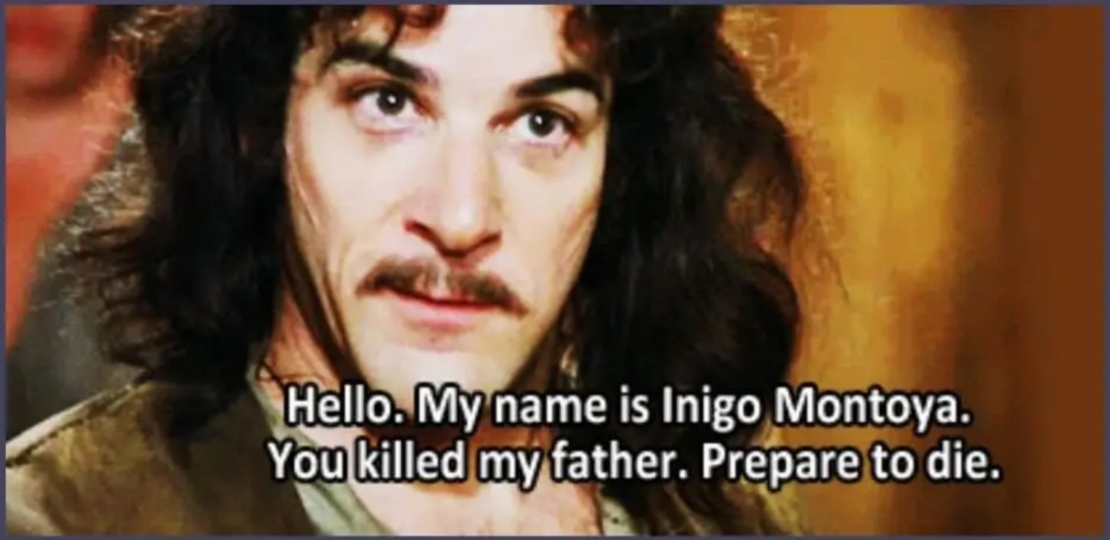
Diamonds are a forensicator's best friend - intelligence support for DFIR

Kamil Bojarski

QUOINTELLIGENCE

Agenda

- **whoami**
- **Threat Intelligence and other sec functions**
  - Incident Response support
  - F3EAD
- **CTI and IR**
  - Translating the Diamond Model
  - Who, how, will
  - Intelligence analysis in evidence assessment
  - Anti-forensics and gap detection
- **Conclusions**


Hello. My name is Inigo Montoya.
You killed my father. Prepare to die.

Remember Inigo Montoya:

1. Polite greeting
2. Name
3. Relevant personal link
4. Manage expectations

Picture source: https://tommccallum.com/2018/08/31/inigo-montoya-masterclass-on-introducing-yourself/

$whoami

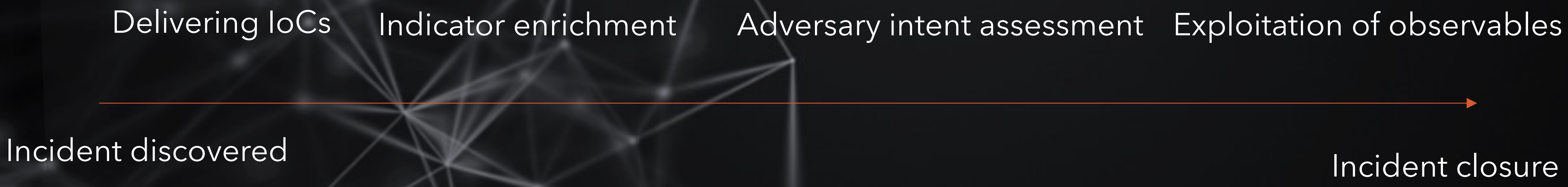
- **Principal Cyber Threat Intelligence Analyst at QuoIntelligence (views are my own).**
- **Teaching Assistant for SANS FOR578 Cyber Threat Intelligence Course.**
- **You can read my thoughts on OSINT, natsec and threat intel at counterintelligence.pl**
- **I also like ABC..**
  - Aviation
  - Balisongs
  - Climbing
- **Feel free to connect!**
  - **Twitter @lawsecnet / LinkedIn**
  - **Email: kamil.bojarski@lawsec.net, kamil.bojarski@quointelligence.eu**

