Active Cyber Defence Alliance Whitepaper

Active Incident Response
How to Respond to a Cyber Crisis

A document developed by the Active Cyber Defence Alliance
Draft version as at 29 September 2020

Incident Response Guide - Ransomware Attack

Who is the Active Cyber Defence Alliance (ACDA)?

The Active Cyber Defence Alliance (ADCA) is special interest group comprised of industry, academic and government stakeholders whose aim of is to foster awareness, adoption and capability in Active Cyber Defence practices across Australia with the goal of lifting Australia's cyber resilience.

Active Cyber Defence Alliance (ACDA) Steering Group;

Andrew Cox
CEO – Avantgard Pty Ltd

John Powell
Principal Consultant for – Telstra Purple

Ben Whitham
CEO – Penten Pty Ltd

Rob Deakin
Director Cyber Security – ACCC

Helaine Leggat
Attorney at Law – ICT Legal Consulting

Duncan Unwin
Managing Director – Tobruk Security

Executive Summary

Active incident response seeks to grasp the initiative with attendant negotiating power and assurance that the threat is eliminated with the aim of producing better outcomes than a passive response. For example, a conventional passive response to a ransomware attack leaves the entire initiative with the adversary and renders the target a passive victim, vulnerable to repeat attacks and without negotiating power.

What does an Active Incident Response look like?

Conventionally, when attacked with ransomware the victim focuses on containment, mitigation and sustaining business continuity, engaging in negotiation only if all else fails.

An active response engages the attacker from the beginning using cyber intelligence tools to verify whether the attacker is just an opportunist or is a focussed and motivated adversary (say a business competitor or a state actor) Active response uses cyber deception, negotiation and dark web intelligence to extract intelligence from the attacker, shape attacker behaviour and assure eradication. Such an intelligence led approach provides better outcomes with greater assurance of recovery and lowered risk of repeat attacks.

Active vs Conventional Cyber Defence

When attacking civilian targets, cyber criminals and even state actors take for granted that generally, their targets will respond passively. They do not expect to suffer any negative consequences from their attack, even if the attack fails. An active defence is designed to make your organisation a hostile target. The idea is to empower you to fight back[1] and exact a cost from your adversary making them invest extra effort and resources while raising the risk of third party sanctions and possibly exposing their valuable tools and techniques. This moves the target organisation's posture from that of a passive victim that an active adversary.

By Passive (or Conventional) Cyber Defence[2] we refer to conventional cyber security practices such as network hygiene, firewalls, virus filters, good user behaviour etc. These are necessary but insufficient. By itself, passive cyber defence has proven ineffective against sophisticated attacks. Active cyber defence builds on the foundations of good cyber hygiene and user behaviour (passive defence) using intelligence, deception, active threat hunting and other lawful measures to engage and often defeat cyber adversaries. A balanced cyber defence incorporates both active and passive measures, tilting the balance of power back in favour of the defender.

Passive Cyber Defence is necessary but insufficient

[1] "Fight Back" does not include "Hacking Back" or offensive actions which are the sole domain of government security agencies

[2] Edward Morgan & Maj Gen Marcus Thompson: 181023_InformationWarfare pages 22-23

Why Conventional Cyber Defence Fails

To use a metaphor, think of a boxer fighting with both eyes blindfolded and both ears blocked against an opponent with open eyes and ears. He does not know where the next punch is coming from and can only flail around blindly. Once in a while he may land a lucky punch, but he is destined for a severe beating. His alert opponent circles around and strikes at the victim's most vulnerable points with little risk to the aggressor. However, if the blindfold and ear plugs are removed, the now seeing victim can assess his adversary's strengths and weaknesses and block the attacks. He can expect to land counter punches and event call on the ref for a foul blow. The adversary is now at risk of hurt, must guard himself and be far more cautious.

To illustrate this look at these findings from *Ponemon Institute Cost of Malware Containment Report 2017* which demonstrate that there are a lot of blind boxers and that they're getting a hiding. Despite large investment in new technologies, procedures and operator training (such as SIEM, SOC, SOAR and EDR) these numbers have not moved much in recent years.

Table 1 Conventional Cyber Defence Statistics[3]

205	Average number of days for a business to detect an intrusion
34%	Proportion of those businesses that detect their own data breach
16,937	Number of alerts a week created by the average organisation's IT security systems
40	Number of incidents a week that an analyst can process
423	Number of analysts needed by average organisation
81%	Percentage of cyber alerts that are false alarms

Active vs Conventional Incident Response.

