Remediate by nccgroup

An NCC Group Publication

Looking forward: How to learn from cyber incidents and plan ahead

Lloyd Brough, Technical Associate Director at NCC Group

A cyber breach or incident can be an incredibly stressful situation for any business to go through. Amongst the urgency to assess and eradicate a threat, it can be hard to see the light at the end of the tunnel.

However, a measured, thought-out response to a cyber incident is absolutely crucial in shaping how your organisation emerges from a breach. With that in mind, here's how you can effectively respond to an incident and build the lessons learned into a long-term, practical security improvement plan.

Containment, avoiding Whack-a-CTA and eradication

If you have a well-considered incident response (IR) plan in place, it is important that you follow that plan whilst being as pragmatic as possible – new or unexpected information can dramatically alter the path of an investigation.

The first and most important stage should involve gathering and analysing as much information as soon as you have been alerted to a cyber threat actor (CTA) – whether this was through technical system logs and events, a staff member or third-party company.

A running theme across the vast majority of IR investigations is a lack of logging and information to investigate an incident. To establish this, a real-world recommendation is to perform some desktop-based scenarios; we find the best way to do this is to augment it with a purple team exercise to add realism.

Too many logs can be overwhelming. However, it is critical that you have the correct logs and events. If you are in this scenario, consider looking at NCSCs Logging Made Easy, a self-install tutorial for small organisations to gain a basic level of centralised security logging for Windows clients and provide functionality to detect attacks. NCC Group also has commercial enterprise security information and event management (SIEM) skills and also provide managed protective monitoring.

This initial log analysis, combined with digital forensics and incident response (DFIR) from a cyber incident response team (CIRT), should enable you to establish how, when and where an attacker has infiltrated your systems or network, which can then be used for triaging appropriate containment and eradication actions.

Knowing the extent of an incident is crucial and will help your organisation know if the relevant parties and regulatory bodies need to be informed. In the case of a personal data breach, this should be reported within 72 hours of being made aware of the breach under the General Data Protection Regulation for organisations operating or dealing with personal data from the European Union.

Don't be afraid to call a CIRT to assist the investigation from a DFIR angle. This should be done sooner rather than later, enabling you to get more accurate information quickly, which will cost less in the long-run.

Flushing the CTA out

The next steps are particularly crucial and involve establishing a strategy to get rid of the attacker who has breached your systems. At this point, you should understand their tactics, techniques and actions. You should then look to control or prevent the attacker's access to critical information by making a containment plan.

During a live cyber incident, time is of the essence and any mitigations and measures should be carefully thought out. 'Sticking plaster' fixes are not effective in these instances. An attacker can quickly notice them and change their approach accordingly, making the remediation process much more complex.

Containment and eradication both utilise the same skillsets and approach to a technology-based security improvement and remediation programme. The eradication process should be a coordinated effort and involve actions that will inhibit the attacker's ability to perform any further activity within your environment. All tools or files used by the attacker, such as malware and exploit kits, should also be contained and removed as soon as possible.

This isn't always fully possible, but if you're able to review the various attack chains and gain understanding of a commonality such as the lateral movement component, this would have a big impact and disrupt the majority of attack chains for little cost and effort to the business.

Once you have eradicated the attacker from your systems, it's important to monitor your environment in case the attacker makes a return. While this is often a worst-case scenario, all organisations should be prepared for this.

Return of the CTA?

This is the key point of this blog – DFIR investigation, containment and eradication are not the end of this journey.

After you're confident that the attacker is no longer active and have implemented measures to prevent further access to your systems, it's important to take a step back and assess your organisation's short to long-term cyber security posture.

Creating and implementing a robust security improvement plan is a great way to prepare your organisation for future incidents. This will ensure that your business has the tools it needs to make measurable changes that prevent or mitigate the impact of a malicious actor.

