CTIPs
CREST Threat Intelligence Professionals

Cyber Threat Intelligence in a Business Context

Finding the Right Partner to Meet Your Challenges

CREST

Contents

Introduction

Cyber Threat Intelligence (CTI) is a domain specific practice of data collection and analysis to help people make the best-informed decisions possible. At present there is little to no guidance on how best to select the right CTI partners for a business.

The aim of this paper is to provide readers with a short guide to formulate the decision-making process when searching for CTI partners so that security challenges can be met adequately and efficiently, thus maximising the return on investment for your organisation.

For those who wish to learn more about CTI, please refer to the CREST whitepaper "**What is Cyber Threat Intelligence and how is it used?**"[1]

Solving the right problems

CTI, when consumed correctly, is tremendously powerful as it will significantly help mitigate the impact and in some cases, prevent cyber threats from materialising.

Whilst it is tempting to simply procure CTI products and services for the sake of completing a compliance tick box requirement, this is considered a poor practice as this will unlikely be adding any real material value to the business' security posture. The focus should **not** be on CTI access but on CTI consumption. That is, *how will your business be utilising CTI to mitigate the relevant cyber risks and threats to minimise the impact of cyber attacks.*

With the right partners involved, CTI will help transform your company's security posture from reactive (e.g. act after an incident occurs) to proactive (e.g. prevention). The first step to maximising the value of a CTI program is by identifying the current business requirements that drive the need for CTI (the "what").

1. Know Your Business

The first step towards identifying the real business drivers for CTI is by understanding the business you are trying to protect. This can be broken down systematically as follows:

a. **Products and Services**: the most fundamental step is to identify the key revenue drivers of the business as it will help identify the business critical assets as well as intellectual properties that must be protected. This will then help identify the relevant cyber risks and threats that are most relevant to the business and in turn, helps defining the cyber threat profile of the business.

b. **Affiliated Sectors**: attackers have limited resources and they too are likely to specialise in targeting specific sectors. This is especially true for hackers-for-hire (including those who are state sponsored) who, like CTI vendors, specialise in sectors most relevant to their clientele. It is therefore vital to identify the sectors in which the business operates under so that the most relevant cyber risks and threats can be identified. This should include the industries of the business partners, affiliates and clients through which the business may be indirectly associated with. For example, the company may be sponsoring a high profile event or working with a high value target such as a government entity and may therefore be caught as collateral in a campaign against those sectors.

c. **Geographical Footprint:** some businesses operate globally with business entities registered in various different countries. Local offices may be set up with staff members hired from the region to provide physical presence in the area. This will likely expose the business to threats that are specific to the region and therefore requires specialised intelligence coverage that may require specific linguistic capabilities and regional expertise.

d. **Social-Political Support**: depending on the products and services offered, affiliated industries and the geographical footprint of the business, it is important to be aware of the general societal and government support for the business. For example, some businesses may be more likely to be targeted by environmental activists whereas others may be targeted because of their affiliations with certain political entities or governments.

e. **Business Strategy and Mission**: aligning the cyber security program with the overall business strategy will help set realistic expectations of the security team as well as identifying the right metrics to reflect success. This will also help identify security challenges as they may be unique to specific business models such as compliance requirements but some may be even more specific. For example, some businesses may require hiring a significant number of contractors to maintain business critical assets and the temporal nature of these hires may bring about a different set of insider threat challenges an in-house team may not possess.

2. Know Your Gaps

The next step is to identify the gaps in capabilities required to meet the identified challenges. Below are a few actions that will help highlight capability gaps:

a. **Historical Incidents Against the Business**: examining past incidents against the business will help further narrow down the risks, threats and capability gaps. For example, there may have been a large volume of Business Email Compromise (BEC) attacks against the finance department that were not blocked or detected over the past six months. In this case, the *risk* would be a substantial financial loss to the business, the *threat* would be BEC actors looking to social engineer personnel in the finance department to make fraudulent financial transfers and the *gap* is detecting and blocking the incoming attacks. It is important to take a broad unbiased scope for the review and include cyber incidents even if they were ad-hoc and had a low impact (e.g. banking trojan or ad-hoc ransomware infections) as the idea of the exercise is to obtain a clear picture of the cyber threats against the business and the gaps in defensive capabilities.

b. **Historical Incidents Against Relevant Peers**: similarly, examining past incidents against peer organisations within similar sectors will help broaden the horizon on the type of cyber risks your organization may be facing and further helps illuminate the cyber security capability gaps your business may have. This should include past incidents against similar sectors in other geographical regions as there are no borders in the cyber domain and it is possible that those same threat actors may broaden their scope and target multiple regions.

c. **Maturity Assessment**: last but not least, the CREST Threat Intelligence Professionals (CTIPs) have produced a diagnostic tool[2] to help businesses assess their current CTI maturity. This will further help identify the capability gaps your business may have.

