Analysis Without Paralysis

Mastering the Art of Investigation

Terryn Valikodath

Senior IR Consultant

Cisco Talos Incident Response

https://chocolatecoat4n6.com

- DF/IR all day, everyday
- You'll see me on your worst day ☺

How I got here

- Rooting and jailbreaking
- Help Desk > Sysadmin > Cybersecurity > DF/IR

We are not taught investigation

Why do you need structure in an investigation?

“Jumping In” leads to burnout and mistakes

Sets realistic expectations, explain your brain

We are taught to analyze not investigate

Background

Digital Forensics

Medical Examiner
Detective
Arson Investigator

Collecting, preserving, analyzing, and presenting digital evidence.

DF/IR

Responding to significant technology events through analysis and planning.

Incident Response

ER Doctor
SWAT
Firefighter

Identifying, managing, and mitigating security breaches or attacks.

What is an investigation?

Investigations are all about moving from the unknown, to the known, and then further to the provable.

Observation Question Hypothesis Answer Conclusion

Investigative Mindset

Think before you act

Evidence

- Know your evidence
- Interpret your evidence
- Explain your evidence

Question Everything

- Challenge your bias
- Use questions and hypothesis to lead your investigations
- Why is this malicious?

Know Normal

- Computers
- Networks
- Industries
- Human Behavior

MITRE ATT&CK

Used for threat intelligence, checking your defenses and threat hunting

Tactics	Techniques	Procedures
The adversary's goal	How the adversary achieves their goal	Implementation of steps for the technique
"Persistence"	"T1053: Scheduled Task/Job"	"Earth Lusca used the command schtasks /Create /SC ONLOgon /TN WindowsUpdateCheck /TR "[file path]" /ru system for persistence"

ADAPT Methodology

A.D.A.P.T.

Add structure and planning to your investigation

Approach Discovery Association Profile Timeline

Approach

Discovery

Association

Profile

Timeline

Approach

- Organize and document evidence
- Create a plan of action, don’t rush in
- Set clear objectives
- Identify TTPs with indicators
- Use templates to move quickly

© 2025 Cisco and/or its affiliates. All rights reserved.

Notes Template

Investigation Notes

Contents

Console/Log Analysis

EDR

SIEM

Firewall

[Console]

Hosts

HOST1

Operating System:

IP Address:

Function:

Primary User:

Additional Notes:

Artifact

[Analysis Notes regarding the artifact]

Artifact2

[Analysis Notes regarding the artifact]

HOST2

Operating System:

IP Address:

Function:

Primary User:

Additional Notes:

Artifact

[Analysis Notes regarding the artifact]

Artifact2

[Analysis Notes regarding the artifact]

Indicators

Network

[IP Address/DNS]

File

[File Name/Hash]

Users

[Domain and Username]

© 2025 Cisco and/or its affiliates. All rights reserved.

Know where to look

- If you don’t have evidence, you are assuming.
- Don’t forget, a lack of evidence may also be evidence.

Approach
Discovery
Association
Profile
Timeline

Approach

Hunting for the adversary

- Malicious behavior may not always be identified before your analysis begins.
- A baseline of expected activity will make it easier to identify suspicious behaviors
- Use the hypothesis approach to set end points.
  - PEAK Threat Hunting Framework
- There will likely be several paths to follow.
- Note them down, but finish your current hypothesis

© 2025 Cisco and/or its affiliates. All rights reserved.

Approach
Discovery
Association
Profile
Timeline

Discovery

- Organize your findings by the evidence source
- Write out findings in “report format”
- Write them for the audience
- UTC all day, everyday

© 2025 Cisco and/or its affiliates. All rights reserved.

Findings

Components to always include in your notes.

Finding Example

Artifact1 [Windows Event Logs]

[Analysis Notes regarding the artifact]

At 2022-01-01T12:34:56Z, a network logon occurred from 'WKSTN01' to the host "DC1" using the account 'spartan'. A truncated copy of the event is shown in the Figure below. The event was deemed suspicious due to the recent creation of the account as well as the fact that it accessed a domain controller. Blue team verified with additional teams that the account is not a previously utilized account and does not match standard naming conventions.

```
Subject:
    Security ID: SYSTEM
    Account Name: spartan
    Account Domain: WORKGROUP
    Logon ID: 0x3E7
Logon Information:
    Logon Type: 3
    Elevated Token: Yes
Network Information:
    Workstation Name: WKSTN01
```

© 2025 Cisco and/or its affiliates. All rights reserved.

