Why collaboration makes cybersecurity stronger

While the last few years have been defined by nation states untangling long-standing international collaborations on cybersecurity, 2021 will see security vendors and professionals step up and collaborate to fill the void, writes Neil Thacker, CISO EMEA at Netskope.

Cybersecurity professionals have a great record of collaboration. Cybercrime pays no regard to international borders and so fighting it is a process that has always relied upon countries collaborating and sharing data. It is for this reason, perhaps, that many in this sector have felt a degree of trepidation this year, as geopolitical manoeuvres have cast uncertainty around some of our established mechanisms for collaboration.

Clarification of the frameworks and regulations that will replace some of the tried, tested but outgoing agreements have been drip-fed through to IT and security leaders; however, many of us are still feeling confused about both obligations and opportunities for cyber defence tactics.

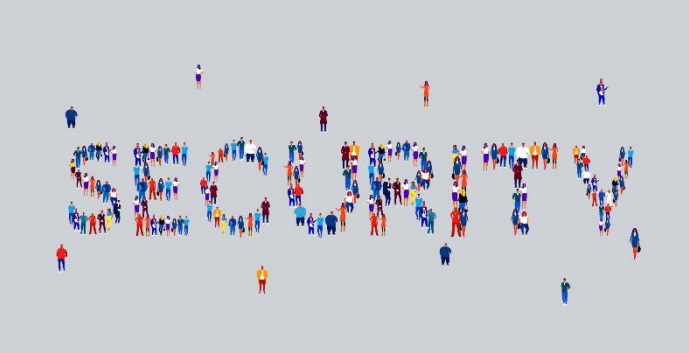

Figure 1 - Collaborative Teamworking for Security

Brexit has been one of the more pressing concerns for organisations, but obligations are being clarified. For example, in May 2020, the European Commission issued a statement clarifying which areas of the NIS Directive will, and will not, continue to apply to UK businesses after Brexit. Nevertheless, collaboration around cyber and data defence isn't just about obligations.

A collaborative past

Historically, the UK has been the second biggest contributor to Europol Information Systems. This is undoubtedly one of the reasons why Michel Barnier, the European Commission's top Brexit negotiator, told attendees at Web Summit 2019 that the EU and the UK must join forces after Brexit to fight cyber-threats:

'Our new partnership should include the exchange of information on cyber incidents, attackers' techniques, threat analysis and best practice, including when those target the correct functioning of democratic systems. Crucially, we need to have capacity to respond jointly to such attacks.'

So, while (after 20 years of involvement) the UK no longer has a place on the team that manages Europol, we know there's both appetite for collaboration to continue and a natural inclination among cybersecurity professionals to work together. The opportunities for collaboration have not gone away.

A collaborative enemy

The bad news, however, is that collaboration is also something that threat actors do very effectively. In recent years, we have seen no abatement to the increasing levels of organisation and collaboration among malicious actors. They are a sophisticated adversary. We know that when government agencies manage to flip cyber criminals and get them to provide intelligence on the networks in which they operate, we find a tangled, well-funded and profitable web of recruiters, programmers, hosting providers and distributors.

Why collaboration is so powerful in cybersecurity

Collaboration comes in many forms. The exchange of information through Interpol is just one, very top-level example, but not necessarily one that we cybersecurity professionals will be involved with day to day. But, our forms of collaboration are no less effective.

Figure 2 - The Power Of Collaborative Connection

We can work with our colleagues from non-tech departments more effectively; we can form better connections with our peers from other organisations; and we can insist upon our technology partners working in a much less siloed manner. All of these efforts will see significant reward.

Let's start with the last of those three: in the past, security vendors worked in pursuit of a vision of their brand being the sole or primary provider of a customer organisation's security estate. If other vendors had to be involved, there was a clear hierarchy and these 'competitors' were kept at arms' length by the bigger vendor who wanted to own the ear of the CISO.

The benefits of collaboration between vendors are, however, undisputable and fortunately now being understood.

Yonatan Striem-Amit, Chief Technology Officer and Cofounder of Cybereason, says that 'Intelligence gathering and information sharing is vitally important to detecting, preventing and mitigating risks and hardening our cyber resiliency.'

