Explaining Incidents to executives in ways they understand

You can get these slides at the end ☺

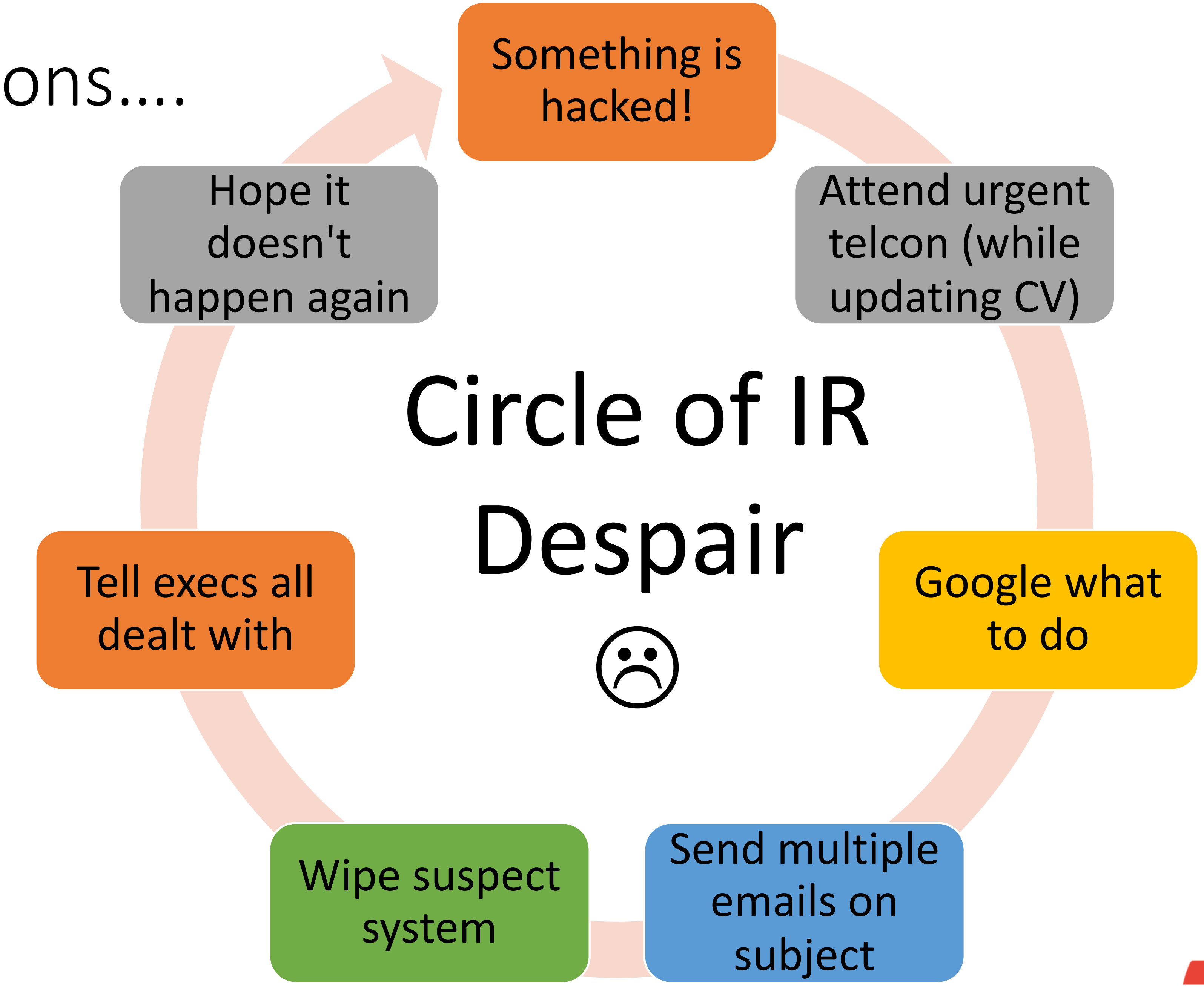
What we are talking about

- Incident Response and how you are cleaning up after the bad guys
- “Executives briefing needs” ☺
- Incident Metrics so you can tell if things are getting better or worse

Who is this guy?

- Steve Armstrong – currently teaching the SEC504
- Former RAF Provost Officer working in Cyber when it was IT Security
- Established Logically Secure 11 years ago
  - Doing the usual testing, consulting and DFIR work
- Incident Responder for 9 years
  - Working from the trenches to the boardroom
  - During on particular APT attack in 2012, conceived the core ideas for our Incident Management portal CyberCPR, patented in the U.S. 4th July 2017
- This talk is about what I have seen work

In many organizations....



Circle of IR Despair ☹

Something is hacked!

Attend urgent telcon (while updating CV)

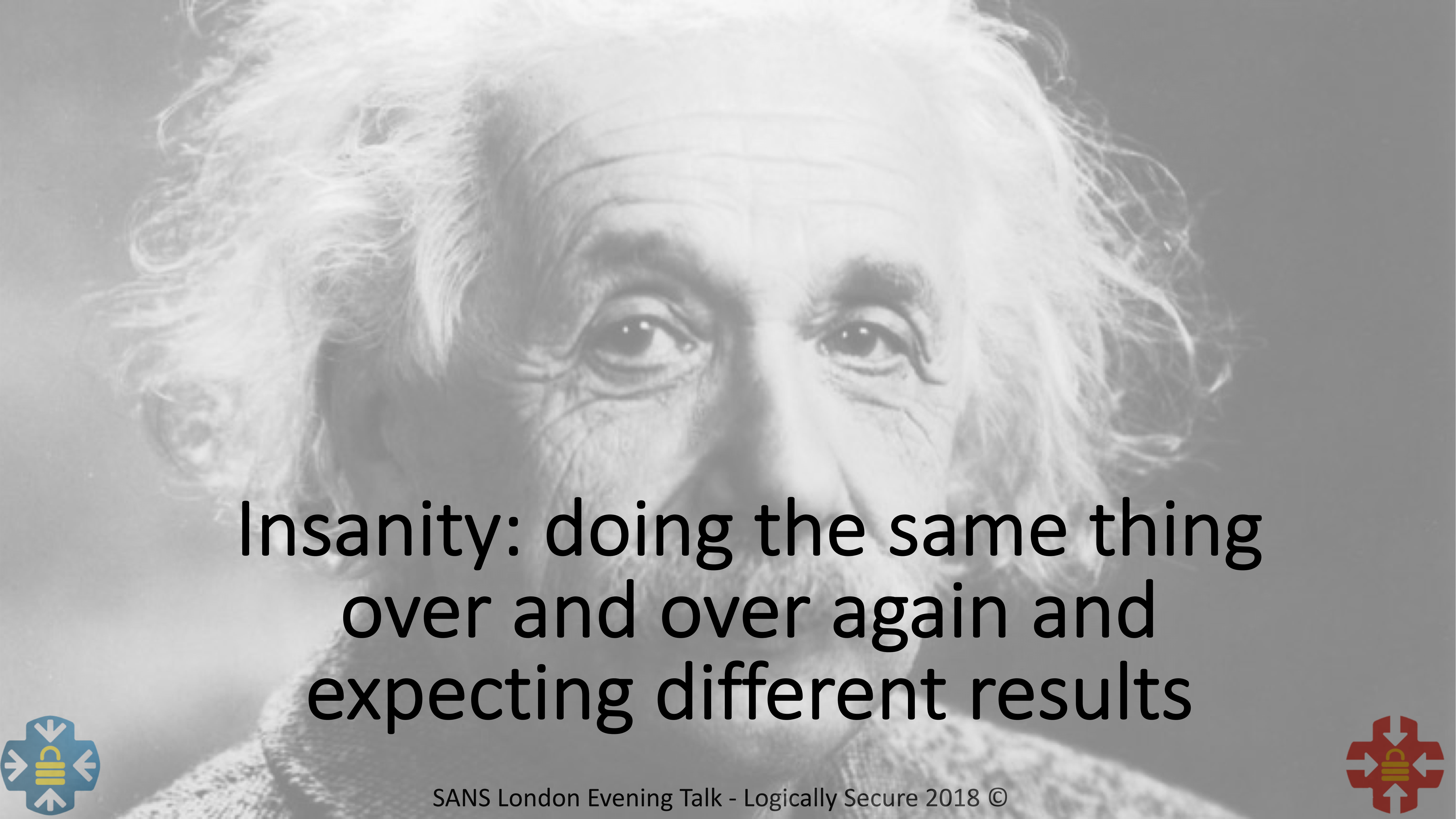
Google what to do

Send multiple emails on subject

Wipe suspect system

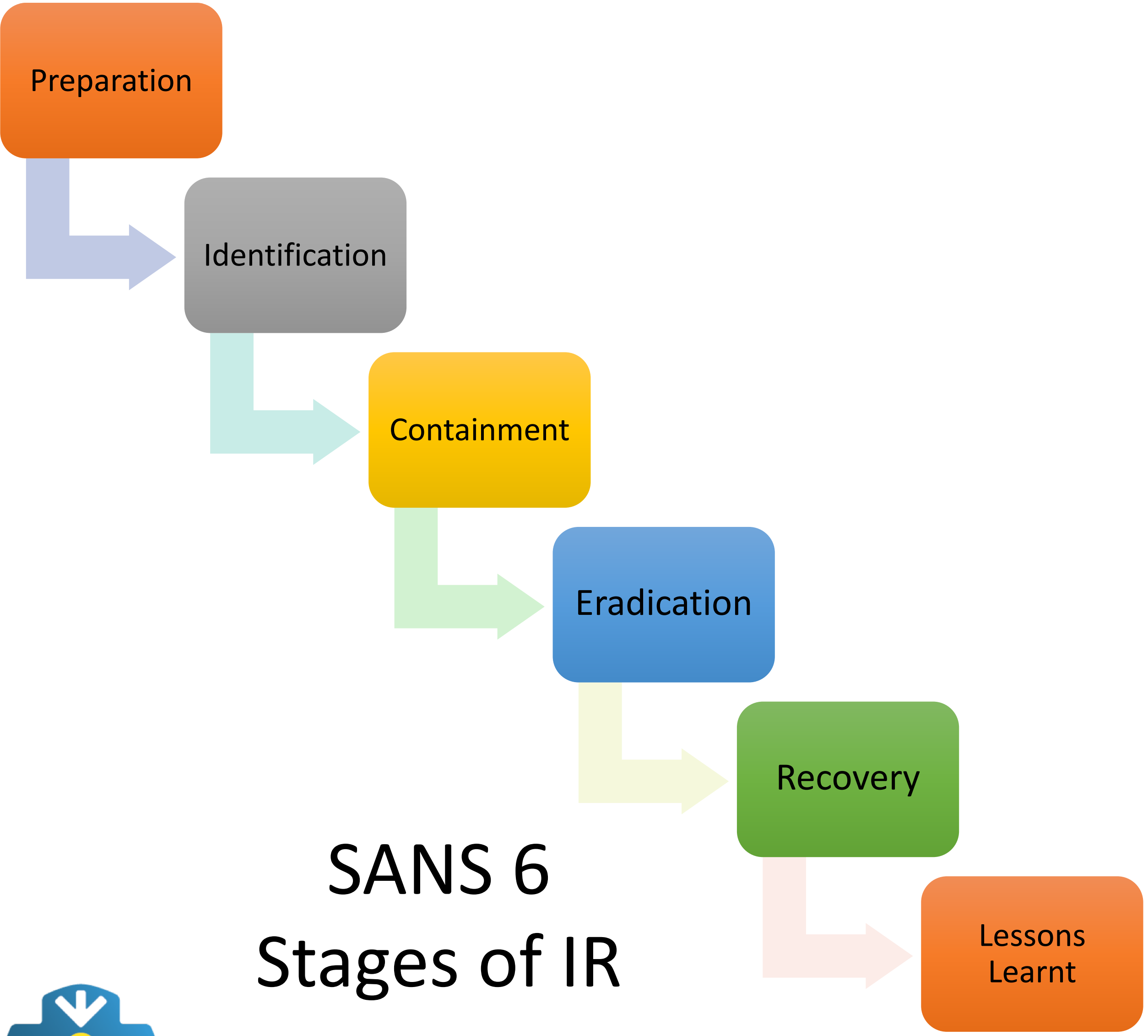
Tell execs all dealt with

Hope it doesn't happen again



Insanity: doing the same thing over and over again and expecting different results