Approach
Discovery
Association
Profile
Timeline

Association

- Take individual events and see how they fit together
- What is the chain of events?
- What fits? What doesn’t fit?
- Begin to record the indicators and timestamps in a central location.

© 2025 Cisco and/or its affiliates. All rights reserved.

Approach
Discovery
Association
Profile
Timeline

Association

Normalization

- Use standard time notation for events
  - ISO-8601 in UTC
  - 2022-01-01T12:34:56Z
- Use consistent terminology to identify similar fields from difference log sources.
  - Connected IP or Source Network Address = Source IP
- Write it like you're writing for someone who doesn’t know what your job is

© 2025 Cisco and/or its affiliates. All rights reserved.

Approach
Discovery
Association
Profile
Timeline

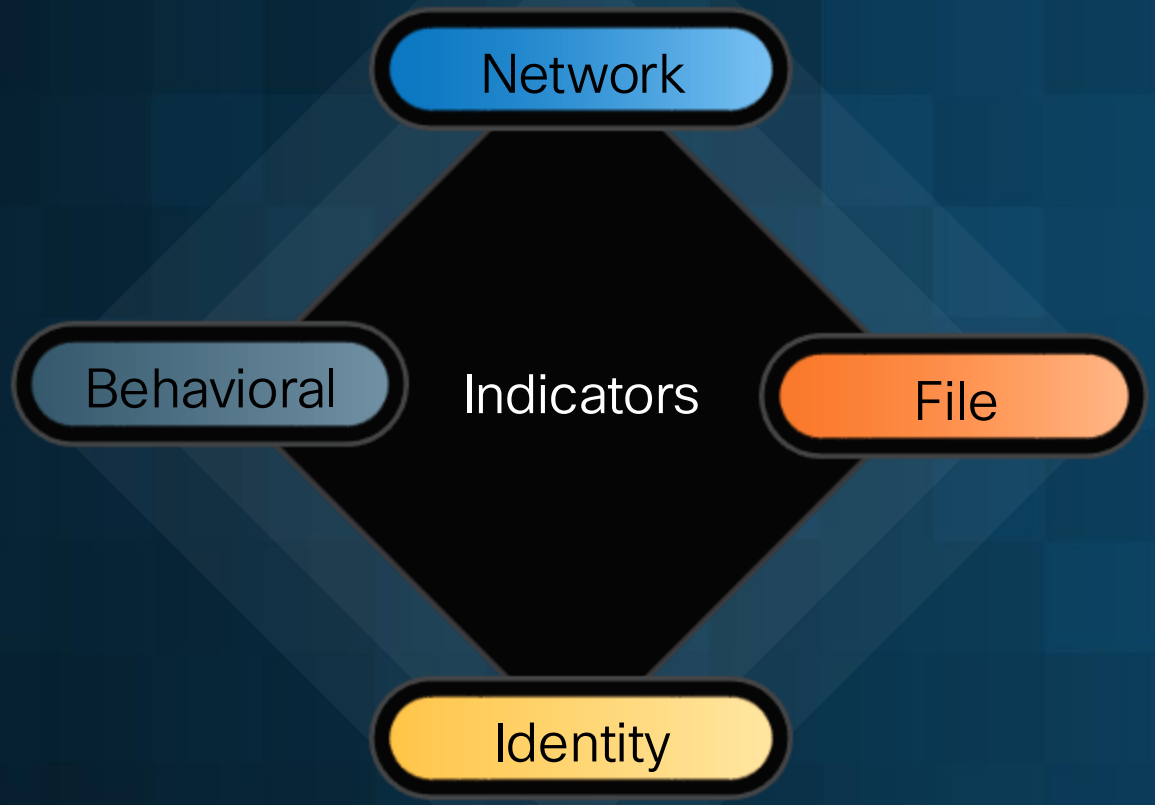
Profile

- Have we or someone else seen this before?
- It is not intended to be exhaustive or comprehensive
- MITRE ATT&CK provides a useful framework for documenting common TTP’s often leveraged by adversaries.
- What intelligence exists around the identified TTPs and indicators?

© 2025 Cisco and/or its affiliates. All rights reserved.