Incident response support

- Preparation - purple teaming, analyzing incident response procedures in terms of threat lanscape.
- Identification - providing indicators of compromise, enrichment of findings.
- Containment - assessing risk to the environement, analysis of criticality of assets.
- Eradication - identification of persistance mechanism.
- Recovery - hardening and monitoring.
- Lessons learned - providing briefing on activity groups, discussion on possible further threats.

Incident response support

- Responders need to deal with technical assessment of forensic findings and assessing scope of the incident at the same time.
- Support can be related both to delivering analysis of indicators of attack as well as directing scoping.



Delivering IoCs

Indicator enrichment

Adversary intent assessment

Exploitation of observables

Incident discovered

Incident closure

Incident response support

- Resp f forensic findi me time.
- Supp ndicators of attac

Delive ation of observables

Incident discovered

Incident closure

QUOINTELLIGENCE

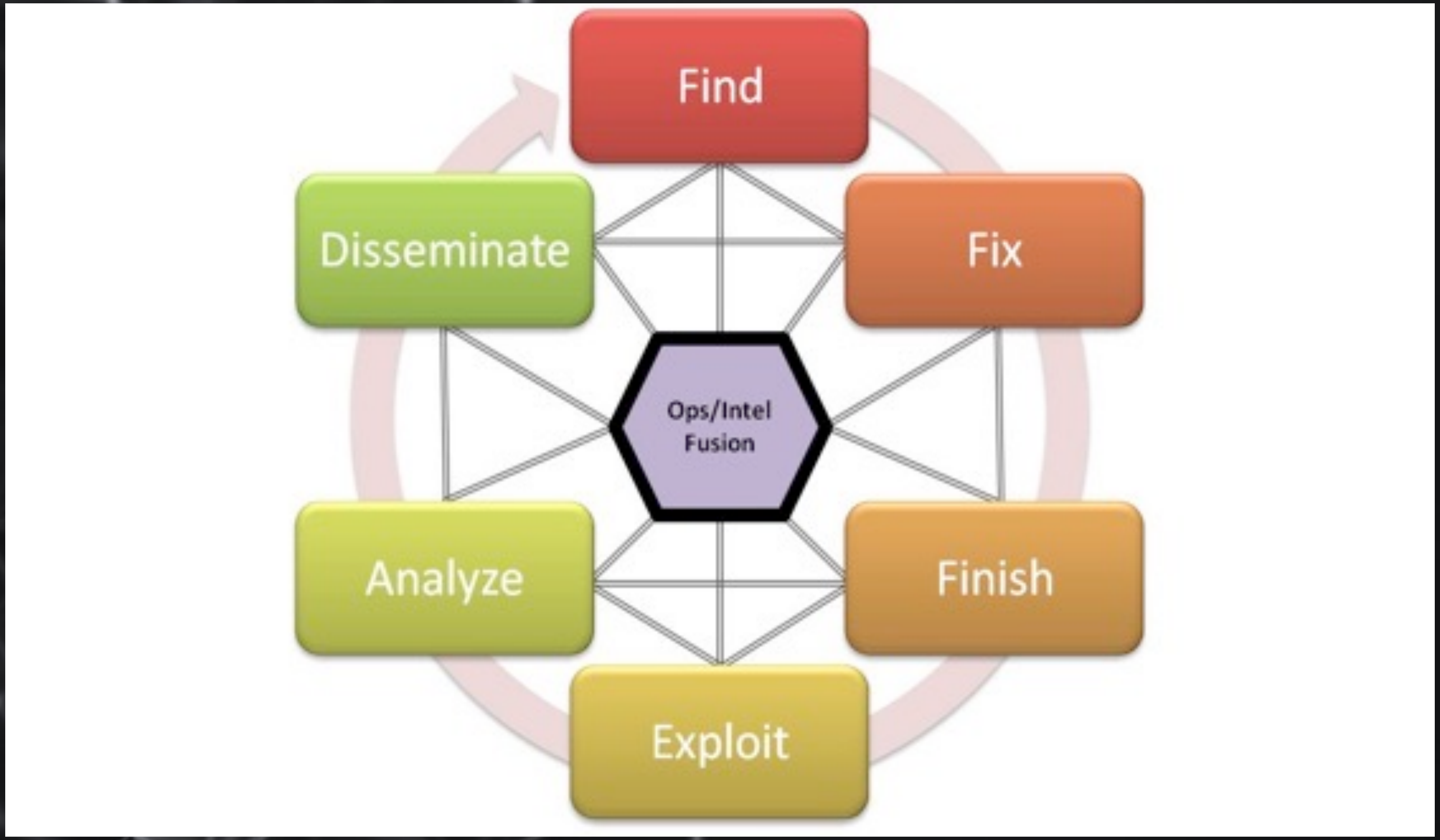
Picture source: https://i.pinimg.com/originals/db/88/36/db8836117623c14019df01afe8f6fd72.jpg