3. Priority Intelligence Requirements (PIRs)

With the cyber threat profile and capability gaps identified, the last step is to breakdown the problem into a set of intelligence requirements which are prioritised by business needs. It is recommended that PIRs are reviewed on a frequent basis as some may no longer be relevant and new ones may be required.

A useful guide is provided by the Federation of American Scientists (FAS)[4]:

"Just as there are no standard situation templates or friendly COAs (courses of action) that will serve in all situations, there is no standard set of PIR. Good PIR, however, have some things in common:

- They ask only one question.
- They focus on a specific fact, event, or activity.
- They provide intelligence required to support a single decision."

A good intelligence requirement should be specific because the more specific it is, the narrower the scope and therefore more likely to be answered in full. A good IR should reference a specific **threat** against a **target** (asset) and where applicable, the **action** to be mitigated.

Below is an example approach in identifying intelligence requirements:

Threat: The business has a global footprint and critically relies on SWIFT. It is known that threat actors associated with the Democratic People's Republic of North Korea (DPRK) have been actively targeting businesses with SWIFT access.

Intelligence Gap: The business has no insights into DPRK threat actors that could enable defence.

Example Intelligence Requirements:

1. Are DPRK actors still targeting SWIFT functions?
2. Which DPRK actors are responsible for these attacks?
3. What tactics, techniques and procedures (TTPs) are these actors using?
4. What indicators of compromise (IOCs) have been used by these actors?
5. Are there any detection signatures that will enable the detection of tools used by these actors?
6. Are there any defensive measures that can be used to prevent successful compromise by these actors?

CTI Solutions

With intelligence requirements captured for your business, the next step is to know what CTI solutions are available and how they can help solve the challenges your business is facing.

To provide readers with an overview of common solutions available, CREST researchers conducted an open source research exercise on 100 CTI vendors from around the world. Below is a list of common components in a CTI solution:

- **Intelligence Report Feed**: subscription to a stream of tactical, operational and/or strategic intelligence products. Some solutions offered differ in terms of access:
  - Portal Access: many vendors offer access to bespoke portals with access priced per seat.
  - Automated Access: as interoperability becomes ever more popular particularly for companies procuring for multiple intelligence partners, access through Application Program Interface (API) is also offered to provide customers with a way to automatically consume intelligence.
- **Ongoing Monitoring**: aside from access to intelligence reports, some CTI vendors offer ongoing monitoring and alerting for high priority threats such as data leaks and imminent threats against your business.
- **Request For Information (RFI)/Analyst Time**: to accommodate customers who are looking for a more bespoke solution, many vendors offer customers the option to submit company specific RFI requests. Some also offer direct access to dedicated analysts.
- **Customisation**: there are many aspects of a CTI subscription that can be customised to offer your business the most relevant and impactful experience. This includes customised subscription to specific types of intelligence products, intelligence on specific sectors and some may even offer platform customisation to offer your analysts a bespoke user experience.
- **Integration with Other Platforms**: many CTI vendors have partnerships with prominent platform vendors in the market so the cost of integration is effectively significantly lowered as integration is already built-in at no extra cost to the customers.
- **Analytics**: management requires metrics and some vendors are known to offer customisable metrics dashboards to capture performance and business success. However, this is more common for platform vendors than CTI reporting vendors.
- **Data Feeds**: This is predominately threat data that is made up of, 'indicators of compromise' (IOCs), such as malicious IPs, file hashes, coversations captured from dark web forums and messaging platforms etc. These are almost always automated and integrate into secure tools.
- **Consultancy Services**: These services are usually in the form of formal reporting for larger CTI projects or deliverables, such as Threat Assessment, Capability Development, Third Party or Sector assessments.

