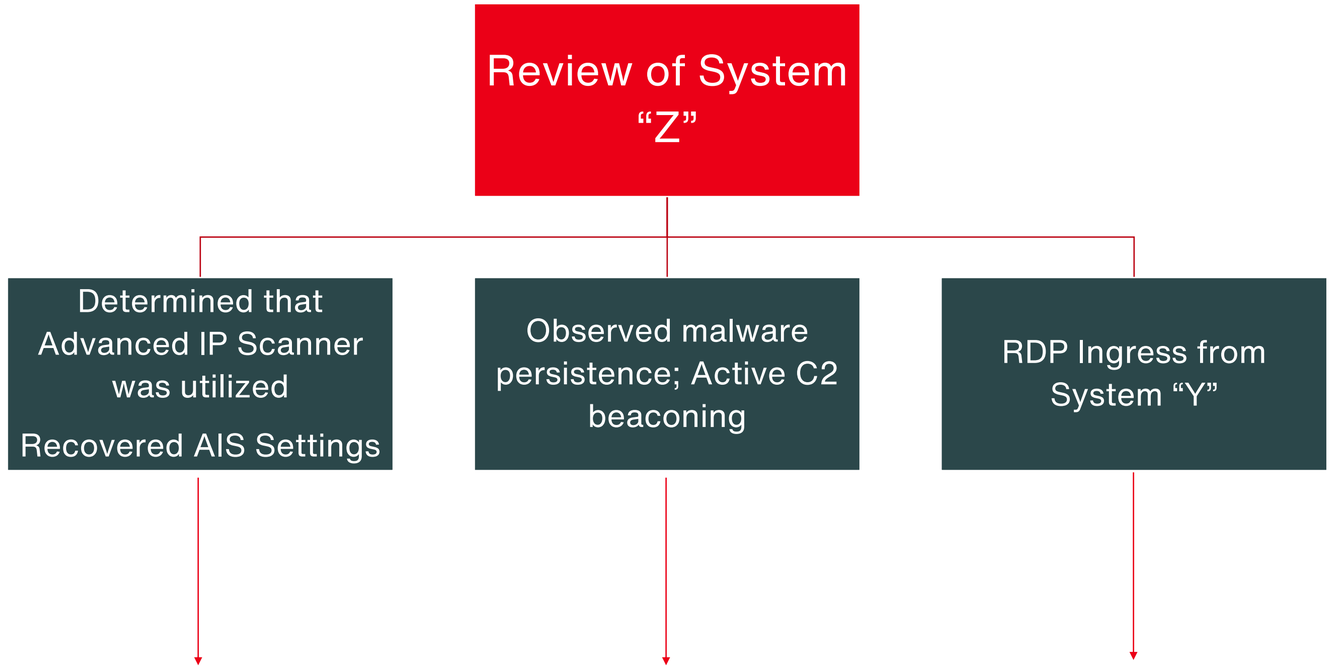
Called in to assist with investigating two devices where unauthorized IP scanning was observed in a large network

Challenges

Logs rolled over/not forwarded	3% EDR deployed; Moving from AV	Limited network visibility