Incident response support

QUOINTELLIGENCE

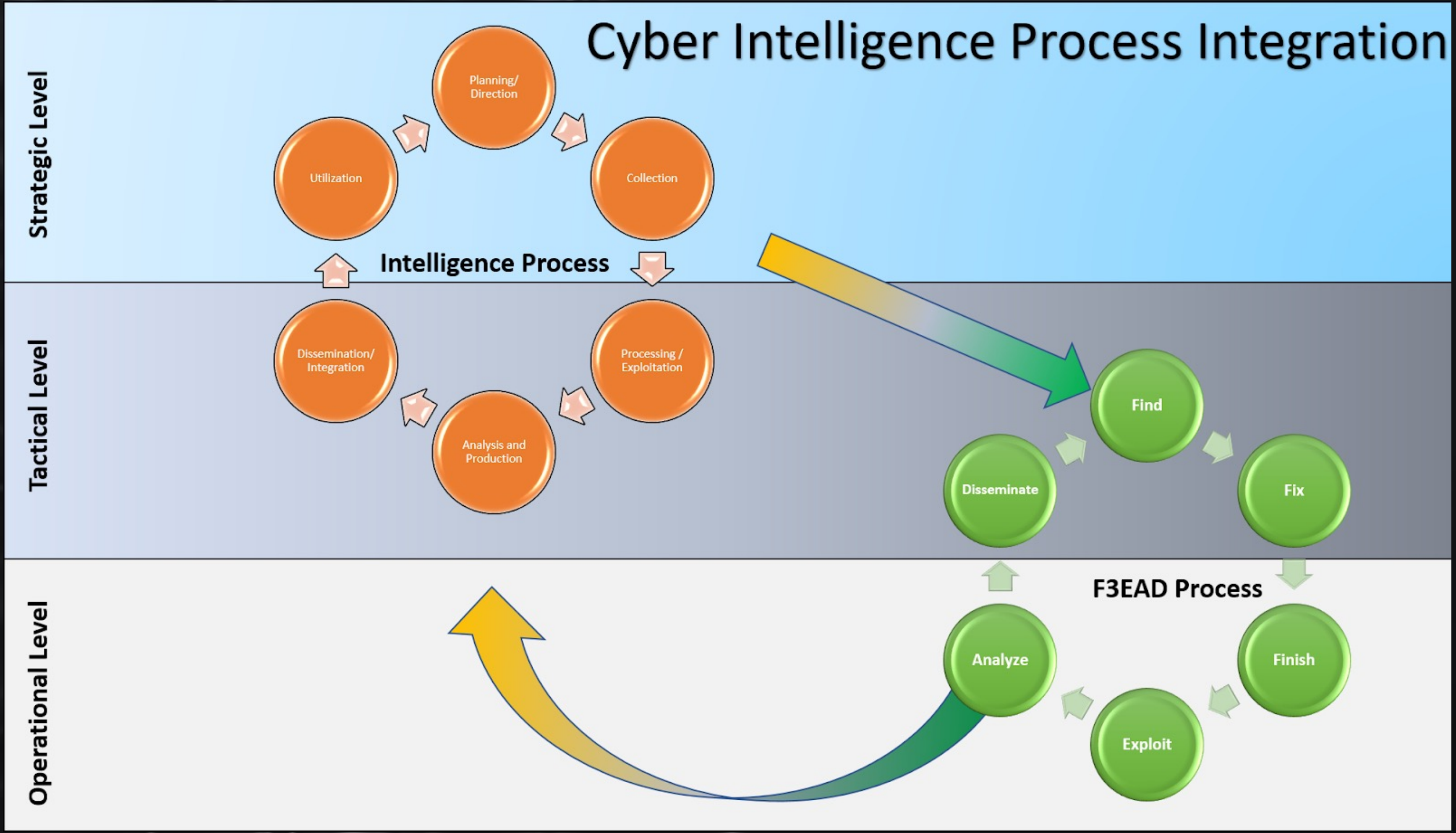
Picture source: https://static.wikia.nocookie.net/spaceballs/images/b/b9/Combing_the_desert.jpg/revision/latest?cb=20181207011738

