CTIPs
CREST Threat Intelligence Professionals

Assessment of Global Intelligence Led Penetration Test Frameworks

CREST

Contents

Executive summary

The global proliferation of Intelligence Led Penetration Testing (ILPT) frameworks across all industry verticals since 2014 has seen massive increases in regulatory understanding of common vulnerabilities in organisational cyber resilience. However, throughout this period little changes to frameworks has been seen, nor research into how the frameworks are perceived by either the customers or delivery consultants. This paper has drawn upon research conducted with the support of CREST approved Cyber Threat Intelligence (CTI) providers to try and identify common themes and to make suggestions as to how to move the frameworks forward.

As a caveat, this paper has only considered intelligence led testing against Tier 1 firms as it is noted that recommendations made may not be as appropriate for SME engagements, many of whom have a lesser internal Cyber Threat Intelligence capability.

Overall, and as discussed in greater detail later in the paper, conclusions that have fallen out of this research can be summarised as follows:

- Customer desire for a singular ILPT framework
- Requirement for increased flexibility in report formats to better support customer needs
- Positive support for use of Mitre Adversarial Tactics, Techniques and Common Knowledge (ATT&CK) framework to deliver attack scenarios
- Growing support for active reconnaissance by CTI providers, with caveats
- Potential requirement for upskilling of CTI providers to support active reconnaissance
- Strong support for CREST CTI Maturity Assessment
- Desire to expand framework to incorporate ‘Purple Teaming’
- Perceived lack of engagement and value by National Intelligence Agencies

Based on these conclusions, a number of suggested recommendations are made and have summarised below. Full details of each recommendation can be found later in the paper.

- Global regulatory bodies are encouraged to continue existing collaboration around delivery of ILPT and should potentially consider development of a singular global ILPT framework acceptable to all.
- ILPT framework owners should engage with CTI providers, possibly using CREST Threat Intelligence Professionals (CTIPS) as an intermediary, to help develop more applicable Targeting and Threat Intelligence report formats.
- CTI providers should be encouraged to design attack scenarios that contain enough freedom of movement for Red Teams should primary attack paths relating to their chosen threat actor not be successful.
- ILPT scenarios provided by CTI teams should be mapped to Mitre ATT&CK, with Red Teams layering the actual TTPs used into the same tables.
- The issue of active reconnaissance should be explored further by framework owners, potentially through pilot engagements, to identify whether this practice brings the expected benefits to Red Teams and customers.
- The focus of each ILPT engagement should be switched from being primarily identifying vulnerabilities within target organisations to helping them upskill their internal defenders through developing greater understanding of attacker methodology. Further, CTI reporting should not just be tailored to support red team activity but should provide value to the client by helping them to reduce their targetable footprint.
- National Intelligence Agencies involved in supporting ILPT frameworks should be encouraged to discuss with framework owners how they can increase their perceived value to organisations.

Introduction

To support broadening industry knowledge around existing global intelligence led penetration testing (ILPT) frameworks, CTIPS commissioned a piece of research into better understanding consultant areas of concern related to the frameworks, and where potential improvements could be made following several years of delivery.

The aim of this paper is to provide an overview of these findings, following thematic analysis, based on a limited number of survey responses received from CREST approved Threat Intelligence providers. Each provider was provided with a set of defined questions relating to ILPT frameworks via Survey Monkey and asked to provide comment based on their own experiences.

The findings in this paper are not reflective of CREST or CTIPS and are merely an anonymised representation of views from the respondents, all of whom are employed by those firms responsible for delivery of these frameworks in support of global regulators.