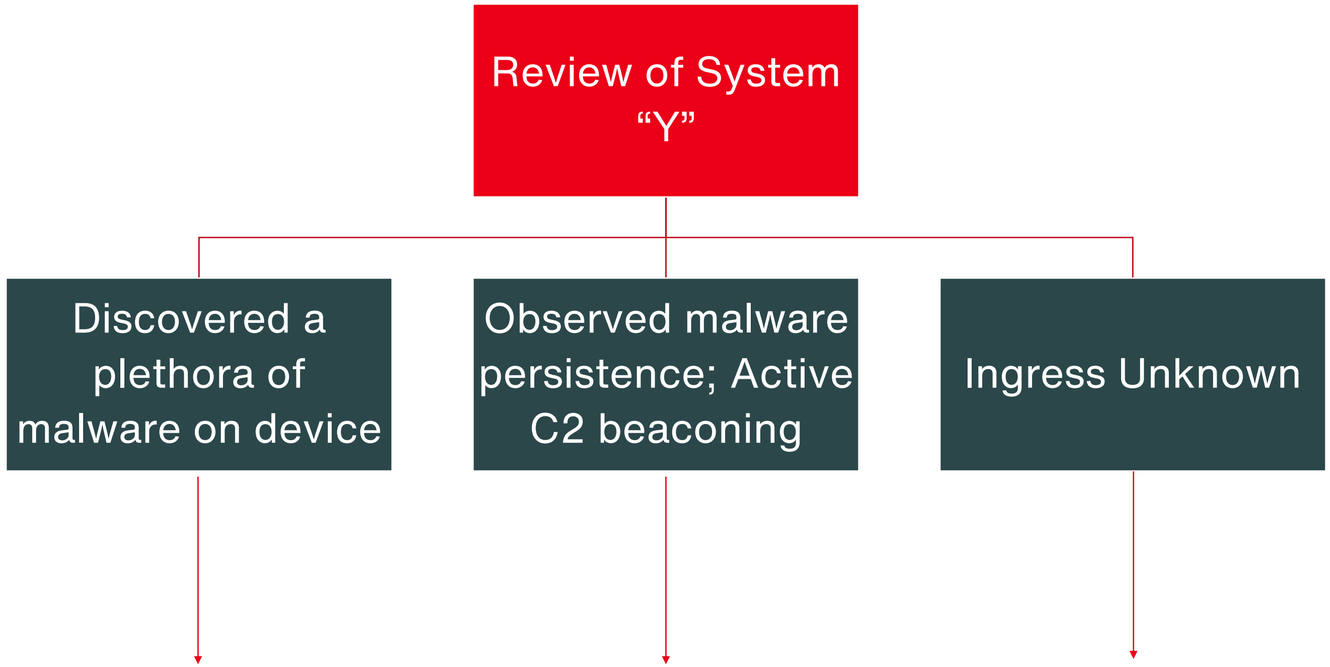
Investigating IP Scanning activity on System “Z”

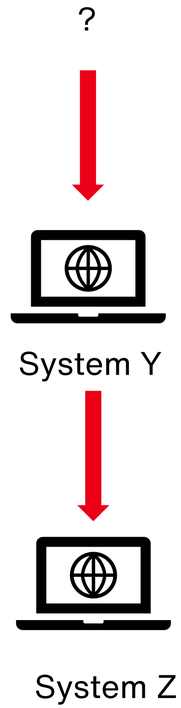
Reviewing Windows Registry to determine settings used by the threat actor



Investigating System “Y”

Staging server used by the threat actor





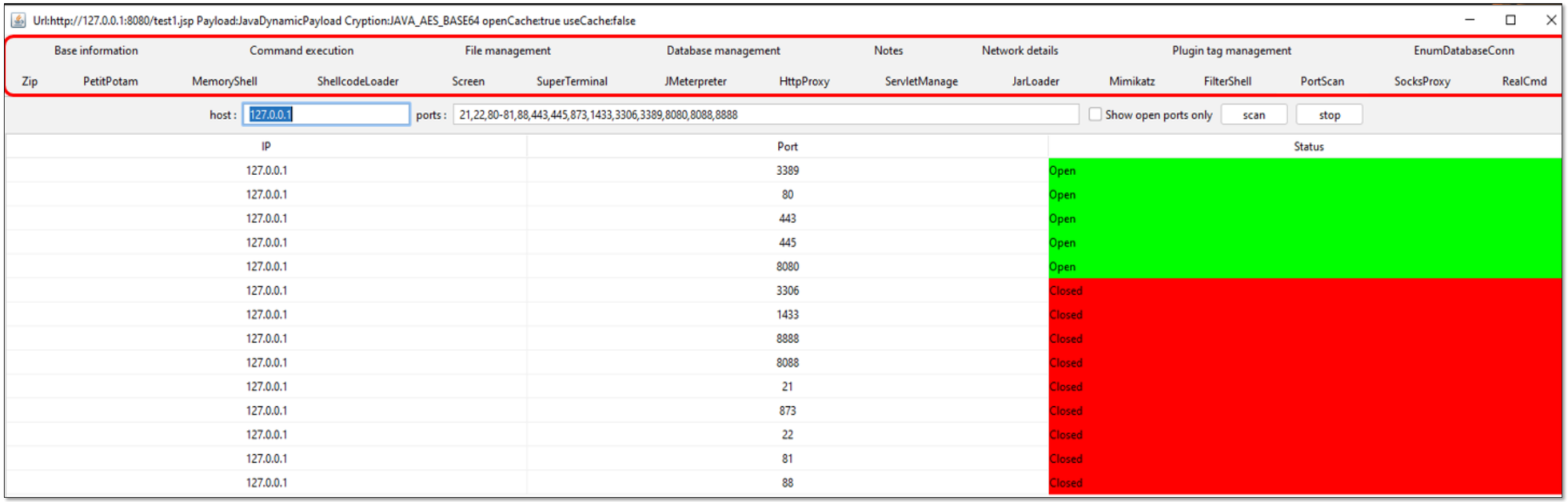
What now?