F3EAD



Source: https://smallwarsjournal.com/jrnl/art/f3ead-opsintel-fusion-%E2%80%9Cfeeds%E2%80%9D-the-sof-targeting-process

F3EAD



Source: https://www.first.org/global/sigs/cti/curriculum/methods-methodology

QUOINTELLIGENCE

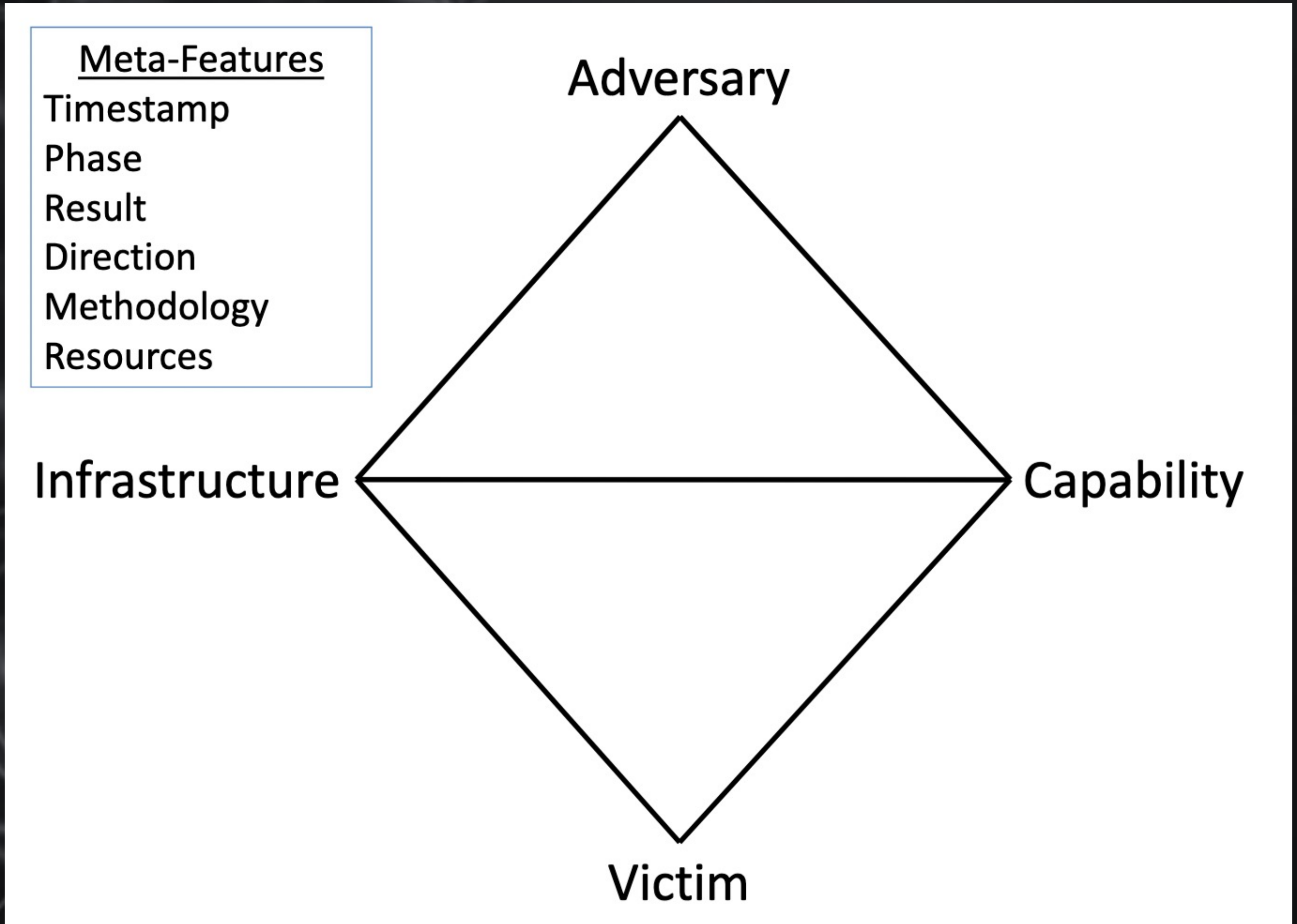
F3EAD

- Find – determining relevant threat groups, information gathering.
- Fix – scope assessment, affected assets, containement of devices, establishing visibility.
- Finish – eradication of activity, mitigation of vulnerabilities, recovery of environment, post incident hardening.
- While exploitation, analysis, and dissemination is most often associated with threat intelligence, its role in Fix and Finish is as important.

Hunting vs IR

- Support to hunting and IR function will overlap in process.
- Identification of scope of incident vs hunting for indicator of malicious actions.
- The same processes that support huting hypothses building are useful in incident scoping.
  - Hunting hypotheses -> incident scope assessment.
  - Testing requirements -> visibility assessment.
  - Hypotheses verification -> detection of further affected assets.

