STRATEGIC SHIELD

LEVERAGING THREAT INTELLIGENCE FOR SECURITY RESILIENCE

LEVERAGING THREAT INTELLIGENCE

OVERVIEW

In today's rapidly evolving cyber landscape, organisations face increasingly sophisticated and persistent threats. Against this backdrop it is vital that enterprises properly understand threat actors' methodologies to effectively protect themselves through the use of threat intelligence.

During this recent Infosecurity Magazine webinar, in partnership with SCC, a panel of experts explored the core concepts of threat intelligence and its critical role in proactive defence strategies. They discussed how enterprises can effectively use threat intelligence to respond to incidents and enhance their existing security capabilities.

OPENING PRESENTATION

This session began with Paul Allen, Practice Director, SCC, taking us on a journey through threat intelligence. Allen noted that the challenges faced by organisations and consumers are significant with a huge number of phishing campaigns being experienced every second of every day.

To be more efficient and adept at defending against these threats we must be willing to learn, Allen said. He noted that threat intelligence only becomes intelligent when it becomes actionable. It is about taking those indicators of compromise (IOC) and understanding how they can be applied to enhance security.

For example, there may be data sets that need to be used tactically and then can have a technical layer of intelligence applied that enables Security Operations Centre (SOC) staff to enrich and contextualise threat actors and deliver outcomes faster.

It could be that you are looking to provide information on specific attacks and threat actors; the concept of attribution is challenging but useful if you want to understand your adversary. This will have an impact for security managers as to how they structure and organise defences, Allen highlighted.

Other things to consider are how the adversaries are evolving and becoming more adept at protecting themselves from the defenders. Allen said that keeping up with tactics is important to stay ahead.

When operationalising threat intelligence, CISOs need to seek outcomes and how benefits, including efficiency savings and cost savings, can be delivered from the intelligence. It is important to provide context to the data that is presented, and it must be applied to the real world.

Does your organisation leverage cyber threat intelligence?

A) Yes, we are able to collect and analyse data internally (60%)
B) Yes, we work with external parties to provide these insights (20%)
C) No, but this is something we are considering (20%)
D) No, we do not think these insights are necessary (0%)
E) No, we do not have the resources/capabilities (0%)

THE EVOLVING FIELD OF THREAT INTELLIGENCE

Cyber threat intelligence (CTI) is a fast-moving world and Mark Tibbs, Cyber Intelligence Director, Mishcon de Reya LLP, noted that in his eight years of experience in the field, organisations now have greater situational awareness and have become more aware of the importance of CTI as a proactive approach to mitigating cyber threats. He pointed out that the WannaCry ransomware attack in 2017 marked a turning point in how people approach CTI.

In addition, there is now more of an emphasis on the strategic importance of CTI and linking it with how to prioritise resources. Finally, Tibbs noted how threat hunting is more apparent than ever, moving beyond just the passive gathering of intelligence.

Jonathan Care, Advisor, Lionfish Tech Advisors, observed that threat intelligence has evolved beyond the point of “that’s interesting” to it being highly actionable and machine consumable. On the latter point he noted that IOCs can now be fed into firewalls, SIEMs and other tools to produce useful, strategic outcomes.

IMPLEMENTING CTI

Looking ahead, for organisations that are considering consuming and using threat intelligence, there needs to be a strategy and understanding of ‘why’ and defined objectives should be devised, Allen said. He also emphasised the automation of processes as beneficial when dealing with time critical intelligence.

It is important to for enterprises to consider “what level is good enough.” Allen explained that depending on the organisation’s risk profile and security posture there may be other fundamental security activities to be done first before adding the intelligence piece that ultimately gives you the additional layer of capability.

Care concurred that a high level of maturity in other elements of security should be in place before considering the intelligence piece. Tibbs noted: “You will give your organisation the best chance of succeeding and responding to an incident should it happen if you have threat intelligence feeding your security operations, strategy and incident response than if you didn’t have it.”

CTI can assist incident responders in speeding up their processes and response, to get systems up and running more quickly. It also helps identify if a threat is credible or not. Tibbs said that it is more difficult to measure the value of CTI in preventing attacks happening but is vital in “oiling the wheels” of the response when an incident does happen.

There are of course challenges many organisations will face when implementing CTI into their security operations and the panel provided advice on how to overcome them. Allen said one of the biggest challenges is always the actionability question – how to get the best outcomes from CTI. SCC looks to communicate the value of CTI to their customers so they have a clear view of what is looking to be achieved and why.

Having the required skillsets to interpret and action the data can also be a challenge for companies and Allen highlighted that managed service providers, like SCC, can be there to step in and provide those skills that may be missing in-house and can help organisations achieve maturity more quickly.

What is the biggest challenge with leveraging cyber threat intelligence into organisations' security strategies?

A) Time/resources to analyse data and make it relevant to individual organisations (50%)
B) Skillsets to interpret and action the data (33%)
C) Co-ordinating with third parties – e.g. threat intelligence and MDR providers
D) Other (17%)

THE IMPACT OF AI

Time is a critical factor and with IOC there is an element of time sensitivity. Therefore, if you can identify things quicky and action them accordingly you are in a much better place, Allen noted. As we look at the drive to using automation and AI more effectively, with things like Microsoft's 365 Copilot, you're going to see us try and support analysts to make things actionable, he added.

"I hope that the time to value from an intelligence perspective can be reduced but all of these things are a work in progress, and we are evolving at a huge pace at the moment," he said. Tibbs noted that regarding the role of emerging technologies, machine learning and automation has already been incorporated into many tools and businesses that are generating CTI.

He said that he is interested to see where generative AI and large language models (LLMs) go in the future and predicted that it is probably going to be an arms race between attacker and defender as to how it will be used to achieve their respective objectives.