Collaboration reduces the time between new threat discovery and protection implementation, allowing organisations to keep up with the ever-evolving threat landscape. Interpol is working hard to identify and stop the malicious actors, but in the meantime, those of us who are tasked with protecting our organisation from these threats still need information on the latest threats to avoid falling foul of them.

Speeding the delivery and dissemination of threat intelligence is crucial for building a strong cybersecurity programme and vendors need to make it as easy as possible to break down the silo walls between security disciplines and automate the exchange of threat indicators.

Let's put this into context. According to Netskope's August 2020 Cloud and Threat Report, cybercriminals are continuing to use the cloud as an attack vector in new ways, and this has only been exacerbated by the surge in remote working caused by the COVID-19 pandemic. Between January 1 and June 30 2020, cloud malware delivery and cloud phishing were the two most common types of cloud threats and 63% of malware was delivered over cloud applications.

Mitigating these types of attacks requires multiple defences with unique capabilities and focus points, all sharing timely threat intelligence. A threat actor may combine multiple types of attacks including phishing, malware and data theft. An organisation improves their capabilities to stop such an attack by sharing details of the threats across all of their protections.

Barriers to collaboration

Driven by the traditional approach of security vendors, historically, there have been multiple barriers to sharing threat intelligence, which made it difficult to implement at scale. For example, vendors might use APIs or data formats that require proprietary tools or plug-ins to commercial products for translation.

In addition, the tools were typically built in a hub and spoke manner, making it possible for a single vendor (the hub) to benefit from multiple sources of threat intelligence (spokes), but lacking the ability to set up any other type of threat sharing arrangement.

Collaboration in action

In the autumn of 2020, Netskope announced the Cloud Threat Exchange (CTE), a free tool that can be used by any member vendor and their customers to exchange threat intelligence. At launch there was already a strong list of certified members, including Netskope, VMware Carbon Black, CrowdStrike, Cybereason and SentinelOne. This ecosystem was designed to help organisations maximise the benefit of their protections by leveraging threat intelligence across multiple enforcement points.

The goal of collaboration between vendors in this way is to rise above competitive attempts to work in isolation and combine knowledge of indicators of compromise (IOCs) to enable customer organisations to improve their overall threat prevention posture. It is a noble goal.

In practice, the approach sees the ingestion, curation and real-time sharing of threat intelligence across enterprise security enforcement points. It automates the delivery and distribution of high-value, actionable threat intelligence, thus reducing the time to protection and eliminating gaps in coverage. Threat indicators that are shared include file hashes, malicious URLs, and DLP file signatures.

Crucially, this model is not hub and spoke - communication can flow directly between vendors and customer organisations and does not require intermediation by any one central 'master' vendor. All vendors that have signed up to the CTE will be able to notify each other's systems of any attack that their technology identifies.

A web gateway can identify a threat, share the information to the CTE central repository and the other solutions within the security architecture will be able to draw down that information. This is designed to vastly improve joint customers' speed of response to threats and avoid intelligence sitting in silos.

CISO collaboration

Vendor-driven collaboration isn't the only positive sign of a new appetite for working together among the cybersecurity profession. The unique challenges facing CISOs amid the COVID-19 pandemic in 2020 have been a driver for stronger peer support among user organisations too.

Perhaps ironically, given face-to-face networking was not an option, there have been reports of a growing openness to knowledge and idea sharing in CISO forums such as (ISC)2, ISACA, ENISA and ISF.

These networks enable security leaders to share best practice and discuss their challenges in a safe space, because two heads are always better than one for problem solving. These sorts of peer networks can, in time, also become powerful influences in driving security vendors to further collaboration for the benefit of customers.

Conclusion

Over the last few years, we have seen a lot of changes which have the potential to make our jobs as cybersecurity professionals more difficult to carry out day to day. And these challenges have emerged while we have seen the malicious actors - against whom we do daily battle - benefit from greater funding and closer operational collaboration. But there are clear signs that we are learning good lessons, both from our previous successes and those of our enemies. Security professionals are successful when we collaborate and I am confident that none of the challenges we have seen in 2020 and beyond will thwart us in our natural inclination to work together.

See more on Security Training from TSG Training