Insight Space

cyber insights programme

nccgroup

Ollie Whitehouse

Technical Viewpoint

Building your cyber defence:

start with the basics

Cyber defence is not about magic amulets, it is about discipline

When we talk about cyber resilience and defence, organisations are often swayed by solutions that promise untold success with comparatively little effort. These solutions will often talk about how they will be able to shore up an organisation's cyber defences and increase its overall resilience quickly, cheaply and with very little effort.

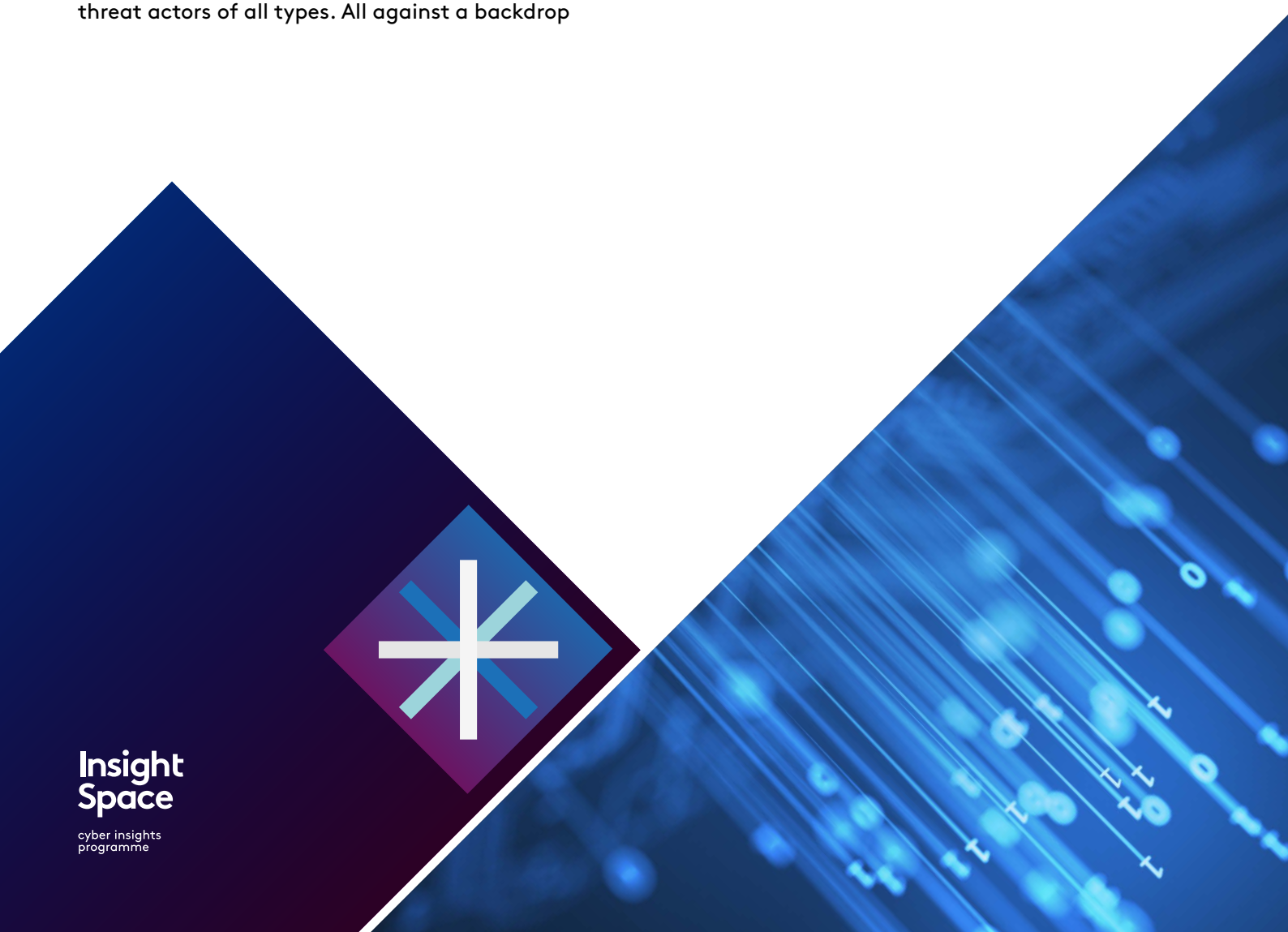
The reality, however, is that resilience takes hard work. In order to establish and successfully achieve a state of robust cyber defence, far more effort has to be put into transformation and operational improvement than in magical solutions.