However, he cautioned that we have not really seen the full application of how that can come to fruition and the fraud and threat landscape has not been changed dramatically just yet.

Tibbs added that if you have the capability to learn an attacker's behaviour it is likely that you will then develop a great defence.

Care said in financial fraud AI models have already been used to identify patterns that are below the limit of human observability.

He noted that, relating to the clients he works with, generative AI is being explored in relation to whether it can be used in conjunction with an ML model that is giving a risk decision.

However, with every defender using AI there is another side of the coin and Care cautioned that “we have seen attackers use AI.”

CONCLUSION

Ending the session, each panellist gave their key takeaways relating to the use of CTI over the coming years.

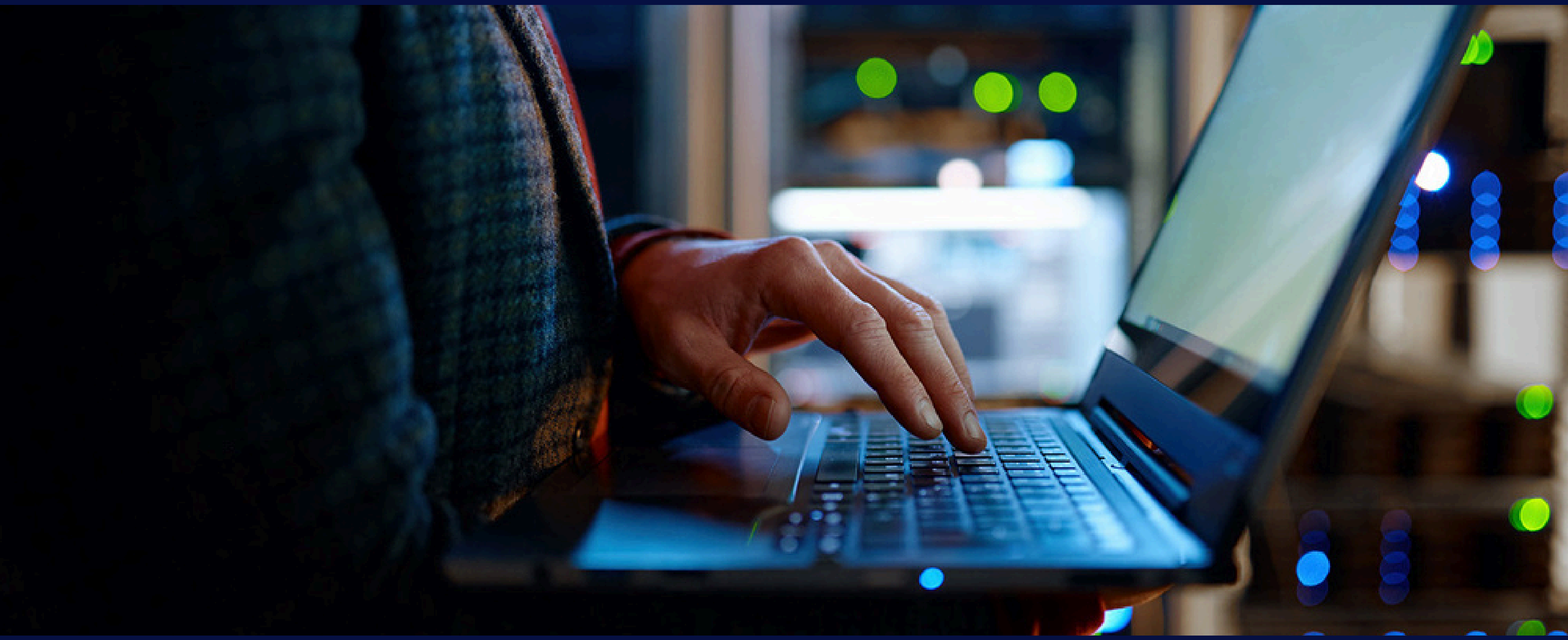
Allen said: “For any organisation considering CTI or a cybersecurity strategy it is key to plan, understand and define what you would consider to be a good outcome, and to look at your stage gates along that process. If you are moving through a crawl- walk-run process, consider how you identify each of those phases, sign them off and move on to the next”.

He noted that planning is key, this goes for the threat intelligence perspective and companies should consider how to make the marginal gains required, as well as how to be as efficient as possible given the operational and real-world constraints that exist.

“There is no such thing as a silver bullet, and everyone has operational blockers within their world. It is about how you add as much value as you can within those constraints that will make a difference between a good or a bad outcome,” Allen said.

Tibbs noted that having a well-defined strategy, the right technology investments and the correct skills development within the team are also all key.

Finally, Care concluded that understanding what you are expecting from your CTI sources and providers and understanding how those fit into your detection, protection and response models is vital.



CREATING CYBER CONFIDENCE WITH SCC

At SCC, we redefine cybersecurity by seamlessly blending reliability, expertise, and a commitment to your journey in the digital landscape. Our comprehensive solutions are tailored to your organisation's needs and its maturity level, ensuring a robust defence against ever-evolving cyber threats.

Moving beyond today’s security paradigms, we're architects of a new era—one where security isn't just a measure but a culture.

Our people make the difference—through collaborative partnership, and proactive support, we create the confidence to push boundaries securely.

With expert guidance tuned to your growth ambitions, we help clear obstacles, accelerate outcomes, and embed effective security principles across people, process and technology.

Our cyber advisory services meet you wherever you are on your maturity journey, whether your looking to maintain your posture from the evolving landscape or enhance your risk profile, we are here for you:

- Supporting across people, process & technology
- Trusted cybersecurity advisor
- Simplify the complex