Digital Security
Progress. Protected.

THREAT INTELLIGENCE – KNOW YOUR ENEMY, KNOW YOURSELF!

2023

Progress. Protected.

INTRODUCTION

In today's interconnected world, where cyber threats loom at every corner, the importance of staying ahead of potential adversaries cannot be overstated. As organisations increasingly rely on digital systems, they face a constant barrage of sophisticated attacks, with hackers becoming more cunning and resourceful with each passing day. To effectively combat these threats, a proactive and informed approach is crucial.

By understanding the tactics, techniques, and procedures (TTPs) employed by malicious actors, businesses and individuals can proactively fortify their defences, detect potential threats, and mitigate the risks associated with cyberattacks. But with so much information available, deciphering what is relevant and what needs to be actioned presents a significant challenge.

We brought together a number of CISOs, senior security managers, and heads of information security to share their thoughts, ideas and experiences surrounding these challenges at a series of roundtables. This eBook captures the key insights of these conversations.

OUR CONTRIBUTORS?

THE PROFESSIONALS WHO JOINED US AT THE ROUNDTABLES HOSTED AND MODERATED BY RELA8 GROUP'S TECHNOLOGY LEADERS CLUB INCLUDED:

- **CISO** at a world-famous manufacturer of luxury sports cars
- **Head of Information Technology** for a multinational financial services company
- **Head of Cyber Operations** for a major insurance provider and constituent of the FTSE 100
- **Information Security Manager** at one of the UK's largest retail supermarkets
- **Cyber Threat Intelligence Manager** at a leading personal financial service company in the UK
- **Information Security Manager** for one of the biggest football clubs in the Premier League
- **CISO** at a global business & technology management consultancy
- **Head of Cybersecurity** for a multinational bank and financial services company with assets around $1.1 trillion
- **Information Security Manager** within a major public healthcare system
- **VP of Product Management** at a multinational insurance company and component of the Euro Stoxx 50
- **Senior Manager of Cyber & Threat Intelligence** at a leading multinational telecommunications company
- **Head of Information Security** for the UK's largest independent hotel brand
- **Cybersecurity Operations Manager** at a global supplier of industrial products and constituent of the FTSE 250

OUR EXPERTS HIGHLIGHTED 5 MAIN CHALLENGES THEY EXPERIENCED WHEN NAVIGATING THREAT INTELLIGENCE

CHALLENGE 1:
GATHERING INTELLIGENCE

CHALLENGE 2:
CURATING YOUR FEEDS

CHALLENGE 3:
ACTIONING YOUR INTELLIGENCE EFFECTIVELY

CHALLENGE 4:
MEASURING THE VALUE & COMMUNICATING WITH THE BOARD

CHALLENGE 5:
ANTICIPATING THE FUTURE

ESET Digital Security **Progress. Protected.**

rela8 group | technology leaders club

CHALLENGE 1:
GATHERING INTELLIGENCE

HOW DOES THE BUSINESS GATHER INTELLIGENCE?

The function for intelligence is critical, but you need to know what you are getting and where from. There is no single source of truth for intelligence and no single feed is going to provide coverage for all possible threats – so how do organisations decide what intelligence to take in?

REAL WORLD SOLUTION: START BY UNDERSTANDING YOUR OWN RISK AND PRIORITISING KEY AREAS

Every organisation is unique and therefore will require a unique approach to gathering intelligence. There is no value in taking on every feed available to you if they are unlikely to have any relevance for your organisation. Therefore, to better optimise intelligence gathering, organisations must first have an understanding of their risks to build out their own intelligence requirements. For example, one provider might be offering intelligence on threats from the dark web, but does your organisation actually need it?

Once intelligence requirements have been established, then businesses can look at the intelligence sources available to them. Most organisations will find themselves constrained by budget, so when sourcing intelligence, prioritise feeds around your critical systems. You can't address everything with the same approach, so prioritisation gives you a chance to focus on the most pressing risks and build from there. Most businesses will be looking at a MSSPs and other threat intelligence solutions for the sourcing of their feeds, but ultimately, no provider will give you all the coverage you need, it's up to organisations to consolidate these providers and build them into their own ecosystem.

Outside of intelligence providers, it is worth remembering that there are a number of other sources available. For example, your pen-testers will have insights on the TTPs used against your organisation. If you are a Microsoft house, their Sentinel and Defender tools will provide intelligence relevant to your infrastructure. There is also a lot of value to be found in open-source intelligence and reports, however open-source intelligence will never be as contextualised and relevant to your organisation which means that it will need to be sifted through by your security teams to what is relevant to your organisation.

At the end of the day, threat intelligence is a game of resource management. Whether you are taking in intelligence from a service provider or are taking open-source feeds and mapping those to your organisation, balancing your available resource to ensure that relevant intelligence is being surfaced and actioned effectively is key.