When attacking civilian targets, cyber criminals and potentially state actors, may take for granted that they generally won't suffer negative consequences from their attack, even if the attack fails. Active defence is designed to invalidate this assumption. By using cyber deception and intelligence tools you get high visibility of adversary actions and objectives so that you can defend yourself and frustrate your attacker's objectives eg. they steal dummy data, not real data. Your cyber posture should no longer be that of a passive victim but rather an alert and dangerous adversary. Active and passive measures are mutually supportive and, when combined effectively, will deliver much better outcomes for the defender.

Conventional Incident Response is necessary but insufficient

How Active Defence works

Modern deception technology can deploy a variety of lures and traps that emulate native software and hardware that are indistinguishable from their real counterparts on the network. Once an attacker penetrates the network perimeter, they conduct reconnaissance to map the network and move laterally to explore potential targets. A network containing deception lures or artificially generated traffic provides the attacker with tempting targets in the form of credentials or software tokens needed to access other portions of the network. These lures lead attackers to traps that mimic physical devices such as servers or individual workstations or virtual / cloud-based assets. As the attacker proceeds further along the path formed by these lures and traps, the deception continues, allowing the attacker to install malware within traps, creating the illusion of a successful attack while isolating the malware from the actual network[4] and exposing the attacker's tools, techniques and procedures to the defender. The defender is now actively engaging the attacker, shaping his behaviour and perceptions while exposing weaknesses and informing potential countermeasures.

[3] *Ponemon Institute Cost of Malware Containment Report 2017*

[4] Quoted from Deception as a Security Strategy

Questions Asked

Active defence asks a different class of questions. In fact, everyone asks those questions – but in many cases their organisation does not invest the effort required to answer them.

Table 2 Active vs Conventional – The Questions Asked

Active IR Stream – Questions

- Who has done this? (adversary identity, location & reputation)
- What is their objective?
- Is this a tailored campaign launched by a highly motivated adversary (e.g. business competitor) vs an opportunist attacker?[5]
- Would paying ransom ensure data recovery?
- If we don't pay the ransom
    - Can we recover our data?
    - Will they do something worse?
    - Will they attack us again?
    - Could we keep them out next time?
    - Will they extort us by leaking?[6]
- Have we eradicated the adversary's foothold?
- Will they come back?
- What lawful counter measures are available?

Conventional IR Stream – Questions

- What is the extent of damage?
- Is my data locked and unusable?
- Has data been stolen?
- What can't I confidently recover from backup?
- What is the impact on my business?

With the help of a skilled IR team it is possible to answer these questions and retake the initiative. In fact, you should ask such questions and deploy your active defence ahead of time. Modern deception tools yield personalised intelligence that gives visibility of attacks developing before you are seriously breached and greatly reduces average number of days for a business to detect an intrusion.

Improved outcomes

An effective active incident response can reduce the damage to your organisation, reduce the cost and time of recovery.

Table 3 Likely outcomes - Active vs Conventional Incident response in a serious extortion attack

Active Stream Augments Conventional IR

- Active defender gains the initiative and accelerates recovery
- Informed negotiation reduces ransom costs
- Intelligence & deception tools give assurance of containment & eradication
- Risk of return attack is greatly diminished

Conventional IR Stream

- Business mitigation plan fails to recover timely operations.
- As last resort, the victim pays ransom and hopes for the best.
- Or, victim doesn't pay and accepts the damage.
- Victim lives with the risk of a return attack.

[5] The answer to this question will affect the entire decision making process – an opportunistic attack requires minimal response phases while a motivated adversary will mandate the customer expect a 2nd wave.

[6] REvil ransomware creates eBay-like auction site for stolen data

Incident Response – Triage;

Naturally, when a cyber incident occurs you turn to trusted advisers to inform your statutory and reporting obligations, public relations plan etc. These are essential to an effective response but insufficient to move into the active realm. For a serious incident you will need a range of specialist resources that are particular to your circumstances, people who do this daily for a living. The best first step for specialist advisors is a triage engagement across the critical first two/three days. A triage engagement typically entails drawing at need from a pool of specialist resource types and consuming overall 6-10 person-days of intense effort over 2 or 3 days elapsed of critical response. The triage objective is to assess the incident severity, assess the adversary and inform strategy and tactics for the response