Do we call it off? Call the investigation contained?

Discovery and Analysis of Initial Access

Compromised Confluence server

- **UAL analysis on System “Y” exposed Patient 0**
  - Lateral movement from a compromised Confluence server
- **Threat actors exploited a vulnerability**
- **Vulnerability used to drop a webshell**



So, with P-0 discovered, the next question is scope of impact

Is it just these 3 systems or more than that?

Forensic artifacts collected and reviewed from thousands of systems

Forensic Findings

Credential Dumping

- **NTDS.dit extracted from Volume Shadow Copy**
  - Identified through RDP Bitmap Cache

Data Exfiltration

- **WinSCP usage including threat actor username and IP**
  - Identified through RDP Bitmap Cache and TrayNotify key in registry

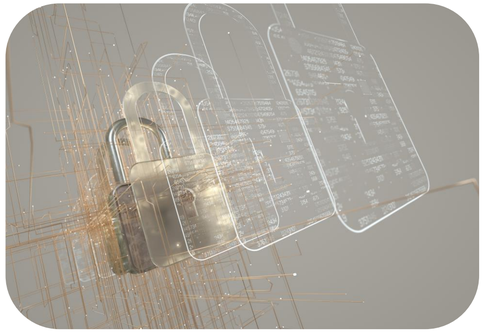
Takeaways

“

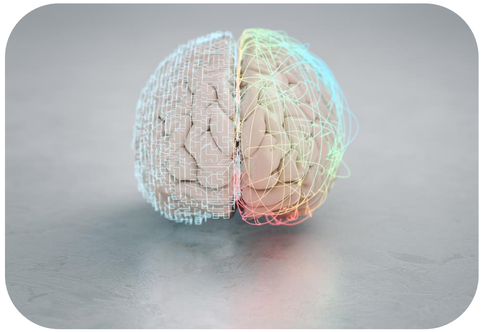
Never rely on one tool for DFIR investigations.

”

Takeaways



Tool configuration matters



Need for holistic investigations

Historical insights are important

Forensics aid in profiling threat actors

Skilled investigations to counter evolution of threats

Forensics provides legal Context

Special Thanks

Thank you to our mentor Sankara Shanmugam for inventing the idea for this talk and for all the guidance over the years.

Props to our colleagues who provided anecdotes or screenshots, wrote blog posts, and provided their thoughts for this presentation including:

- Andre Maccarone
- Eduardo Mattos and Rob Homewood
- Ann Romer, Hailie Shaw, Zach Reichert
- Bashar Shamma

Follow us:

@StrozDFIR

Check out our blog:

aon.com/cyber-solutions/aon_cyber_labs/

Have Questions?

Meet us in the Speaker Lounge!

Or reach out to our speakers via social media:

Twitter: @4n6research

LinkedIn: linkedin.com/in/alwar

LinkedIn: linkedin.com/in/carly-b-27905998

Sources

1. VMWare ESXi: https://www.vmware.com/topics/glossary/content/bare-metal-hypervisor.html
2. Memes created with: https://imgflip.com
3. Shellbags Explorer by Eric Zimmerman: ericzimmerman.github.io
4. UAL discovery by KPMG: https://advisory.kpmg.us/blog/2021/digital-forensics-incident-response.html

AON