Common textbook Stages of IR



Preparation

Identification

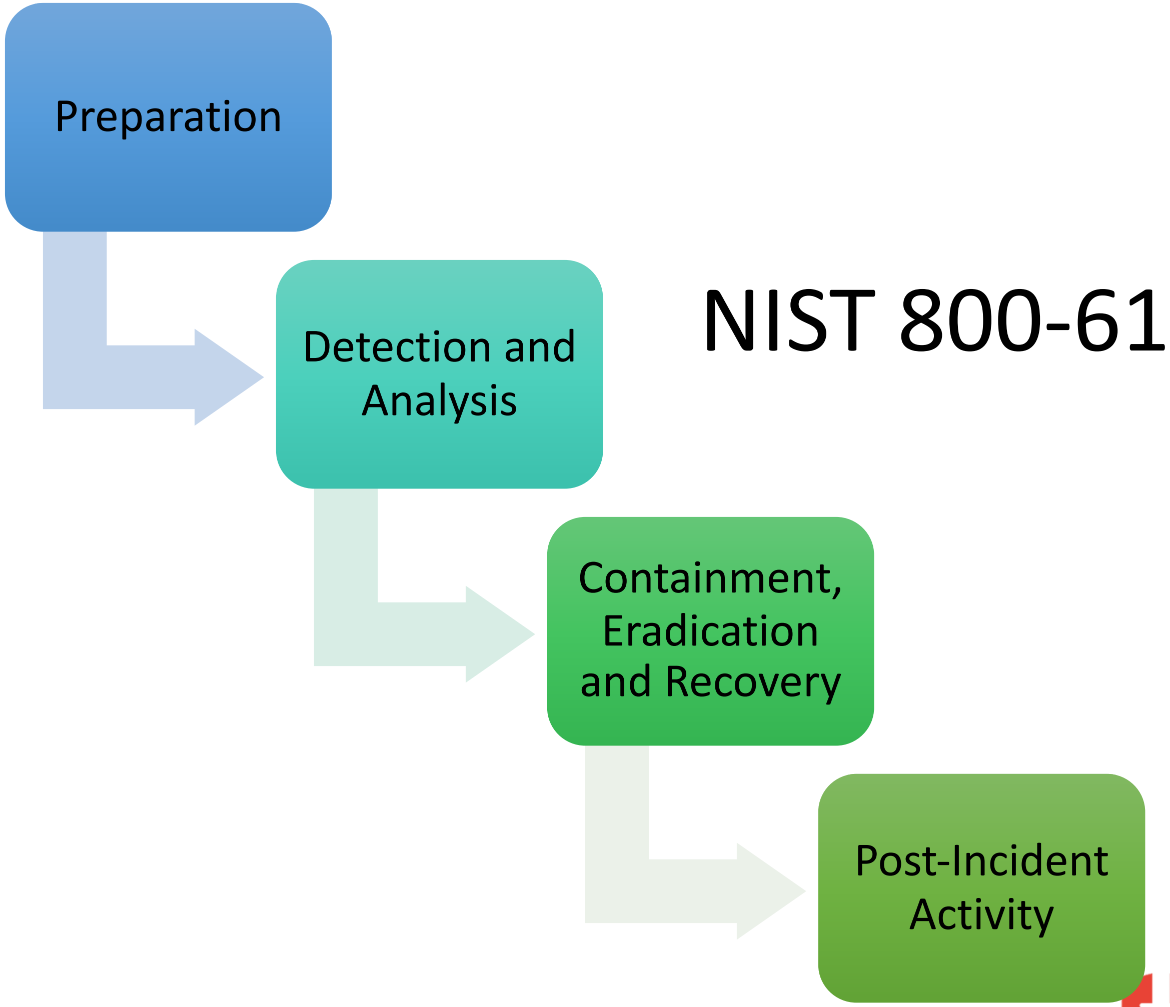
Containment

Eradication

Recovery

Lessons Learnt

SANS 6 Stages of IR



Preparation

Detection and Analysis

Containment, Eradication and Recovery

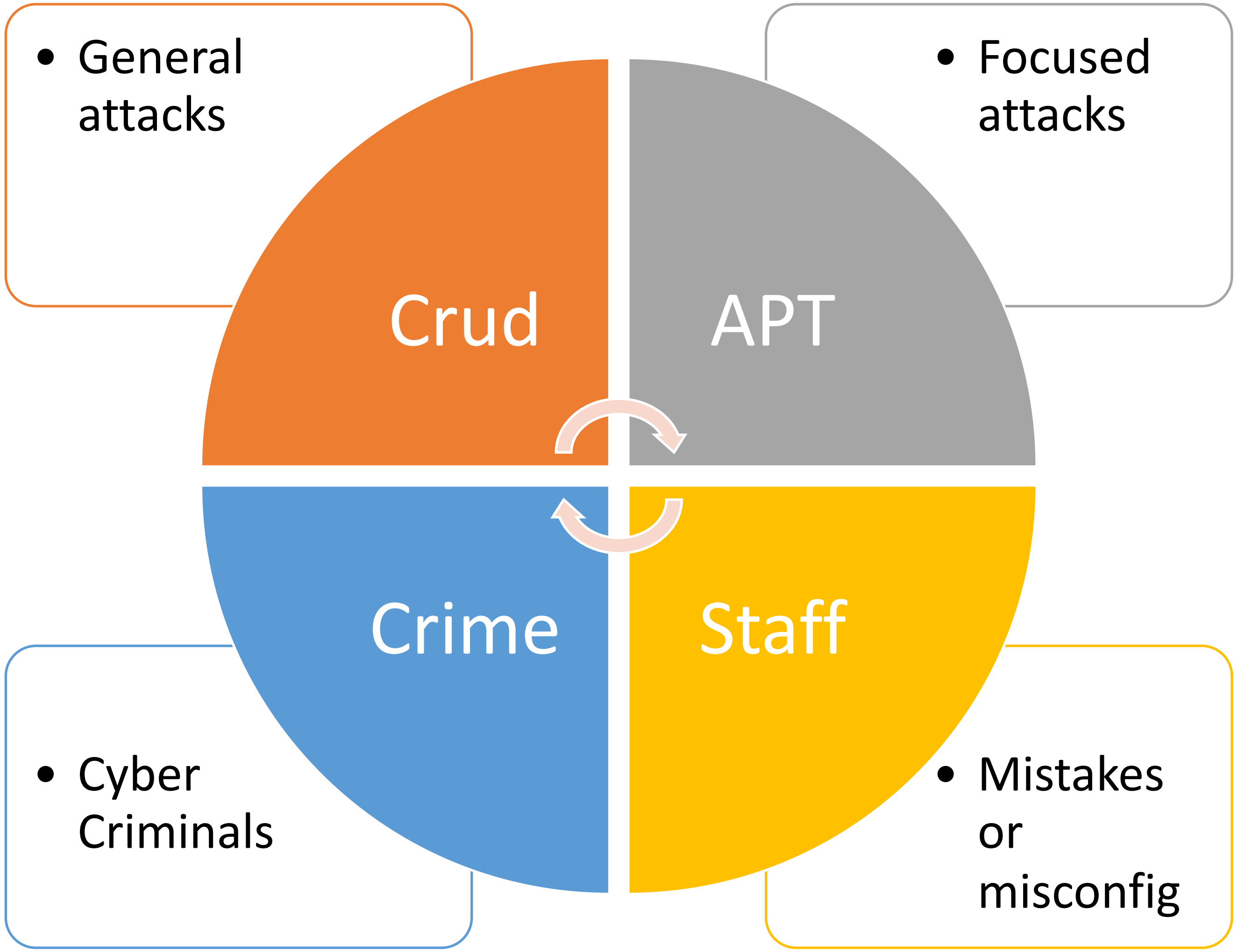
Post-Incident Activity

NIST 800-61

https://www.sans.org/course/hacker-techniques-exploits-incident-handling

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Incidents types (not to scale)



- General attacks

- Focused attacks

Crud

APT

Crime

Staff

- Cyber Criminals

- Mistakes or misconfig

Which ones are important?

- How do you communicate this difference of importance?
- How do the executives tell you which ones are important to them?

Image from http://dilbert.com/

You both need to understand the business and your mission

What is this talk actually about?

Well, you know when your network is hosed……..

- *This talk is about options to evict the bad guy*
- *It's about you taking back your network*
- *It's about giving you choices and options*
- *It's about trying different strategies to see what works*

- ***It's about putting together a UFP…….***

Not The UFP: ***No it’s an***

?

Un

Fuck

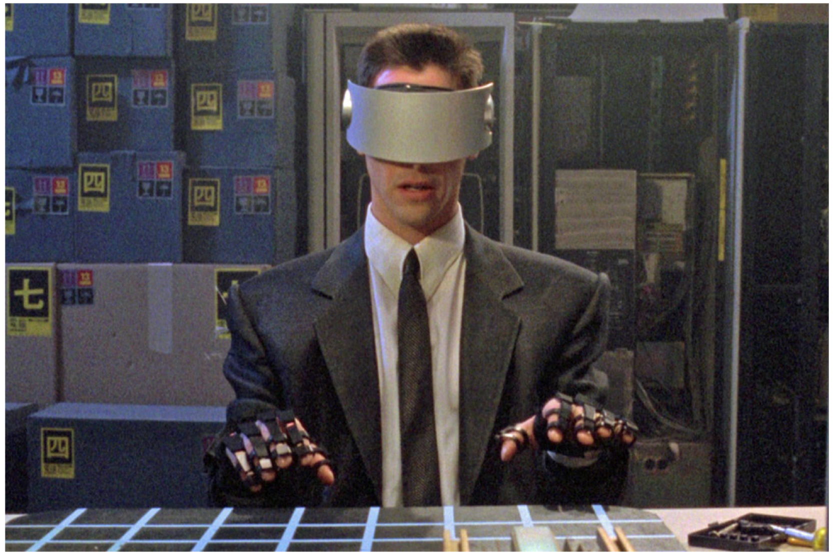
Plan

The Execs this the attackers look like:

“Them”

They think we look like:

“US”



When in fact is could be more like:

“Them”

https://www.rt.com/usa/164964-chinese-military-hacking-aerospace-industry/

But we are sometime still like:

So why do we care who is doing what?

- We should understand the adversary and their goal
  - So we can plan remediation events appropriately (more on this shortly)
- We should not assume we are better than the attackers
  - Don’t have a false sense of security
- We should respect the adversary
  - They are in most cases better equipped, better resourced, better informed
  - We should assume they are better skilled – this is important when talking to executives

Don’t them stupid script kiddies; they beat you!

A Maryland man linked to the notorious hacking groups Lizard Squad and PoodleCorp has pleaded guilty to running a "hacking-for-hire" service that plagued companies worldwide and harassing thousands of people. Zachary Buchta, 20, pleaded guilty to one count of conspiracy to commit damage to protected computers in a federal court in Chicago on Tuesday (19 December).

In his plea agreement, he also admitted to being a founding member of the hacker groups Lizard Squad and PoodleCorp that charged a $20 (£15) fee to target anyone for online harassment.

Ryan Cleary, 21, of Wickford, Essex, previously admitted joining the hack attacks, and is currently awaiting sentencing.