Whilst not formally part of the solution, it is also worth bearing in mind the following:

- **Dissemination**: CTI vendors should offer ways in which data and intelligence can be shared in a structured and secured way. This includes strict sharing restriction labelling (e.g. using the Traffic Light Protocol[6]) and the use of industry standards such as Structured Threat Information eXpression (STIX) and Trusted Automated eXchange of Intelligence Information (TAXII)[7].
- **Customer Support**: there will likely be times when analysts come across technical difficulties or have questions regarding specific intelligence products. It is therefore important for the CTI vendor to offer ongoing support for their customers. Vendors should also be willing to offer training for onboarding technical solutions such as using their intelligence portal or automated ingestion via the API.

Vendor Assessment

The final step is to identify the right CTI partner who understands your business and can best satisfy those CTI requirements. The set of vendor assessment criteria to be considered can be categorised as ***functional*** (CTI related) and ***non-functional***.

Functional Requirements

Guided by the PIRs, the following criteria will help your business compare and contrast the capabilities of the different vendors by examining ***how*** they will be satisfying the PIRs:

- Breadth of coverage: as mentioned earlier in the article, intelligence vendors tend to focus on specific areas of CTI depending on the skillsets of their team and the demand from their existing customer base. Some categories of intelligence include:
  - **Types of threat intelligence**[1]: tactical, operational and strategic intelligence. Each requires very different expertise and they satisfy different types of intelligence requirements.
  - **Types of threat actors**: commonly categorised under espionage/state sponsored, financial and ideological motivated actors. This is usually dependent on the data source the vendor has access to and the sectors in which they specialise in. For example, some vendors only cover financially motivated actors because the majority of their clients are in the financial sector.
  - **Domain expertise**: some intelligence vendors are highly specialised in specific domains (e.g. industrial control systems) whereas others tend to cover intelligence more broadly across many different sectors.
- **Depth of coverage**: whilst it may appear that the more actors and verticals a vendor claims to cover, the better the return on investment would be, it is also important to assess the depth of their coverage. This is best done using in-house intelligence analysts who are already familiar with CTI and can ask relevant questions which the right CTI partner should be able to answer.
- **Personnel**: the quality of the vendor depends entirely on the team producing the products. It is therefore a useful guidance to assess the quality of the personnel who may be involved in the relationship with your business. This includes the skill sets, experience and qualifications (such as CREST certifications[3]) the analysts hold, as well as the quality of the leadership team. Company level accreditation may also be useful to be taken into consideration depending on your PIRs.
- **Uniqueness**: if the business is looking for multiple intelligence partners then each partner should be satisfying specific subsets of the PIRs without significant overlaps. Uniqueness and depth of coverage are inter-related as a vendor who has very deep coverage of specific areas will be able to produce intelligence that very few if not no other vendors can produce. For example, an intelligence vendor who specialises in cybercrime intelligence may invest heavily in obtaining access to underground communities. They will therefore be able to provide intelligence on actors and activities that other vendors without access will not be able to replicate.
- **Timeliness**: the purpose of intelligence is to enable a proactive forward looking security team so they can prevent if not detect and mitigate a threat as early as possible. Therefore, the time from threat discovery to client notification is of paramount importance.
- **Relevance**: the right intelligence partner should be able to produce intelligence that can satisfy the set of PIRs for your business. Some vendors who lack resources may only be able to produce intelligence that is applicable for the wider sector whereas some may have the resources for more flexibility, such as providing regular customer-specific intelligence reports.
- **Accuracy**: intelligence is only useful if they are accurate and so it is vital to assess how accurate the intelligence produced will be. There are a number of different ways to assess accuracy depending on the type of intelligence produced.
  - **Tactical**: for tactical intelligence (e.g. indicators of compromise), false positive rate should be minimal and this can be assessed by examining the intelligence production methodology the vendor uses which should include robust quality control and indicators management processes e.g. indicators aging and detection signature decommissioning.

  - **Operational/Strategic**: the accuracy of qualitative intelligence can be assessed by examining the facts presented in the reports and the language used by the analyst when conveying their assessment. As defined by the Professional Head of Intelligence Assessment (PHIA)[9], an analyst assessment should be communicated "clearly, succinctly, and in plain language, to articulate your assessment, using the PHIA Probability Yardstick to communicate uncertainty".