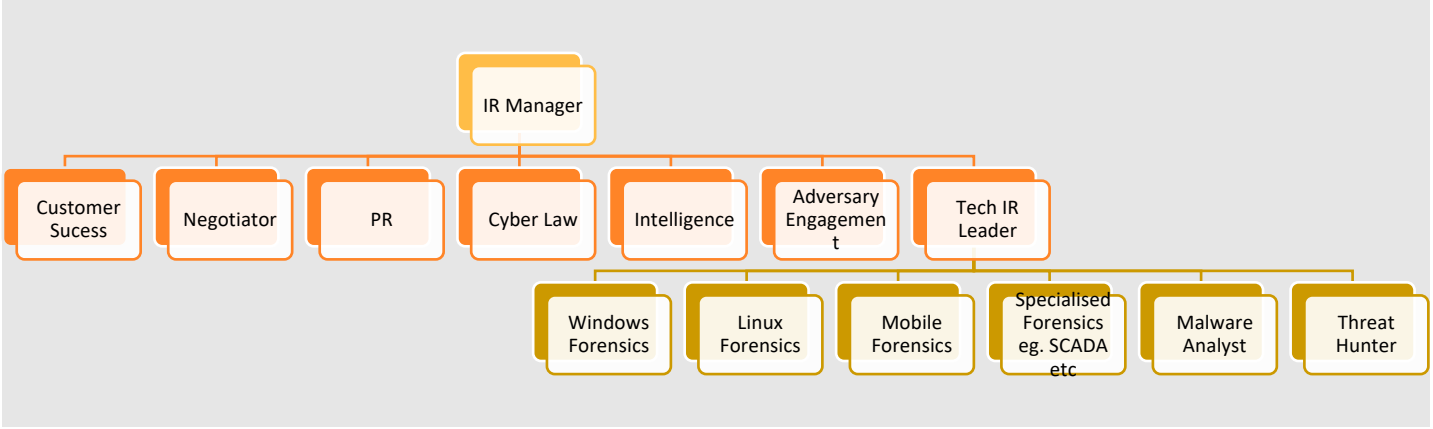
Triage deliverables;

- Adversary Intelligence – A view on the capability and intentions of the adversary. Is this simply an opportunistic attack by a small cyber-criminal, a major cyber-crime organisation or a well-resourced state actor.
- Damage assessment – A view on the extent of damage and potential damage to your assets, your organisation and your stakeholders.
- Interventions and countermeasures – Assist your internal team to block further damage while planning containment and recovery.
- Legal advice – An informed understanding of the range of lawful interventions and countermeasures available to you in defence of the attack.
- Ransom advice – A view on the likely consequences of paying or refusing to pay any part of a ransom demand.
- Next Steps – A plan of action to minimise damage and optimise recovery outcomes.

Incident Response Team Capabilities;

An effective cyber response team must able to draw on a range of expert resources on short notice. Here is a summary of the response team structure we have found effective.

Figure 1 Cyber Incident Response Team



Incident Response Manager

It is highly recommended to assign a specialist a specialist incident response manager for this job and mandatory to assign a C-level stakeholder from the org itself to work closely with the incident manager. The IR Manager is the guiding hand for the response with an overarching view of all resources and activities. This person has ability to draw in resources, coordinate actions and keep the key stakeholders continuously informed. They must be decisive, moving focus rapidly to ensure time is not wasted on dead ends and the teams work together to quickly and efficiently resolve the incident. A key responsibility of the IR Manager is reporting and time management;

- Executive summary of the IR team once every X hours,
- Research team time management – allocating X hours per research branch so we won't exhaust the resources on specific items,
- Measure the timers for the attacker's threats (eg. 24 H to pay, 48 H for the next DoS wave or Data release…),
- Regulation timers like 48 Hrs from the IR kick off till a report is required

Forensic Specialists and Threat Hunters

Time is of the essence in a cyber incident so the forensic team must aim to make progress quickly and be disciplined in stopping fruitless lines of enquiry. It is the responsibility of the IR manager to coordinate efficient and aggressive use of resources while keeping information flowing within the team and with stakeholders. Cyber forensic analysis demands profound technical knowledge of the systems compromised. Almost any incident will require specialists in windows, Linux and likely mobile devices. Industrial control systems breaches will also demand expertise in SCADA and relevant proprietary control protocols and industry specific workflows. Not all technical specialists are good threat hunters. An effective threat hunter will think like the adversary and relish the battle of wills. An effective IR team will have a mix of these skills and personalities.