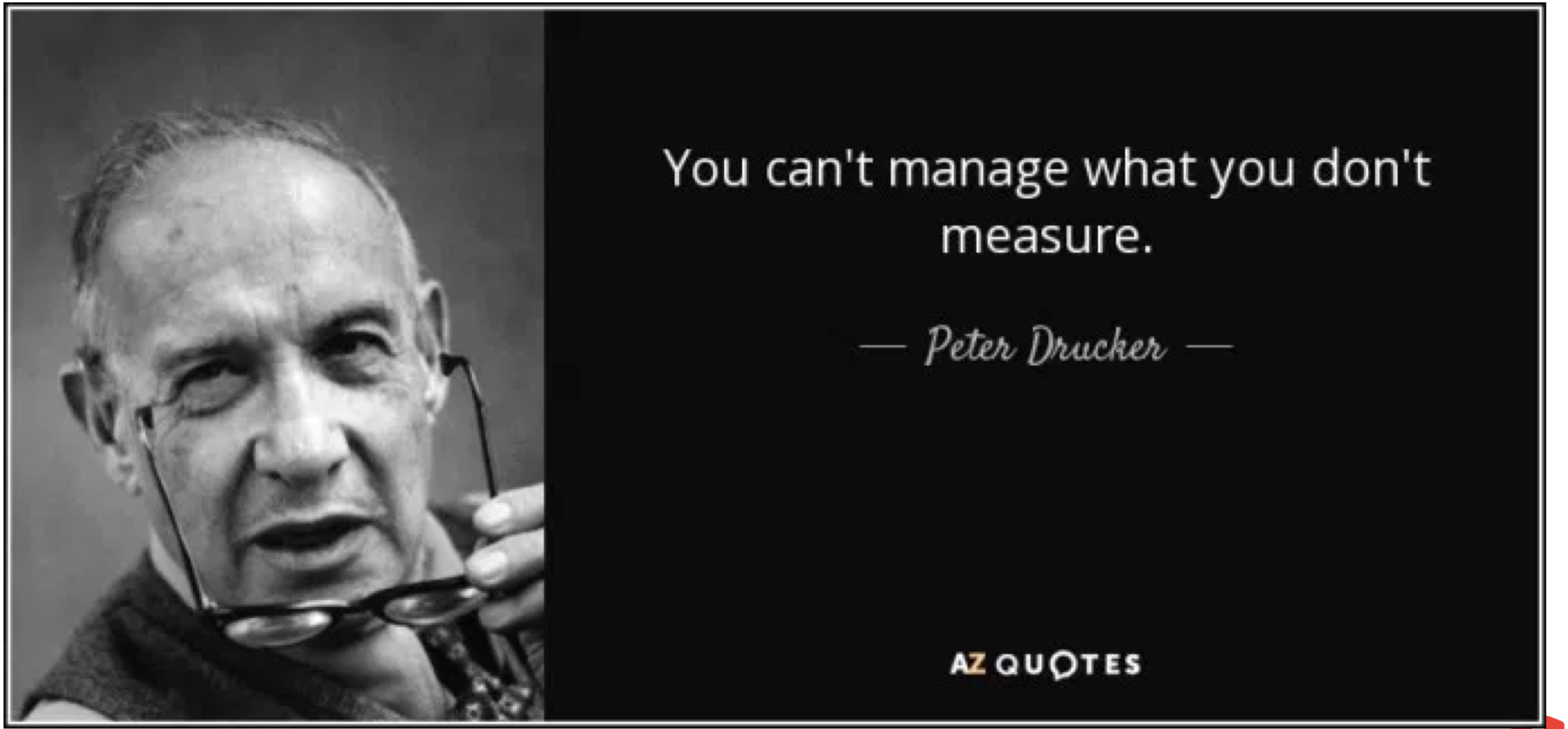
© Anthony Devlin/PA Wire

In January, noted security journalist Brian Krebs laid out evidence that pointed to a 20-year-old New Jersey resident as being responsible for the Mirai botnet.

ONE DOES NOT SIMPLY
IMPROVE ONE'S IR CAPABILITY
imgflip.com

If we want to improve we should

- Know what we need to improve
  - Not why we want to improve that area
- Know why we need to improve that aspect
  - how the organisation will benefit
- Know what results will look like
  - So we can tell if we are having an effect and what
- Know when we have achieved our target improvement
  - So we can declare the improvement goal as achieved



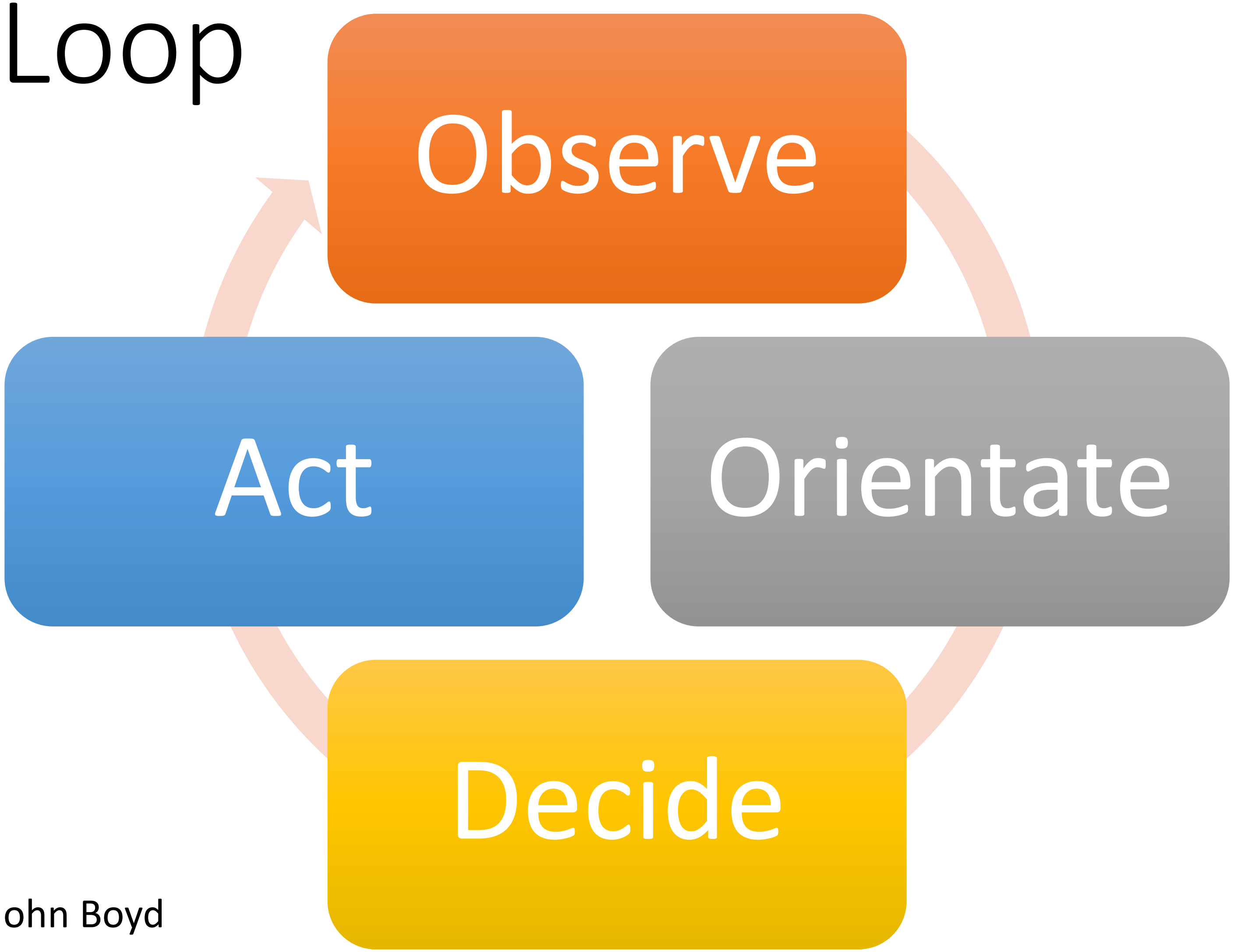
You can't manage what you don't measure.

