baesystems.com/theintelligencenetwork

Understanding Adversaries

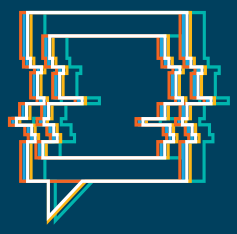
The Future of Cyber Threat Intelligence

BAE SYSTEMS

The market for threat intelligence is evolving rapidly. But there are still many challenges to overcome in terms of how data is being shared and used. Here we explore what the future holds...

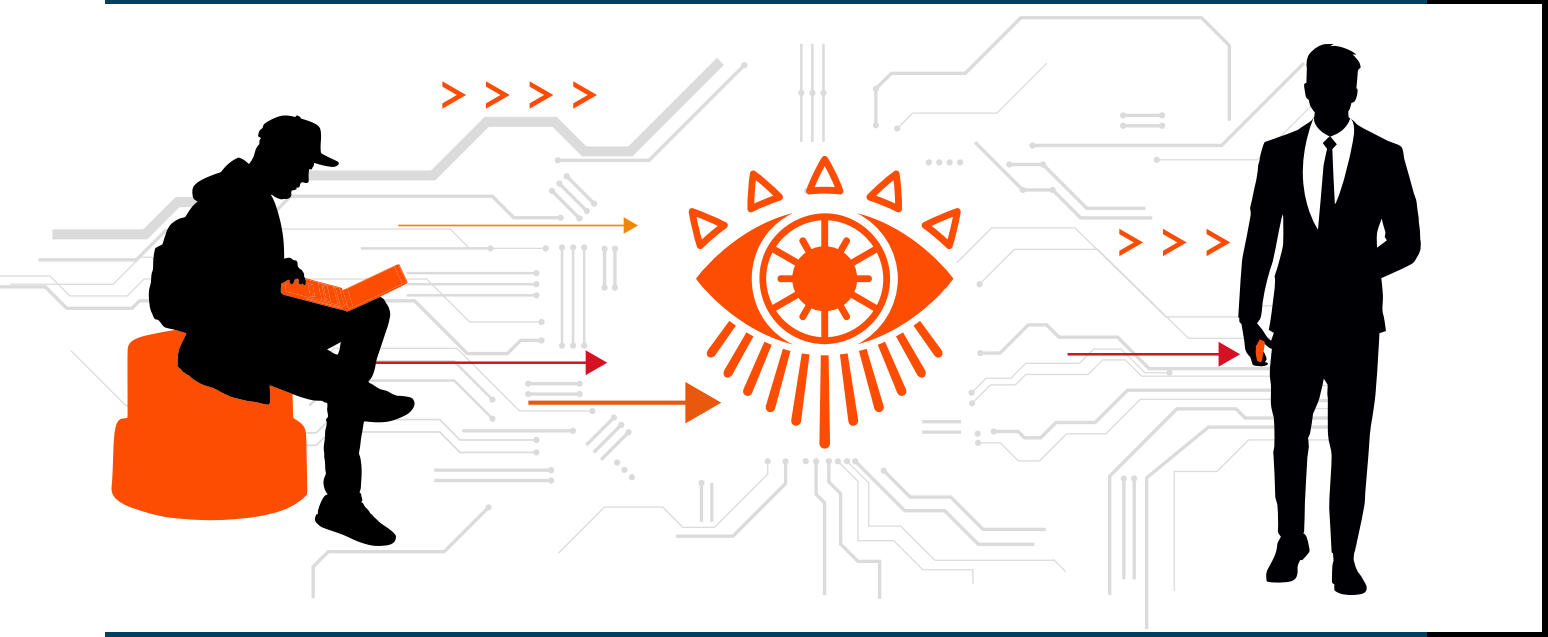
There are two distinct views held in the cybersecurity industry about threat intelligence. One states that you can't defend unless you understand who and what you're defending against. The other holds that you don't need to know who the attackers are as long as you have your defences ready. The truth lies somewhere in between. While getting the security basics right is certainly a vital part of building cyber-resilience, anyone who has played a part in a threat intelligence team will know that understanding your adversaries is absolutely crucial in defending against them.