Each respondent was provided with the following 11 question and asked to comment:

- Given that the various global ILPT frameworks (*BEST/TIBER/iCAST/etc) have each adopted slightly different approaches to the delivery of threat intelligence reporting, which approach have you found to be preferred by clients, Red Teams, yourselves and why?
- Post-ILPT engagement, what is the most common piece of feedback you have received from both Clients and Red Teams regarding CTI reporting? What changes, if any, have you made to your processes as a result of this feedback?
- When considering both Threat Assessments and Targeting reports, which elements do you believe to be essential and which do you believe are redundant? Applying MoSCoW to your response would be advantageous.
- Do you think that CTI providers should be able to conduct active CTI collection in support of ILPT engagements?
- What do you believe would be the benefits associated to this?
- If active CTI collection was supported by framework owners what additional risks would you envisage, and how would you mitigate these risks?
- When designing attack simulations / threat scenarios what is your preferred format(s)? What are the benefits of these preferred option(s)?
- Are Threat Actor profiles beneficial to delivery of an ILPT engagement or just extraneous information? What are the positive and negatives of including them?
- What is your view of the new CREST CTI maturity assessment? What are the benefits of this assessment replacing existing KPIs and being considered a standard element for future ILPT engagements? (A refined, less detailed version is currently being authored)
- Wide changes: If you could make wider changes to the existing ILPT (not just the reporting) what would it be, and why?
- Wide changes: If you could make changes to the Red Teaming stages specifically, what would they be?

Thematic Analysis

This section will now look at each question in more depth and will use the responses provided to draw out key themes in relation to each.

Q1. Given that the various global ILPT frameworks (*BEST/TIBER/iCAST/etc) have each adopted slightly different approaches to the delivery of threat intelligence reporting, which approach have you found to be preferred by clients, Red Teams, yourselves and why?

Whilst responses to this question are mixed it does appear that the respondents tend to find that overall the existing *BEST framework is the best defined, and that the regulators are most engaged in TIBER engagements. Given that this particular question was not framed to illicit either a positive or negative view of regulatory involvement this perception may be viewed two ways, firstly that the EU regulators desire closer participation to ensure validity of results, or that remaining regulators prefer to place greater trust in their providers through a thorough accreditation process and a more hands-off approach. From a client point of view responses indicated no real preference for a particular framework.

One interesting theme that did arise from this question was that both providers and multinational organisations in the global financial sectors would prefer to see a singular framework rather than the existing suite being used. For multinationals this position of undertaking a singular test, accepted by each regulator, has many benefits including cost and resource savings, simplified scoping and regulator liaison, and consistency in remediation.

Q2. Post-ILPT engagement, what is the most common piece of feedback you have received from both Clients and Red Teams regarding CTI reporting? What changes, if any, have you made to your processes as a result of this feedback?

When looking at existing ILPT threat intelligence reporting two key themes emerge; reports can be too generic and too lengthy. Looking firstly at the issue of uniqueness, this is an issue that has been previously raised around ILPT Threat Intelligence reports with verbal feedback received questioning their relevance to the target organisation. In the financial sector it feels that this perception can be slightly enhanced given that the majority of those undertaking this form of test are likely to face very similar threat profiles based on their role and function. Overall, Targeting reports are stated as being most useful to clients given that they are more tailored in nature.

With regards reports being too lengthy, this again has been raised in relation to Threat Intelligence reports in the past but is also to an extent now true of Targeting reports, some of which stretch to over 100 pages. During the survey respondents queried whether it might be better capping the number of pages in the main reports and adding raw data as either separate appendices or separate documents.

Q3. When considering both Threat Assessments and Targeting reports, which elements do you believe to be essential and which do you believe are redundant? Applying MoSCoW to your response would be advantageous.

Across the board the overwhelming view is that the Targeting report (also known as the Targeted Threat Intelligence report) is an essential element of Intelligence Led Penetration Testing. Whilst the content of this report is not directly covered there appears to be a view that the format should be left to the relevant providers as this allows greater flexibility and means that reports can be better tailored to the customer rather than following a standardised ‘one size fits all’ structure.

When looking at Threat Intelligence reports (also known as Generic Threat Landscape reports for TIBER) opinion is slightly more split as to the relevance and content with only 25% of respondents favouring inclusion of threat actor profiles as a must have element. The prevailing view indicates that respondents would prefer to include defined threat scenarios, developed around the Mitre Adversarial Tactics, Techniques, and Common Knowledge framework (Mitre ATT&CK), which are then supplemented by detailed analysis of capability and intent for threat actors considered most likely to manifest attacks against the core elements of the customer’s business. In terms of supporting customer internal risk functions this inclusion of ‘likelihood’ of attack is viewed as key to enabling customers to understand their risk profile and remain within risk appetite.

