TRIDENT SEARCH

THE TI CLUB SUMMER GET TOGETHER

Exploring Intelligence Fusion

THE TI CLUB SUMMER GET TOGETHER

In July 2024, Trident Search welcomed expert guests and leading industry figures to the second get together of the TI Club. Having explored critical trends earlier on in the year, we wanted to pivot the focus to one of the most exciting and, in many ways, under-represented areas of threat intelligence – intelligence fusion. With input from three exceptional panellists, Stewart Bertram, Aadrien Luke and Ellen Hallam, we explored why intelligence fusion is so important, the trends we can see with it over the next few years and the lessons we can take from the military to the mainstream.

The TI Club

Set up by Trident Search in 2023, the TI Club is an exclusive network for the threat intelligence community. Designed to be a hub where we can come together to discuss the intelligence landscape, share our latest developments and explore trends, tools and opportunities with others in the industry, the Club has swelled to over 200 members, and is now a strong network of TI professionals.

Whether you're a seasoned expert or just starting out in your career, the TI Club is a dedicated space for you to share insights, exchange intel and connect with peers across the industry.

With thanks to our panel of industry leaders who shared their insights and experiences over the course of the evening:

Stewart Bertram,
Nomura

Aadrien Luke,
SecAlliance

Ellen Hallam,
Bytes

SecAlliance TRIDENT SEARCH BYTES NOMURA

WHAT IS INTELLIGENCE FUSION?

Put simply, intelligence fusion refers to the integration of various data sources and analytical techniques to provide a comprehensive overview of the threat landscape.

By combining information from areas such as network security, dark web intelligence, physical security and even external intelligence feeds, CTI teams can identify patterns and concerns that might be missed when looking at data in isolation. Aadrien Luke summed it up well, by commenting that fusion is essentially **"CTI plus anything else"** and that the purpose of analysis within a fusion cell is to **"grab uncurated information and make something of it!"** Many security teams are likely already doing this, but it remains a largely misunderstood area of the CTI landscape.

Yet there's plenty of evidence that taking a more holistic view enhances the detection of sophisticated threats, improves incident response times and reduces the likelihood of false positives.

As proponents of integrating intelligence fusion into standard industry processes, our panel took us through many of the benefits. One of the most interesting talking points from the evening came from Stewart Bertram, who outlined how fusion poses very different opportunities for organisations at each end of the development spectrum.

For SMEs or startups, the main benefit is to maximize your resources. With limited tools and technologies, you must be able to use every asset at your disposal, whether these are unpolished or not. Yet for larger enterprise firms with the ability to finance extensive tooling, fusion is primarily an important means of catching **"low contact adversaries"** who leave a more scattered digital footprint.

OTHER BENEFITS INCLUDE:

Improved Incident Response: Correlating data in real-time allows for faster identification and mitigation of security incidents.

Reduced False Positives: Enhancing accuracy in threat detection by cross-referencing diverse data points will minimize the number of false alarms you face. Using fusion helps to validate sources of information and corroborate what your teams are seeing.

Proactive Threat Management: As Ellen Hallam says, it's better to be **"proactive than reactive."** Fusion helps you to identify potential threats early, enabling organisations to take preventive measures before incidents escalate.

Combat Misinformation: Cross-checking multiple sources helps to identify and address false information, ensuring that decisions are based on accurate and reliable data. In effect, filtering out the noise to find the key information you need.

Enhanced Collaboration: One united fusion cell instead of multiple silos means better communication and coordination across different departments. This also benefits clients looking to take on security partners by reducing the number of providers they need to use.

Resource Optimization: Streamlining security operations ensures a more efficient allocation of resources by prioritizing high-risk threats.

Adaptive Security Posture: With so many information sources, fusion teams continuously evolve and adapt to new threats by integrating emerging data sources and advanced analytical techniques.

THE CHALLENGES FACING CTI TEAMS

With so many benefits, the question needs to be asked – why is fusion not being used more widely in our security architecture?

Ultimately, says Ellen Hallam, it comes down to resourcing. Intelligence leads often have a hard enough time getting across the value of CTI, so getting the CISO or executive team to buy into fusion is a real challenge. In the vendor space, getting clients to commit to the service is a fight given the volume of CTI options in the market.

For those who have transitioned to the private sector from the military, there is also an adjustment to be made regarding the differing permission sets professionals are able to work within. To access some of these data sources, particularly human or dark web intelligence, private sector providers have to work to the parameters set by their clients. It is somewhat of a grey area, as handling and analysing large volumes of data can raise concerns about privacy and regulatory compliance, necessitating robust governance frameworks which not all businesses have.

With the aim of there being **"a golden thread from pen testing to auditing"** connecting all intelligence functions, there's clearly a long way to go.

So, what can we do?

To push fusion to become more mainstream, companies must prioritize the sharing of intelligence and information across various platforms and stakeholders. Our panel noted that events like the TI Club where professionals can network, exchange information and foster relationships across the sector are a game changer for enhancing our collective security efforts.

Furthermore, promoting open CTI initiatives ensures that everyone benefits from shared knowledge and resources, making us all more reliant in the face of cyber threats. This collective, information sharing approach helps those struggling to demonstrate the value of CTI to improve proactive and reactive threat intelligence capabilities, thus increasing the ROI of investment in the function and securing future buy-in.

Finally, and most importantly, persistent advocacy in your own organisation is essential – if those within CTI see the benefit, it won't be long until Boards and Leadership teams can be brought on board too.

TRIDENT SEARCH

In an era where cyber-attacks are increasingly sophisticated and prevalent, proactive and experienced defensive teams are critical for safeguarding sensitive data, ensuring operational continuity and maintaining trust with stakeholders. As an industry, it's time we came together to share our lessons and learnings – the more collaborative we can be, the better our chances against attackers. Ultimately, better cooperation benefits everyone.

Thank you to all our panellists and incredible guests who came from across the CTI sector to share their insights and feedback during the event. The TI Club is a forum for exchanging these ideas, and the community is always keen to share.

If you would like to become more involved in the TI Club or become part of our network, contact:

Maurice Mackness
CTI Recruitment Lead, Trident Search
E: maurice.mackness@tridentsearch.co.uk
M: +44 (0)7903 098569