Insights from a nation-grade offensive capability

NCC Group is one of the few organisations in the private sector that operates world-class, at-scale offensive and defensive capabilities under one roof.

On one hand, we help clients attack hardware, software, systems, processes and people to assess real-world impact and resilience. On the other, we respond to cyber incidents globally, monitor hundreds of organisations, millions of endpoints and track threat actors of all types. All against a backdrop of helping organisations design, build and operate resilient and compliant products, services and organisations.

Based on these insights, we recently had our Red Team distil the factors that make their lives easier, as well as those that force them to take more risks and invariably fail more if implemented.



Insight Space

cyber insights programme

The basics are crucial

The key findings from our Red Team were:

- Organisations leak too much information.
- Organisations don't know what is in their computing estate.
- Organisations don't reliably maintain their computer estate.
- Organisations place trust in networks and not solely on identity of devices, its software and users.
- Organisations don't have visibility of what is happening in their estates.
- Organisations place too much faith in their security technologies and their efficacy.

The above makes pretty uncomfortable reading. However, the reality is that organisational complexity, apathy towards robust technology management and, often, an unwillingness to change due to fear of failure can lead to a toxic mix which undermines cyber defence.

Without paring back this problem, addressing the root causes, and driving discipline and rigour, there is little chance organisations will repel an attack, let alone detect and contain one in a reasonable period of time.

Addressing the things we can

Within this list, there are some issues which can be difficult to address. For example, trying to stop all information leaking is a path to likely failure. The goal should be that the leaks don't impact the security of the organisation materially.

Instead we want to focus on the areas that, if addressed, will have the greatest impact.

Threat actors will always be able to adjust their methods to counteract defences or particular approaches. They will be able to identify new and novel techniques to breach networks and systems, know where to persist (or not), and establish command and control channels.

Instead we should focus on making it awkward for them, and ensure that anything – and we mean anything – which happens within a material environment is logged. Through robust understanding and visibility we can make it difficult for threat actors to carry out attacks.

Know what is out there, who owns it, what it does, its lifetime and its purpose

Creating an asset inventory of both physical and virtual assets, including those which are ephemeral, is key. Build it, maintain it, and care for it – it is the single source of truth of what makes up an organisations technology estate and its systems.

Without a near real-time asset inventory, it's almost impossible to know when a part of your system is end-of-life, unmaintained, or previously compromised.

Your asset inventory in 2020 should go all the way up the stack including various "as a service" components, whether it's Infrastructure, Platform or Software, including serverless concepts.

Log everything that is critical and practicable for as long as possible

Detection and analysis rely on effective logging. With incomplete or inconsistent coverage, detection, containment and response missions will not be as effective. We've seen many massive breakthroughs in either detecting or understanding the activity of a sophisticated actor because of high quality logs stretching back years.

If we solely rely on the logs from security products to feed detection, then there is significant exposure. NCC Group's Red Team, like other sophisticated threat actors, spends time and money to acquire and subvert security products and logging in general.

However, the reality is that attackers can't spend time trying to avoid it all if we expect to be successful in our mission. As such, trying to access an environment with mature and persistent logging is like trying to break into a car in a flood lit car park with CCTV and a helicopter circling overhead, whilst trying to break into a car – in other words, awkward and difficult, with a high chance of being caught.

Enrichment in the understanding of assets and users

Not all assets within organisations are created with equal value. As such, understanding of a system, function or user and their role provides valuable context. This context is useful in understanding the risk they present, as well as the impact when security events occur.

By ingesting a wide range of supplementary information, we can build a level of understanding of an organisation's detection and response capabilities, as well as an understanding of what things do and why they matter.

Once we have the foundations we can build with confidence

Much like business operations, good management information and intelligence enables you to operate and make decisions with confidence.

Similarly, with cyber defence, if we have visibility over our systems, their state, their purpose and who is accessing them, we can have confidence that if something suspicious happens now or in the future, we'll have information on the event.

These individual threads on their own may not tell us anything, but when weaved together they provide a rich tapestry, enabling understanding. This understanding gives confidence, and confidence in turn enables business agility and quantified risk taking.

If you want to take the next step on your cyber security journey, we can help - get in touch with our team today.

Insight Space

cyber insights programme

Insight Space

cyber insights programme

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 15,000 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.

www.nccgroup.com