— Peter Drucker —

Remediation Options

One size doesn’t necessarily fit all

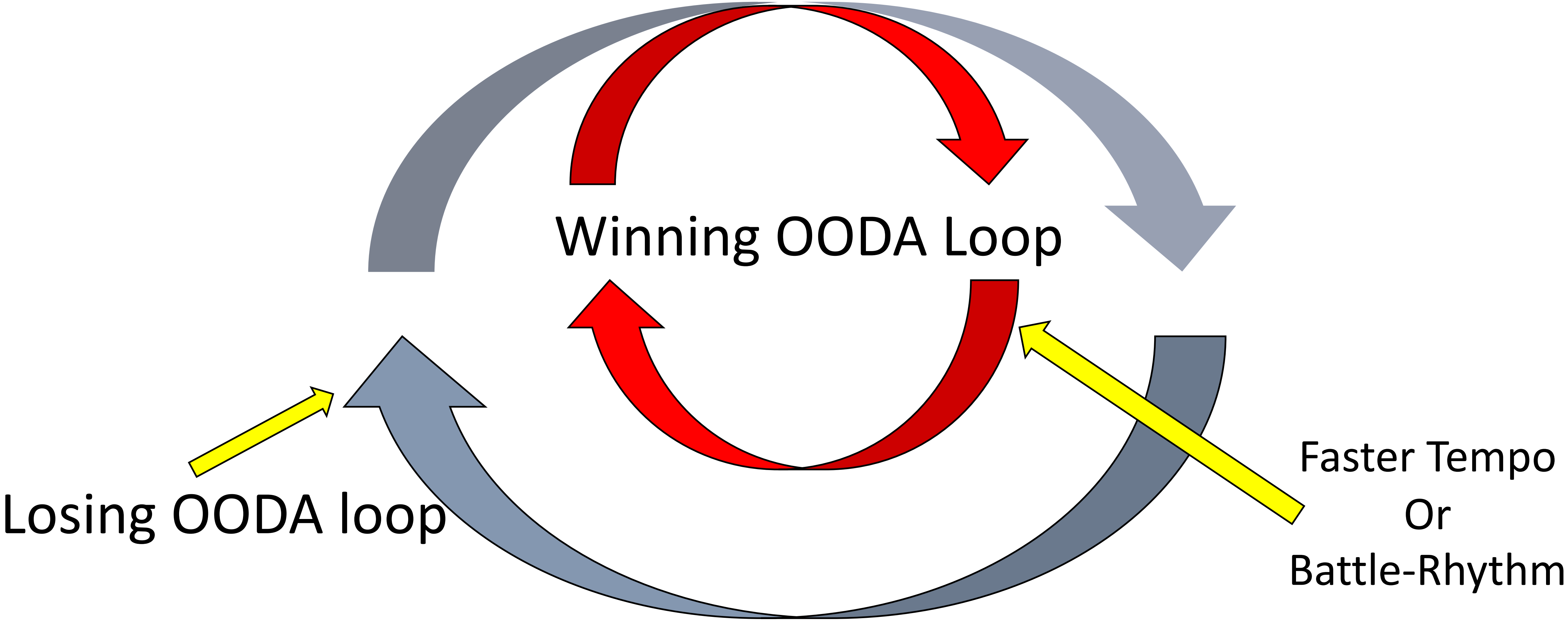
The OODA Loop



- O - Observe
- O - Orientate
- D - Decide
- A - Act

- Attributed to U.S.A.F. Colonel John Boyd

Out thinking the opponent



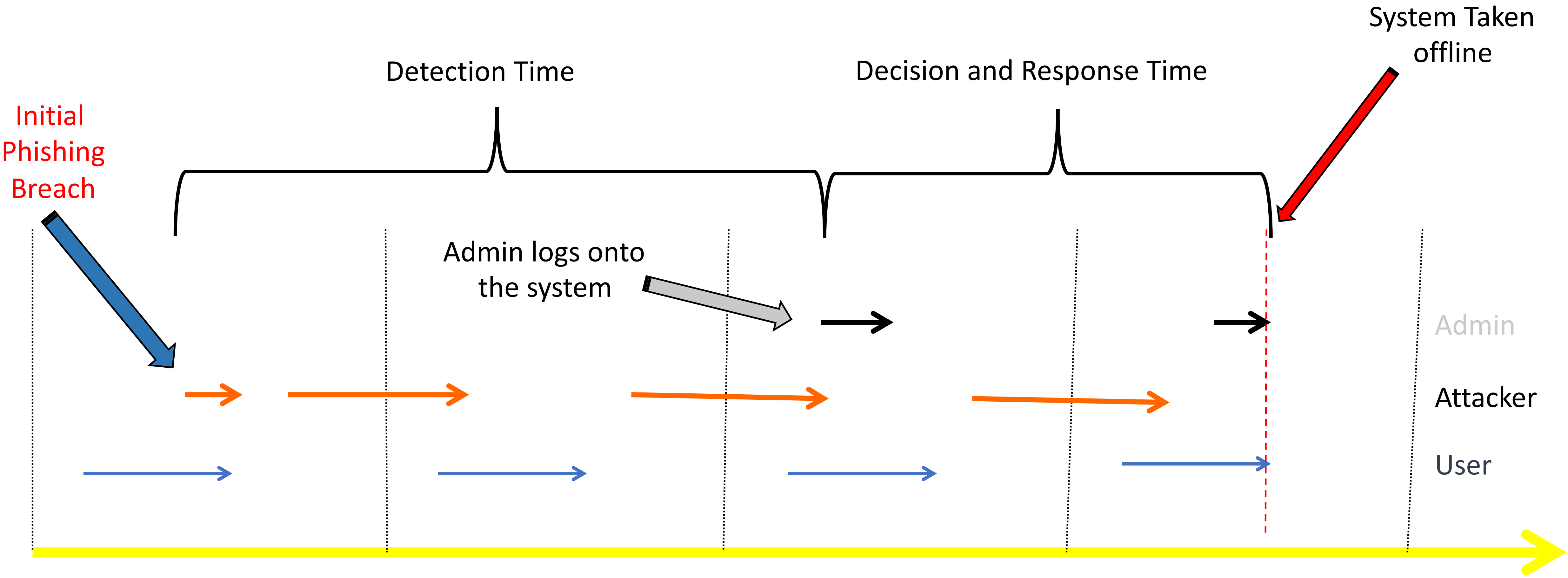
Winning OODA Loop

Losing OODA loop

Faster Tempo
Or
Battle-Rhythm

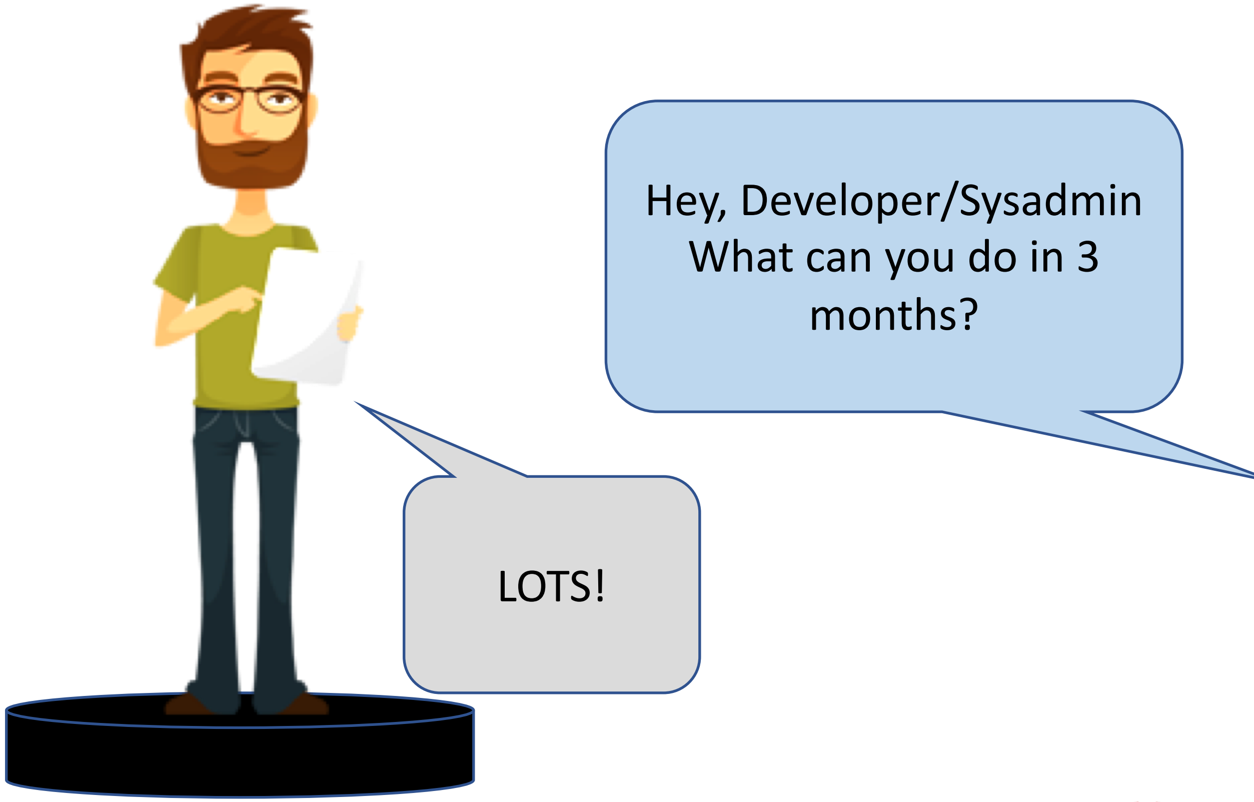
Chuck is 78 years old
who here would fight him? Why not?

Telegraphing your response


System Taken offline
Detection Time
Decision and Response Time
Initial Phishing Breach
Admin logs onto the system
Admin
Attacker
User

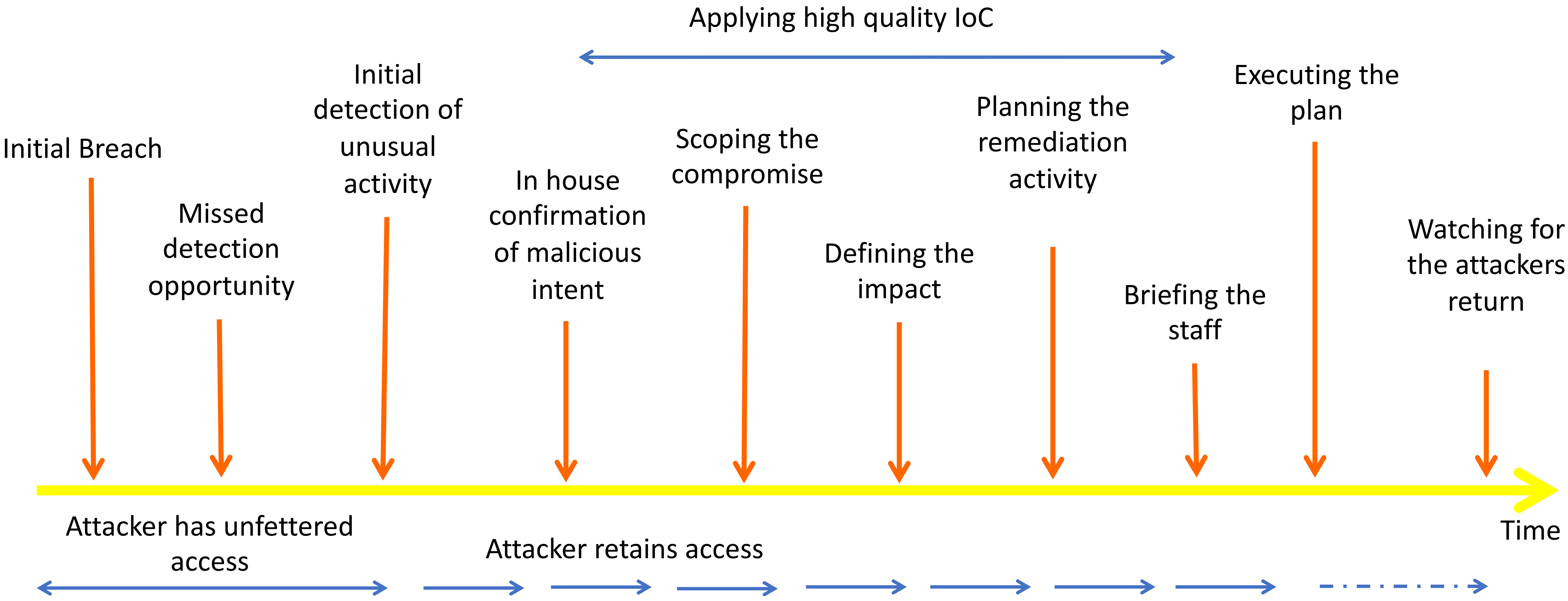
Trends in detection (Mandiant data)

- The time from breach to detection:
- 2011 – 416 days
- 2012 – 243 days
- 2013 – 229 days
- 2014 – 205 days
- 2015 – 146 days
- **2016 – 99 days**



Latest edition:
https://www2.fireeye.com/rs/848-DID-242/images/Mtrends2016.pdf

A textbook ‘normal’ incident (timeline not to scale)



Applying high quality IoC

Initial Breach

Missed detection opportunity

Initial detection of unusual activity

In house confirmation of malicious intent

Scoping the compromise

Defining the impact

Planning the remediation activity

Briefing the staff

Executing the plan

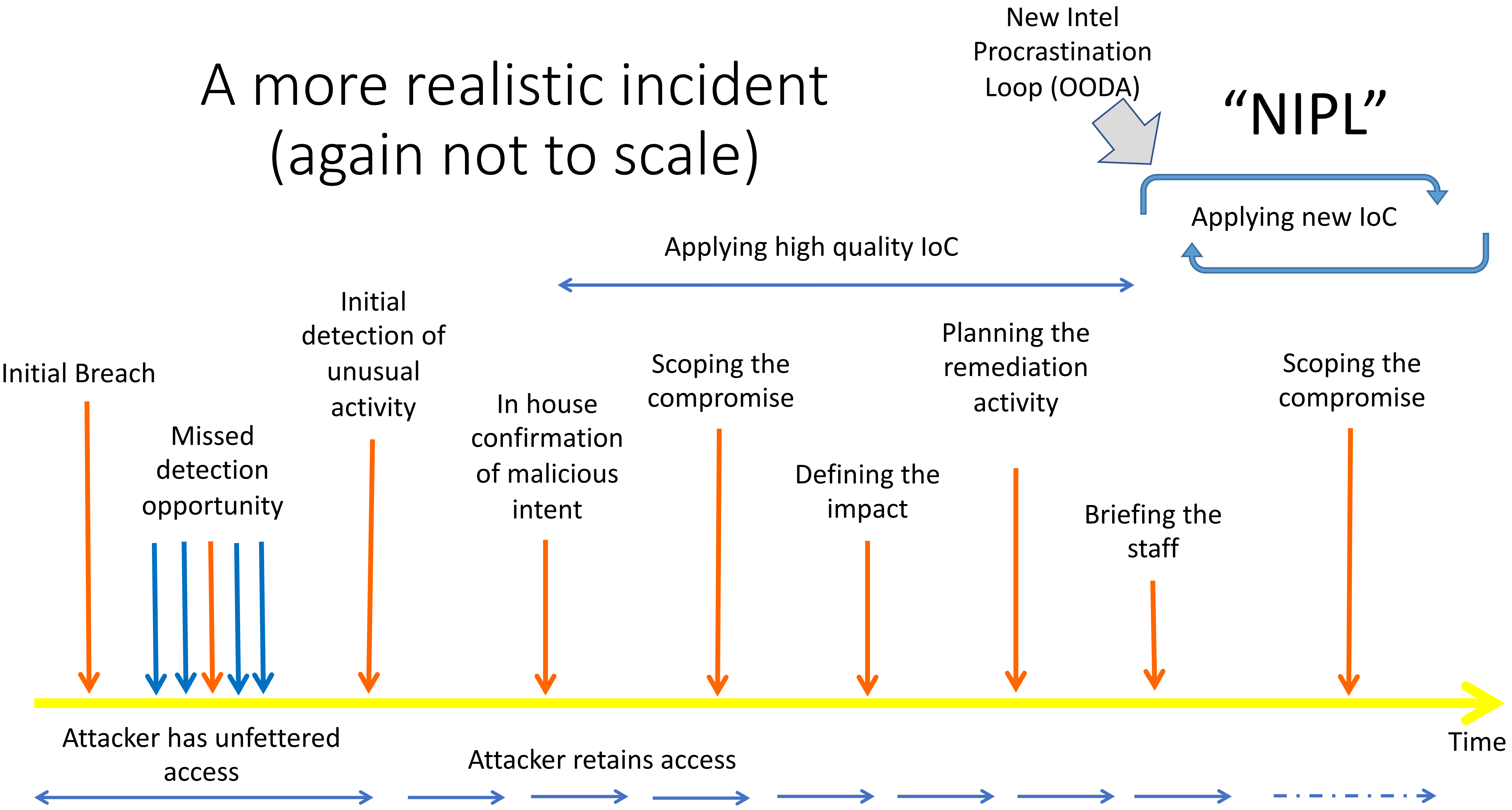
Watching for the attackers return

Attacker has unfettered access

Attacker retains access

Time

A more realistic incident (again not to scale)



New Intel Procrastination Loop (OODA)

"NIPL"

Applying new IoC

Applying high quality IoC

Initial Breach

Missed detection opportunity

Initial detection of unusual activity

In house confirmation of malicious intent

Scoping the compromise

Defining the impact

Planning the remediation activity

Briefing the staff

Scoping the compromise

Attacker has unfettered access

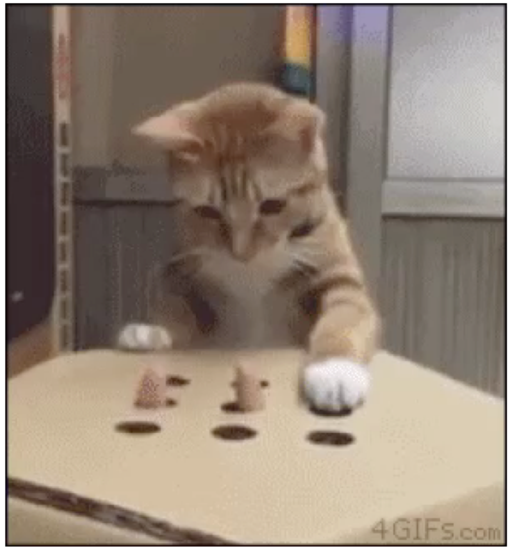
Attacker retains access

Time

What response do you do?