Intelligence & Adversary Engagement

Your adversaries are people with personalities, intentions, strengths and weaknesses. The object of an active incident response is to understand as much about your adversary as feasible to enable you to frustrate their intentions and defeat their attack. Experienced intelligence specialists can make a big contribution here, allowing you to think ahead and predict likely adversary behaviour in the various scenarios that may unfold. This is invaluable to your ability to resolve an incident with minimal harm and cost to your organisation. We had a case in which the attacker negotiated over email, unintentionally leaving timestamp fingerprint – allowing us to differentiate between the time the email received at the local time zone and sent on our time zone – revealing he was coming from GMT + 3 (Ukraine). In addition, he had the default "re" and "fw" over the email mentioning his operating system native language, revealing he uses a Cyrillic keyboard. Those together led to a conclusion it's an opportunist with no real familiarity of the targeted business. Another means of assessing the attacker's

awareness of the business is – who is the ransom demand email directed to? Is it the top-3 C-levels that can be found in your "About us" webpage or some real decision makers that have no presence? In another example attackers opened a dark web market for data already stolen from the victim. Therefore, the victim had to keep in mind that if they chose not to negotiate – they would likely get hit with a wave of public data exposure with attendant reputational and stakeholder damage. The best defence here is to have pre-seeded the databases with honey records. Honey records are fake database entries which, when paired with an internet and dark web search system, can be used to identify stolen records and provide an indication of which system or backup was breached. They can also be used to taint the data so the adversary cannot have confidence in what they have stolen. Is the stolen data real or fake? It is very hard for the thief to distinguish the real records from the fake ones, so they are less likely to expose themselves to reputational damage by by selling the records in a criminal marketplace. The same technique can also frustrate information operations where data is stolen to influence an election as demonstrated in the Macron presidential election.[7]

Skilled Negotiator

In a ransomware incident specialised ransom negotiation skills are essential. Not every negotiation process is the same. Each campaign looks different and the negotiator objectives may differ. One objective is to reduce the costs, another is to extract knowledge about the adversary. A good negotiator will design the path from the kick off to the end-game, along with all of the potential tipping points along the way. Even if you have no intention of paying ransom the negotiator should engage the adversary as early as possible with a view of mitigating damage, gaining intelligence on the adversary and slowing down their actions. Communication with your attacker often provides a valuable of intelligence on their intentions, capabilities, objectives, identity and location. The best negotiators often may have a background in security agencies with experience in hostage and terrorist negotiation.

Communication

Your communication with the many stakeholders affected by a cyber incident will be a critical success factor in your management of the incident. In a serious incident you maybe need to communicate;

- With the relevant CERT (Computer Emergency Response Team)
- With the police / ACSC
- With information sharing groups (ISAC)
- With statutory authorities

All of the above will (hopefully) enrich the IR team with additional information about the attacker and their Modus Operandi

You need to communicate frankly with your stakeholders;

- Internal – employees, decision makers, owners
- External – providers (that may suffer a direct hit or get some lateral movement), customers

Here is an example of a good PR announcement structure taken from an incident response by Reddit;

Table 4 Example PR Template

We had a security incident. Here's what you need to know.