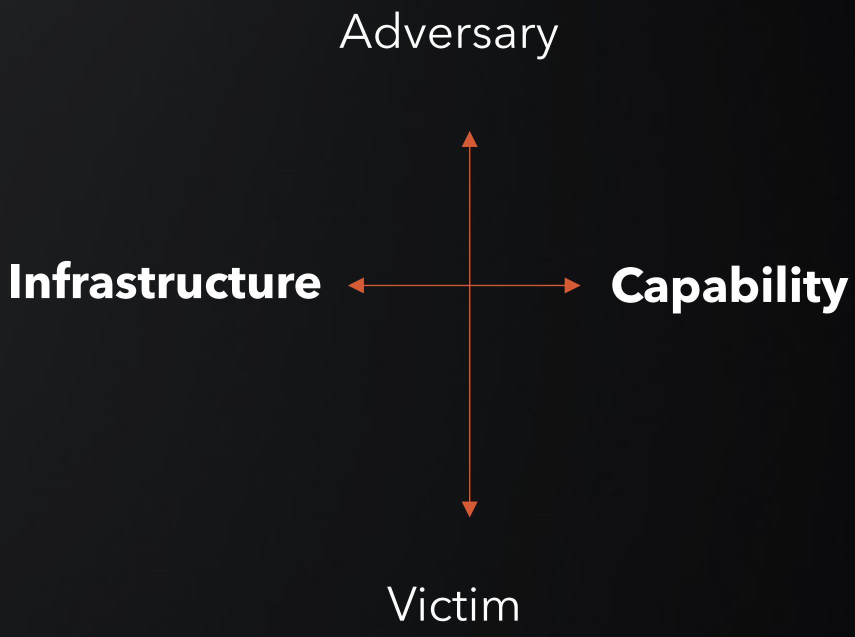
Diamond Model



Source: https://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf

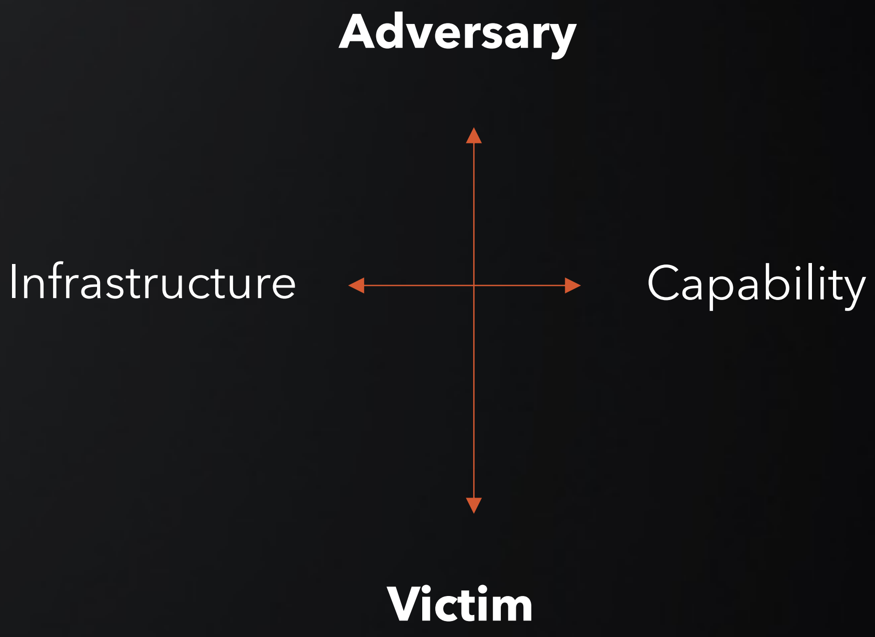
Diamond model

- Assessing the technical axis.
  - What capabilities are likely to be deployed?
  - What infrastructure is used and how C2 is conducted?
  - What persistence mechanism can be used?
  - What indicator removal techniques can be used?



Diamond model

- Assessing the sociopolitical axis.
  - What is the motivation of the attack?
  - What is the intent of the adversary?
  - What methods of attack are likely to be used?
  - Are attackers interested in long or short-term goals?



Assessement of intent

- While difficult, analysis across the sociopolitical axis of the diamond model can be useful for IR.
- Depends on the attribution capabilities and how detailed activity groups are described.
- Assessment of intent can support IR with more efficient containment of the incident and making sure that business continuity is affected in a manner proportionatl to the threat.
- Is there a need to contain a server? What can be consequeneces of allowing further operations of the adversary?

Who, how, will

- Who – incident responders, digital forensics examiners, incident managers.
- How – matching indicators with findings of forensics, looking for indicators of the environement to determine scope.
- Will – does the indicators you provide meet the format the tooling uses, what enrichment are you able to provide.

Evidence assessment

- Depending on the purpose of IR, different level of evidence scrutiny may be necessary.
  - Will there be need to present evidence in court?

- Hypotheses assessment and critical analysis of evidence is common intelligence issue, use your expierience to support.
- Analysis of competing hypotheses and other SATs, bias identification.