- **Innovation**: if your business is looking to innovate new processes and systems to scale the security operations, it would be important to assess the technical flexibility offered by the vendor. This can include simple capabilities such as automated access to the intelligence feeds or more bespoke solutions that could further enable you to create solutions that best solve your business challenges.
- **Outreach**: one of the best ways to assess the quality of a vendor is to see whether they have been active in the security community in terms of research publications, knowledge sharing at high quality conferences and involvement in security partnerships such as law enforcement investigations. Research publications (e.g. blog posts) and conference materials are generally freely available so they are highly recommended to be used for vendor assessment.

Non-Functional Requirements

As procurement is in essence a business relationship and a significant financial commitment for your business, it is vital to also assess whether the vendor can satisfy business oriented requirements. These may include:

- **Understanding of your business**: how well does the vendor understand your business and the challenges you are facing.
- **Relationship**: as both sides will be entering into an ongoing relationship, it is important that those involved are comfortable in interacting with the personnel from the vendor side.
- **Business stability**: the financial health of the vendor and whether there is any chance they may not be able to fulfil the entirety of the contract.
- **Business scale:** can the vendor adequately support your organization? This can include business hour coverage and physical presence in specific geographical locations.
- **Ability to safeguard your information**: as the vendor will be part of your supply chain their capability in safeguarding your information should also be taken into consideration and necessary legal safeguards should be put in place in the service level agreements (SLA) to cover for any potential losses. Other factors that should be considered include:
  - **Business threat exposure**: how likely will the vendor be targeted by threat actors? For example, an intelligence vendor from the Aerospace & Defence industry may be more exposed to targeted threats than a cyber threat intelligence boutique vendor.
  - **Compliance certifications**: has the vendor achieved basic information security compliance? For example: General Data Protection Regulations (GDPR) and ISO27001.
  - **Security policies**: it is worth assessing the approach the vendor has taken for their own cyber security such as whether they conduct regular penetration testing exercises.
  - **Cyber health checks**: it may be possible to request the results of the most recent penetration testing exercise against the vendor as evidence that the vendor has proven capability to safeguard your information.
  - **Breach history**: many cyber incidents are publicly disclosed and so it is worth looking for any past data breaches the vendor has been involved with.
  - **Plan to access your data**: it is important to request for plans on data access and depending on the products and services offered, this should include more elaborate documentation such as data flow diagrams.
- **Offer**: based on the functional requirements assessment as well as the non-functional considerations above, the final decision is the offer at hand and whether it is the right one for your business. Key things to consider includes:
  - **Pricing**: is the pricing justified by the likely return on investment as determined by how well they satisfied the functional requirements? Is the price within your budget?
  - **Commitment**: is the deal for a single or multi year subscription? What is offered as part of the subscription? E.g. is API access included in the package?
  - **Terms & Conditions (T&C)**: will the deal require your business to agree to the vendor's terms or will they be open to sign up to your terms?

Bringing It All Together

As aforementioned at the beginning, the purpose of this paper is to provide a quick guide to help those who are looking to procure the right CTI partners on formulating their decision-making process. There is no hard and fast rule to CTI procurement as each business is unique and only those operating from within would know how CTI can be used to solve relevant business problems. The key, therefore, is to be able to first identify the right problems to be solved and then finding the right partners to work with your business on finding the solution. To bring together all the points made in this paper, below is a hypothetical scenario to illustrate how a business could approach CTI procurement.

Example Scenario

Business: Rocket Dynamics

Rocket Dynamics is a global multibillion-dollar business with offices in more than 30 countries and operates within multiple sectors including aerospace and defence, automotive and manufacturing. With cyber-attacks making headlines on a daily basis, the CEO is eager to ensure the company is safeguarded appropriately and have recently hired a CISO to build a world class cyber security capability. Whilst the company already has a Security Operations Centre (SOC) to detect and respond to incidents, the CISO wants to make sure the company can stay one step ahead of the criminals and therefore is looking to procure CTI and integrate it into their existing cyber defence capability.

CTI Procurement Approach

Below is a list of questions the CISO should be looking to solve:

What is the cyber threat landscape of Rocket Dynamics?