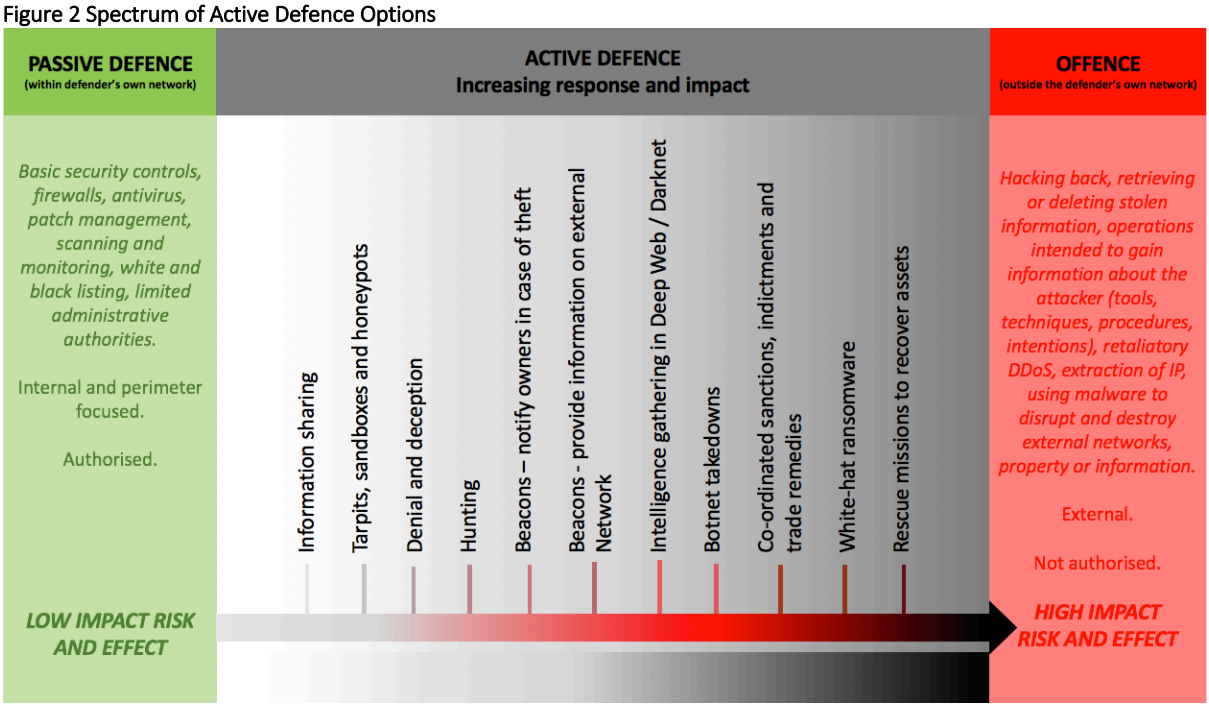
- **What happened?**
- **What information was involved?**
  - *What was accessed*
  - *How to tell if your information was included*
- **What are we doing about it?** Eg;
  - Reported the issue to law enforcement and are cooperating with their investigation.
  - Are messaging user accounts if there's a chance the credentials taken reflect the account's current password.
  - Took measures to guarantee that additional points of privileged access to our systems are more secure (give details)
- **What can you do?**
  - Simple instructions to affected stakeholders on how to mitigate their risk of loss.

[7] How Macron's Team May Have Changed Cybersecurity Forever

Cyber Law

You are not defenceless. Companies are persons before the law and have the same rights, privileges and responsibilities as individuals. The laws relating to self-defence, trespass and theft of private property also apply to the cyber realm and there are a range of lawful measures available to you when you respond to a cyber; attack, trespass, theft, extortion etc. However, as you move from passive to more active defence the risk of misstep will increase. To ensure you mount a robust defence you will need a legal adviser who thoroughly understands cyber law and can assist you in actively defending yourself squarely within the law.