Wait, what, there are options??????

Operational Instant Clean-up (Whack-a-Mole - WAM)



- Favoured by Execs and Ops as "We are doing something!"
- Ok for non targeted attacks:
  - non APT or drive-by-common malware or Trojans from p2p sites
  - Off-the-shelf generic Cyber Criminal financial based fraud
- Questions to ask execs:
  - What are you trying to achieve? You are only treating the symptoms!
  - If this doesn't work immediately how long are you prepared to carry on rebuilding kit?
  - If you blow away the systems how will we learn about the attack vectors?
  - ***Crude Question: When your dog craps in the house you say nothing and clean it up?***
- IR Staff Aim: DO NOT LET WAM BECOME THE BUSINESS AS USUAL (BAU) RESPONSE PROCESS

Mass Simultaneous System Remediation (MSSR)

- The is favoured by many of the large IR companies
  - "It offers many the best chance of cleaning out the attacker"

- 'Simple' concept – identify all the systems, all the C2 and all the compromised accounts

- On a selected date conduct a mass simultaneous unplug of systems, reset of accounts and blocking of all C2 (all must be complete in a matter of hours)
- Conducted during attacker down-time to maximise impact

Difficulties with MSSR

- The work effort required can be huge
- The OPSEC needed to protect the plans gets difficult the bigger the size of the compromise
- If you miss one system…… The attacker will slip back in
- Requires that you can monitor the HTTP/HTTPS/DNS/P2P traffic to spot all the systems
- The systems have to be more secure or the entire plan is folly

Execs and MSSR

- If your OODA is big & your Execs are worried by collateral damage or they get timid legal advisors in to ‘assist’, you will get stuck in the New Intel Procrastination loop (NIPL)
- Meanwhile they have to watch the attacker gain ground
- This can be weeks or even months in the planning stages

New Infrastructure (Rebuild)

- There are times when a new build is warranted however:
  - Unless you change admin and user behaviour you will revert to type very soon
  - Where are you building it from?
  - Who's building it? The same admins? Same PWs?
  - What is different to the current network?
  - Are the plans for the new network secure?
  - How much will this cost and how long will it take?
  - What happens in the meantime?

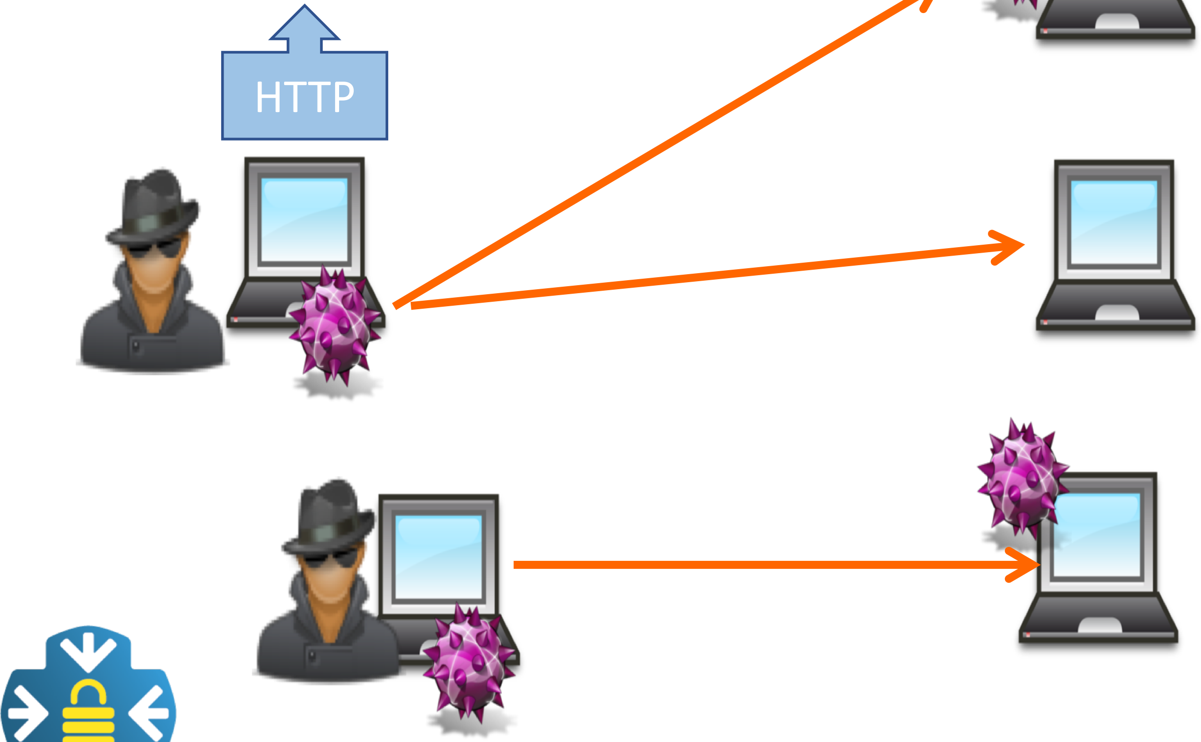
Sector Synchronized Isolation and Cleanup (SSIC)

- This is a mini remediation that can be stealthy deployed to geographical sites
- The aim is to conduct a clean up that looks like a site upgrade
  - Great to get people of old servers and old desktops too
  - Doesn’t burn the Intel as the attacker assumes you are doing updates etc
- Works well if you are improving security a site at a time and keep the attacker out of the site once the update/SSIC is completed

Hostile Asset Recovery Method (HARM)

- Out running the attacker – possible in the early stages of a compromise
  - Must be a small beachhead of about 50 systems max
- Works on premise that attacker needs to attack a system with valid creds and from a compromised system
- Defenders MUST HAVE V TIGHT OODA with awesome monitoring
- Defenders must know the TTP of the attacker and understand all possible C2

Hostile Asset Recovery Method (HARM)



- All systems are pulled immediately
- All malware hashes blocked at boundary and on local systems
- All systems reporting that malware are pulled
- All accounts on all machines are reset (all of them regardless of when used)
- All C2 IPs/DNS/HTTP elements blocked
- In this scenario the attacker tried to get three machines but loses them and the two he came from

Issues with Hostile Asset Recovery Method (HARM)

- Out running the is hard work for the IT staff
- This is most effective when compromised systems are distributed across the enterprise (otherwise the SSIC is the better method)
- You need spare systems to reduce the server downtime and the user outages as systems are rebuilt
- Your IT department staff (not the execs will hate you)
- You need to set deadlines to review this – as it hurts (and costs large)

Summary of Remediation's options

Its nice to have options, but in reality circumstances (execs) will dictate the chosen route – but don't be afraid to reassess your options and choice

- Operational Instant Clean-up or Whack-a-Mole (WAM)
- Mass Simultaneous System Remediation (MSSR)
- New Infrastructure (Rebuild)
- Sector Synchronized Isolation and Cleanup (SSIC)
- Hostile Asset Recovery Method (HARM)

For all remediation events remember

- You are burning high quality Intel – so chose when to do this
- The attacker knows, that you know, about his C2 methods, malware and malicious IPs; thus they can work out how you know too
- Once you have remediated – share the Intel as its value to you is reduced

Briefing the Execs

1. It’s simple – treat them like kids
2. Don’t surprise them and don’t scare them (unless you need to)
3. Give them something to focus on and give them options to decide over so they feel they have had input
4. Trust takes time to build between IR Staff and Execs
   - Remember that not staff mesh well!

Simple way to explain an incident

- Given to me by a C-level executive of a huge company

1. Tell them what has happened
   - What the attacker did
2. Tell them what is happening now
   - What your team are doing about it now (from detection to ½ to next meeting)
3. Tell them what is happening next
   - What the team are doing after 2 as you will be mid way through this for the next briefing

At subsequent briefings

1. Tell them what has happened
   - What you have detected the attacker doing since the last brief
   - What you have done since the last meeting
     - a summary of findings and results from previous briefings steps 2 & 3
2. Tell them what is happening now
   - What your team are doing now
3. Tell them what is happening next

But what if your IR is not fast enough?

How can you improve something as big as IR?

Metrics to understand IR

How do you measure it?

By infections, by compromises, staff head count, laptops protected, malware analysed, blogs read, courses attended?

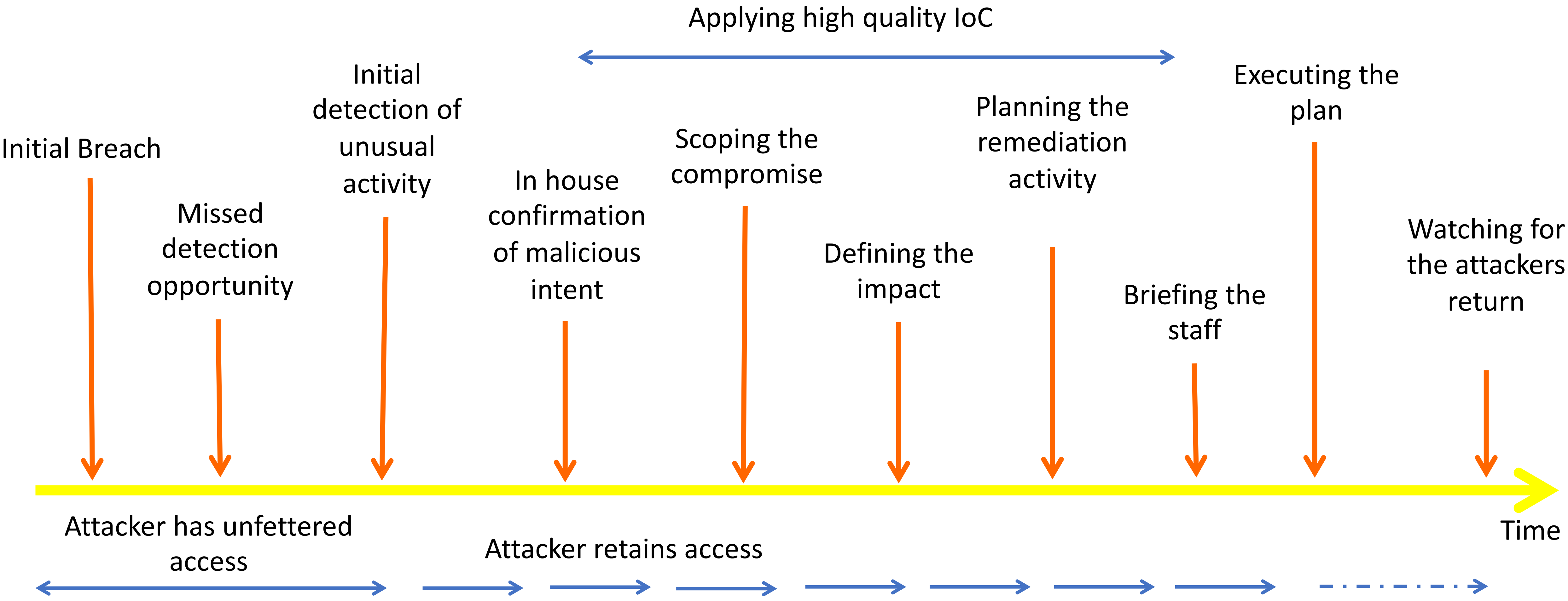
Lets think about events that we can timestamp

- Time/Date hacked
- Time/Date alerted to breach
- Time/Date execs briefed
- Time/Date GDPR notification made
- Time/Date logs gathered
- Time/Date investigation started
- Time/Date Press informed
- Time/Date Users informed
- Time/Date cleanup started
- Time/Date cleanup planned
- Time/Date cleanup completed
- Time/Date malware detected
- Time/Date malware recovered
- Time/Date malware analysed
- Time/Date malware IOC found
- Time/Date IOC deployed
- Time/Date mitigations completed