Indicators

- They come in all shapes and sizes
- Let your Intelligence team/partners in on the fun
- Keep a list of indicators for future searches



Indicators Example

	A	B	C	D
1	**Indicator**	**Indicator Type**	**Context**	**Additional Notes**
2	*8.8.8[.]8*	*Network*	*Blocked at the firewall at 2022-02-04*	*Looks to be associated with a weird search engine*
3	*spartan*	*User*	*Unknown user logon on DC1*	*Username is not commonly used within the organization*
4	*C:/Temp/wort[.]exe*	*File*	*Unknown executable*	*Likely a ransomware encryptor based on execution timing and malware analysis*
5	*88.198.55[.]22*	*Network*	*IP of earliest suspicious logon*	*Sangheili-owned IP address according to WHOIS records*
6	*noble6*	*User*	*Domain adminstrator*	*Administrator account previously used for setting up domain. No longer used after 2010*
7				

© 2025 Cisco and/or its affiliates. All rights reserved.

Approach
Discovery
Association
Profile
Timeline

Timeline

- Take your findings and input them into a table (CSV or Excel)
- Headers
    - Timestamp (UTC)
    - Origin
    - Target
    - User
    - Evidence Source
    - Event Type
    - Description
    - MITRE

© 2025 Cisco and/or its affiliates. All rights reserved.

Incident Timeline Example

	A	B	C	D	E	F	G
1	Timestamp (UTC)	Origin	Target	User	Evidence Source	Event Type	Description
2	2022-01-01T07:22:37Z	88.198.55[.]22	WKSTN01	noble6	NetFlow Logs	Suspicious Logon	A suspicious network logon (4624 Type 10) for th
3	2022-01-01T08:00:07Z	WKSTN01	-	noble6	Azure Audit Logs	User Creation	User 'spartan' was created, logs indicate WKSTN
4	2022-01-01T08:02:22Z	WKSTN01	-	noble6	Azure Audit Logs	User Group Addition	User 'spartan' was added to the group 'Remote A
5	2022-01-01T12:34:56Z	WKSTN01	DC1	spartan	Windows Event Logs	Suspicious Logon	A suspicious network logon (4624 Type 3) from th
6	2022-01-01T14:44:35Z	-	DC1	spartan	Prefetch, Registry	Malicious Execution	The user executed the file 'C:/Temp/wort[.]exe' t
7	2022-01-01T14:45:15Z	-	DC1	-	SuperEDR Console	EDR Block	SuperEDR blocked 'C:/Temp/wort[.]exe'
8							

© 2025 Cisco and/or its affiliates. All rights reserved.

Summarizing A.D.A.P.T.

Add structure and planning to your investigation

Approach Discovery Association Profile Timeline

Output

What following ADAPT gets you

Report	Timeline	Accomplishments
The final report is 80% complete.	Easy to digest chain of events	Clearly show how you contributed
A document you can speak to when asked	Looks great in a final report	Proof of your hard work
No need to rely on just memory	Database of incident details	Documented findings to drive change

Approach
Discovery
Association
Profile
Timeline

Resources

Highly recommend if any of this talk interests you

- Anson, S. (2020). *Applied incident response*. Wiley.
- Hess, K. M., Orthmann, C. H., & Cho, H. L. (2022). *Criminal investigation* (12th ed.). Cengage Learning.
- Sanders, C. (n.d.). *Investigation theory* [Online course]. Chris Sanders. https://chrissanders.org/training/investigationtheory/
- Sanders, C. (n.d.). *Effective information security writing* [Online course]. Chris Sanders. https://chrissanders.org/training/writing/
- Shavers, B. (2024). Placing the suspect behind the keyboard: DFIR investigative mindset.
- Shavers, B. (n.d.). *Brett Shavers Blog*. https://www.brettshavers.com
  Valikodath, T. (n.d.). *ChocolateCoat4n6 Blog*. https://chocolatecoat4n6.com

© 2025 Cisco and/or its affiliates. All rights reserved.

Thank you!

Questions?

@CyberCoat on Twitter

@ChocolateCoat
everywhere else
(Mastodon, BlueSky,
etc)

https://github.com/chocolatecoat/DFIR-Templates

Templates for Scoping, Forensic Notes, and Reports.
Always open to more ideas of what may be helpful.

https://chocolatecoat4n6.com/