Q4. Do you think that CTI providers should be able to conduct active CTI collection in support of ILPT engagements?

Q5. What do you believe would be the benefits associated to this?

Given their close association responses to Questions 4 and 5 have been merged together.

Firstly, across all response's opinion was equally split with 50% of respondents favouring active CTI collection and 50% against. In terms of the arguments posed for each the following is noted:

In Favour

Whilst passive reconnaissance is viewed as the lightest touch it is also underpinned by a belief from respondents that information collected in this manner is often dated, uncorroborated and unvalidated. The general view of those in favour of this methodology is that active reconnaissance would allow them better opportunities to reduce false positives in reporting, potentially raising customer perceptions about the overall value of the products.

Against

The prevailing argument against active reconnaissance appears to revolve primarily around the perceived skills of those conducting the activity rather than a direct rejection of this form of methodology. The view of the respondents is that without the right skill set to perform this action CTI providers could accidently trigger internal alarms alerting defenders to their action, in the case of 'black box' security testing this alert could result in a higher state of readiness during actual testing and skew the overall results.

Whilst the view against active reconnaissance is equally split it is possible that this balance could shift towards 'in favour' should the activity be conducted by a trained security tester perceived as more adept at this action.

Overall, whilst opinion is split, this is more associated with the skill of the individual rather than direct opposition. If CTI providers were to employ specialists into this role with a security testing background it is likely that any opposition to this methodology would drop away.

Q6. If active CTI collection was supported by framework owners what additional risks would you envisage, and how would you mitigate these risks?

Three key areas were flagged by respondents in response to this question, time, legality and operational security. With regards time there is a belief that in order to fully validate results the length of time provided for CTI collection may need to be extended. No specific preference was noted in the responses as to whether this increased time should fall before security testing activity commences or run concurrently.

The second key area flagged was around CTI providers obtaining suitable legal authorisation from the customer for active reconnaissance given its propensity to directly impact network operations. Strict boundaries would need to be considered, similar to how security test plans are developed, to ensure that CTI providers stick to specified parameters and do not cause any network outages as a result of their actions.

The final area considered as a potential risk to test activity harks back to the answers to the previous question and relates to a lack of operational security by the CTI providers potentially triggering responses from internal defenders.

Q7. When designing attack simulations / threat scenarios what is your preferred format(s)? What are the benefits of these preferred option(s)?

As highlighted in Question 3, respondents were overwhelmingly in favour of utilising the Mitre ATT&CK framework for development of attack scenarios. The common view is that this framework provides suitable flexibility across its tactics and techniques to allow development of credible scenarios and enable Red Teams to use slight variations should the primary attack path be unachievable. This flexibility is viewed as key to achieving greater realism from test activity. However, as Intelligence is also about the 'so what' consideration should also be given to keeping written dialogue for both 'pre-cursers' to attacks and the so called 'denouement' (fallout/impact) to ensure the scenarios provide the 'so what' in a business context.

Q8. Are Threat Actor profiles beneficial to delivery of an ILPT engagement or just extraneous information? What are the positive and negatives of including them?

Whilst Question 3 called out CTI provider preference to exclude threat actor profiles in threat intelligence reports there were contrasting views as follows:

Positives

For smaller organisations it is felt that threat actor profiles can be useful. This perception is based upon the belief that these types of firm may not yet have fully mature threat intelligence functions and therefore could benefit from a greater understanding of those actors considered most likely to attack their network. In addition, although only a minority opinion, it is felt that the profiles provide context to the attack scenarios and help set the scene. An additional benefit of including threat actor profiles, and this is applicable across all sizes of organisation, is that they can help support validation of internal threat modelling perceptions, which from an audit perspective can be a valuable tool to customers.