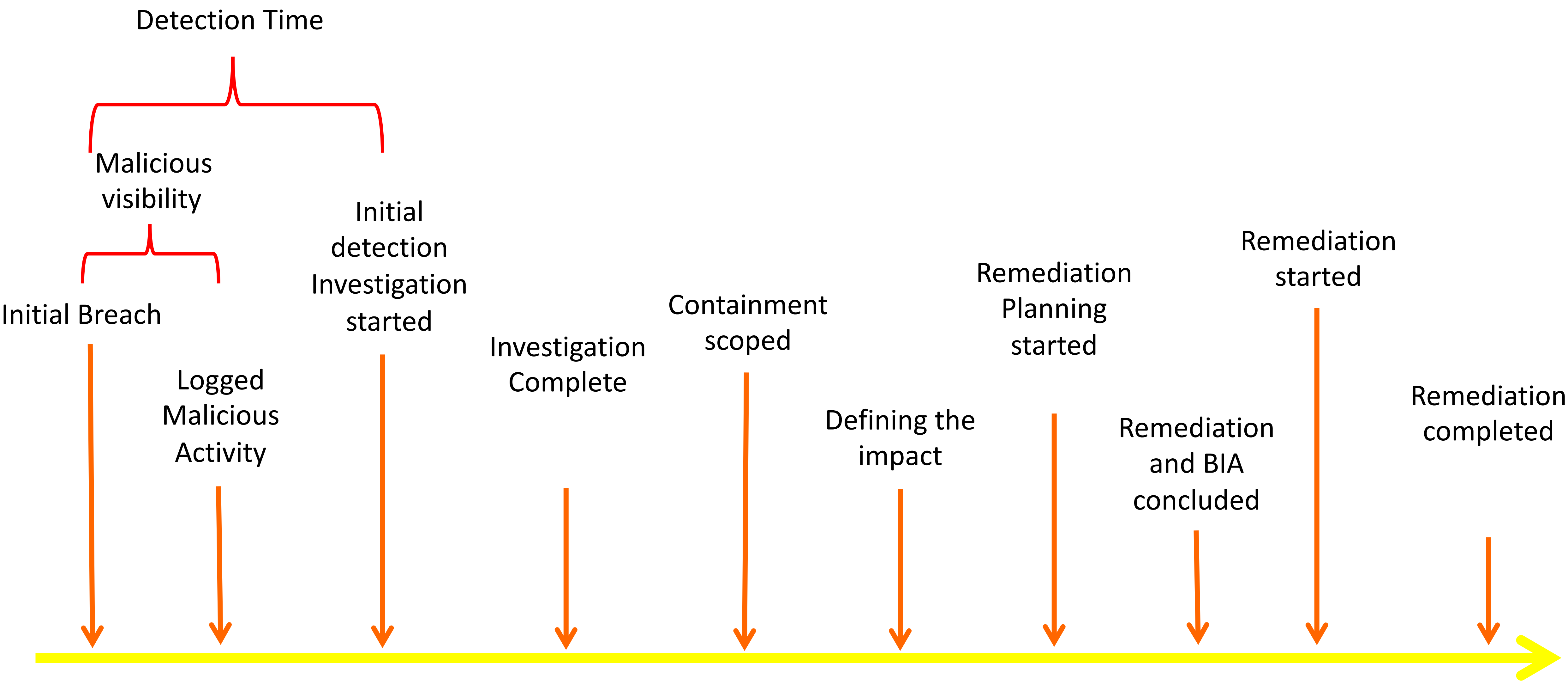
Which ones are useful:

- Time/Date hacked
- Time/Date alerted to breach
- Time/Date execs briefed
- Time/Date GDPR notification made
- Time/Date logs gathered
- Time/Date investigation started
- Time/Date Press informed
- Time/Date Users informed
- Time/Date cleanup started
- Time/Date cleanup planned
- Time/Date cleanup completed
- Time/Date malware detected
- Time/Date malware recovered
- Time/Date malware analysed
- Time/Date malware IOC found
- Time/Date IOC deployed
- Time/Date mitigations completed

Let’s look at this again


Applying high quality IoC
Initial Breach
Missed detection opportunity
Initial detection of unusual activity
In house confirmation of malicious intent
Scoping the compromise
Defining the impact
Planning the remediation activity
Briefing the staff
Executing the plan
Watching for the attackers return
Time
Attacker has unfettered access
Attacker retains access

I’ll change the headings



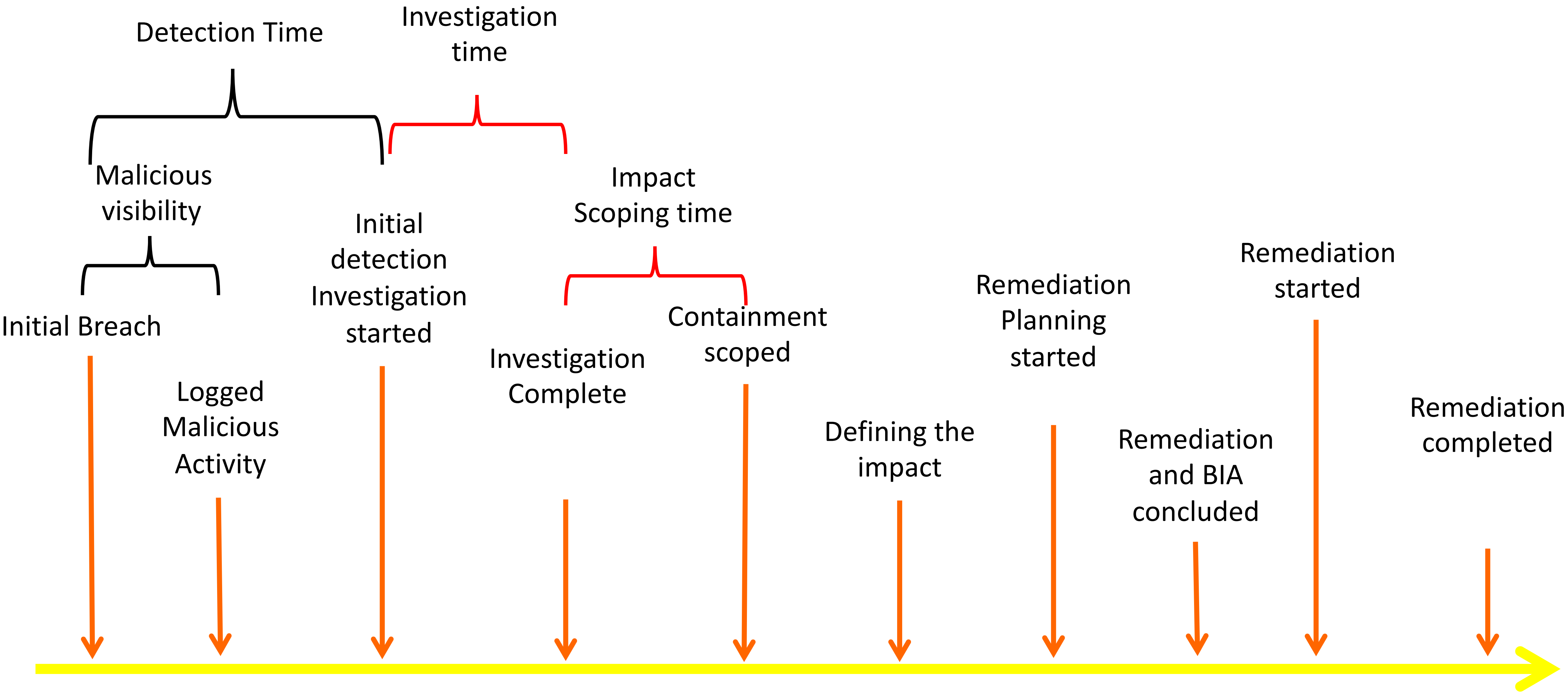
Malicious Visibility

- If you have poor visibility you will have more damage to your infrastructure before you detect anything bad

- High times for this are really expensive
- Shortening this will improve your Observer part of the OODA loop

Detection time

- The detection can only start when malicious activity has been logged somewhere
- Low levels of automation mean that detection does not happen based upon IOCs but from analyst assessing logs
- This introduces varying quality as different teams work at different rates "night shift syndrome"
- Reduce this through the use of IOC detection, watch-lists and other flags to staff that there is something worthy of a short initial investigation



Detection Time

Investigation time

Malicious visibility

Impact Scoping time

Initial Breach

Logged Malicious Activity

Initial detection Investigation started

Investigation Complete

Containment scoped

Defining the impact

Remediation Planning started

Remediation and BIA concluded

Remediation started

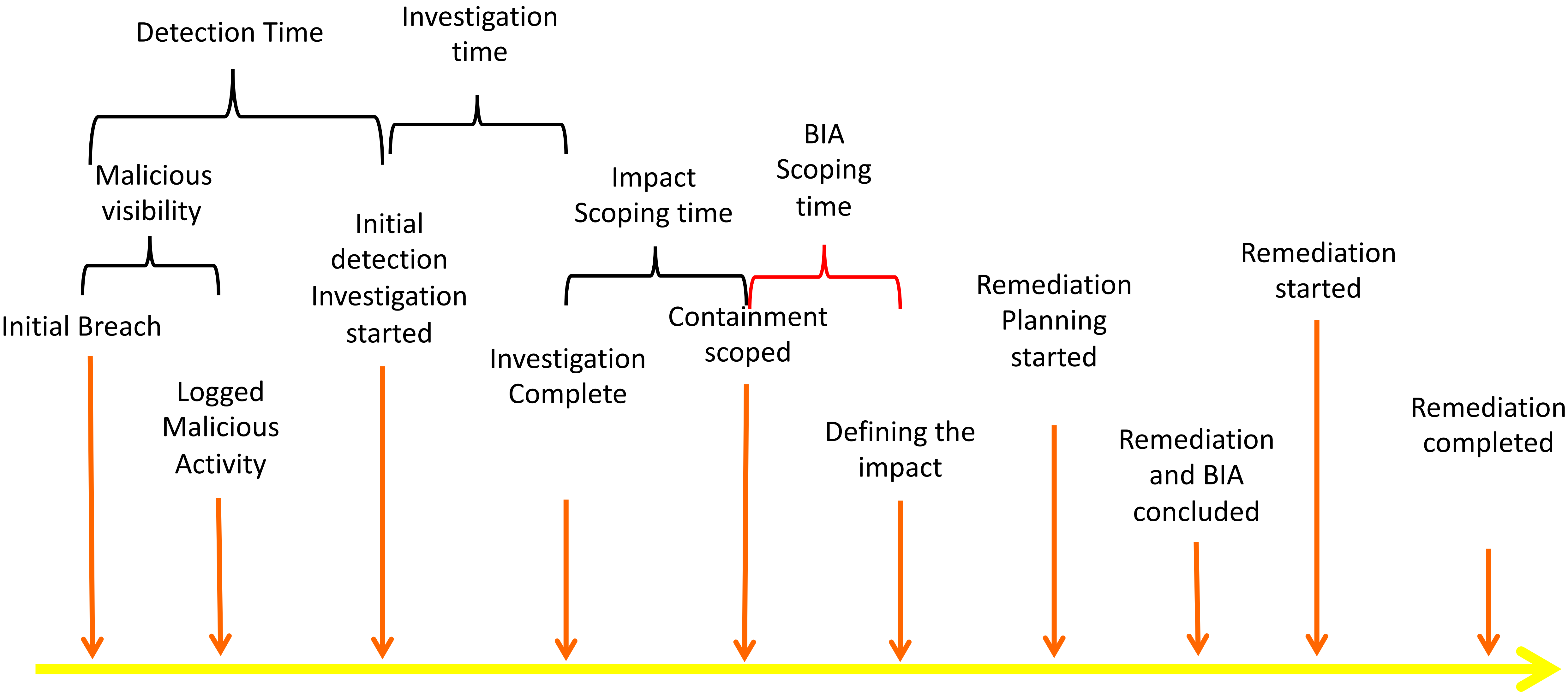
Remediation completed

Investigation time

- Well equipped teams can auto-process files, malware and triage things quickly
- A lack of log access, poor system visibility and poor support from IT staff and execs will delay the access to corroborating and investigation data
- Look to reduce this by getting more quality and coverage of logs to DFIR staff and give them the system access they need