Given its global presence and involvement in multiple sectors, Rocket Dynamics faces many different cyber threats some of which maybe specific to geographies, industries and events. Therefore, the CISO should first seek to gain a full picture of the cyber threat landscape the company faces.

One way to achieve this is for the CISO to hire a CTI partner with experience in tracking not just generic cyber threats but also threats that are specific to the geographies and industries that Rocket Dynamics operate within. In this case, the CISO should be looking for CTI vendor who has a proven track record in serving clients in aerospace and defence, automotive and manufacturing. The vendor should also possess proven capability in strategic cyber threat intelligence that could provide a strategic outlook on cyber threats that are specific to each region Rocket Dynamics is present in.

How capable is Rocket Dynamics in detecting and responding to the identified cyber threats?

With a good understanding of the cyber threats Rocket Dynamics faces, the CISO should seek to benchmark their current detection and response capability. The best way to objectively test a detection and response capability is to conduct a CTI-driven penetration testing exercise (e.g. CBEST[4]) where the attackers, called the “red team”, simulates the modus operandi of cyber threat actors who have been identified in the cyber threat landscape assessment to be likely to target Rocket Dynamics. The purpose is to test the current detection and response capability under a controlled environment that should reveal capability gaps including both technical and procedural issues.

In addition to testing detection and response, it is also important to test the maturity of the current CTI capability which includes how it is being applied to drive detection and response, as well as integration into business decisions (e.g. leadership awareness). This can be carried out using the “Cyber Threat Intelligence Maturity Assessment Tools”[2].

Results from the two exercises will help identify overall cyber defence capability gaps that need to be solved and provide a good baseline to measure progress.

Who should we choose to partner with?

Results from the red team exercise and CTI maturity assessment found that Rocket Dynamics has limited detection capability and a low CTI maturity score as the company is not receiving any CTI. Of particular concern is that the current detection capability is based on outdated signatures and so the current security posture is predominantly reactive.

To turn their security posture from reactive to proactive, Rocket Dynamics should be looking for CTI partner(s) who can provide the following:

1) Consultation on building a new in-house CTI program that includes building an in-house CTI team, CTI management process and internal data collection capability that can be used to produce CTI that is specific to Rocket Dynamics