In these terms, threat intelligence is a key enabler of cyber-defence at every level of society: from national security at one end, to the protection of small organisations at the other. Whether you run your own threat intel team or outsource it to a third party, there are key challenges of supply, consumption and sharing that must be addressed if we want to optimise the industry going forward.



New initiatives such as the BAE Systems-backed **The Intelligence Network** offer a fantastic opportunity to tackle some of these challenges. With over 2,000 members and counting, it's helping to drive a new era in cross-industry collaboration and is comprised of like-minded cyber and financial crime professionals, academics and industry influencers. The Intelligence Network has identified seven critical areas for change before 2025, which includes **understanding adversaries.**

To kick-start the understanding adversaries strand, we held a virtual roundtable with participants from NCSC, Microsoft, MITRE, and Red Hat. We debated the two perspectives discussed above.



The story so far

The cyber threat intelligence market today is booming. Estimates suggest that it will grow at a CAGR (Compound Annual Growth Rate) of **17.5% over the next five years, to reach nearly $14 billion by 2025.**[1] To see why, we only need to look back at the threat landscape over the past decade or more.

In recent years, the majority of successful cyber-attacks have been caused by commodity malware and simple mistakes on the part of victim organisations and their employees; such as reusing passwords across accounts, failing to patch promptly, or clicking through on phishing links. These are incidents which give rise to broad industry findings like these:

One vendor blocked over **27.8 billion unique threats** in the first half of 2020 alone, 93% of which were email-borne[2]

Nearly a quarter (22%) of breaches now involve phishing[3]

However, at the same time, the story of cyber-threats over the past 10+ years has been one of sophisticated operations such as Stuxnet, Cloud Hopper[4] and NotPetya. Unfortunately, the Tactics, Techniques and Procedures (TTPs) seen in attacks such as these are starting to become more commonplace.

Here are a few observations about how the threat landscape is evolving along these lines:

- Cybercrime groups including Maze, DoppelPaymer and REvil are combining a variety of access vectors with efficient use of pen-test tools (such as Cobalt Strike) and 'living off the land' to target a broad range of victim organisations with ransomware[5]. The BAE Systems Threat Intelligence team has been tracking this closely and recently published an infographic Ransomware's Perfect Storm.[6]
- Some state-sponsored threat actors are moonlighting, using their skills in financially motivated attacks[7]
- Supply chain attacks are an increasingly popular method for sophisticated groups to target high value organisations via their partners and software supply chains, exposing smaller firms to advanced threats
- Hacker-for-hire groups like Dark Basin have emerged to offer another possible source of advanced threats, with multiple similar groups coming to light in recent months[8]
- Modern organisations are increasingly investing in hybrid cloud and infrastructure from multiple providers, as well as SaaS apps to serve an increasingly distributed workforce. These trends offer more endpoints, accounts and systems for attackers to probe.

Why threat intelligence works

In this context, threat intelligence is an increasingly critical tool for organisations to have at their disposal. It matters not just for larger big-brand targets and those in high-threat industries such as government, defence and hi-tech, but also their supply chain partners, and other, possibly smaller, organisations that may not have previously considered themselves targets of advanced attacks.

As well as helping to spot and respond to attacks before they affect an organisation, threat intelligence can help by:

- Enhancing the success of other cybersecurity strategies: for example, by helping to prioritise patches as part of vulnerability management programmes, or understanding how effective implementing industry frameworks have been for the organisation
- Providing C-level executives with the information they need to make accurate risk-based business decisions, such as whether to expand into new regions which play host to hostile, state-backed incumbents
- Elevating cybersecurity as a strategic board-level function (as above) and one which should be consulted before major investment decisions are made

Some way to go

Unfortunately, there are problems with supply, consumption and sharing of threat intelligence. While the market may be booming, it has also become bloated. Buyers are faced with hundreds of aggressively marketed solutions, which can make it difficult to find the right fit for their organisation. Most vendors only tackle a limited set of use cases, so organisations that can afford to end up buying multiple potentially overlapping solutions, while those that can't struggle to get full coverage. Neither approach is ideal.