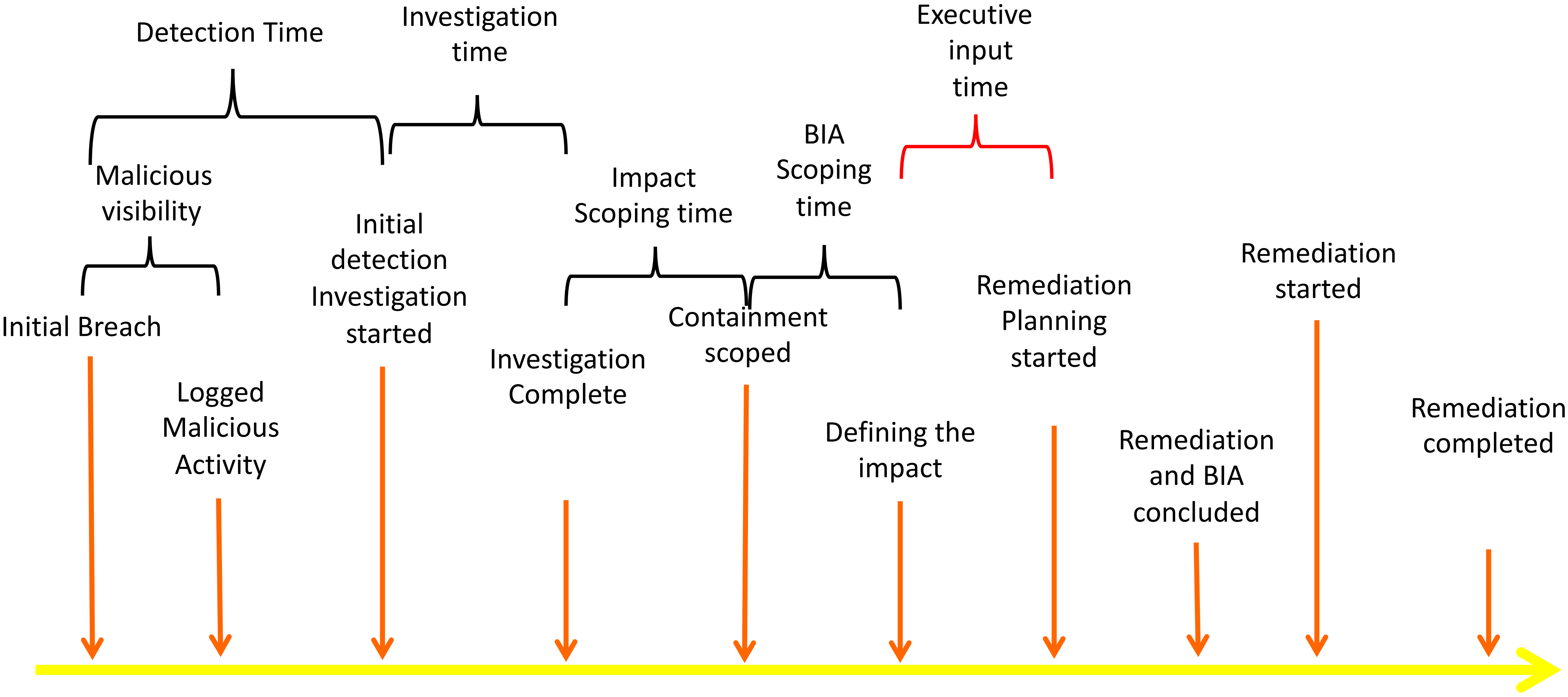
Impact Scoping time

- Understanding your network and the critical servers will reduce this
- Network visibility will improve this
- Enterprise wide ability to check for suspected IoC will improve this
- Efficient secure communications
- Enterprise wide IR response platform will improve this
- Sufficient staff to conduct the initial scope of the breach assessment
  - Lots of fast IR skills required
  - Network visibility will help reduce this time as detecting lateral movement is critical


Detection Time
Investigation time
Malicious visibility
Initial detection Investigation started
Impact Scoping time
BIA Scoping time
Initial Breach
Logged Malicious Activity
Investigation Complete
Containment scoped
Defining the impact
Remediation Planning started
Remediation and BIA concluded
Remediation started
Remediation completed

BIA Scoping time

- Better other Business Unit (BU) support will improve this
- Project manager support improves this
- Team experience and senior DFIR staff will improve this
  - People that speak more than tech
- Good secure enterprise communications
- Security aware and supportive staff in other BUs



Detection Time

Investigation time

Executive input time

Malicious visibility

Impact Scoping time

BIA Scoping time

Initial Breach

Logged Malicious Activity

Initial detection Investigation started

Investigation Complete

Containment scoped

Defining the impact

Remediation Planning started

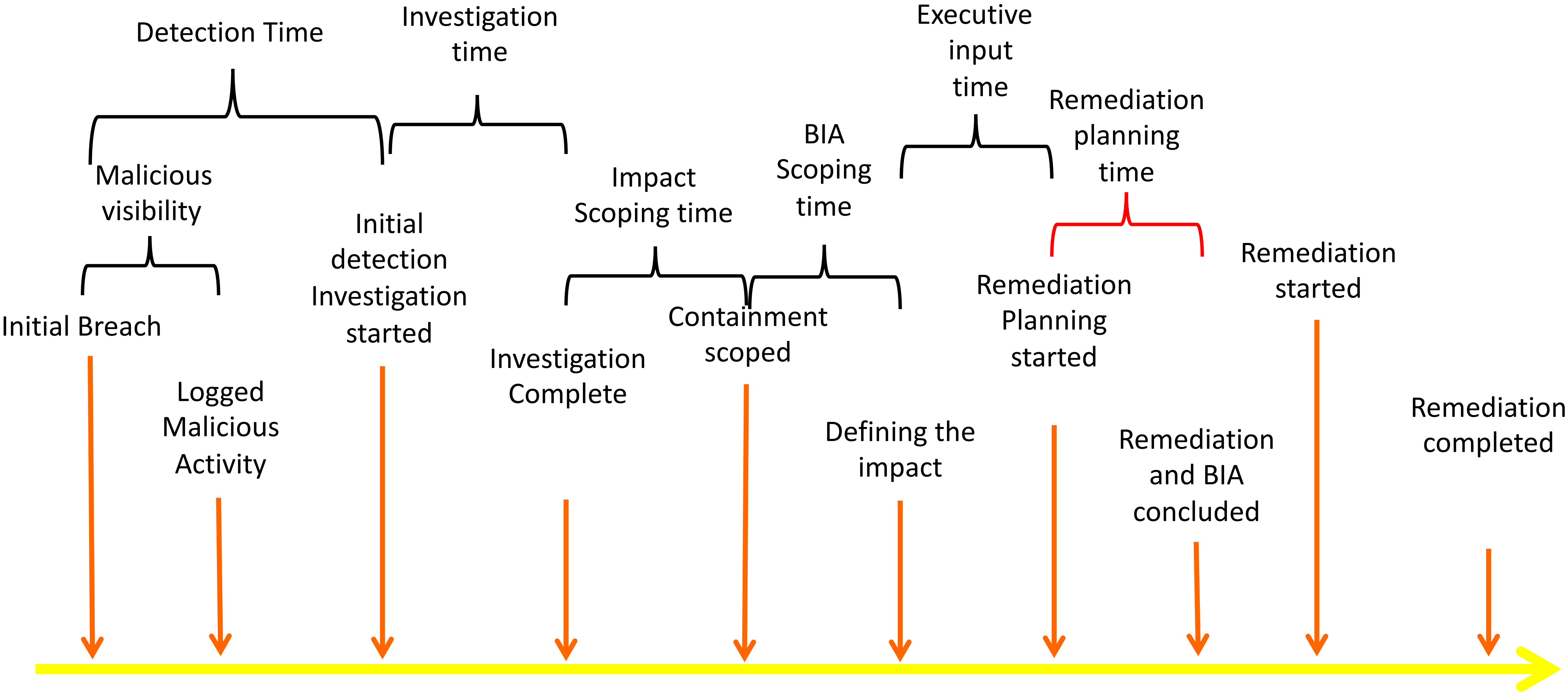
Remediation and BIA concluded

Remediation started

Remediation completed

Executive Input time

- Security experienced executives that are slightly technical will help
- Strong working relationship between C-levels and DFIR staff
- Good communications between DFIR and C-Levels
- Trust on both sides
- Clear and concise briefings from DFIR staff
- Plan of action proposed by the DFIR team
    - With options for C-Levels to assess and select based upon risk appetite



Detection Time

Investigation time

Malicious visibility

Initial Breach

Logged Malicious Activity

Initial detection Investigation started

Investigation Complete

Impact Scoping time

Containment scoped

BIA Scoping time

Defining the impact

Executive input time

Remediation Planning started

Remediation planning time

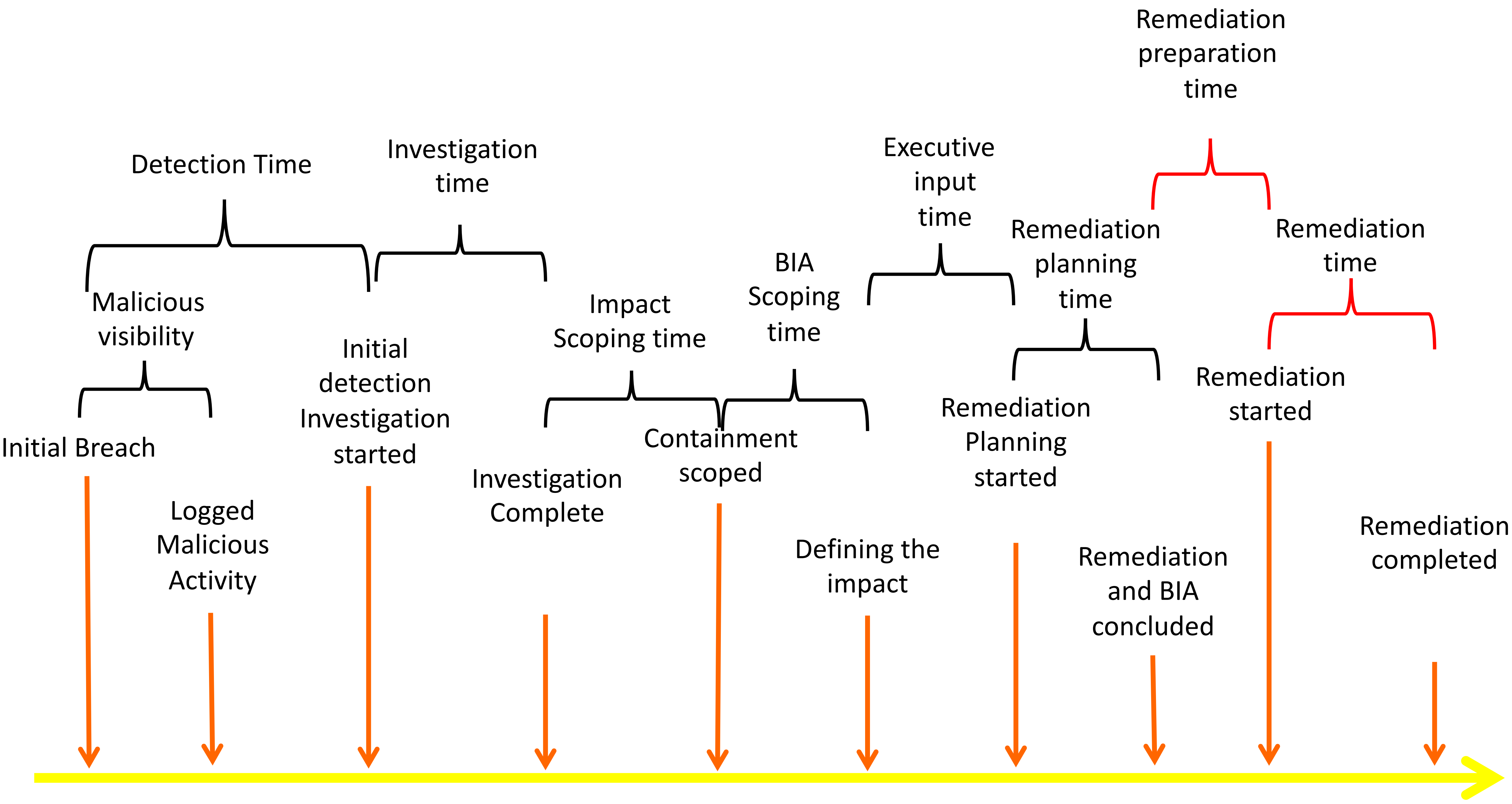
Remediation and BIA concluded

Remediation started

Remediation completed

Remediation planning time

- Understanding of the network
- Good BIA assessments
- Good IT support – IT dept that can rebuild systems fast
- Spare servers for new builds
- Spare secure laptops for admins to work from when other systems are compromised (the must not plan remediation from compromised systems)
- Good liaison between BU, IT and DFIR
- Plenty of staff and flexible overtime ☺