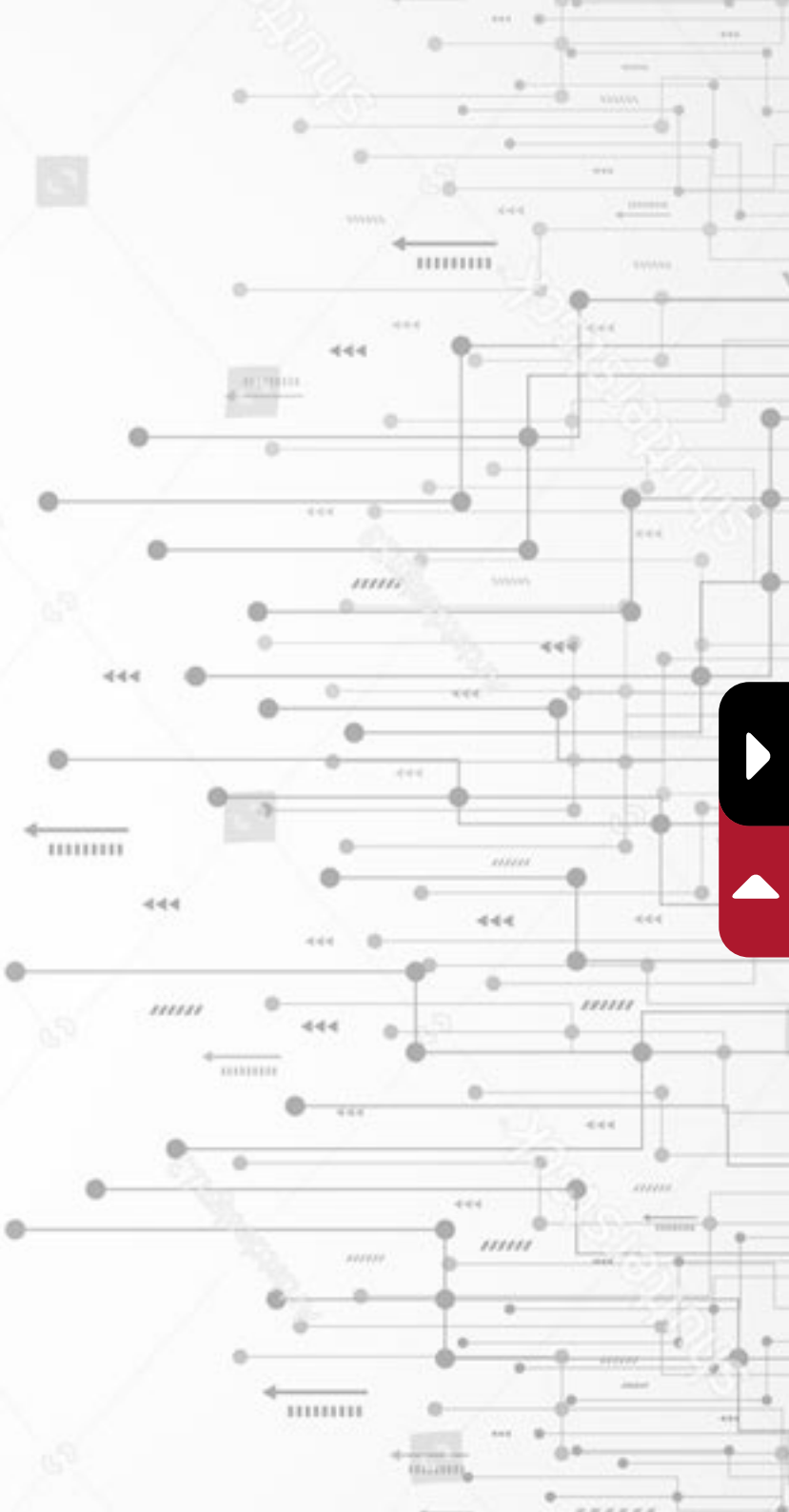
2) Intelligence on external threats targeting industries including aerospace and defence, automotive and manufacturing

3) Intelligence on threats associated with geographies in which Rocket Dynamics operate

4) Technical threat intelligence capability particularly on malware threat detection

5) Regular strategic threat intelligence on Rocket Dynamic’s threat landscape and implications on business risks

6) Innovating bespoke solutions to help integrate CTI feeds into detection and response processes



References

[1] "What is Cyber Threat Intelligence and how is it used?" **https://www.crest-approved.org/wp-content/uploads/CREST-Cyber-Threat-Intelligence.pdf**

[2] "Cyber Threat Intelligence Maturity Assessment Tools" **https://www.crest-approved.org/2020/01/10/cyber-threat-intelligence-maturity-assessment-tool/index.html**

[3] "CREST exams" **https://crest-approved.org/professional-qualifications/crest-exams/index.html**

[4] "CBEST" **https://www.crest-approved.org/schemes/cbest/index.html**

[5] "TIBER-EU" **https://www.crest-approved.org/tiber-eu/index.html**

[6] "Developing Priority Intelligence Requirements" **https://fas.org/irp/doddir/army/fm34-2/Appd.htm**

[7] "Traffic Light Protocol" **https://us-cert.cisa.gov/tlp**

[8] "Cyber Threat Intelligence Technical Committee" **https://oasis-open.github.io/cti-documentation/**

[9] "Professional Development Framework for all-source intelligence assessment" **https://files.civilservicejobs.service.gov.uk/admin/fairs/apptrack/download.cgi?SID=b3duZXI9NTA3MDAwMCZvd25lcnR5cGU9ZmFpciZkb2NfdHlwZT12YWMmZG9jX2lkPTc4NjA0NiZ2ZXJpZnk9Yjg4MDZhNmVmZjA4ZTYxYWFkMDViY2YzMGYxZTRkNjU=**

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

This document and any information therein are the property of CREST and without infringement neither the whole nor any extract may be disclosed, loaned, copied or used for manufacturing, provision of services or other purposes whatsoever without prior written consent of CREST, and no liability is accepted for loss or damage from any cause whatsoever from the use of the document. CREST retains the right to alter the document at any time unless a written statement to the contrary has been appended.

© CREST (International) 2021. All Rights Reserved.

CREST®