Negatives

One of the greatest issues with the inclusion of threat actor profiles is that they are viewed as merely being added to 'pad out' the Threat Intelligence report rather than adding any specific benefit. In addition, there is a view that more mature organisations already have this information available and do not see the worth.

Q9. What is your view of the new CREST CTI maturity assessment? What are the benefits of this assessment replacing existing KPIs and being considered a standard element for future ILPT engagements? (A refined, less detailed version is currently being authored)

The new CREST CTI maturity assessment is viewed by the majority of respondents as being a great tool for organisations looking to build their capability and maturity, although the full version is seen as quite cumbersome given the length of time required to complete. Overwhelmingly, respondents support the framework but would favour introduction of a less detailed version that could be used in a more agile manner.

Q10. Wide changes: If you could make wider changes to the existing ILPT (not just the reporting) what would it be, and why?

Across the whole gamut of ILPT a number of common themes are seen in response to what changes could be made to benefit the frameworks:

Closer collaboration between Cyber Threat Intelligence (CTI) and Red Teams (RT)

One of the key areas called out in responses is the desire for CTI and RT to be more closely integrated during these forms of assessment with testers being included in briefings and updates to the customer from the beginning to allow them greater preparation time. Mandating CTI involvement in the red team phase and red team involvement in the CTI phase could be considered. Additionally, it is felt that including key findings from the Targeting reports in post-test remediation plans would allow customers to better target a reduction of their attack surface through encouraging removal of 'low hanging fruit'.

Relevance of National Intelligence Agencies

Whilst National Intelligence Agencies remain globally involved to varying degrees in validating CTI products for ILPT engagements, question marks were raised as to the ongoing relevance of the NCSC in the UK in the threat intelligence phase of *BEST engagements. In the early days of CBEST it was felt that the NCSC were more engaged in the process and provided more detailed feedback to the CTI providers; something that is perceived to have dropped off slightly as the framework has expanded across sectors. Further, the agencies operate at a higher-level classification and rarely provide additional intelligence that adds value to either the sector threat picture or the individual Firm being tested.

Flexibility in Testing

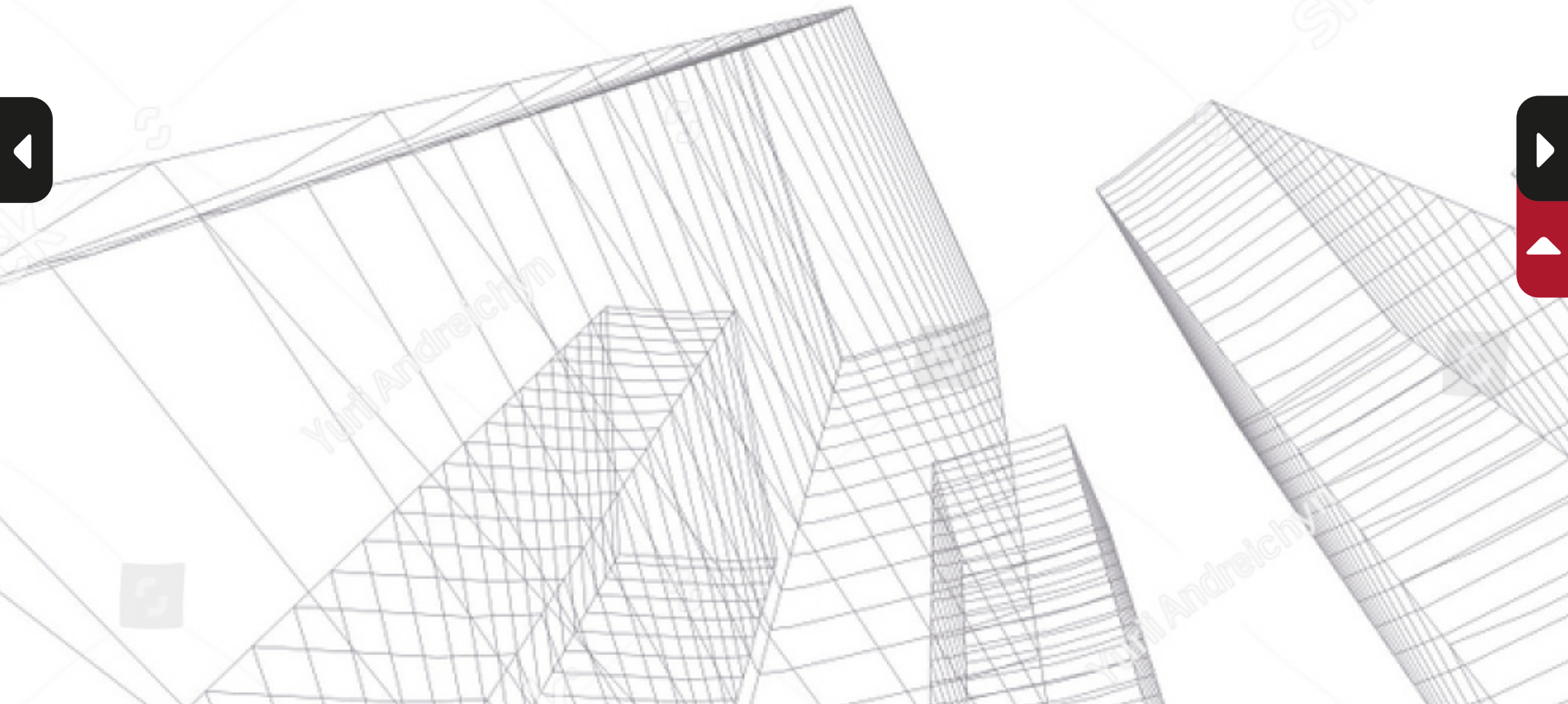
Although scenarios are generally seen as valuable there is a perception that they can sometimes be too rigid and inflexible. From a Red Team perspective having the flexibility to 'tweak' attack methodology, in line with the action a threat actor would naturally take, would help increase realism and should be considered a standardised and acceptable process.