At the same time, there are also inefficiencies on the customer side. There are often difficulties in implementing and then operationalising threat intelligence, with teams flooded with alerts and chasing dead-ends. Both in-house and third-party threat intelligence teams can also be hamstrung in investigations due to uncertainty over whether specific actions are legal or not, which is an area being looked at by the CyberUp Campaign.[9]

More information sharing is often held up as the pre-eminent way to tackle cyber-adversaries. Some argue that threat intelligence should be free to all defenders—but in that case: who funds threat intelligence teams, and what happens when hostile nations and cybercrime groups also gain access to threat reports? There are many sharing schemes currently in operation, but they vary in terms of the speed and quality of intelligence they produce, and how actionable insights are. Organisations have also been reluctant to share in the past for reasons of commercial sensitivity and concerns about the impact on brand reputation—even though these details could be invaluable in helping others to improve resilience.

Time for action

Intelligence sharing between defender communities has undoubtedly improved in recent years. In the UK, the National Cyber Security Centre (NCSC) has had a positive impact on the industry since it was spun out of GCHQ in 2016. However, things are still nowhere near where they should be. The commercial imperative too often trumps any collective desire to enhance threat intelligence and response. Progress must be made on several fronts.

A key step will be to change the narrative around cyber-incidents: from one in which the victim organisation is usually to blame, to one that's common for most other crimes, where the focus is on criminal intent. This could help to persuade more organisations to come clean about specific incidents — to their peers, if not the wider public.

We also need to move towards a common language and framework for identifying and classifying incidents. Two positive developments are:

- **MITRE ATT&CK®** provides an extensive list of attacker tactics and techniques, backed up by real-world evidence and allows for a variety of use cases to improve defences. The BAE Systems Threat Intelligence team has recently published its observations on the high-end threat landscape and trends in use of different MITRE ATT&CK tactics and techniques.[10]
- **Malware Information Sharing Platform (MISP)** is used extensively across government and private enterprise for ingesting threat intelligence, and is becoming the industry-standard as a technical means of sharing threat information.

The bottom line is that threat intelligence is a team sport: organisations must overcome their hard-coded reluctance to reach out more, to network with peers and rivals. For more information on The Intelligence Network and our latest reporting, **click here**

References

[1] Threat intelligence market – growth, trends and forecast (2020-2025) Mordor Intelligence (accessed 6 October 2020)

[2] Data Breach Investigations Report 2020 Verizon (accessed 19 October 2020)

[3] Securing the Pandemic-Disrupted Workplace Trend Micro (26 August 2020)

[4] APT10 – Operation Cloud Hopper BAE Systems Threat Research Team, BAE Systems (4 April 2017)

[5] Ransomware groups continue to target healthcare, critical services; here's how to reduce risk Microsoft Threat Protection Intelligence Team (28 April 2020)

[6] BAE Systems Ransomware's Perfect Storm Infographic

[7] Double Dragon APT41 a dual espionage and cyber crime operation, FireEye (accessed 14 September 2020)

[8] Dark Basin John Scott-Railton, Adam Hulcoop, Bahr Abdul Razzak, Bill Marczak, Siena Anstis, and Ron Deibert, Citizen Lab (9 June 2020)

[9] Cyber Up Campaign

[10] BAE Systems MITRE ATT&CK Matrix paper

BAE SYSTEMS

At BAE Systems, we provide some of the world's most advanced technology, defence, aerospace and security solutions.

We employ a skilled workforce of 82,500 people in over 40 countries. Working with customers and local partners, our products and services deliver military capability, protect people and national security, and keep critical information and infrastructure secure.

Global Headquarters
BAE Systems
Surrey Research Park
Guildford
Surrey GU2 7RQ
United Kingdom
T: +44 (0) 1483 816000

BAE Systems
8000 Towers Crescent Drive
13th Floor
Vienna, VA 22182
USA
T: +1 720 696 9830

BAE Systems
Level 1
14 Childers St
Canberra, ACT 2601
Australia
T: +61 1300 027 001

BAE Systems
Suite 905 Arjaan Office Tower,
Dubai Media City
Dubai
T: +971 (0) 4556 4700

BAE Systems
1 Raffles Place #42-01, Tower 1
Singapore 048616
Singapore
T: +65 6499 5000

BAE Systems, Surrey Research Park, Guildford, Surrey, GU2 7RQ, UK

E: learn@baesystems.com | W: baesystems.com/theintelligencenetwork

linkedin.com/company/baesystemsai

twitter.com/baesystems_ai