Anti-forensics and gap detection

- Anti-forensics are activities aimed at:
  - Evading detection.
  - Thwarting collection of evidence.
  - Making collected evidence unreliable.
  - Increasing time spend by the forensic analyst on the case.

Anti-forensics and gap detection

- You can't analyse what you don't know about.
- Intelligence regarding tracks covering techniques (ATT&CK T1070 – Indicator Removal on Host).
- Fix phase need to take into account that adversarial activity cause visibility gaps and IR/TI need to adjust accordingly.
- Assessing value of evidence.
- Acquisition of alternative indicators through external sources.
- During preparation phase planning for the possibility to need redundant visibility sources.

Anti-forensics and gap detection

- Adjustment of the IR/DF process can involve:
  - Assessment of different visibility sources.
  - Assessment of evidence most likely to be compromised.
  - Assessment of most significant threats to evidence gathering process (destruction of artifacts, compromise of data sources, evidence counterfeiting).
- “Threat model” for the standard of evidence you need to obtain.

Anti-forensics and gap detection

- Intelligence requirements:
  - How our visibility/log sources will be affected by successful deployment of X technique?
  - How can we achieve visibility into host/netowork/AD indicators in case of failure of system Y?
  - What will be the consequence of compromise of visibility source Z?
  - What are the indicators that the anti-forensic techniques has been deployed?

Anti-forensics and gap detection

- File deletion
  - APT29 temporary file/scheduled task replacement (Mandiant).
  - Aquatic Panda deleting executables from the ProgramData and Windows\temp\ directories (CrowdStrike).
- Detection
  - 4663(S): An attempt was made to access an object.
  - 4660(S): An object was deleted.
  - Sysmon Event ID 23/26.
  - Indicators for file carving.

Anti-forensics and gap detection

- Timestomping
  - APT38 using timestamps of the files in the same directory (US CISA).
  - Kimsuky backdating files to 2016 (Cybereason).
  - Shamoon setting value to 2012 (McAfee).
- Detection
  - Nanosecond precision.
  - USN Journal anomalies.
  - $SI/$FN discrepancies.
  - Sysmon Event ID 2.

Anti-forensics and gap detection

- Clear network connection related artifacts
  - Sunburst removing firewall rules after the network reconnaissance was completed, also disabling event logging using AUDITPOL and re-enabling it afterward. (Microsoft)
  - Removal of RDP connection history - \Software\Microsoft\Terminal Server Client\
- Detection
  - External log storage.
  - Hunting for registry/network configuration command execution.
  - Audit MPSSVC Rule-Level Policy Change.

Measuring impact - KPIs

- Mean time to respond.
- Mean time to finish scoping.
- Mean time to remediate.
- Number/percenatage of indicators pivoted with intelligence data.
- Mean cost of breach.
- What does the incident response team think about that?
    - Is it decreasing workload?
    - Does it allow to uncover artifacts that are not usually analysed?

'You are the only one who gets to decide what you will be remembered for.'
Taylor Swift

Thank you for your time!

Picture source: https://www.etonline.com/taylor-swift-selena-gomez-set-for-late-night-interviews-with-jimmy-fallon-192670

References

- https://www.crowdstrike.com/blog/overwatch-exposes-aquatic-panda-in-possession-of-log-4-shell-exploit-tools/
- https://us-cert.cisa.gov/ncas/alerts/aa20-239a
- https://www.cybereason.com/blog/research/back-to-the-future-inside-the-kimsuky-kgh-spyware-suite
- https://www.mcafee.com/blogs/other-blogs/mcafee-labs/shamoon-returns-to-wipe-systems-in-middle-east-europe/
- https://www.youtube.com/watch?v=n0ObbSsrqGI
- https://smallwarsjournal.com/jrnl/art/f3ead-opsintel-fusion-%E2%80%9Cfeeds%E2%80%9D-the-sof-targeting-process
- https://www.mandiant.com/resources/blog/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor
- https://www.microsoft.com/en-us/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/