Accreditation

To ensure quality of both CTI and RT provision, and to ensure that ILPT frameworks are held in high regards, all frameworks should ensure that the providers are certified and accredited to deliver against the frameworks.

Q11. Wide changes: If you could make changes to the Red Teaming stages specifically, what would they be?

Beyond the previously stated improvements called out by the respondents to improve the Red Team phase of ILPT perhaps the most pertinent is for the overall focus of the test to place greater emphasis on ‘purple teaming’, i.e. greater post-test interaction with internal defenders to walk them through attack scenarios and highlight areas of weakness in their detect and response capability. In terms of value to the customer this interaction with the client is considered an area where ILPT can have the greatest impact.



Conclusions

Overall, this survey has revealed a number of key areas that could help support improvement in ILPT frameworks. The primary conclusions drawn from the full range of questions are as follows:

- Desire for a singular ILPT framework: Whilst the *BEST framework is viewed as the most structured there is a growing demand from customers for regulators to develop and implement a singular framework that supports all requirements. This singular assessment is viewed as being most beneficial for global or multi-national organisations who are being required to fund and undertake multiple forms of the same assessment as a result of their geographic reach.
- Flexibility in report formats to better support customer requirements: Targeting reports are viewed across the board as an essential element of ILPT engagements, however, Threat Intelligence reports are believed to be too long for mature Firms. Whilst accepted that threat actor profiles have some benefit to smaller organisations they are viewed as less relevant for large enterprises. A key change could be to either allow greater flexibility in the report content (so that it becomes more customer focused) or to create templates that reflect the variation in likely participants. A consideration could be to focus structure and content around threat landscapes and attack scenarios, or to introduce various templates that support greater flexibility for providers to provide more tailored reports.
- Positive support for use of Mitre ATT&CK framework: Attack scenarios developed using the Mitre ATT&CK framework, and mapped to the CTI scenarios, are heavily supported by all respondents. This framework is viewed as being more detailed than the Lockheed Martin Cyber Kill Chain, and if applied correctly, flexible enough to allow credible and realistic attack scenarios to be developed.
- Support for active reconnaissance, with caveats: Active reconnaissance as a whole would enable greater validation of results and reduce false positives in the Targeting report. However, before implementation there would need to be greater assessment of CTI provider capability to deliver with a focus on ensuring that skill levels are sufficient to conduct this activity without either causing network outages or pre-warning internal defenders of the ongoing engagement.
- Upskilling of CTI providers: Whilst not necessarily relevant to all CTI providers there is a perception that employing an experienced security tester to support active reconnaissance activity could be beneficial, both to reduce accidentally alerting defenders and to support greater validation of targeting report results.
- Wide Support for CREST CTI Maturity Assessment: Across the board respondents indicated support for the new CTI maturity assessment but did express a desire for a more slimmed down version that could be more rapidly completed.
- Expansion of Purple Teaming: When looking at improvements to the existing frameworks it is felt that customers would get more benefit from the assessments if they contained a more purple team focus that better supports upskilling of internal defenders, not just identification of vulnerabilities.
- Perceived lack of engagement by National Intelligence Agencies: Whilst only called out in reference to the NCSC in the UK, respondents did indicate that they felt that there was a declining level of engagement in the CTI phase from national intelligence agencies.