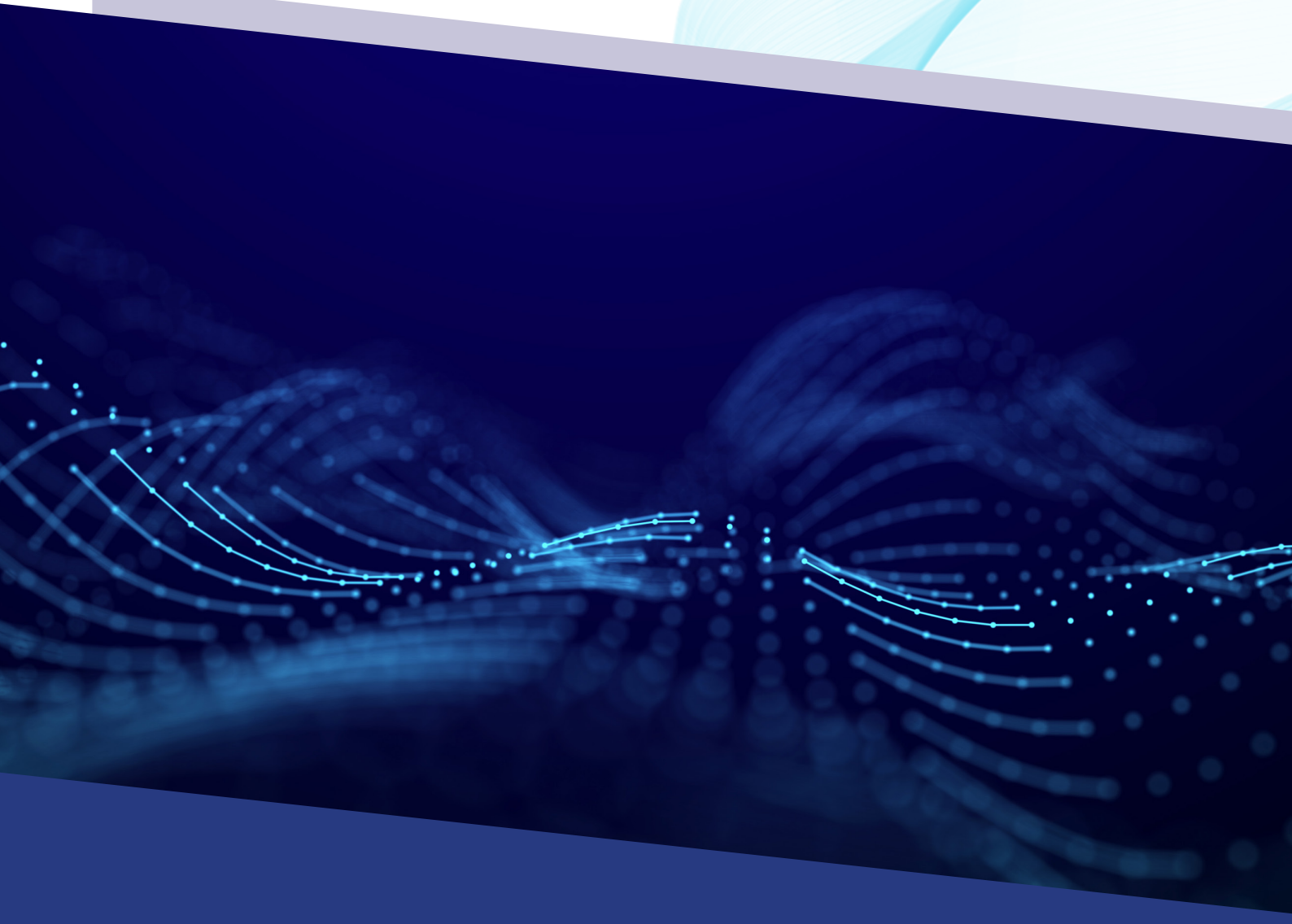
However, without the right active support throughout this process, many organisations find it hard to navigate incident response and subsequent remediation due to resource constraints, a lack of detailed technical knowledge or other reasons. This is where security expertise, threat intelligence and knowledge from third parties can significantly improve the remediation process.

> "Creating and implementing a robust security improvement plan is a great way to prepare your organisation for future incidents"

