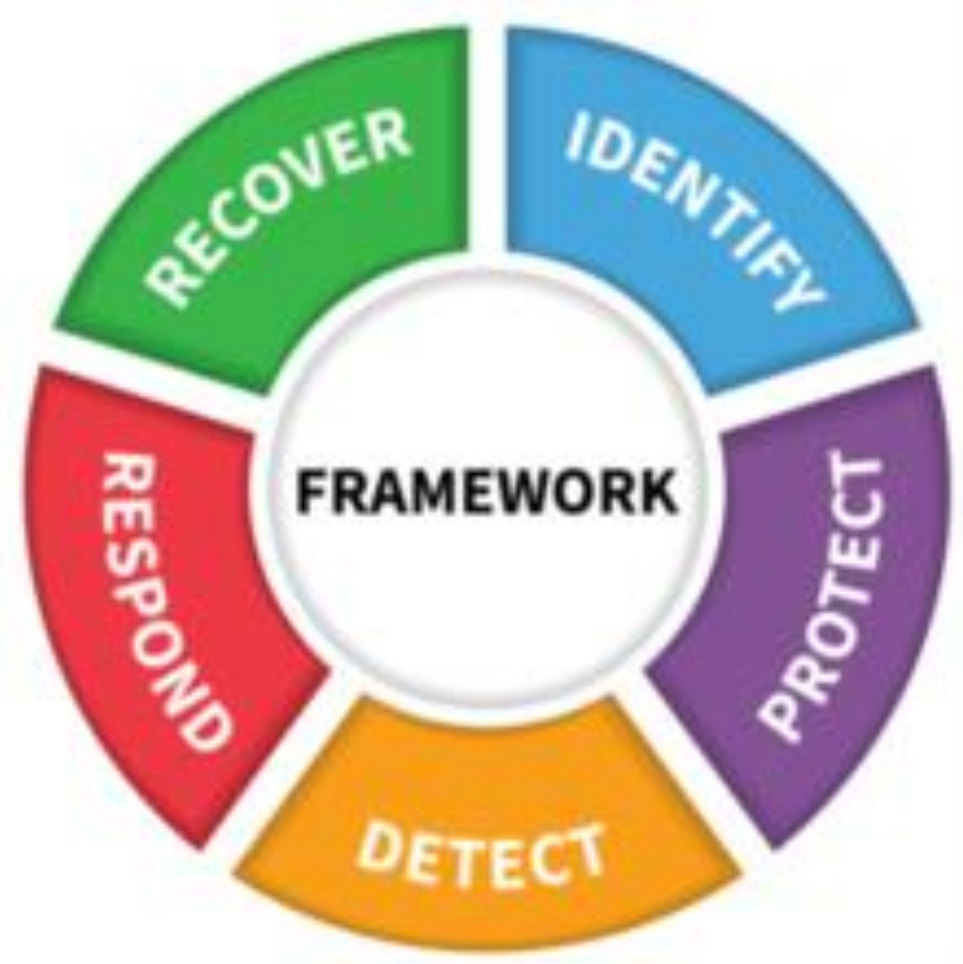
# Cyber Security – What does getting it right look like?

## Fact Sheet by ParaFlare

I encourage people to think about cybersecurity from a holistic perspective. There are five broad areas you need to consider. These are outlined in the National Institute of Standards and Technology (NIST) wheel – a US-designed framework for cyber security.

1. **Identify**. This is about knowing what is on your network.
2. **Protect**. Defend and harden your systems. This is what we call passive defence.
3. **Detect** and
4. **Respond**. This is the foundation of Active Cyber Defence, or the ability to detect, respond and contain a breach in real time.
5. **Recover**. These are the activities that help an organisation to return to normal operations to reduce the impact from a cybersecurity incident.



Detection and response make up around 40% of the NIST wheel however these two critical areas do not always achieve the level of effort or visibility they deserve.

The good is news is that Microsoft has two of the industry-leading detection and response tools: Azure Sentinel and Microsoft Defender suite.

When it comes to producing a resilient Active defence capability, I like to think of these five key ingredients.

1. **Deploy the core technology.**

Security Information and Event Management (SIEM) and Extended Detection and Response (XDR) are the minimum pay-to-play tools. Azure and Sentinel are your first tooling ingredients, and this is where you want to start.

While there is a plethora of security tooling in the market, you need to get your core technologies right first.

When it comes to detection, response, and containment many people are prioritising network visibility tools, which are important however not my first focus. Defender for IOT, Nozomi or Dragos are great products and serve an excellent outcome however they are not the first stop on the journey.

2. **Aggregate your security tools.**

When it comes to technology, connect your existing security tooling (alerting) to Sentinel (or your SIEM). Don't waste that investment and ensure you are aggregating and centralising these incidents. This a particularly important message for CISOs. Microsoft Defender for endpoint gives you a huge amount of benefit, and Sentinel is an excellent tool; but your aim is to aggregate your other security tooling that you have already spent money on and get more out of it – particularly visibility into multi-stage threats across the kill chain.

3. **Commit people and time to your platform, and triage alerts.**

The purpose of these platforms (SIEM/XDR) is to generate alerting. When committing people, don't just commit them to 'eat the alerts,' or you will end up with some unhappy and fatigued analysts. Spend time tuning and rationalising all alerts to make sure your people are happy and doing the things they like. I like to suggest that you should reserve 20% of your time at a minimum for tuning.

Once you have your resourcing and technology mix right, and that is your minimum viable product for detection and response, you need to commit to triaging the alerts and have a strong process in place for doing that. It is important to have guardrails around your process that guides an analyst through triage but is flexible enough to deviate from the course if something interesting comes up. Sentinel and Defender for Endpoint have a component of protection in place, however their job is to generate alerts that require investigation. Someone needs to run these alerts to ground. You can automate some alerts, but not all of them.

4. **Have a plan for when things go wrong and test it.**

All organisations should have a cyber incident response plan in place to make sure they can respond and recover quickly if a threat makes it past the security controls. This plan should be tested and regularly reviewed. There is some valuable information available on the Australian Cyber Security Centre website: https://www.cyber.gov.au/acsc/view-all-content/publications/cyber-incident-response-plan

The last thing you want to do is test an incident response plan with a live incident.

5. **Rationalise and take a platform approach.**

Integration is never perfect. Many Microsoft tools are integrated out of the box or require minimal effort compared to other vendors. If your security is integrated, choose carefully if you want to take components beyond that platform. Stick within an ecosystem and only deviate when you have a strong use case to make exceptions.

If you are going to set up an active defence capability, set a target. My first target is to be prepared to catch your pen tester while they are conducting a test. If you don't catch them along the way, or you can't trace the pen test back to your alerting, you have not achieved your target. You don't need to catch them in a 15-minute response time, but at least know if you have the data set to detect them. The dangerous space is to be in is when you pay someone to be in your environment, and you have no idea what steps they took to penetrate your network.

**Core tooling**

There are many things you can do with core tooling. The bare minimum is XDR tool. It is difficult (not impossible) to attack an environment without traversing an end point. The vast majority of most networks' attack surface is their operating system; that's your Linux, Mac, or Windows. In most attacks it's common for an adversary to touch one of those endpoints or be involved with it along the way.

For a more mature organisation, SIEM gives you additional coverage. SME's might get away with XDR only, but as you start to move up the technology food chain it soon becomes the right time for SIEM and XDR.

Our advice is to get the first two right, and then look at Internet of Things (IOT) tools, such as Defender for IOT. Microsoft has a platform play for all three, and best of all, they are integrated.