Figure 2 Spectrum of Active Defence Options



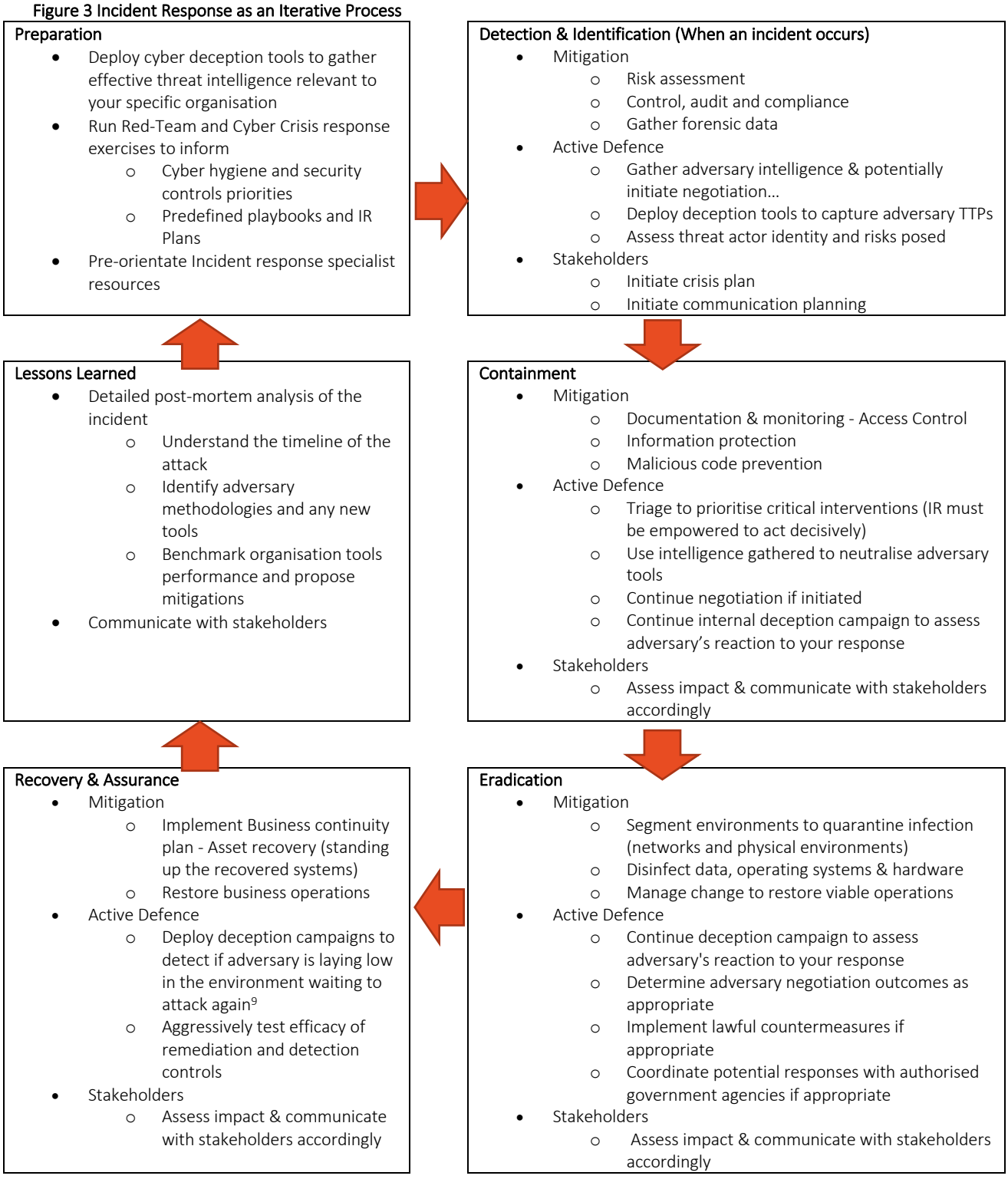
It is tempting to say 'Let's just stay passive.' but the Australian Cyber-Security strategy 2020 emphasises the need to "Actively defend" networks and critical infrastructure. To quote Australia's Head of Information Warfare Maj Gen Marcus Thompson; "a non-state actor we haven't talked about is industry. When we think about cyberspace .... the vast majority [of cyber infrastructure] is privately owned...."[8]. Australia and our allies have huge industry cyber resources that are sidelined in the cyber conflict because of a poor understanding of their freedom of action. A good understanding of active defence (e.g as explained in this article by cyber law expert Helaine Leggat; https://ictlegalconsulting.com/docs/Helaine_Leggat_IJCWT_10.3.pdf) will empower Australian industry to present a much more hostile attack surface while maintaining predictability/stability by working within the boundaries of properly understood legal norms and standards.

[8] LinkedIn Post and Commentary

The Incident Response Cycle

Effective incident response is a cyclical process. It starts with preparation and ends with an incident post mortem to learn new lessons and improve preparation for next time.

Figure 3 Incident Response as an Iterative Process



[9] Catching-APT3-with-cyber-deception.pdf

Procuring Incident Response Services?

There are typically two ways in which incident response services are procured. You can acquire IR services via an annual retainer with a service level agreement or you can buy them on-demand after an incident occurs.

Spot Resources

You can certainly buy incident response services on the spot and many have, but be warned, these are scarce resources. If buying on-demand you will pay premium rates and there is no guarantee that the skilled resources, you need will be immediately available at a time when an adversary is at loose in your network and every hour counts. In addition, the service achieved will be less efficient as the IR team will not already be familiar with the business logic, infrastructure in use, stakeholders, etc.

Retainer with SLA

If you acquire IR services via retainer, you should receive a service level agreement to provide the needed resources within a specified period of time and generally the cost of services is materially lower. An arrangement like this should include an on-boarding project to orient the provider to your business, network, assets, applications, personnel procedures etc. which will enable the IR team to be productive immediately when they are engaged for an incident, reducing the IR KPI's of MTTD (Mean-Time-to-Detect) and MTTR (Mean-Time-to-Respond).

In the event that no incidents occur in a given year the residual value of the retainer should be delivered in services to improve your security readiness such as vulnerabilities assessment or participation a cyber incident drill.

In Closing

We hope you found this white paper valuable. The Active Cyber Defence Alliance provides assistance to organisations who want to explore active cyber incident response. If you'd like to participate in an ACDA active incident response exercise or get more information about the ACDA please reach out to the contacts below.

ACDA Contacts

Andrew Cox
andrew@avantgard.com.au
+61 448 545 897

Ben Whitham
Ben.whitham@penten.com
+61 433 944 794