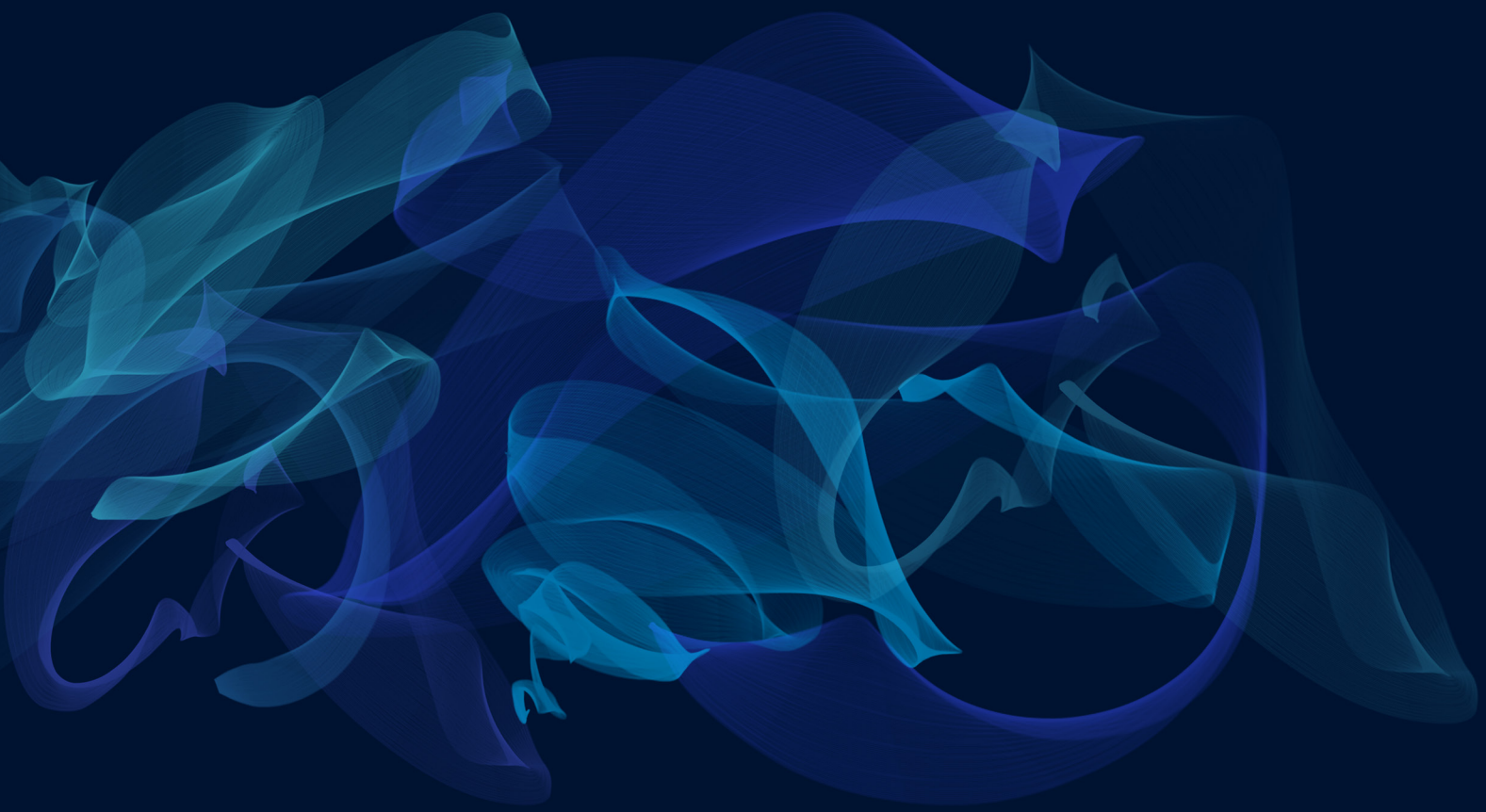
How can NCC Group help?

Our vision is to make the world safer and more secure. To achieve this, we need to give every business the tools they need to assess threats and understand their security posture and make sustainable, long-term improvements.

Our specialists will work with you to determine how the breach or incident occurred, the likely capabilities and the extent of infiltration achieved by the threat actor. Then, we give you the knowledge and support as an implementation partner that you need to eradicate these threats from your systems, and the tools and security improvement plans needed to actively bolster your cyber defences.



Remediate by nccgroup



About NCC Group

NCC Group exists to make the world safer and more secure.

As global experts in cyber security and risk mitigation, NCC Group is trusted by over 14,000 clients worldwide to protect their most critical assets from the ever-changing threat landscape.

With the company's knowledge, experience and global footprint, it is best placed to help businesses identify, assess, mitigate and respond to the evolving cyber risks they face.

To support its mission, NCC Group continually invests in research and innovation, and is passionate about developing the next generation of cyber scientists.

With over 1,800 colleagues in 12 countries, NCC Group has a significant market presence in North America, continental Europe and the UK, and a rapidly growing footprint in Asia Pacific with offices in Australia and Singapore.

To discuss managing your risk alongside BAU, speak to our team today.

+44 (0)161 209 5111
response@nccgroup.com
www.nccgroup.com