"MOST ORGANISATIONS WILL FIND THEMSELVES CONSTRAINED BY BUDGET, SO WHEN SOURCING INTELLIGENCE, PRIORITISE FEEDS AROUND YOUR CRITICAL SYSTEMS. YOU CAN'T ADDRESS EVERYTHING WITH THE SAME APPROACH, SO PRIORITISATION GIVES YOU A CHANCE TO FOCUS ON THE MOST PRESSING RISKS AND BUILD FROM THERE. "

CHALLENGE 2:
CURATING YOUR FEEDS

HOW DO YOU CURATE YOUR FEEDS TO FILTER OUT THE NOISE, LEAVING BEHIND THE MOST RELEVANT INTEL?

It can be easy to mistake value in threat intelligence for quantity. The more feeds and intelligence you have coming in, the more threats you are aware of, the better protected you are – right? You can have multiple intelligence sources feeding into your system with the hopes of achieving some sort of 'completeness', but what of all of that intelligence is relevant, and more importantly, actionable for your business?

REAL WORLD SOLUTION: LEAN ON YOUR PROVIDERS AND EMBRACE AUTOMATION

When it comes to curating your intelligence feeds, taking the load off of your security teams should be your priority.

It is a waste of your resources and your teams' talent to saddle them with the chore of sifting through endless IoCs and IP addresses and will ultimately lead to burn out and SOC fatigue.

Furthermore, if you are taking in an uncurated feed and then spending a day filtering through it, you are already a day behind the intel. Instead, work with your providers. If you are paying for a threat intelligence feed, it should already be curated for your environment. The same goes for MSSPs, if they are taking in the intelligence feeds, then their output needs to be curated for your business from the start. If you offload the curation onto your providers, your second line security team in-house can spend their time analysing the data around relevant threats and taking quick action if needed.

If an organisation isn't able to outsource their SOC, the burden of feed curation should be offloaded onto automation and machine learning wherever possible. It's a good exercise to dive into open-source intelligence like MITRE and look for new information about TTPs and other IoCs and configuring it back into your platform, but it isn't sustainable in the long term without automation. Automation allows organisations to quickly search through feeds and incorporate updated alerts and indicators quickly and automatically into the protection layer.

There is a shift towards automation as a means of enhancing security response times and minimising human intervention. However, there will always be a need for human analysis, particularly when it comes to understanding how to respond quickly and effectively to new threats.

> **"IF YOU OFFLOAD THE CURATION ONTO YOUR PROVIDERS, YOUR SECOND LINE SECURITY TEAM IN-HOUSE CAN SPEND THEIR TIME ANALYSING THE DATA AROUND RELEVANT THREATS AND TAKING QUICK ACTION IF NEEDED."**

CHALLENGE 3:
ACTIONING YOUR INTELLIGENCE EFFECTIVELY

HOW DO YOU TAKE YOUR INTELLIGENCE AND ACTION IT EFFECTIVELY?

You could have the best threat intelligence feeds in the world, but it is completely useless if you have no resource or capability to do anything with it. Being able to act upon your intelligence is the whole point, but actionability and timeliness all come down to intel quality and resource availability.

REAL WORLD SOLUTION: FOCUS ON DATA QUALITY AND WORK WITH YOUR RESEARCHERS

Being unable to immediately act on reliable and relevant threat intelligence is indicative of a resource issue that needs to be prioritised before any more intelligence investments are made. These issues are usually caused by either poor data quality, or a lack of resource on-team to respond.

If you have outsourced your threat intelligence to a provider, having access to the researchers providing intelligence reports is a key element of their value. It might be that intelligence has come in, but a lack of certainty or confusion is slowing the response. It is at these times when the ability to quickly reach out to the researchers becomes so valuable. Being able to follow up and pull out more information from the experts is paramount from both sides of the equation as your researchers will learn more about your experience and network to better improve future research. Another notable benefit of having a researcher in your pocket is the ability to speak to an expert when big new threats hit the news-stands. It's good to be able to quickly speak with someone to discuss risk and exposure – particularly if the board or clients are on your back.

When on-team resource is the blocker, understanding where your team's time is being spent and reallocating as necessary is vital. Again, automation and machine learning can go a long way to free up your team to focus on responding to relevant intelligence. If your team is spending too much time analysing intelligence that can't be offloaded onto an MSSP or automated, prioritising your critical assets should be the main priority. If you focus your intelligence around specific areas, you can be quicker to respond, and it is easier to expand out from there as opposed to going all in and trying to catch everything.

You'll never get a complete picture of threat intelligence so understanding where you invest your efforts is key. If resource is an issue, focus efforts on the risks and potential damage that can be caused. If everything starts at risk, you can quite quickly determine what intel you need and what action you need to take.

> **"IF YOUR TEAM IS SPENDING TOO MUCH TIME ANALYSING INTELLIGENCE THAT CAN'T BE OFFLOADED ONTO AN MSSP OR AUTOMATED, PRIORITISING YOUR CRITICAL ASSETS SHOULD BE THE MAIN PRIORITY. "**

CHALLENGE 4:
MEASURING THE VALUE & COMMUNICATING WITH THE BOARD

HOW DO YOU MEASURE THE VALUE OF THREAT INTELLIGENCE INVESTMENTS AND COMMUNICATE WITH THE BOARD?