Recommendations

Based on the findings, and drawing from the conclusions, the following recommendations are suggested as a means to improve both perception and implementation of global ILPT frameworks:

- Global regulatory bodies are encouraged to continue existing collaboration around delivery of ILPT and should potentially consider development of a singular global ILPT framework acceptable to all or sign memorandums of understanding between each other that allows each regulator to fully accept and support findings from engagements conducted in other jurisdictions. The benefit of this action would not only see reduced regulatory overheads and reduced costs for organisations but also could lead to improved regulatory interaction across sectors / national boundaries and deeper understanding of the global Cyber Resilience status of their members.
- ILPT framework owners should engage with CTI providers, possibly using CTIPS as an intermediary, to help develop more applicable targeting and threat intelligence report formats that better align with customer needs. Primary to this discussion should be the value of threat actor profiles within threat intelligence reports and Red Team input into content contained within targeting reports.
- CTI providers should be free to design attack scenarios that contain enough freedom of action for Red Teams should primary attack paths relating to their chosen threat actor not be successful. This recommendation is in line with actions seen by threat actors who will automatically pivot to another technique should their primary methodology be thwarted by internal defenders or security controls. Rigid attack scenarios that do not allow Red Teams variety in their methodology (within given bounds) should be discouraged as they fail to provide full value to customers and can potentially create a false sense of resilience.
- The issue of active reconnaissance should be explored further, potentially through pilot engagements, to identify whether this practice brings the expected benefits to Red Teams and customers. Consideration as to whether CTI providers have sufficiently trained employees to conduct this action should be key to any decision, although a possible short-term option whilst any upskilling is conducted could be time limited attachment of a suitable Red Team member to CTI providers. This attachment could either support full delivery of the targeting report or could just be used to help validate results.
- Switch the focus of the assessment from being primarily focused on identifying vulnerabilities within target organisations to helping them upskill their internal defenders through developing greater understanding of attacker methodology. A more collaborative Purple Team engagement whereby Red Teams complete testing and then walk through each scenario and show defenders how to identify their activity would provide significantly more benefit to the organisation.
- No further recommendation is made regarding development of a lightweight version of the CREST CTI Maturity Assessment as the author understands that this is already in development (and may even be deployed by the time of publishing).
- National Intelligence Agencies involved in supporting ILPT frameworks should be encouraged to discuss with framework owners where they feel they can best contribute to provide more value to organisations. Whilst resource constraints may restrict the amount of support that can be provided it is felt that additional value to the customer could come through these agencies as a minimum endorsing the selected scenarios for testing. This however should not impact the speed or effectiveness of delivery of the project.

For further information, please contact CREST at **www.crest-approved.org**

CREST (International)

Level 2 The Porter Building,
1 Brunel Way, Slough, Berkshire SL1 1FQ, UK

Call: +44 (0) 20 3058 3122

CREST®