Remediation preparation time

Detection Time

Investigation time

Executive input time

Remediation planning time

Remediation time

BIA Scoping time

Impact Scoping time

Malicious visibility

Initial detection Investigation started

Initial Breach

Containment scoped

Remediation Planning started

Remediation started

Investigation Complete

Logged Malicious Activity

Defining the impact

Remediation and BIA concluded

Remediation completed

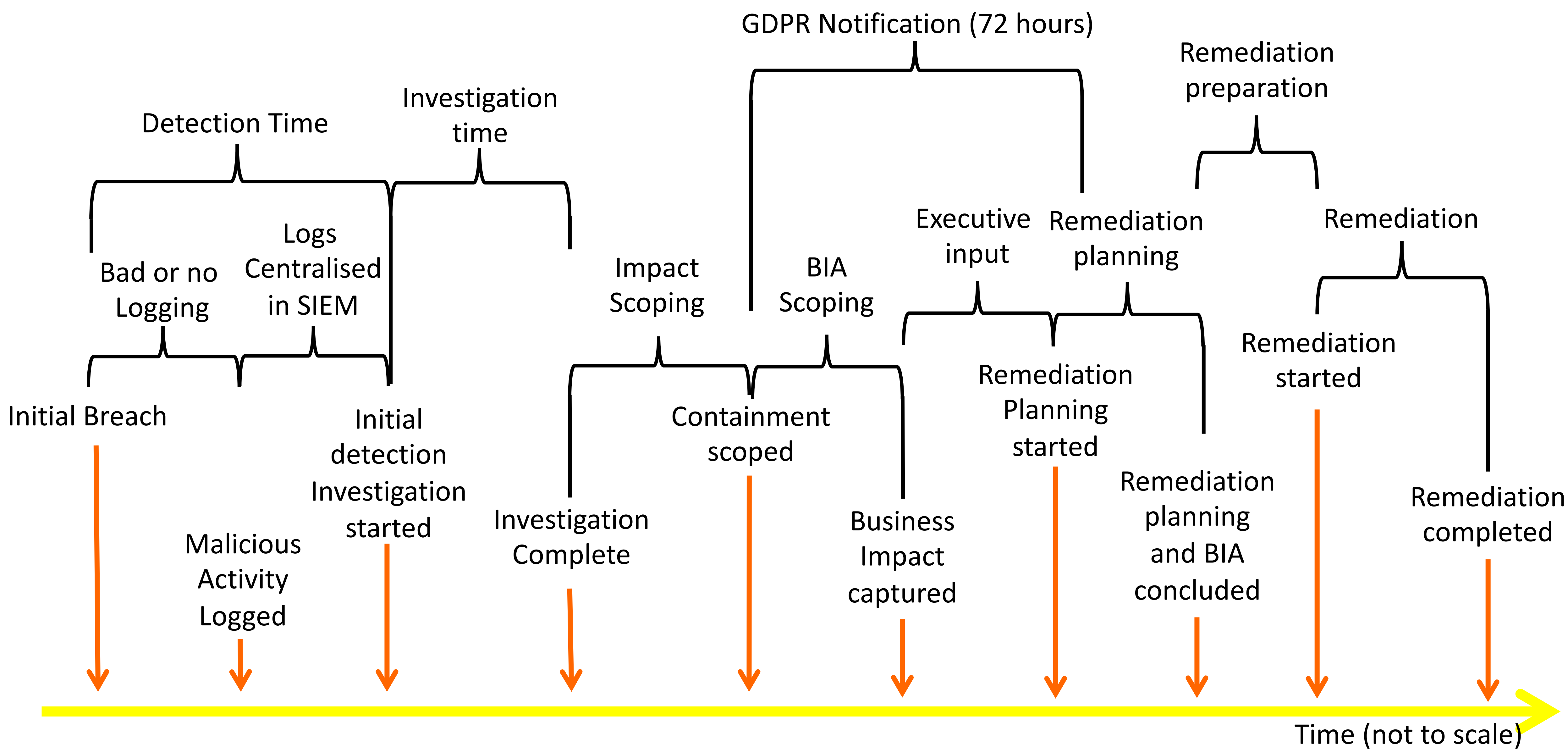
Remediation preparation time

- Building spare servers takes time and staff
- Briefing staff takes time
- Noting having to conduct massive upgrades improves this

Remediation time

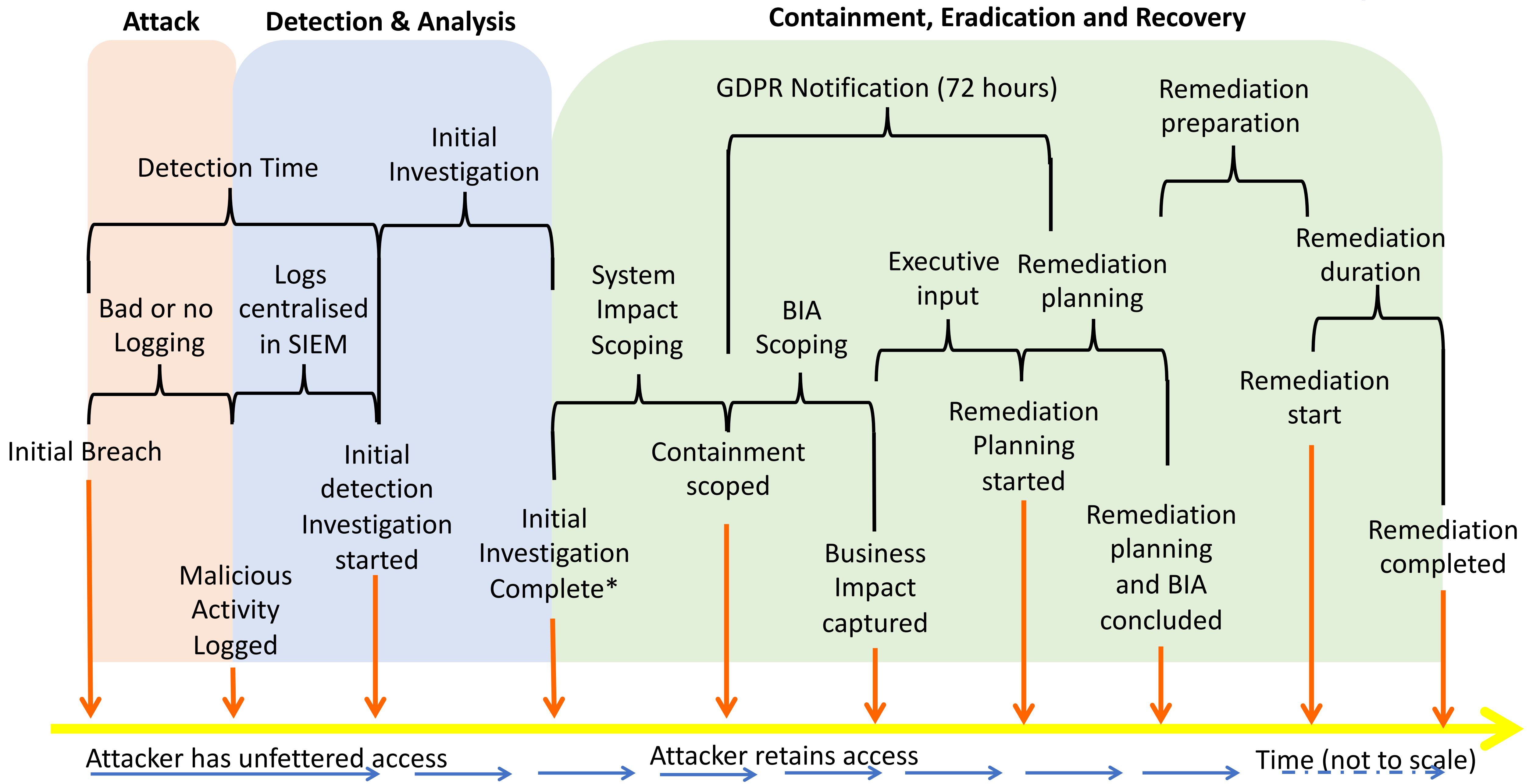
- Improve this by having smaller incidents
- Improve this by automating the system swap-outs
- Improve this with better planning
- Improve this with more experienced and skilled staff

IR Timeline stages



IR Timeline stages

logically secure



Attack

Detection & Analysis

Containment, Eradication and Recovery

Detection Time

Initial Investigation

GDPR Notification (72 hours)

Remediation preparation

Bad or no Logging

Logs centralised in SIEM

System Impact Scoping

BIA Scoping

Executive input

Remediation planning

Remediation duration

Initial Breach

Malicious Activity Logged

Initial detection Investigation started

Initial Investigation Complete*

Containment scoped

Business Impact captured

Remediation Planning started

Remediation planning and BIA concluded

Remediation start

Remediation completed

Attacker has unfettered access

Attacker retains access

Time (not to scale)

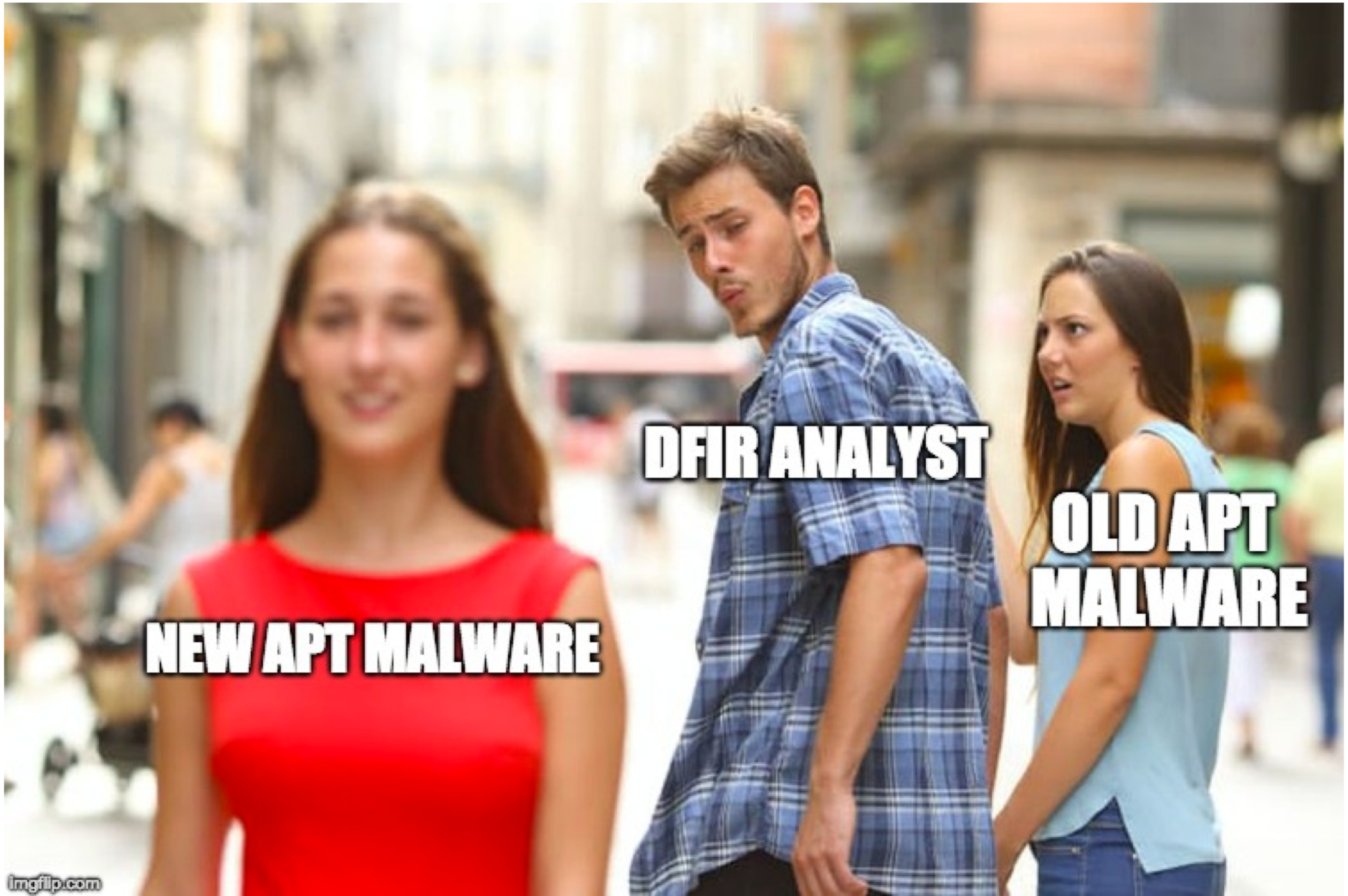
So how do you use these?

- Start tracking incidents
- Start capturing time lines and see how long things take
- Look to baseline the time needed
- Identify bottlenecks – these include
  - Staff
  - Equipment
  - Access to systems / logs
  - Training
- Set dates by which to remove the bottlenecks
- See how you improve and see how the KPIs reflect this

Remember that IR is constantly evolving

That’s because the network is alive and the attackers are responding to our tactics; improving their OODA loop ☺

Any Questions?



To get these slides

- Email: steve@logicallysecure.com
- Twitter: @Nebulator
- Slides (later) :
- https://www.logicallysecure.com/blog/sans-sept-london-talk/