Threat intelligence is a relatively new industry and with plenty of organisations jumping on the bandwagon, it can be hard to measure the value of any investment. Alongside that, boards are clamouring for threat intelligence without really understanding what they are asking for. All of this creates a perfect storm whereby security teams struggle to articulate the value of their expensive investment to a board who doesn't understand it in the first place.

REAL WORLD SOLUTION: LET YOUR THREAT INTELLIGENCE SPEAK FOR ITSELF

When establishing value, it is helpful to be aware of the metrics of success you can use to measure value. For threat intelligence, reliability, actionability, and timeliness are all key metrics for good threat intelligence, but unfortunately don't mean much in terms of ROI to the board. Sometimes it is easier to present metrics in a way that they can action and support. For example, a good KPI for threat intelligence shouldn't be how many risks or threats have been identified, but the actions taken as a result of them. In this sense it is not what your intelligence has pointed out, but rather the actions you have taken as a direct result of it.

Another key element of communicating with the board is taking the intelligence and making it readable. Not only because their ability to understand it helps them to grasp its value, but also because it's the same intelligence that will be pushed up the line to communicate the risk to the higher ups. Having access to the people creating intelligence reports will help with summarised versions of threat reports better suited to be handed to the board.

THREAT INTELLIGENCE IS MORE THAN A MEANS OF MANAGING RISK, IT IS ALSO YOUR LIFELINE WHEN COMMUNICATING WITH THE BOARD. WHEN AN ATTACK HAPPENS, THE BOARD WANTS TO KNOW WHO, WHAT, WHY, AND HOW. IF YOU HAVE INTELLIGENCE REPORTS, YOU CAN EVIDENCE THESE ANSWERS AND SPEAK TO SOMEONE ON REMEDIATING THEM QUICKLY. HAVING THIS EXTERNAL VALIDATION ALSO HELPS TO DEMONSTRATE THE ROI OF THE INVESTMENT.

CHALLENGE 5:
ANTICIPATING THE FUTURE

HOW DO YOU ANTICIPATE THE FUTURE OF THREAT INTELLIGENCE?

Threat intelligence is a rapidly evolving space by necessity. As long as attackers are continually changing and upping their strategies, there will always be a need for ever more advanced threat intelligence. With the entire industry in flux, it can be difficult to anticipate the future of threat intelligence.

REAL WORLD SOLUTION: THE FUTURE IS COLLABORATIVE

One thing is for certain when it comes to the future of threat intelligence, it will become increasingly more important from a regulatory and compliance standpoint. Already some cyber insurance organisations have stipulated a requirement for a threat intelligence provision. Elsewhere, the New York Stock Exchange has proposed new cyber reporting guidelines that will require every publicly traded company to have a cybersecurity member on the board. Changes like this often spread like wildfire when implemented, so there is a strong possibility that the landscape for threat intelligence becomes far more streamlined and regulated in the coming years.

With more security experts on boards and a stronger emphasis on threat intelligence, the future is positioned to be far more collaborative.

Even now, security leaders are finding support within their industry in the form of shared threat intelligence networks because competitors know that there is more value in sharing intelligence than there is in hoarding it.

Instead of the same bit of intelligence being shipped around to countless organisations, greater cohesion could allow for a centralised network of reliable and relevant threat intelligence that is tailored by industry and geography.

COLLABORATION IS THE FUTURE OF THREAT INTELLIGENCE - THE CRIMINALS WORK TOGETHER, SO WHY SHOULDN'T WE? WITH NEW AND INCREASINGLY SOPHISTICATED THREATS EMERGING, WORKING TOGETHER TO ADVANCE THREAT INTELLIGENCE PROVISIONS WILL BE CRITICAL.

IN CONCLUSION...

Threat intelligence is a powerful and essential tool for proactive protection of digital assets. However, achieving true effectiveness requires more than just gathering vast amounts of data. It necessitates a strategic approach that prioritises key areas, understands risks, and builds intelligence requirements tailored to your organisation.

In the realm of threat intelligence, the pursuit of "completeness" is a fallacy. It is vital to curate your feeds and understand the data you receive, its sources, potential duplications, utilisation, value, and the gaps in your intelligence. Quality always surpasses quantity when it comes to threat intelligence. By focusing on relevant threats and curating your strategy accordingly, you can optimise resource utilisation and take swift action in response to emerging risks.

The ultimate purpose of threat intelligence is to drive action. It goes beyond simply alerting you to the presence of a fire; it provides the knowledge and guidance to extinguish the flames or prevent them from igniting in the first place. By embracing the power of threat intelligence, organisations gain the ability to stay one step ahead of their adversaries in the dynamic and ever-evolving digital world.

THANK YOU

We would like to thank everyone who participated in our roundtables. The frank and open discussions helped to shine a light on the challenges happening in the real world, and some of the solutions they have adopted to address them.

For more information about ESET's solutions, please visit **eset.com/uk/**

For more information about Rela8 Group and the Technology Leaders Club, please visit **www.rela8group.com**

ESET® Digital Security Progress. Protected.

rela8 group | technology leaders club